# Recalibrating Risk: Translating Convergence into Coherence

## Avoiding the Thousand-Cut Fracture of Financial Crime Strategy

October 2025

Plenitude

# Table of Contents

# Executive Summary

**The financial crime landscape continues to become more complex, faster-moving, and more interconnected. Criminal networks cut across geographies, products, and technologies.**

In response, institutions have been moving towards convergence, bringing together compliance, fraud, technology, data, operations, and commercial functions into more integrated operating models. This shift is essential: no single team can hold the full picture of risk.

Yet convergence alone does not guarantee success. Proximity is not alignment. When different disciplines sit closer together but continue to work in their own languages, incentives, and delivery contexts, misalignment is not reduced, it is merely hidden.

This paper argues that the missing capability is translation. Convergence describes interdependence. Translation ensures coherence. It is the active process of surfacing assumptions, exposing tensions, and making deliberate trade-offs across perspectives of risk, success, and accountability. Without it, organisations risk paper alignment but practical fragmentation.

The cracks that emerge are usually not dramatic failures. They are the accumulation of small mismatches in terminology, expectations, incentives, or delivery pressure. Over time, these compounding gaps create what we call the "thousand-cut fracture", where a strategy that looks aligned on paper fractures under operational stress.

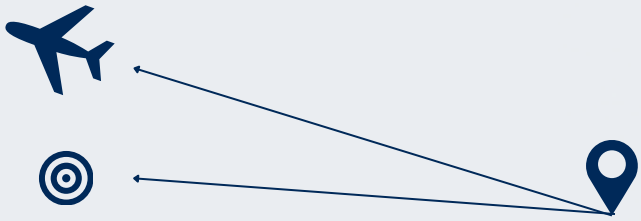
We introduce the concept of the calibration gap: the distance between what leaders intend at the strategic level and what is actually experienced on the ground. This gap is shaped by four forces:

- **Language**: each function speaks its own dialect of risk.
- **Incentives**: what gets measured and rewarded varies across teams.
- **Maturity**: some units are far ahead, others lag behind.
- **Communication**: assumptions are often unspoken or misunderstood.

Bridging this gap requires more than breaking down silos. Deep domain expertise remains critical. What is needed are translators, individuals, tools, and forums that can bridge between domains, reconcile priorities, and ensure that risk decisions play out as intended.

Translation should be treated as infrastructure: embedded in decision points, built into governance, and reinforced through deliberate practices. This does not mean slowing down or adding policy layers. It means creating the connective tissue that allows strategy to survive contact with reality.

Ultimately, the goal is not perfection. It is intentional progress, from assuming alignment to deliberately building it. Institutions that make translation a core discipline will not only improve their defences against financial crime but also strengthen commercial resilience, operational agility, and regulatory confidence.



In aviation, the 1-in-60 rule says that being just one degree off course means missing the target by a mile for every 60 miles flown. At take-off, that small error seems minor, but left uncorrected, it can put you in the wrong country.

The same is true in financial crime risk management. If one team sees a risk as reputational, another as regulatory, and another as operational, but no one aligns, those small differences can add up to major gaps.

Catching and correcting these misalignments early isn't just useful, it's essential to stay on course.

Plenitude

# 1 Setting the Scene

**In today's financial crime landscape, convergence is no longer a theoretical ambition but a functional necessity. As the boundaries blur between compliance, fraud, technology, data, operations, and commercial teams, convergence increasingly describes the need for these functions to work in a more coordinated and integrated way.**

Institutions, and the wider industry, are being forced into new operating models. However, proximity does not equal alignment. Sometimes, what seems like a unified approach may actually conceal deeper problems , from clashing incentives to gaps in communication.

Teams may be working in the name of 'financial crime prevention', but they are not necessarily working toward the same practical outcomes. One group sees risk as a matter of fines and enforcement, another as a threat to customer experience, another as a drain on efficiency, and yet another as a reputational flashpoint. These differences are not merely semantic. They shape how risk is understood, prioritised, and addressed.

What is often missing is the ability to translate between these perspectives , to surface assumptions, reconcile tensions, and make deliberate, cross-functional trade-offs. Without this kind of translation, convergence remains a structural ambition rather than an operational reality.

This paper examines why translation , not just collaboration , is the critical infrastructure needed for convergence to succeed. It explores the fault lines between teams and across the wider ecosystem, unpacks the myths around shared goals, and presents a pathway toward genuine recalibration using practical tools and reflective checks. Ultimately, it argues that without translation, convergence between teams seeking to align FCC objectives will fail , and may even deepen institutional risk.

## 1.1 The Tension Triangle: Strategic Trade-offs & Translation Gaps

Every institution faces a delicate balancing act between operational feasibility, commercial demands, and an evolving threat landscape. In theory, these forces can coexist within a well-designed strategy. In practice, they create a constant state of recalibration, and often, tension.

- **Operational Burden**: How much can be expected from overstretched teams? New policies or models may be launched without appropriate training, or legacy systems may constrain what is realistically achievable. Front-line teams are expected to implement nuanced interpretations of risk, often with limited context, competing priorities, and little space to question or refine the ask.

- **Commercial Pressure:** No institution can afford to become paralysed by its own controls. Business leaders must weigh compliance and risk mitigation against customer experience, onboarding speed, and competitive advantage. When controls create friction or erode trust, the resulting commercial fallout can be swift, whether through customer attrition, reputational damage, or lost market share.

- **Evolving Threats**: Financial crime typologies shift faster than most control frameworks can adapt. Institutions may invest in analytics or AI, but many still operate on legacy assumptions or static thresholds. Teams are asked to innovate, but only within parameters that may lag behind the threat landscape.

These tensions are inevitable, but the calibration gap arises when they are not explicitly recognised and translated into conscious, cross-functional trade-offs. Too often, these decisions happen by default, not design, through political negotiation, overburdened staff, or KPIs that push in opposing directions.

What is missing is a lightweight, embedded way to surface and reconcile trade-offs in real time, not another layer of policy, but a clear mechanism for translating between competing realities. One that enables teams to ask: What are we prioritising? What are we delaying? What are we accepting as risk, and why?

### Reality Check

- **Are trade-offs being made explicitly, or absorbed invisibly by teams who lack the authority or resources to push back?**
- **If we mapped our current priorities, delays, and accepted risks, would everyone agree with the list? Would they even recognise it?**

## 1.2 Organisational Maturity: A Hidden Variable in Calibration

Not all institutions approach risk from the same starting point. Differences in organisational maturity, across governance, infrastructure, expertise, and mindset, can significantly influence how risk is interpreted, operationalised, and communicated. These differences are not always visible, but they play a quiet and powerful role in shaping the effectiveness of any ecosystem-wide response.

Some firms are still building foundational compliance programmes, focused on meeting baseline regulatory expectations. Others have developed advanced capabilities, with integrated risk functions, real-time monitoring, and forward-looking analytics. Most sit somewhere in between, balancing strategic ambition with resource constraints, competing priorities, and legacy systems.

These maturity differences introduce a hidden calibration gap. Guidance or tooling that assumes a certain level of sophistication may be inaccessible or impractical for less mature firms. Conversely, overly simplistic standards may feel limiting or irrelevant to those further along the curve. The same typology, regulation, or vendor solution can land very differently depending on a firm's operating reality.

This variability also affects risk translation internally. Less mature firms may struggle to move from policy to practice, relying heavily on external language and frameworks without the capacity to contextualise them. More mature firms may face a different kind of misalignment, where strategic risk thinking becomes decoupled from frontline delivery, or overly engineered frameworks lose sight of operational nuance.

These challenges become particularly visible in collaborative settings. Industry bodies, PPPs, and regulatory consultations are often shaped by institutions with the capacity to contribute,

skewing expectations and outputs toward those with more advanced capabilities. Meanwhile, smaller or less resourced firms may lack the time, access, or confidence to engage, further widening the gap.

And across the spectrum, all firms face a shared constraint: commercial reality. Calibration decisions are rarely made in a vacuum, they are made under pressure. Pressure to deliver, protect margin, move quickly, or satisfy multiple stakeholders at once. In competitive environments, risk management can be seen as a cost centre unless it demonstrably protects revenue, brand, or compliance posture. This can result in pragmatic trade-offs: deprioritising controls that are not mandated, delaying enhancements where ROI is unclear, or over-rotating to satisfy visible regulators rather than building long-term resilience.

Recognising maturity as a variable, not a hierarchy, is critical to addressing these translation gaps. It's not simply a question of doing more or investing further. Calibration requires awareness of What is feasible, proportionate, and meaningful for each institution at its point on the curve. Without this, even well-intentioned efforts can miss the mark, creating guidance that is unevenly applied, controls that are poorly embedded, or expectations that are misread.

### Reality Check

- **Are our expectations , internally or externally , pitched to the actual capability and context of the organisation in question?**
- **Do our frameworks assume a level of maturity we haven't yet reached , or that others may never share?**

## 1.3 Case Study: De-Risking Without Recalibrating

A major financial institution launched a remediation programme to strengthen its response to high-risk customer segments. This included exiting certain categories of customers considered too complex or outside of the firm's risk appetite. The decision was made following regulatory feedback and internal reviews, with strong backing from compliance and risk committees.

Policy leads updated the risk appetite statements and onboarding rules. The technology team updated exclusion logic in the onboarding system. The operations team was briefed on the new rules and began implementing account closures. From a compliance perspective, the programme was a success: clearer boundaries, lower exposure, and a cleaner risk profile to report to the regulator.

But cracks began to emerge:

- The business team hadn't been fully briefed on which customers were being exited, or why. Relationship managers couldn't explain the rationale to long-standing clients, damaging trust and resulting in complaints.
- Customer experience teams were overwhelmed with queries, with no escalation path that made commercial or operational sense.
- Front-line operations flagged edge cases that didn't intuitively feel high risk but were still subject to closure, based on rigid logic that hadn't been locally validated.
- The business interpreted "high risk" as referring to regulatory sanctions or fraud exposure, yet many of the exited clients were small businesses with unusual ownership structures or overseas ties, not bad actors. This misalignment in definition created confusion and reputational blowback when loyal clients were caught in the net.

- The regulator, months later, asked for evidence that decisions were proportionate, customer-centric, and in line with financial inclusion obligations. The bank struggled to evidence those decisions beyond policy references.

What had started as a targeted risk reduction effort had triggered customer attrition, internal confusion and reputational issues. The control was technically sound. The intent was legitimate. But the translation between compliance intent, operational execution, and business perception of risk had failed.

# This wasn't a policy issue. It was a calibration issue.

The risk appetite was recalibrated on paper, without recalibrating how that appetite would play out through people, systems, and perception.

This scenario is not rare. It is a real and recurring pattern across the industry. Each function believes it is solving the same problem - but in reality, the problems they are attempting to solve, are skewed towards their own incentives, risk appetites, and operational realities.

Too little attention is paid to the reality of a translation barrier. This is not about miscommunication in the conventional sense, it's about a deeper disconnect.

When people use the same words, like 'risk', 'control', or 'escalation', but mean slightly different things, alignment becomes superficial. The consequences are not just inefficiency and friction, but the potential for missed threats. Each small gap in understanding may seem minor, but together they create structural weaknesses, cracks that sophisticated criminal actors are all too ready to exploit.

## Reality Check

**Before implementing a new control or policy shift, have you:**

- **Mapped how it will be experienced by front-line staff and customers?**
- **Stress-tested whether operational teams can apply it consistently under time pressure?**
- **Prepared a clear, defensible explanation for regulators, customers, and internal stakeholders?**

**If not, we're not managing risk - we're distributing it invisibly across the organisation.**

# 2 Organisational Breakdown: Why Translation Can Fail

**As fraud and financial crime risks evolve in complexity and scale, expanding the range of contributors to prevention and response strategies is essential.**

Convergence brings more people to the table, each with their own operational priorities. But without an agreed method of translation of how these operational priorities realistically form a solid foundational response, the conversation, and ultimately the overall approach, risks becoming fragmented. Organisationally, this plays out in four primary ways.

## 2.1 Risk Is not a Universal Language

Risk, as framed on paper, whether in theory or policy, can serve as a unifying construct, fostering a shared understanding and coordinated need for action across stakeholders, each of whom is theoretically aligned on the elements required for a cohesive response. However, once risk is removed from the vacuum of theory, the reality tells a different story. Each function within an organisation speaks a distinct dialect of risk, shaped by its specific mandates, exposures, and operating conditions. The MLRO is focused on regulatory accountability and personal liability. The fraud team centres its efforts on real-time detection and fraud loss mitigation. Technology leads prioritise system uptime and service integrity. Finance quantifies risk through the lens of budget impact and operational efficiency. The board and executive layer translate risk into strategic, reputational, and commercial terms.

These operational realities are not anomalies, they're embedded, persistent, and necessary. The challenge is not to collapse them into a single definition of risk, but to recognise their legitimacy and understand how they interact. A compliance concern without a clear regulatory driver, for example, may be deprioritised in a resource-constrained environment, not due to negligence, but because budgets, KPIs, and incentives are calibrated differently across teams. In such cases, the ripple effects of competing priorities can significantly shift the scale, urgency, and even the feasibility of a response.

This complexity becomes even more layered when considering the divide between group-level and regional or business unit teams. While group functions are often responsible for setting standards, defining policies, and ensuring global consistency, regional teams operate at the front line of delivery, adapting those policies within the constraints of local regulation, resource availability, and operational practicality. These adaptations are both necessary and expected. But they can introduce a different type of risk: one where the original intent becomes diluted or misaligned in translation.

A standard that is sound at group level may take on a very different shape by the time it reaches implementation. Not because it has been ignored or resisted, but because the local context demands trade-offs, balancing regulatory expectations with what is realistically achievable on the ground. Without deliberate effort to preserve meaning through this translation process, well-intentioned adaptations can result in fragmented execution and uneven outcomes.

Alignment doesn't come from forcing consensus on a singular view of risk. It starts with acknowledging the multiple, valid lenses through which risk is perceived, and building the muscle to translate between them. Only then can organisations calibrate responses that are not only compliant or efficient, but also realistic and sustainable.

## 2.2 Format and Friction

It is not just the definition of risk that diverges, it's how that risk, and any proposed solution, is communicated. Each team operates in its own ecosystem, shaped by its tools, objectives, and audience.

These differences are compounded by contrasting operational realities. Some teams work in clear black-and-white terms, rule-based, binary, and codified. Others operate in shades of grey, where judgement, context, and nuance are essential. When insights flow between these different environments, things can go wrong in two main ways.

First, a team may present insight in a way that makes sense to them, assuming others will interpret it correctly, without recognising the contextual gap. Second, a team may try to tailor their message for a different audience but, lacking deep understanding of that domain, oversimplify or misframe the issue.

Either way, critical nuance is at risk of being lost or misunderstood. A fraud model with real commercial value might fail to gain funding if its strategic relevance is not clearly expressed to a board audience. A serious compliance gap might be overlooked if buried in language that operational teams cannot interpret or prioritise. Over time, these disconnects lead to failed handovers, fragmented governance, and missed opportunities for timely action.

## 2.3 Misaligned Incentives

Even when teams appear to be working toward the same objective, what drives their behaviour is often very different. Realistically, each function is shaped by its own set of incentives - what gets measured, rewarded, or deprioritised. These incentives influence how teams define success, interpret risk, and make trade-offs.

Some teams are focused on regulatory assurance and risk mitigation. Others are under pressure to reduce cost, streamline delivery, or meet commercial targets. Often, these goals are in quiet conflict. For example, a programme may be positioned as "strengthening the financial crime control framework"- but the unspoken expectation is that success will be measured by how much money it saves. Or a new control might be recommended to reduce fraud exposure but ultimately dropped because it adds friction or operational cost.

These tensions are rarely made explicit. There's a tendency to assume that shared goals mean shared priorities - but unless the underlying incentives are surfaced and addressed, alignment remains superficial. Recognising and naming these incentive misalignments is essential to avoiding fractured delivery and missed opportunities. Without doing so, even the most well-intentioned collaboration can falter before it starts.

## 2.4 The Top-Down Disconnect

Some of the most critical disconnects are not just between teams - they're within them. While horizontal misalignment often stems from differences in language, tooling, or incentives, vertical misalignment occurs when the intent behind policies, frameworks, or decisions is not meaningfully carried through to those responsible for operational delivery.

Senior team members - those shaping strategy or defining controls - often have a clearer line of sight into the broader context: regulatory expectations, risk trade-offs, reputational exposure, and strategic goals. But as that thinking filters down, it's often distilled into simplified instructions, process maps, or templates – unintentionally stripped of nuance and purpose.

This is not a question of capability. Junior or delivery-level staff often work under real-time pressures, balancing multiple responsibilities and tight timelines. Without the full context, even a well-implemented control can default to box-ticking.

# Teams may comply with the letter of a requirement but lose sight of the spirit.

Opportunities to raise risk signals, suggest improvements, or challenge flawed assumptions are missed, not out of indifference, but because the 'why' was perhaps never fully embedded or aligned. This top-down disconnect is easy to overlook, especially when on paper everything appears compliant. But when the operational layer is not meaningfully engaged in the intent, the risk of shallow implementation, blind spots, and diminished outcomes increases.

## Reality Check

Do we assume that collaboration equals alignment?

- When was the last time we tested whether our language, incentives, or delivery expectations actually match , not in principle, but in practice?
- Could include a lunch and learn type of activity - how often are senior policy makers speaking to the front line and explaining what they're doing, hearing and how they are feeding this into the work of the front line?

Table 1 offers an illustrative snapshot of how different teams within the financial crime ecosystem interpret and communicate risk. It highlights the layered nature of these interpretations, from language and incentives to delivery priorities, and how small misalignments can compound into systemic friction. While not exhaustive, the matrix underscores just how easy it is for well-intended teams to work at cross-purposes if translation and calibration are not actively maintained.

## Table 1: The Language Matrix

| Functional Domain | Team | Language They Speak | Key Drivers | What 'Risk' Means | Language Calibration / Risk Translations |
|---|---|---|---|---|---|
| 2LoD | FCC – AML / Sanctions / AB&C | • "Is this aligned with policy?" • "Can we evidence it?" | Framework compliance, thematic coverage | Regulatory breaches, ineffective implementation, personal liability | Often speak in policy terms not always digestible to 1LoD; can seem risk-averse and inflexible |
| | Fraud Risk Oversight | • "Do we have controls for this typology?" • "Are we monitoring the right channels?" | Detection strategy, customer protection | Exposure to attack vectors, poor control mapping | Can clash with Fraud Ops who want binary decisions; operates in grey zones but expects black-and-white results |
| | Compliance Advisory | • "Has the business consulted us?" • "Are we regulatory-aligned?" | Clear guidance, defensible positions, business enablement | Misinterpretation of rules, business going rogue | Language often feels academic or overly legalistic to commercial stakeholders |
| | Policy & Standards | • "Is this consistent globally?" • "Is this embedded?" | Harmonised policies, implementability | Inconsistencies, misapplication, unclear expectations | Frustrates 1LoD by not accounting for nuance; expects 'read and apply' rather than contextual adoption |
| | Operational Risk | • "What is the inherent/residual score?" • "Logged in the RCSA?" | Risk register integrity, event tracking | Unmitigated risks, poor issue management, audit findings | Talks in frameworks and metrics; can seem abstract to delivery teams |
| 3LoD | Internal Audit | • "Can you evidence this control?" • "Where is the governance record?" | Independent assurance, control effectiveness | Undetected failures, gaps between design and operation, audit issues | Highly rules-based; expects black-and-white evidence where nuance is often needed |
| **Tech, Data & Change** | Model Risk & Validation | • "Has this been independently validated?" • "Where's the documentation?" | Governance, compliance with MRM standards | Model bias, lack of explainability, unvalidated decisions | Focused on model risk, not financial crime outcomes; disconnect with Fraud/FCC who want performance over process |

| Functional Domain | Team | Language They Speak | Key Drivers | What 'Risk' Means | Language Calibration / Risk Translations |
|---|---|---|---|---|---|
| Tech, Data & Change | Data Stewards / Governance | • "Is the data field used or populated?" • "Can we trust this source?" | Data quality, lineage, traceability | Poor input to systems, audit failures, detection degradation | Data quality expectations do not always match operational realities; prioritisation gaps |
| | AI / Analytics Teams | • "How is the model performing?" • "Any bias detected?" | Accuracy, false positive reduction, innovation | Model drift, regulatory scrutiny under AI rules | Works in probabilistic terms; often misunderstood by linear policy or legal functions |
| | Change / Transformation | • "What is the delivery timeline?" • "Is this regulatory-driven or strategic?" | On-time delivery, stakeholder alignment | Project failure, regulatory delay, missed benefits | Sees regulatory change as a delivery requirement, not a cultural or risk shift |
| Group-Level Oversight & Execs | Group FCC / Group Risk | • "Can we aggregate risk across entities?" • "How mature is the framework?" | Consistency, regulatory perception, Board assurance | Enterprise-wide non-compliance, siloed risk, regulator concerns | Talks in aggregated metrics; local teams often cannot map their work to Group-level priorities |
| | CRO / CCO / COO / CFO | • "What is our exposure?" • "What is the cost of compliance?" • "How does this affect our bottom line" | Operational resilience, financial accountability | Strategic risk, high-cost remediation, executive liability | Views risk at a macro level; struggles with technical nuances or operational blockers |
| | Board / Board Committees | • "Are we within risk appetite?" • "What is our regulatory posture?" | Oversight, reputation, performance | Systemic failure, enforcement, reputational damage | Needs simple, high-impact messaging; operational detail overwhelms or is filtered out |
| Legal, Governance, & Ethics | Legal / Regulatory Affairs | • "Is this defensible?" • "Have we met our disclosure obligations?" | Mitigating liability, regulator trust | Fines, litigation, enforcement | Legal framing can seem disconnected from commercial or operational concerns |
| | Ethics / Whistleblowing | • "Has this been escalated appropriately?" • "Any pattern of conduct?" | Conduct integrity, early warning | Internal misconduct, cultural failure | Focuses on ethical tone and culture, often sidelined in technical delivery discussions |

| Functional Domain | Team | Language They Speak | Key Drivers | What 'Risk' Means | Language Calibration / Risk Translations |
|---|---|---|---|---|---|
| **External Interface & Assurance** | Regulatory Reporting / SAR Teams | • "Have we submitted on time?"<br>• "Was this a good-quality SAR?" | Accuracy, timeliness, transparency | Regulatory breach, missed suspicious behaviour | Operates under strict legal thresholds; grey-zone cases frustrate frontline teams |
| | Skilled Persons / External Auditors | • "Show us the evidence."<br>• "How mature is the control environment?" | Independent scrutiny, external validation | Negative findings, regulatory action | Expects evidence, structure, and maturity models; real-world variation often undervalued |
| | Third-Party Risk / Procurement | • "Has this vendor been risk assessed?"<br>• "What are the contract controls?" | Vendor compliance, SLA adherence | Third-party failure, data leaks, unmanaged risk | Risk language focused on contracts and procurement KPIs, not fraud or AML concerns |

# 3 The Wider Ecosystem: Misalignment Beyond the Organisation

**The calibration gap doesn't stop at the boundaries of a single organisation. It extends across the wider ecosystem of players who influence, oversee, or enable financial crime risk management, from regulators to tech vendors to industry bodies.**

While they broadly share the same goals - reducing harm, strengthening controls, improving outcomes - their tools, mandates, and constraints differ. Even minor misalignments in how risk is framed or operationalised across this landscape can gradually compound, creating friction, diluting intent, and undermining the cohesion needed for a truly effective collective response.

## 3.1 The Limits of Regulatory Intention

Regulators are often seen as the north star for risk calibration, setting expectations and driving accountability. But their guidance must serve a broad audience, firms with different risk profiles, business models, and levels of maturity. Overly prescriptive rules can encourage a tick-box mindset; overly broad ones leave room for uneven interpretation. Firms may delay critical investment if pressure feels low or expectations seem vague.

Adding to this is the unavoidable time lag: regulatory cycles move slower than the threats they aim to address. This lag is not a result of inaction, but of the deliberate time required for consultation, legislation, and consensus building. Financial crime typologies evolve rapidly, driven by technology, geopolitics, and criminal adaptation. By the time a framework is finalised, bad actors may have already shifted tactics. The result is a persistent gap between regulatory intent and real-world implementation.

At the policy level, this is further complicated by competing political priorities and the need for cross-sector consensus. National strategies often reflect compromise, helpful in setting direction, but too general to guide day-to-day operational decisions.

## 3.2 Industry Bodies & Public-Private Partnerships: Collaboration with Constraints

Industry bodies and public-private partnerships (PPPs) are meant to serve as connective tissue between sectors, bridging public oversight and private capability, and offering platforms for dialogue, shared learning, and, at times, co-design of policy or best practice. But their ability to drive alignment is constrained by structural realities.

A key challenge is the asymmetry of information flow. Private firms bring rich behavioural and transactional insights but often lack access to the intelligence that informs public priorities. Public agencies, meanwhile, may hold sensitive data they are unable to share. Data sharing, in this context, is a double-edged sword: legal and ethical safeguards are necessary to protect confidentiality, but they also mean information can be incomplete, delayed, or difficult to interpret in full context. This creates inevitable blind spots, missed connections, relevance gaps, and uneven understanding of risk.

Compounding this is the diversity of actors involved. Forums often include everything from global banks to regional fintechs and solution vendors, each with different maturity levels, resources, and incentives. Achieving consensus requires trade-offs, often resulting in high-level principles that are sound in theory but difficult to operationalise without further translation.

**These challenges do not negate the value of collaboration, they reflect its complexity.**

Legal, regulatory, and organisational differences shape how risk is interpreted, prioritised, and communicated. Even with shared goals, differing language and timelines can create subtle misalignments that accumulate over time. Recognising these constraints helps firms focus on what such forums can realistically offer: not definitive answers, but directional insight, peer context, and early warning of evolving expectations.

### 3.3 Technology and Data Vendors: Innovation vs Integration

Vendors providing fraud and financial crime technology - whether for transaction monitoring, fraud detection, or screening - play an increasingly central role in shaping how risk is surfaced, quantified, and operationalised. These tools sit at the heart of many firms' control environments, yet vendors themselves often remain outside the core governance and decision-making structures of the institutions they serve.

The risk frameworks embedded within vendor models typically carry implicit design choices - about which behaviours to flag, how thresholds are set, and what constitutes an effective response. While many firms take deliberate steps to align these tools with their own risk appetite and regulatory obligations, the process is rarely straightforward. Even with rigorous calibration efforts, subtle mismatches in scope, logic, or thresholds can emerge - reflecting the inherent challenge of adapting a general-purpose solution to a specific risk context.

This is particularly relevant when considering the interorganisational calibration issues discussed earlier. Translating risk across internal functions is already complex - fraud teams, compliance officers, and technologists each interpret and prioritise signals differently. That complexity deepens when firms must also interpret and adapt third-party tools. For example, how do you translate contextual nuance - like behavioural red flags, geographic risk overlays, or evolving fraud typologies - into a binary alert? What is a meaningful anomaly in one business line may be noise in another. Without a shared understanding of what the technology is designed to detect - and why - there's a risk of false confidence, missed signals, or unnecessary friction.

These challenges become more pronounced with AI-powered systems, where explainability, model drift, and embedded bias add further layers of complexity. Vendors may prioritise performance metrics like detection rates or scalability, while firms remain accountable for regulatory outcomes, customer experience, and operational burden. This creates a subtle but important responsibility gap, particularly when firms rely on outputs they cannot fully interrogate or adjust.

Finally, where products are sold as off-the-shelf solutions, there's a risk of standardising responses in ways that flatten meaningful distinctions between institutions. While shared typologies and industry standards are important, one-size-fits-all tools may fail to reflect variations in business model, customer profile, or regulatory environment, leading to fragmented alignment between control effectiveness and actual risk exposure.

### 3.4 Academia and Think Tanks: Influencing Strategy Beyond the Front Line

Academia, policy think tanks, and civil society organisations contribute significantly to the conceptual framing of risk, surfacing blind spots, interrogating assumptions, and influencing long-term policy direction. While they are often removed from the practical constraints of operational delivery, their insights help shape the strategic discourse, expanding how risk is understood, debated, and prioritised across the ecosystem.

Much of this work operates at a different cadence and level of abstraction than the day-to-day realities of implementation - where organisational constraints, regulatory processes, and commercial pressures influence how ideas are translated into action. This divergence doesn't diminish their value, but it does highlight a calibration challenge: how to ensure that conceptual thinking meaningfully informs operational decision-making without losing nuance or becoming overly theoretical.

Crucially, these groups often serve as a kind of temperature check for real-world consequences - tracking how financial crime policies, frameworks, or interventions play out in practice, particularly for underrepresented groups or unintended outcomes. This feedback loop adds an important layer of context to the ecosystem, helping to challenge assumptions that may otherwise go untested in commercially or politically driven environments.

**Their role in pushing the ecosystem forward remains vital.**

By introducing alternative perspectives, independent scrutiny, and a degree of public accountability, they provide essential checks and long-term thinking that may otherwise be deprioritised. But for that thinking to shift practice from a realistic operational perspective, deliberate translation is needed - between strategy and delivery, concept and implementation, insight and action.

#### Reality Check

- Do we understand how our internal interpretation of risk aligns (or misaligns) with external partners, regulators, and other third parties?
- Have we built any feedback loops to catch where misalignment is likely , or do we only find out when something breaks?

Even with shared goals, ecosystem actors interpret and act on risk differently. Table 2 provides examples of how these differences in perspective, incentives, and language can lead to subtle but consequential misalignments across the financial crime landscape.

## Table 2: The Wider Ecosystem

| Ecosystem Stakeholder | What Risk Means to Them | Primary Drivers / Incentives | Translation Breakdown Points | Mindset Orientation |
|---|---|---|---|---|
| Traditional Banks | Regulatory breaches, customer impact, reputational damage | Regulatory compliance, risk-adjusted growth, customer retention | Between compliance interpretation and technology implementation | Rule-bound but layered with commercial nuance |
| FinTech / Challenger Banks | Operational fragility, product abuse, onboarding failures | Speed to market, investment attraction, competitive edge | Between innovation drive and regulatory understanding | Commercially agile, context-driven |
| Crypto Platforms | Illicit finance exposure, sanctions risk, reputational fallout | Innovation, decentralisation, user anonymity vs. trust | Between decentralised structure and centralised oversight | Innovative, libertarian, risk-normalised |
| Technology Vendors | Client failure, liability avoidance, model bias or underperformance | Client renewal, scale, reputational safety | Between technical specs and risk relevance to clients | Functional and delivery-focused |
| Regulators | Market-wide stability, systemic vulnerability, public trust | Policy clarity, enforceability, public protection | Between expectation-setting and actual institutional capability | Principle-based, policy-centric |
| Enforcement Agencies | Undetected crime, low prosecution rates, deterrence failure | Successful investigations, high-value intelligence, prosecution rates | Between actionable intelligence and operational handoffs | Evidence-based, outcome-focused |
| Industry Bodies / PPPs | Cross-sector risk awareness, inconsistent standards, member value | Member engagement, consensus-building, influencing policy | Between high-level alignment and operational usability | Consensus-driven, representational, facilitative |
| Think Tanks / Academia | Systemic vulnerability, unintended consequences, policy gaps | Independent research, thought leadership, agenda-setting | Between conceptual framing and practical applicability | Analytical, future-facing, socially anchored |
| Civil Society / NGOs | Real-world harm, inequality, gaps in protection | Advocacy, accountability, safeguarding vulnerable populations | Between lived experience and institutional response | Impact-driven, rights-focused, community-aware |
| Consulting / Advisory Firms | Client delivery risk, reputation, perceived independence | Maintaining credibility, delivering insight, expanding market share | Between strategic framing and ground-truth complexity | Abstract, cross-sectoral, message-led |

# 4 So What? The Reality of Implementation

**Every institution has an idea of what 'good' looks like: seamless governance, agile controls, aligned communication, and customer-centric risk management. But between aspiration and implementation lies a translation challenge.**

These gaps are not the result of neglect, they're reflections of organisational complexity, time pressure, and competing incentives. Acknowledging this is not a weakness, it's the first step in recalibrating.

Understanding the calibration gap is not just an academic exercise. It has real implications for how financial crime controls are designed, implemented, and sustained. These are not failures of effort or intent, but reflections of the practical, competing realities that shape how work gets done.

Translation gaps rarely stem from a single cause. They emerge from a combination of misaligned incentives, legacy systems, unclear accountability, and a lack of shared language. Most critically, they are often invisible until something goes wrong, when an alert is missed, a typology is misunderstood, or a regulator questions how policy has been operationalised.

The challenge is not to eliminate these tensions, they're inherent to any large institution or multi-stakeholder system. Instead, the focus must be on making them visible and manageable, so that decisions are not made by accident or default. That means building in translation capability, the ability to intentionally bridge between strategy and implementation, policy and platform, control and context.

Without this, institutions risk repeating the same patterns: over-indexing on documentation without operational reality checks, investing in technology without cross-functional clarity, or setting expectations that no team is realistically empowered to meet.

### Reality Check

- Have we pressure-tested our vision of alignment against operational reality , or are we assuming it will land as intended?
- Who owns the calibration gap in our organisation , and do they have the visibility and mandate to fix it?

## 4.1 Recalibration in Practice: Translation as a Strategic Lever

There is no perfect solution to the calibration gap, because risk itself is dynamic, and because every institution, vendor, regulator, and stakeholder works within their own set of constraints. But the absence of perfection should not excuse inaction.

Recalibration is an ongoing process, not a one-time fix. It requires institutions to:

- Acknowledge divergence: Recognise that different teams, stakeholders, and ecosystem actors will interpret and act on risk differently.
- Surface trade-offs explicitly: Use structured forums, translation prompts, and scenario-based planning to ask: What are we solving for, and at what cost?
- Embed translation into decision points: At every key junction, policy development, tool design, implementation, ask whether assumptions have been clearly and contextually communicated across relevant teams.

- Invest in cross-functional fluency: Develop people and roles that can speak multiple dialects, legal, technical, operational, commercial, and act as translators, not just advisors.

- Accept some friction: Perfect alignment is not realistic. But informed friction is better than accidental misalignment. Challenge, when purposeful, is part of good governance.

- Reground in purpose and direction: Periodically step back to recall the destination, what outcomes are we ultimately solving for? Keep team, firm, and societal goals in view, not just process fidelity. Use frameworks and control points to ensure alignment with core intent, not just procedural completion.

Recalibration happens not through volume of documentation, but through clarity of communication, alignment of incentives, and space for cross-functional reflection.

**This is not about creating more policy, it's about creating better reflexes.**

### Reality Check

- When did we last redesign a control, policy, or report not just for technical accuracy , but for clarity, comprehension, and usability by someone two steps removed from the design process?

- If we stopped mid-implementation, could each stakeholder explain both what they're doing and why it matters to others?

## 4.2 Translation as Infrastructure

If convergence is the goal in an evolving financial crime landscape, every effort must be made to ensure it is set up for practical success. That means bridging the gap between intent and execution, not just through strategy, but through translation.

Translation is the connective tissue that turns convergence from concept into capability. It's what enables a data insight to become an action, a policy to become a practice, a typology to become a meaningful response. Without it, even the most sophisticated frameworks can fail to hold under pressure, misunderstood, misapplied, or simply lost in delivery.

Financial institutions that invest in cross-functional clarity, stakeholder calibration, and shared understanding will not only be more effective at preventing financial crime. They will also be more commercially resilient, operationally agile, and regulatorily prepared.

But this is not a matter of perfection. It's a matter of progress. And progress starts with asking better questions:

- What are we assuming is aligned, but may not be?
- Where is our language drifting without us realising it?
- Which decisions are being made without context, or without challenge?

Above all, steps must be taken to ensure that theoretical concepts and policies can withstand the test of real-world operational application. Not just once, but as a repeatable discipline.

Before you write your next policy, build a dashboard, or sign off a programme, ask yourself: Am I assuming shared understanding, or am I building it?

That one shift may be the difference between compliance on paper and capability in practice.

# Translation Reality Check – Questions to Calibrate Your Response

Use this set of prompts to challenge assumptions and improve cross-functional alignment when designing or implementing risk-related changes:

| | |
|---|---|
| **Framing the Problem and the Objective** | • What is the outcome we are trying to achieve?<br>• What risk are we trying to mitigate, and who defined it?<br>• Has this risk been articulated in operational, technical, and commercial terms?<br>• Are different teams using the same language, but meaning different things? |
| **Assessing Trade-Offs** | • What are we prioritising? What are we delaying? What are we accepting?<br>• Have trade-offs been made explicit, or are they happening by default?<br>• Who owns the decision to accept or defer a particular risk? |
| **Translation Across Teams** | • Have we pressure-tested this decision/tool/policy with all affected functions?<br>• What assumptions are embedded in the design, and who needs to understand them?<br>• Are operational teams set up to realistically implement this? If not, why not? |
| **Upwards and Outwards** | • Can this be explained clearly to the Board, a regulator, and the frontline, in different ways?<br>• Is this aligned with our stated risk appetite and our day-to-day behaviours?<br>• How would this decision be interpreted by a third-party reviewer, auditor, or regulator? |
| **Maintaining Alignment** | • What are we doing to check for drift, between policy and implementation, tech and controls, intent and outcome? Are we also reality-checking against evolving industry norms?<br>• Who is responsible for translation, and is that role formalised or assumed?<br>• When did we last recalibrate to ensure we have addressed gaps and are fulfilling our ultimate objectives?<br>• Have key decisions and rationales been documented clearly enough to create a repeatable, auditable trail?<br>• Are findings and adjustments being proactively communicated to the right stakeholders at the right time?<br>• Have you socialised the journey beyond the immediate team, considering internal alignment, external perception, and potential broader applications?<br>• Have you accounted for unintended consequences as well as cross organisational / stakeholder impacts? |

## About the author

**Olivia Kearney** is the Head of Insights and Partnerships at Plenitude. She brings experience in counter-terrorist financing, security, and think tank engagement. In her role, Olivia leverages the firm's financial crime and compliance expertise to drive strategic engagements, content development, and new business opportunities. She focuses on identifying key industry insights and emerging trends, ensuring that Plenitude's expertise and portfolio evolve in step with the rapidly changing FCC landscape. Olivia is also an Associate Fellow at the Royal United Services Institute (RUSI)'s Centre for Finance and Security (CFS).

**Disclaimer**: While the ideas and arguments in this paper are the authors' own, ChatGPT was used to support editing and structural clarity. The tool was accessed via a secure, enterprise platform that does not use content for model training.

## About Plenitude

Plenitude provides market-leading Financial Crime Compliance (FCC) advisory, transformation, technology, data analytics, and managed services. We are committed to building a secure and resilient financial system, safeguarding society, and empowering our clients to meet and exceed their regulatory obligations.

**www.plenitudeconsulting.com**

Plenitude