



# Beneath the Asset

The New Infrastructure Risk in Global Markets

*A qualitative paper by Thomas Murray*



**Thomas Murray**

Risk Intelligence | Due Diligence | Cyber Security

Executive summary	3
Introduction – The risk beneath the asset	4
Finding 1 – Asset safety is shifting from custody due diligence to infrastructure resilience	6
Finding 2 – CSDs and custodians are increasingly exposed to cyber, operational and third-party technology risks	8
Finding 3 – Geopolitical shocks can create hidden exposure through custody chains, market access, settlement systems and local infrastructure dependencies	10
Finding 4 – Digital assets and tokenisation increase the need for independent infrastructure assurance	12
Finding 5 – Banks and asset owners need live risk intelligence, not annual due diligence alone	14
The new asset safety model	16
Why Thomas Murray	18
Conclusion – The next market shock may start beneath the asset	20
Contact us	22

# Executive summary

For decades, asset safety has been viewed through the lens of custody, settlement and market infrastructure due diligence. The question was relatively simple: where are the assets held, who is responsible for them, what legal protections surround how they are accounted for, and how strong are the controls around custody and settlement?

That question is no longer enough.

The safety of an asset is now shaped by a wider and more fragile chain of infrastructure: central securities depositories (CSDs), custodians, clearing and settlement systems, market access arrangements, technology providers, digital platforms, cyber controls, sanctions exposure, geopolitical dependencies and operational resilience frameworks.

*The next market disruption may not begin with a trading decision. It may begin after the trade.*

A cyber incident at a critical provider, a geopolitical shock in a key market, a failure in a settlement system, a disruption at a CSD, a sanctions event, a custodian concentration issue, or a weakness in digital infrastructure could all create hidden exposure for banks, asset owners and financial institutions.

This paper argues that global markets are entering a new era of asset safety risks. In this new era, asset safety is not simply a custody question. It is an infrastructure resilience question.

Thomas Murray has spent more than three decades assessing the safety, resilience and transparency of the market infrastructures, custodians and post-trade systems that support global investment. Our CSD, CCP and custodian risk assessments, cyber resilience ratings, risk alerts and market intelligence give financial institutions a deeper view of the infrastructure beneath the asset.

## This paper sets out five findings:

1. Asset safety is shifting from custody due diligence to infrastructure resilience.
2. CSDs and custodians are increasingly exposed to cyber, operational and third-party technology risks.
3. Geopolitical shocks can create hidden exposure through custody chains, market access, settlement systems and local infrastructure dependencies.
4. Digital assets and tokenisation increase the need for independent infrastructure assurance.
5. Banks and asset owners need live risk intelligence, not annual due diligence alone.

An aerial view of the London skyline at sunset. The Shard is the central focus, its glass facade reflecting the orange and pink hues of the sky. To the left, the London Eye is visible. In the foreground, the River Thames flows, with the Tower Bridge on the right. The city is densely packed with buildings, and the overall atmosphere is serene and dramatic.

# Introduction

## The risk beneath the asset

Investors spend enormous time deciding what to buy.

They assess asset class, geography, currency, counterparty, liquidity, volatility, credit quality, sector exposure and expected return. But less attention is often paid to the infrastructure that sits beneath those assets: the systems, institutions and dependencies that hold, settle, service and protect them.

That infrastructure was once treated as the quiet machinery of markets. It was technical. It was specialist. It was often seen as back office. It was assumed to work.

## That assumption is becoming dangerous.

Post-trade infrastructure is now exposed to the same forces reshaping the rest of financial markets: cyber escalation, geopolitical fragmentation, sanctions, faster settlement compressing critical control processes, operational resilience regulation, technology dependency, market concentration, digital assets and tokenisation.

*The result is a new form of hidden risk.*

An asset may be financially sound, but it can still be vulnerable because of the infrastructure beneath it. A market may appear investable, but still carry exposure through settlement arrangements, custody chains, local market infrastructure, cyber controls or third-party operational dependencies. A bank may complete due diligence annually, but still miss a fast-moving risk event that changes its exposure within days or hours.

This is the new asset safety problem.

*Asset safety is no longer only about the institution holding the asset.  
It is about the resilience of the entire infrastructure chain behind it.*



# Finding 1

Asset safety is shifting from custody due diligence to infrastructure resilience

The traditional model of asset safety was built around custody, settlement and legal ownership. Institutions were asked whether assets were properly held, segregated, recorded, settled and serviced. This remains essential.

But it is no longer sufficient.

The modern asset safety perimeter is wider. It includes the resilience of CSDs, custodians, sub-custodians, settlement systems, payment dependencies, technology providers, data flows, digital access points, local market rules, operational controls, regulatory oversight and cyber defences.

In this environment, asset safety is not static. It changes as markets change.

A market that looked stable last year may become exposed because of a geopolitical event, cyber weakness, operational outage, regulatory shift, settlement disruption or deterioration in local infrastructure. A custodian may remain financially strong, while still being exposed to technology, concentration or third-party risk. A CSD may perform its core functions effectively, while facing new pressures from digitalisation, accelerated settlement or cyber threat actors.

This means due diligence has to evolve.

The question is no longer simply: "Is this custodian or market infrastructure safe?"

The better question is: "How resilient is the infrastructure chain that protects this asset, and how quickly would we know if that resilience changed?"

That shift matters because the failure point in modern markets may not be obvious. It may not sit with the asset manager, the broker or the investor. It may sit deeper in the chain.

## It may sit beneath the asset.

Thomas Murray is strongly positioned to lead this discussion. Our work has historically focused on the safety and resilience of CSDs, custodians and market infrastructures, and has evolved to own the territory across post-trade infrastructure, cyber resilience, geopolitical alerts, DORA compliance, digital assets and operational resilience.

*Traditional custody due diligence tells you where the asset is held.  
Infrastructure resilience tells you whether the asset can remain safe when  
the market is under stress.*





## Finding 2

CSDs and custodians are increasingly exposed to cyber, operational and third-party technology risks

Central securities depositories and custodians sit at the heart of asset safety. They are essential to ownership, settlement, safekeeping, servicing and market confidence.

But the risk profile of these institutions is changing.

The modern CSD or custodian is no longer just a financial market institution. It is also a technology-dependent, data-intensive, highly connected infrastructure node. It relies on digital systems, external providers, operational processes, communications networks, market participants, cloud or software providers, and cross-border information flows. It is also an entity being pushed to settle faster, adopt new technologies and introduce efficiencies.

That creates a new risk reality.

Cyber risk is now part of asset safety. Operational resilience is now part of asset safety. Third-party technology dependency is now part of asset safety.

A cyber weakness may not immediately impair legal ownership, but it can disrupt access, settlement, reporting, instructions, corporate actions, market confidence and operational continuity. A third-party provider failure may not sit inside the CSD or custodian, but it can still affect the service chain. A technology outage may not change the value of an asset, but it can affect the ability to move, settle or service it, impacting not only trust but also liquidity and balance sheet optimisation.

That is why the line between financial risk and operational risk is collapsing.

Historically, a market infrastructure assessment might focus on governance, financial strength, operational process, regulation, oversight, transparency and legal framework. Those factors still matter, but they must now be read alongside cyber resilience, digital exposure, third-party dependency and response capability.

A market infrastructure can be systemically important and digitally vulnerable at the same time.

This is a board-level issue for banks, asset owners and financial institutions. They cannot assume that because an institution is important, regulated or long-established, it is resilient against modern cyber and operational threats.

Thomas Murray's cyber resilience ratings are the digital extension of our asset safety franchise, the continuation of our authority in post-trade infrastructure into the digital perimeter of the custody chain.

***The digital perimeter is now part of the custody chain.  
A weak cyber posture can become an asset safety issue.***



## Finding 3

Geopolitical shocks can create hidden exposure through custody chains, market access, settlement systems and local infrastructure dependencies

Geopolitical risk is often assessed at country, issuer or portfolio level.

That is no longer enough.

Geopolitical shocks can move through the post-trade system in ways that are not immediately visible from a portfolio holding statement. A conflict, sanctions event, capital control, market closure, infrastructure disruption, regulatory intervention or local banking constraint can affect market access, settlement, asset servicing, liquidity, custody arrangements and the ability to act.

The exposure may not be direct. That is what makes it dangerous.

A bank or asset owner may not hold securities at the centre of a crisis, but it may still have exposure through a custodian, sub-custodian, CSD, local market infrastructure, correspondent relationship, currency dependency, payment channel or operational provider. A geopolitical shock can therefore travel through the custody chain before it becomes visible as a portfolio-level issue.

This is where traditional due diligence struggles. Annual reviews are not designed for fast-moving geopolitical instability. Static questionnaires do not explain how a local market shock might affect settlement, safekeeping or market access. Standard risk reports may identify country exposure, but they often miss infrastructure exposure.

The core question is changing from: “Do we have exposure to this country?”

To: “How could this geopolitical event move through our post-trade infrastructure chain?”

That is a very different question. It requires market infrastructure intelligence, custody-chain understanding, local market knowledge and live monitoring.

The current situation in the Middle East strongly demonstrates this point. Our clients were not simply asking what was happening geopolitically; they were asking what it meant for custodians, CSDs, securities holdings, market access and asset safety. Although Gulf market infrastructures and custodians remained open and fully operational past some initial disruption, but attacks on cloud service providers in the region disrupted operations at some brokers and third-party institutions. That is the new risk conversation.

*Geopolitical risk no longer stops at the border of the portfolio.  
It travels through the infrastructure that holds and services the asset.*





# Finding 4

Digital assets and tokenisation increase the need for independent infrastructure assurance

Digital assets and tokenisation are often presented as a story of speed, efficiency and innovation.

But that is only half the story.

Digitalisation may make markets faster and reduce the amount of idle cash present within the system, but it does not automatically make them safer.

As assets become tokenised, settlement models evolve and digital infrastructures become more embedded in capital markets, the question of trust becomes more important, not less. The market will need to know which infrastructures are robust, which controls are credible, which providers are resilient, which legal frameworks are clear, and which digital arrangements can withstand stress.

In traditional markets, trust is supported by established infrastructure, legal frameworks, regulated entities, custody models, settlement systems and independent assessment. In digital markets, many of those assumptions are being redesigned.

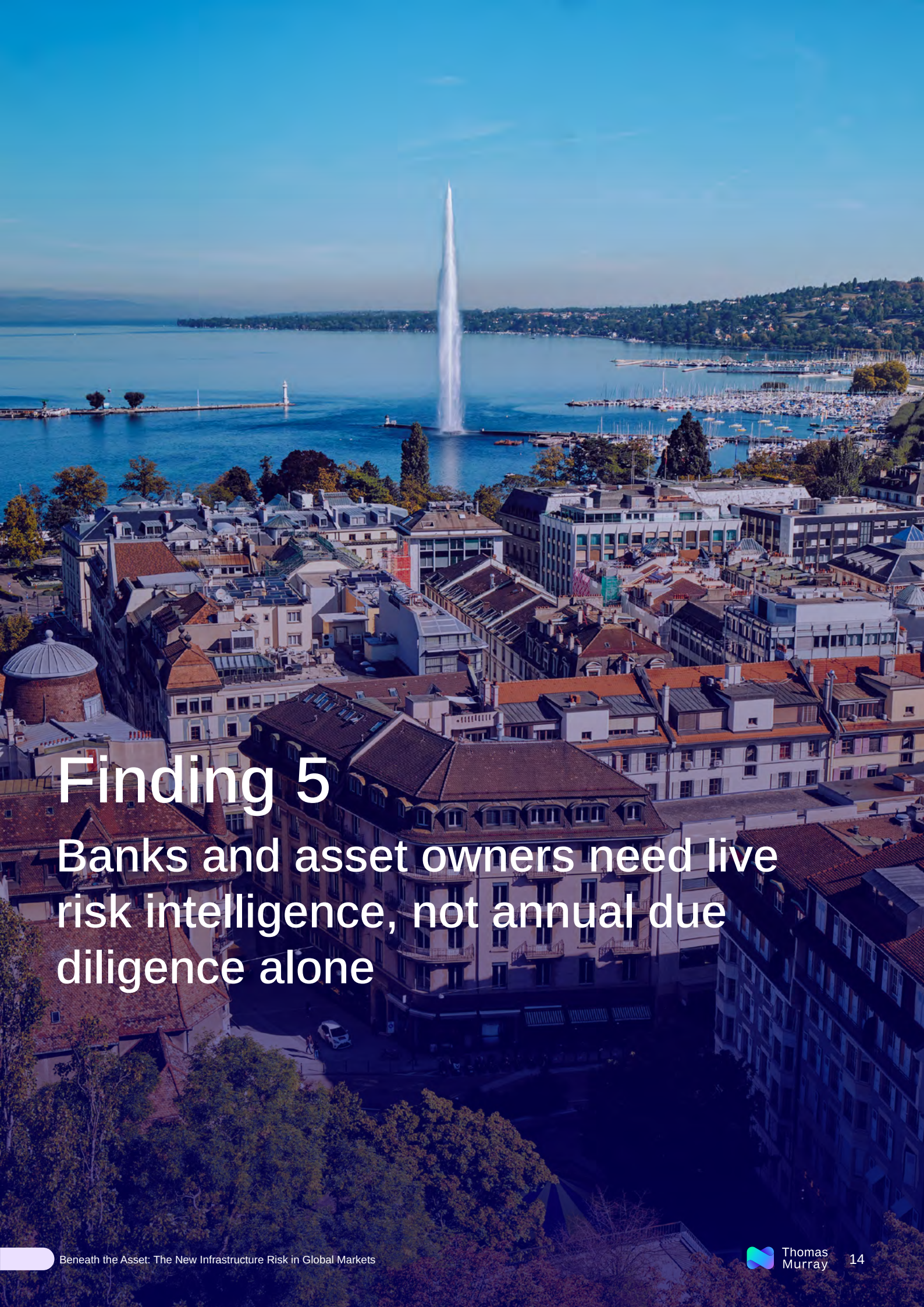
This creates opportunity, but it also creates risk.

A tokenised asset may still require safekeeping, settlement finality, operational control, legal certainty, identity management, cyber resilience, governance, recovery procedures and trusted infrastructure. If those foundations are weak, digitalisation may create the appearance of efficiency while increasing systemic fragility.

Who will independently assess whether the infrastructure behind digital assets is safe, resilient and fit for institutional use? This is where Thomas Murray comes in.

The same disciplines that apply to CSDs, custodians and post-trade infrastructure are increasingly relevant to tokenised and digital asset markets: governance, operational resilience, transparency, settlement integrity, risk controls, cyber posture, oversight and market confidence.

*Digital assets need analogue trust.  
The more markets digitise, the more they need independent assurance rooted  
in market infrastructure expertise.*



# Finding 5

Banks and asset owners need live risk intelligence, not annual due diligence alone

Our final finding is the most commercially important.

The risk environment is moving faster than traditional due diligence.

Annual reviews, periodic questionnaires and static assessments still have value, but they are no longer enough on their own. They were designed for a world in which infrastructure risk moved more slowly, markets were less digitally dependent, and geopolitical shocks were less immediately transmitted through complex global systems.

That world has changed.

Banks and asset owners now need real-time, recurring intelligence on the safety and resilience of the infrastructure beneath their assets. They need to know when risk is rising, where it is rising, why it matters, and how it may affect their exposure.

This does not mean replacing due diligence. It means upgrading it.

*The future model is continuous asset safety intelligence.*

That model combines:

- Independent infrastructure ratings
- CSD and custodian risk assessment
- Cyber resilience indicators
- Geopolitical and country risk alerts
- Operational resilience monitoring
- Third-party dependency insight
- Regulatory intelligence
- Market access analysis
- Digital infrastructure assessment
- Risk committee judgement

We are transforming Thomas Murray's data into recurring signals, including an Asset Safety Signal, CSD Resilience Watchlist, Cyber Resilience Gap, Risk Committee View and Post-Trade Stress Map, through a dynamic market intelligence platform.

The real value is not simply that we have data. It is that we can interpret what the data means for asset safety.

*Annual due diligence tells you what was true at the point of review.  
Live risk intelligence tells you what is changing now.*



# The new asset safety model

The old model of asset safety was built around custody confidence. The new model is built around infrastructure resilience.

Old Model	New Model
Where are the assets held?	How resilient is the full infrastructure chain?
Who is the custodian?	What are the cyber dependencies?
What is the legal structure?	What third-party providers are critical?
Is settlement reliable?	How exposed is the custody chain to geopolitical shocks?
Are controls documented?	What happens if a CSD, custodian or technology provider is disrupted?
Has due diligence been completed?	How quickly would we know if risk changed?
	What live intelligence supports decision-making?
	How does a new organisation or third party affect the existing risk profile?

This distinction matters. A financial institution can complete due diligence and still be surprised by a fast-moving infrastructure event. It can understand its asset allocation and still misunderstand its infrastructure exposure. It can know where its assets are held and still not know how resilient the chain beneath them really is.

*This is the market gap Thomas Murray is filling.*





# Why Thomas Murray

Our authority is rooted in decades of specialist work across CSD risk, custody risk, market infrastructure analysis, post-trade due diligence, cyber resilience and risk intelligence.

We are the independent risk intelligence firm for the new era of asset safety, with a platform that spans CSDs, CCPs, custodians, post-trade infrastructure, cyber resilience, geopolitical alerts, operational resilience, digital assets and regulatory change.

That combination matters because the market no longer needs fragmented views of risk. It needs an integrated view of the infrastructure beneath the asset.

## Thomas Murray brings together:

- CSD, CCP and custodian risk assessments
- Custody and post-trade expertise
- Cyber resilience ratings
- Market infrastructure intelligence
- Geopolitical and event-driven alerts
- Operational resilience insight
- Risk committee judgement
- Digital asset infrastructure assessment

The market doesn't just need more information. It needs independent interpretation.

*That is where Thomas Murray holds the advantage.*





# Conclusion

The next market shock may start beneath the asset

The financial system has spent decades improving the way it prices assets, trades assets and allocates capital.

But the next major disruption may not start with the asset itself.

It may start with the infrastructure beneath it.

- A cyber incident.
- A settlement disruption.
- A CSD weakness.
- A custodian dependency.
- A sanctions shock.
- A geopolitical event.
- A third-party technology failure.
- A digital asset infrastructure flaw.
- A regulatory intervention.
- A market access constraint.

These are not peripheral risks. They are now central to asset safety, and interconnected in ways that traditional due diligence alone cannot identify.

Banks, asset owners and financial institutions need to move beyond periodic due diligence and build a live understanding of infrastructure resilience. They need to know not only what they hold, but what their holdings depend on.

***The era of static asset safety is ending.  
The era of infrastructure resilience has begun.***

Asset safety is no longer a custody question. It is an infrastructure resilience question.

# Contact us

Please get in touch to find out how we can help you to mitigate changing risk.

Find out more: [thomasmurray.com](https://thomasmurray.com)

Contact: [enquiries@thomasmurray.com](mailto:enquiries@thomasmurray.com)

## About us

Thomas Murray provides risk intelligence and ratings covering central securities depositories, custodians, market infrastructures and financial systems worldwide. For more than three decades, the firm has helped financial institutions understand and manage the risks affecting the safety, resilience and performance of their assets across global markets.

