

# TAIL EVENTS ARE HAPPENING MORE OFTEN

Mastering uncertainty in an unpredictable world

June 2025

# Abstract

Alba Partners and ActiveViam were proud to host an exclusive CRO breakfast roundtable at the start of May 2025 on the topic of "Mastering Uncertainty in an Unpredictable World". The conversation flowed from the outset with perhaps one of the key quotes being:

**"It seems that tail events are happening more frequently..."**

This was a very telling statement and one that was explored in more detail throughout the event.

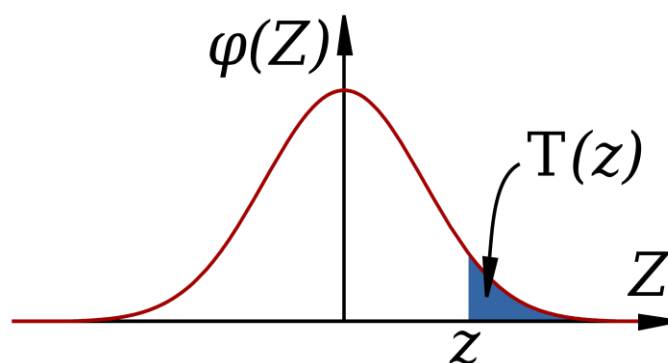
There were a large number of subjects touched upon. Of particular interest was that around the deterioration of the **US ecosystem as a stable and safe haven**. That this was happening was not the discussion point, the focus was more on the first and second order impacts and what were the possible alternatives.

**Operational resilience** was also touched upon, but not in the traditional context, the discussion centering around the link between resilience and the current global events (financial and geo-political). Questions such as how financial and physical supply chains could be assessed and evaluated were raised and discussed. All agreed that the principal challenge was around how well the organisation know their customers: their sensitivities to their own supply chains and how this affects their credit standing and default probabilities.

What quickly became evident was the need to be able to **access more data quickly** and in a flexible way.

While the frequency of tail events may feel unpredictable, organisations are not powerless in their response. The challenge is not merely one of foresight, but of preparedness. Ensuring that the right questions are being asked, the right data is accessible, and decision-making structures are agile enough to respond to disruption in real time. Strengthening operational resilience is no longer about compliance; it is about survival in a world where interdependence is both an asset and a liability. Organisations that invest in better visibility, more dynamic scenario planning, and deeper understanding of their clients' vulnerabilities will be better positioned not just to endure the next dislocation, but to emerge stronger because of it.

This whitepaper explores these themes in more detail.



# The changing relationship with USA

## Deterioration of the US ecosystem

When President Trump was elected in November 2024 markets reacted positively in the expectation of renewed economic growth and financial stability emanating from the USA. Since January, however, as the reality of the new administration's policies started to be understood, that early confidence has vanished and markets are now (May 2025) around 5% off their peak of mid December.

The tariff announcement was not the first sign of trouble though. The change in policy regarding foreign aid, the impatience to impose a settlement to conflicts in Europe and the Middle East, and the drive to reduce federal spending were creating nervousness even before the start of April. For the time being we have some respite but there is a feeling that the markets have not yet adjusted sufficiently. Perhaps companies are running down inventory and taking other tactical measures and that explains the modest 5% correction we currently see. The lack of visibility and resilience in supply chains is discussed later, but we should be ready for a further correction as the new arrangements start to bite.

The response to the tariffs has been uneven and we can draw attention to a variety of responses. Apple announced a plan to reduce manufacturing in China, but rather than bringing that back to the USA, they are transferring, instead, to India. They cite the need for large numbers of qualified scientific and engineering staff needed to support high-tech, high-volume manufacturing and point to the plentiful supply of these skills in China and India. Low-cost, it seems, is not the main driver. This indicates a structural challenge which applies not only for the USA but many other European economies too. The recent trade agreement between the UK and USA makes it possible for American motorists to buy Range Rovers and Jaguars at reasonable prices; the prospect of tariffs does not seem to have reinvigorated their support for domestic brands. On the other hand there appears to be a constructive dialog with China about future trading relationships which was, after all, the President's primary objective.

The Dollar is still the world's reference currency and will continue to be for the foreseeable future but alternatives are emerging in Europe and from China. While there are arguments in favour of using a blend of currencies, the challenges are many and varied.

- The US Treasury market is huge both in terms of volumes and liquidity making it easy to buy and sell large volumes without significant price impacts. Establishing comparable markets for EUR, RMB and others would take time.
- The challenges of co-ordinating multiple central banks, regulators and timezones would be complex and time consuming.
- And the legal and technical networks are set up to use the Dollar; dislodging it would be comparable to shifting the world's business language from English.

A significant development is the serious discussion around a potential move away from the Dollar's dominance, marking a change from the past 80 years.

# Operational resilience in the 'new' world

## Redefining operational resilience

As we follow the general theme of this white paper we can almost follow the development and evolution of Operational Resilience through the financial and geopolitical events of the past decade.

Let's take a moment out to reflect on the "good old days" when interest rates and inflation were low, we lived in (for the most part) peaceful times and apart from some issues which may have impacts in the future (AI and Climate for example) there was little to sway us from a carefree path. In this most perfect of worlds, resilience (and the need for it) had not been invented, our infrastructures were protected by robust disaster recovery processes and tail events were those rare ructions that risk managers built stress tests around to demonstrate preparedness. To put this into context it was only 18 years ago that Nassim Taleb invented the term "Black Swan" (1st edition published 2007)

We now live in a very different world, effectively the past decade has seen a financial and geopolitical regime change, it is as if the world has been turned upside down. The subject of this section therefore is how do financial and geopolitical changes impact Operational Resilience and why is it that "tail events seem to be happening more often"? This is hardly surprising when we think of the three main contributors to the current suite of these Black Swans, namely geopolitical, AI and climate. As all three are now experiencing increased volatility, given their interconnectedness, we would expect to see an increased frequency in Black Swan events. But why does this seem to impact Operational Resilience?

Let's first explore the significantly increased complexity in our financial framework. The geopolitical environment has become a lot more uncertain, and as a consequence significantly more volatile. Strategies need to be fluid and flexible, responses to events more timely and reactive and staff all performing at the top of their game.

There has been a surge, or more accurately an explosion in demand from consumers for tailored products/services, all to be delivered almost instantly. In order to satisfy this demand, physical and financial supply chains have had to become more efficient, with just in time delivery tolerances being shaved to razor thinness. All of this has been predicated on a flexible global supply chain (for physical goods) and IT systems and products which can ensure that this supply is done in the most flexible and efficient manner possible. Banking and financial services are no different with there being more bespoke products and increased demands from clients.

Such complexity carries increased risk. Disruption throughout this physical/financial supply chain has knock-on effects which (to steal the phrase from the financial regulator) cause "intolerable harm to the consumer".

Let's now explore the areas where there is the most complexity, and the risks that this entails.

The first is of course the increasing **concentration** of services and products onto a small number of suppliers. The most obvious here is that around the "Tech Titans", namely Alphabet, Amazon, Apple, Meta and Microsoft. Financial services have, for the large part, developed infrastructures which are almost wholly reliant on these

technologies. The concentration risk here is evident, and of course significant. We now go on to state the obvious, where we have a highly regulated financial services sector highly concentrated into a (largely) unregulated third party systems provider. Now, if we overlay this with the evolving political situation in the US (of which regulations these companies are subject to) we can start to see how political divergence can lead to financial framework instability and hence risk. The concentration risk, and consequences of a failure in any of these “Tech Titans”, would be significant. This concentration again is not just limited to the IT sector. One such example is that of rare earth magnets, 90% of which are supplied by China. A temporary ban on the export from China of these magnets in April 2025 caused significant downstream production delays in dependent industries across the globe. These are used by high-tech industries, from automotive and semiconductor to defense, aerospace and robotics.

The second is that of consumer demand and the “supply chain” needed to support it. The obvious category here is of course IT systems. They have now become increasingly sophisticated with AI being used across many sectors to augment the customer experience. With increased **complexity** comes increased risk. The failure of any component (either through accident or malicious intent) can have significant impacts further on the services sector (of which there are many documented examples).

We have seen cases where well known UK retailers have suffered major outages due to cyber attacks (and as we write this paper are still trying to recover weeks after the attack) as well as a leading automotive company being unable to sell its products over the course of a weekend because of issues with its order/inventory systems. Outside the IT environment we also have real risks to concentrated and complex supply chains. Who can forget the impact on the global supply chain when a single ship became lodged in the Suez canal or the disruption caused when a bridge in Baltimore was suddenly rendered unusable?

The increased use of AI has of course not been limited to those “honest brokers” in the various products of which it is employed. We now have Cyber attack “franchises” where aggressive DDOS tools can be rented. Malicious agents are not bound by policies or procedures, UAT, release schedules and production release windows. Their time to market is a fraction of the time that those on the other side of this arms race face. The genie is out of the bottle, and even a slow down by honest brokers in the use of AI will not slow those with malicious intent down. Now throw into the mix geo-political objectives and the result is a dangerous cocktail of a well funded and capable attack force.

So how can organisations go about protecting themselves? Well in a strange twist of fate, it could be that the Financial Services Regulatory regime may drive best practice with regards to Operational Resilience especially as we see an increasing number of failures with non financial services companies. The concept of “resilience” as distinct from “recovery” starts to have more weight when we apply the objective of the regulations which is to “weather the storm” rather than “don’t let the storm occur”. Now organisations need to accept that Black Swan events WILL occur, and then on that assumption how can they ensure minimum disruption to the client base, and the resumption to normal service.



**Baltimore bridge accident, 2024**

Photo: David Adams / U.S. Army Corps of Engineers, Baltimore District

# Data accessibility and analysis

## Need for more data and flexible data

As we face an ever increasing incidence of tail events, our ability to assess and respond becomes a greater focus. The response to these tail events can not be constructed until we are confident we know where our weaknesses lie. This leads us to the question (which almost all risk managers have asked, or been asked in their careers)

**“how much exposure do we have to...”**

or

**“what would the impact be if....”**

In the previous section we discussed the triple factors driving most current tail events, namely **Geopolitical, Climate and AI**. All of these would almost certainly manifest themselves as impacts to the credit portfolio of financial institutions. We say this because market shocks (including liquidity) are largely portfolio based and well catered for in general risk management practices. In times of crisis, credit becomes very idiosyncratic with portfolio effects all but disappearing.

As an example, when Russia invaded Ukraine for the second time in 2022 there was a double impact on credit portfolios. Firstly we had the sanction regime being significantly enhanced, so that direct and indirect relationships with Russian organisations fell under the restrictions. Secondly we had the direct counter threat by Russia to cut off the gas flows into western Europe.

Risk managers were then asked two questions:

1. What non-Russian organisations were indirectly connected with Russian ones?
2. What was the sensitivity of our clients to a western Europe gas shortage?

In an ideal world, the addition of a couple of filters into your comprehensive credit risk database would yield almost instantly the answer to these two questions. Unfortunately the reality is far from that, even in the most sophisticated organisations. At the core here is how well do the relationship managers really know their customers; there is nothing like a good crisis to really test the quality of your KYC framework.

Obviously once management has the answers, responses can be formulated and enacted, valuations made and writedowns performed as appropriate.

We now have a new class of **client**, our third party suppliers. How well do we really know them? Do we follow the same rigour in our Third Party Risk Management “TPRM” framework as we do for our KYC one?. The regulators expect the answer to be “yes” of course but as for KYC, there is nothing like a good crisis to test your supply chain. How sensitive are your critical suppliers (continuing the Russian gas example) to gas shortages; are they or their upstream suppliers connected with Russian organisations?



How well then do we *really* know our suppliers and the supply chain that supports them?

If we are now applying a full KYC ethos to our suppliers, then by extension the consideration of ascribing valuation via risk management should also be included. We have started to see the inclusion of TPRM into our ICAAP framework. Will we start to see a day where regular “valuations” of our third party exposure is somehow factored into our P&L? Recall that a concept such as CVA has only been with us (formally) since the 2007/08 crisis and now it is a mainstay of our traded credit valuation framework; will we see the day when we have a TPRM equivalent?

The inclusion of TPRM into risk frameworks, apart from questions about methodology and algorithm, raises questions about the availability of high quality, usable and performant data sets. The increasing sophistication of cloud-based data warehouses is reducing the cost of entry for new providers of data. This is, of course, a double edged sword. The technology encourages innovation, making it easier and cheaper than ever before to create and deliver datasets. However, that is no guarantee of quality. Datasets must have a known lineage and be conformant with industry-wide conventions for taxonomy; those attributes are essential if the dataset is to be usable. Finally we need to be confident that the data is up to date and accurate; either timestamped so that we know when it was created or with supplied validity period (required for back testing and retrospective analysis). These temporal characteristics are essential if the dataset is to be performant.

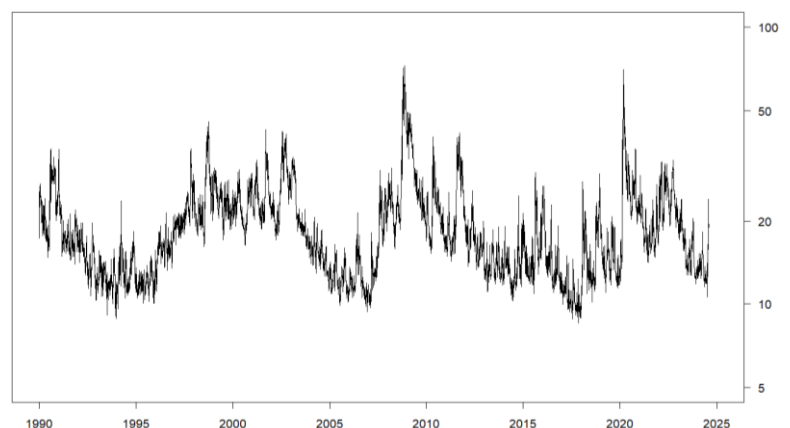
New datasets pose a number of challenges to the analytics and reporting infrastructure. Answering the question posed earlier about transitive data relationships puts the following demands on the analytics layer. It needs to be simple to merge a new dataset into an existing data model and for the taxonomy to be easily mapped (for example does a **rating of A in the new dataset** mean the same thing as an **A in my current dataset?**).

The analytics layer needs to be able to slice, dice and filter by attributes in the new dataset in any combination with existing attributes.

Perhaps the most difficult is to accurately reflect the new filtering into the subtotals and totals in the calculations.

This becomes extremely complex when the aggregation functions are non-linear (such as netted exposures, or value at risk).

**The Vix index  
1990 to 2025**  
A popular  
measure of  
market volatility,  
also called the  
Fear Index



## About ActiveViam

ActiveViam is a fast-growing financial data analytics solution provider. Built for and trusted by leading financial institutions, ActiveViam delivers active intelligence for complex financial analytics. It combines unrivalled technology, continuous innovation and exceptional people to unlock the power of real-time and granular data at scale. Designed as a high-performance semantic layer, ActiveViam's flagship product Atoti, allows clients to implement built-in front office and risk business solutions while accessing customizable technology.

ActiveViam is present in the world's leading financial marketplaces with presence in London, New York, Singapore, Sydney, Hong Kong, Paris and Frankfurt.

For more visit [activeviam.com](https://activeviam.com) or follow on [LinkedIn](#)

## About Alba Partners

Founded in 2020, Alba Partners is a specialist consultancy combining the agility and personal service of a boutique with top-tier delivery expertise. Our Financial Services practice supports leading institutions across regulatory change, risk, and transformation initiatives, including IBOR, Basel III, and Operational Resilience. We have also led complex mergers, acquisitions, exits, and divestments. With deep capabilities in Programme Delivery, Business Change and Data & AI, we help clients respond to fast-moving market demands. Headquartered in Edinburgh, with offices in London, Riyadh, Dubai, and Abu Dhabi, Alba Partners delivers across Europe, the Middle East and beyond.

For more visit [albapartners.co.uk](https://albapartners.co.uk) and follow on [LinkedIn](#)

