SKADI

Emerging Risks

2024 OUTLOOK

INTRODUCTION

Welcome to the SKADI “Emerging Risks 2024” publication for Audit leaders.

This report aims to enable you, and your team, to think beyond the **consensus** and plan for the year ahead. We seek to be thought-provoking, **alternative**… yet **realistic**.

As a result, do not expect to see the acronyms AI and ESG! **We are not discounting these from our thinking**! We see these as exactly the kind of widely-flagged consensus topics that mainstream consultancies will be providing extensive commentary about.

SKADI’s “Emerging Risks 2024” is a tool to help stimulate the thinking that you and your team may be undertaking at this time.

SKADI

KEY DRIVERS

In 2024, rising **geopolitical** tensions and the **elections** in both the US and the UK, are the macro drivers set to dominate the stage. As the geopolitical landscape continues to evolve with shifts in power dynamics and regional conflicts, financial institutions and their customers will be acutely aware of the potential ripple effects on global markets. The US presidential election and the UK general election[1], both significant political events, will introduce a new layer of uncertainty and policy implications that could significantly impact investment strategies, asset allocation, risk management and the direction of travel for regulatory frameworks.

Alongside these two macro drivers, we see three additional emerging themes in 2024: the rise of **insolvencies**, increased **cyber** risks associated with rogue state actors, cloud repatriations, and specific **regulatory and compliance** deadlines driving transitions.

[1] India – the world's largest democracy, and key part of the Finance Industry's supply chain, is also expected to hold elections between April and May 2024.

THEME 1 GEOPOLITICAL

FOCUS

Decision-making committees and forums - Their extent, key operating procedures, reputational risk management, information requests, and third-party risk.

The furore around the "debanking" of Nigel Farage occupied many column inches in June of this year. The incident gained momentum when members of parliament in the UK adopted it as a cause célèbre. The resultant fallout has been the departures of several senior staff at NatWest. The Chancellor calling for the **FCA** to conduct an inquiry into the debanking of politicians. The FCA requesting data from banks on account closures and subsequently revisiting the treatment of domestic Politically Exposed Persons.

The headlines may have been about access to banking and banking services but, as we alluded to in our July 2023 Horizon piece, our concerns are around how data on individuals (and indeed corporations) is documented, retained and communicated by staff.

Within financial institutions there are a number of forums that meet to discuss customers, business proposals and the raising of capital. Information from these meetings is rarely seen or shared outside of these forums, but it is often documented. Minutes are taken which can later be used in regulatory investigations, litigation and disputes.

The "debanking" scandal has raised awareness of how information can be legitimately accessed and then used with devastating effect. In Mr Farage's case, a **Subject Access Request** was used to reveal information held by the bank. This information contradicted information briefed to the press[2].

[2] The BBC initially reported Mr Farage did not meet the wealth criteria to hold an account at Coutts, a point they subsequently withdrew. Reuters cited "commercial reasons". It was later revealed that his political views were discussed and appeared to be instrumental in the decision to withdraw his account.

One can envisage situations where banks could be accused of **misrepresentation** if customers have been given information which later does not tally with documentary evidence which comes to light. For example, a company hoping to issue a convertible bond may have been told that market conditions, or investor feedback, led to an issue being abandoned, when in fact the minutes of the Reputational Risk Committee or say, Equity Capital Commitment Committee, may have concluded that the customer did not have a "good look" for the bank."

SUGGESTED WORKFLOW

Identify and grade what confidential decision-making forums exist.[3] Examine the framework and controls around documenting and sharing views from confidential decision-making forums within the institution. How information is conveyed to customers in such a way as to ensure accuracy, avoid tipping off (in the case of money laundering-driven decisions) and avoid potential future embarrassment.

It seems likely that **Information Requests** will increase in the coming year[4]. In 2023 organisations have been caught out when responses to Information Requests have revealed sensitive information in error. This has often been the case when the response has been handled by **third-party partners**. High-profile examples include data breaches affecting the Police Service of Northern Ireland and Suffolk Police.

SUGGESTED WORKFLOW

Examine the framework and controls around responding to information requests. Review how information held by third parties is risk-managed to ensure accuracy, and minimise the risk of data breaches, particularly those with which partnerships are identifiable and in the public domain.

[3] Recall approach used for identifying benchmark submissions in light of the LIBOR scandal.

[4] An increase could come from others following Mr Farage's example. These could be individuals, the press, through to bad actors seeking to exploit them as a security weakness – "*Ransom without the need for Ransomware*".

FOCUS

Wholesale vulnerability, near-shore programming risk, Global Markets supply chain, Cloud repatriation.

We see an increased risk in 2024 of state-sponsored attacks on Finance and Financial Institutions. We enter a period of increased **geopolitical** tensions. The Russia-Ukraine war will enter its third year. While further east the general sense of unease between Washington and Beijing has the potential to escalate. An **election** in India, with a large outsourcing industry critical to the Financial Supply chain, represents an attractive target from neighbouring China. Also, in our view, the press' assumption that Putin's recent meeting with North Korea's Kim Jong Un was to secure weapons, overlooks the shared track record both regimes have for their involvement in cyber tactics.

Elections have been subject to interference in recent years. Elections are due to take place in the US and UK, both economies where Finance has an outsized importance. In addition to direct meddling, we feel it would be attractive for hackers to look to destabilise the status quo by going after Financial Institutions – the cogs that sit at the heart of the modern capitalist system.

Further, in the past couple of decades, the near-shoring opportunity of using Russian-based programmers with low-cost/high-value programming skills means that there is an intimate knowledge of many of the models and systems used by Financial Institutions in the Wholesale markets and their associated potential vulnerabilities.

SUGGESTED WORKFLOW

Examine what line of sight 1st and 2nd lines have over near-shoring programmer risk. Risk-categorise systems and models which have employed near-shored programming staff from at-risk locations. Examine contingencies and business continuity planning for an attack impacting models, the ability to model, static data or the denial of access to pricing.

Until now the Finance Industry has been relatively overlooked in favour of other less-resourced, but equally high-profile, targets for cyber attackers. The LockBit ransomware group attack on ION Cleared Derivatives and Distributed Denial of Service attack on the German Regulator BaFin this year lays bare the vulnerability of the Finance Industry's **supply chain**. Improvements in the cyber security of industries in the wider economy

increase the attractiveness and feasibility of targeting Finance. Where attacks on the financial industry have come to light, these have tended to be ransomware-type attacks.[5]

SUGGESTED WORKFLOW

Examine whether Global Markets have performed a risk assessment on their supply chain. What work has been done to catalogue and grade the supply chain for the impact of cyber-attacks? Examine what contingencies are in place, particularly if an affected supplier has a market-dominant position.[6] What training is in place to prevent, but also how to respond in the event of an attack?

A large number of institutions, including banks, have moved some or all of their data and processing to the Cloud over the past few years. Cloud costs and the complexity of operating on the Cloud have prompted organisations to consider moving back to traditional platforms. Customers have shared with us their concerns over costs brought about by inefficiencies, and poor planning when Cloud migrations were undertaken. The costs of traditional hosting on servers have also fallen in recent years whilst the cost of Cloud computing has risen, making the cost disparity less apparent. Cloud migrations also took place during the pandemic, when cost projections utilised a much lower yield curve.

It seems inevitable to us that Cloud security, touted as a key migration advantage, will likely be tested in the near future. Hackers will continue to up-skill, and the target area is Cloud-based. A case of "build it and they will come". Whilst the Cloud is seen as disparate, security breaches are harder to contain and provide wider access than breaches affecting local servers.

It seems likely that a hybrid approach of "Cloud-plus" is likely to emerge, combining the benefits of the Cloud with the local advantages of traditional storage, now that understanding is improved. Cloud repatriation in any form would raise as many issues as the initial migration. There are risks which need to be considered. **Data sovereignty**: Users may have become accustomed to pathways and not realise these could change under a repatriation. **Captive contracts**: Businesses may have signed long-term commitments which dependant businesses may not be aware of. **Golden source**: Transfer of data to and from the Cloud has been found to be a source of unexpected cost, as well as replication of data i.e. where users assume replicated data will not be double charged. On repatriation, there is

[5] It should not be discounted that the low incidence of reported attacks on Finance may be due to the industry opting to resolve incidents by paying ransoms. Reuters quoted the ION attackers as saying the money was paid to them by a "very rich unknown philanthropist", resolving that attack.

[6] The ION attack disrupted communications channels between banks and vendors. Email domains were closed off, compromising the ability to communicate.

a risk of localised sources of data being compiled, which are not replicated across the organisation. **Data ownership**: legal issues over data ownership and responsibilities may arise.

SUGGESTED WORKFLOW

Review and update pre-implementation planning in light of possible Cloud Repatriations. Recognise that while similar risks and challenges were presented by migration, repatriation needs awareness, particularly where users may not be aware of changes to pathways. Focus on Data ownership, sovereignty and risks arising from localisation of data sources. Assess what work is being undertaken to generate efficiencies in data storage and repetitive tasks. Assess 1st and 2nd line understanding and awareness of captive contracts, and what dependencies may exist neutralising cost savings assumptions of alternative areas[7].

[7] E.g. Market Risk Management proposes to repatriate some processes unaware that Finance have long term commitments to a Cloud provider which these processes have a dependency on.

FOCUS

Documentation, valuation mechanisms, model risks, ethical conduct and culture.

We know from our own market experience and our work supporting litigation and disputes that contractual clauses are rarely reviewed until they are tested. Clauses agreed in the past can be found to be unworkable at some future date. At worst some clauses can be judged to be egregious or even downright predatory. The resultant impact can be financial loss, reputational damage, and costly litigation.

The more bespoke contracts are, the greater the prevalence of unique clauses, undertakings and covenants. Those businesses that structure bilateral deals and those offering private financing are ones with elevated risk.

With the revival of the single name Credit Default Swap (CDS) market, staff should be aware of the risks posed by customers as well as internal desks negotiating technical defaults triggering credit events.[8]

Public issuance is also at risk of scrivener errors. These come about from bouts of repeat issuance, where staff reutilise templates while failing to correctly update all terms.

SUGGESTED WORKFLOW

Examine what line of sight 1st and 2nd line have over documentation risk. Review Issuance committees, particularly those dealing with Private financing, restructuring and renegotiation of existing debt. Attention on covenants and undertakings for predatory clauses. Sample test areas of repeat issuance, particularly public, for scrivener errors.

Our own experience following the Global Financial Crisis was that Valuation Mechanisms implemented in the case of bankruptcy on some contracts were not fit for purpose. This led to protracted disputes and complex valuation exercises.

The pace of innovation, in the 15 years since the crisis, heightens risk. Risks include the expansion of the number of venues for pricing securities. This

[8] Clauses in new bonds issued by Hovnanian in 2018 prevented the issuer from making interest payments on bonds due in 2019, even though the company had sufficient funds. This technical default caused an uproar.

means the contractually specified venue may no longer be the most, or even near to the most, applicable one for the assets covered.

Others may be in the contractually specified channel of dissemination. Our experience was that market participants had moved on to new channels of communication and no longer posted prices, or indeed had never posted prices, using the contractually specified dissemination channel.

It should be apparent that transactions with the earliest start dates present the most risk.

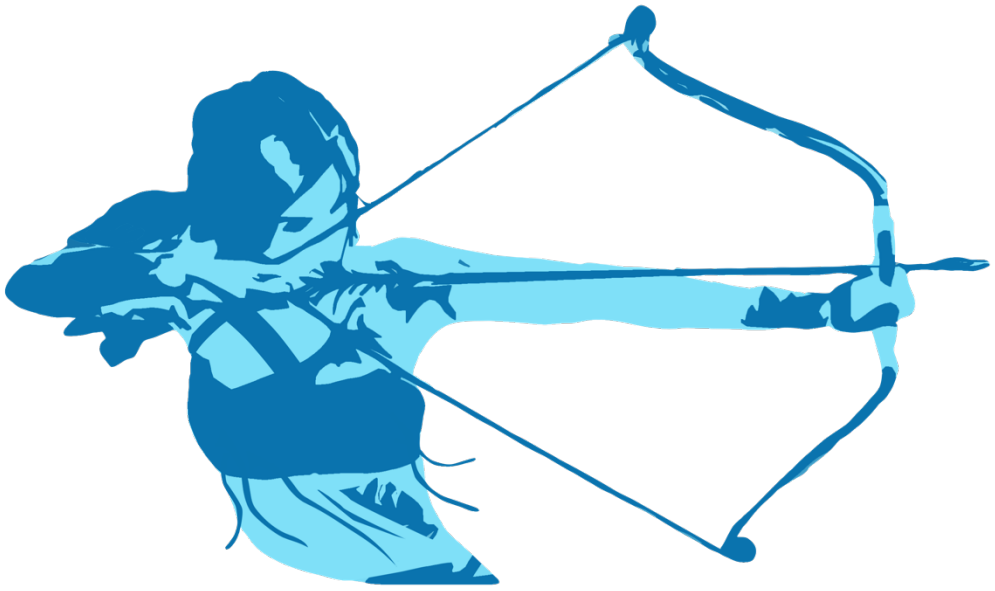
SUGGESTED WORKFLOW

Examine what awareness 1st and 2nd lines have over the Valuation Mechanisms specified in contracts. What steps have been taken, or could be taken, to remediate those relying on outdated or unworkable channels of dissemination? What preparedness is there, or need, for steps such as reserving against future legal costs?

Credit spread and price inputs to models are generally observable, but other inputs such as recovery rates may not be. Particularly having not been considered for extended periods of time. Model inputs during bouts of market stress represent an area of risk, where staff may seek to hide the extent of their risk by adjusting model inputs and static data.

SUGGESTED WORKFLOW

Examine the procedures around adjustment to model inputs and static data. What line of sight do Senior Managers have over their staff making adjustments? What controls do they have in place to verify whether data is being altered, and that changes are justified?



Debt has the unique characteristic of being an asset class that can transition between dealing desks. In worsening credit cycles this can give rise to internal conflicts. Desks may compete for the responsibility to service customers. Distressed desks in particular have unique operating characteristics, dual hatting as liquidity receivers as well as providers. They. also have access to non-public information as a result of their restructuring activities. High Yield desks may experience trading losses as conditions worsen. Where crossover exists between High Yield and Distressed areas a lack of defined responsibilities or pathways for assets to transition can lead to friction between staff, as well as confusion for customers.

SUGGESTED WORKFLOW

Examine what consideration 1st line has given to how credits may transition between desks in Global Markets. Review how 1st and 2nd lines recognise the different operational aspects of Distressed desks from markets desks such as Convertible Bonds and High Yield, as well as the opportunity set, such as access to Price Sensitive Information and external liquidity providers.

FOCUS

Assessment of the money laundering through markets due Q4 24, elevated Money Laundering risk in Commodities

The UK Government's "Economic Crime Plan 2, 2023 - 2026", released in March 2023, has a goal to:

> *"reduce money laundering and recovering more criminal assets, combatting kleptocracy and driving down sanctions evasion and cut fraud."*

Capital Markets is given a specific milestone with a deadline for completion of 4Q 2024. The exact wording of the milestone is:

> *"Renew assessment of the money laundering through the markets threat and dissemination of findings to increase firms' awareness and enhance relevant reporting. (FCA, NECC, FIU)."*

A decade has passed since an estimated US$10bn was moved out of Russia via 2,400 mirror trades carried out between Moscow, London and New York trading desks at Deutsche Bank. In addition to significant fines levied at the time[9], this year the Federal Reserve Board imposed a further fine of US$186m.

Mirror Trading, utilised for its ability to enable cross-border flows of currency, remains the strategy pointed to by Regulators. 5 years have passed since the Finance industry undertook the bulk of the work in relation to Remote Trading and Booking Risk, in the aftermath of the Deutsche Bank scandal. It seems likely that regulatory scrutiny will intensify throughout the year, and it would be a timely move to review controls and think more widely about the risk of Money Laundering through Markets.

[9] NY Department of Financial Services US$425m, FCA £163m.

Political coups in Niger and Gabon raise the risk of Precious Metals based Money Laundering. It remains to be seen what direction Russia's Wagner Group will take following the death of Yevgeny Prigozhin, but further instability is likely in Central Africa. Gold presented from artisanal mining in Zimbabwe has been an established tool for launderers to utilise via routes in Dubai and Hong Kong. Gabon has a similar artisanal mining industry.

SUGGESTED WORKFLOW

Review what awareness 1st line has of the money laundering through markets threat. What training have 1st line undertaken or planned to recognise suspicious transactions. Particularly the use of Commodities and Precious Metals to assist kleptocracy and sanctions evasion. Review of 2nd line for the robustness and completeness of market surveillance systems and the generation of timely Suspicious Activity Reports (SARs) and Suspicious Transaction and Order Reports (STORs). Refresh controls around Remote Booking and Trading.

FOCUS

US moves to t+1

In February 2023 the SEC announced a reduced settlement cycle from t+2 to t+1 for US cash equities, corporate debt and unit investment trusts. The planned implementation date for this is 28th May 2024, and there have been multiple tests run in 2023 to ensure that the transition runs smoothly.

Pre-matching settlement is the norm at depositories such as Euroclear and CREST - this helps prevent settlement failure. However, the depository responsible for settling US equities, DTC (Depository Trust Company), does not pre-match. Instead settlement instructions are put in place which either settle if both sides instructions agree, otherwise the trade will fail.

Electronic trade confirmation tools, such as DTC's Central Trade Matching Platform (CTM), agree trade economics bilaterally and enrich instructions with SSI's (Standard Settlement Instructions) from DTC's ALERT platform. However not all participants use this functionality, which sits upstream of trades feeding to DTC for settlement. In the absence of CTM and pre-matching at DTC to prevent trade fails, traditional methods, such as email or telephone, are used to confirm trade economics and settlement instructions.

We see two areas of risk arising from the t+1 transition. Firstly, increased counterparty fails due to the segment of the market reliant on traditional methods, which face a significantly shortened window to match trades.[10] This may increase the need for capital in support of desks fulfilling customer transactions when counterparties have failed. Has consideration been given to the increased burden of allocating and reclaiming resultant costs? Secondly, those businesses utilising affected US markets and instruments as a peripheral part of their business. What is there level of awareness and preparedness?

SUGGESTED WORKFLOW

Examine preparedness for the move to t+1. Focus 1st line work on peripheral risks such as hedging, and financing. 2nd line focus on capital costs, credit risk, and potential for increased burden of allocation and reclamation of costs.

[10] The Association for Financial Markets in Europe (AFME) notes that settlements teams only have 2 core business hours between the end of the trading window and the start of the settlement window, compared to 12 core business hours in a T+2 environment.

Everyone you'll speak to at SKADI has front line knowledge and a deep understanding of financial products

Our first-hand experience of complex financial products and front office expertise gives us the ability to ask the right questions for you

We make our findings accessible, so you feel confident you understand what's happening when – and why

SKADI

www.skadilimited.com