Under the spotlight

Over the past 18 months, the pandemic and the Robinhood saga have put operational risk in asset servicing under the spotlight, as experts say replacing legacy systems and treating operational risk holistically will help companies manage it with greater robustness

Maddie Saghir reports

The COVID-19 pandemic and the Robinhood saga have put operational risk under the spotlight over the past 18 months. Operational risk relates to the actual losses that can occur as a result of inadequate or failed internal processes, people and systems, or from external events.

In 2001, the Basel Committee Banking Supervision outlined it wanted to enhance operational risk assessment efforts by encouraging the industry to develop methodologies and collect data related to managing operational risk.

But now, with moves to Basel III, there have been changes regarding how operational risk capital (ORC) is calculated. Banks will need to ensure their internal loss data is as accurate and robust as possible to substantiate their calculated internal loss multiplier.

Meanwhile, operational risk managers will have the opportunity to reduce the existing and future ORC by focusing efforts on managing and reducing actual operational losses. Embracing new technologies and techniques will be key in grasping the value of operational risk programmes under Basel III.

As Deloitte states: “A bank’s infrastructure for operational risk management should leverage automated workflows to continuously monitor for emerging problems and ensure the right people receive

the right information in a timely manner, enabling them to respond quickly and effectively."

Asset servicing carries a large amount of operational risk due to the multi-layered value chain, which includes the movement of data and instruction information from issuers to agents, custodians, broker-dealers, fund managers and end-investors — and this all happens within critical timelines.

Operational risk in asset servicing can result from missed or incorrectly processed corporate actions, proxy and class action events. The extent of the financial loss may be determined by position size, event type and market price change for a particular security.

"Every asset servicing operation carries risk, but the level of risk is determined by workload versus headcount, automation versus manual processes, as well as staff knowledge, seasonality and the capacity to accommodate market and business change at a manageable cost," explains Neil Sheppard, global head of business development asset servicing, SmartStream.

The primary sources for corporate action risk are often driven by the growing complexity of corporate actions across the globe, expanded use of derivatives and the associated introduction of intricate intercompany booking models, and higher corporate action processing volumes driven by an increase in announced events and growth in trading activity.

John Byrne, managing partner, Sionic, says: "When you consider each of these factors and couple them with outdated systems and inefficient manual processes, they will incrementally add to the burden within organisations compounding the associated risk exponentially."

Sailing through stormy seas

Managing operational risk can be difficult amid a changing environment, as seen with the COVID-19 pandemic. During the first phases of the pandemic, weaknesses became quickly apparent within the financial services space. Many of these weaknesses can be put down to legacy practices. Describing some of the drawbacks of legacy systems, David Smith, senior director, Broadridge professional services, explains: "First, there is fragmentation of systems, and manual reconciliations are often required between systems — each one of these hops between systems can be a point of failure. Second, legacy systems do not have robust data traceability built into them, so errors can become difficult to identify, diagnose and fix."

Bill Meenaghan, product director, securities processing, IHS Markit, explains: "Legacy systems can be cumbersome to work with to change capabilities. The code may be quite old and there can often be inherent security flaws."

As industry requirements change, it may be hard to change legacy systems to keep up with these requirements which can make processes less efficient. Therefore improving, or at a minimum keeping up with, operational risk management best practices can be difficult.

"New technologies that are released may not easily integrate with existing legacy systems so there has been a desire by some clients to outsource the system management to third parties, or to simply migrate to a managed service and allow the service provider to keep up with industry requirements," comments Meenaghan.

In addition, Byrne suggests problems can also be attributed to mindsets that grew from the bygone era of processing physical securities — along with other practices that have simply failed to evolve over the decades.

"In the end, such traditions and ways of thinking challenged the industry and triggered our ability to reassess how we do our business and adjust to the new remote working environment that many were required to quickly adopt and continue to work from today," comments Byrne.

Many firms are digesting lessons learnt from the past 18 months after facing the challenges of working in a dispersed office environment during lockdowns.

According to Sheppard, those that fared well had invested in industry standard processes with automated practices and systematic control — and those that had not are looking to follow suit to better manage their risks.

Industry standardisation, for example through ISO 15022 and ISO 20022, is a facilitator of automation. ISO 20022 is a single standard that covers all business domains and end-to-end business

processes. It facilitates the creation of new services and enhances straight-through processing (STP), which helps reduce risk in the market.

Industry market practice groups like the Securities Market Practice Group and National Market Practice Groups (SMPG/NMPG) have played an important role in defining best practices that firms can employ to structure efficient workflows. For example, SMPG has been successful in establishing globally agreed harmonised work practices which, integrated with ISO standards, has brought the industry closer to achieving STP.

Sheppard says: "It is a lot of work for industry participants to meet these challenges alone and so they are looking to us [SmartStream] to accelerate the required change with our best-in-class technology, cloud hosting and 'model client' configuration covering requirements across asset classes, event types, country/markets, accounts, positions plus client configurations."

Out with the old, in with the new?

Spurred on by the pandemic, many firms are looking to modernise their systems to reduce risk as legacy systems can be a barrier to improving operational risk management. As firms modernise their systems, they will take away huge swaths of risk — which is a critical reason for embarking on the simplification journey.

Sionic foresees that evolving brokerage and banking operations, expanding customer networks, security, compliance, and many more aspects within the broader post-trade lifecycle ecosystem will be re-evaluated, re-defined and refreshed in one form or another.

Byrne notes: "More importantly, the adoption of new technology to meet the expected permanency of an expanded remote working environment and the need for an improved virtual collaboration landscape will be paramount in their design sessions."

Sheppard states: "A key agenda item today is to protect our business in a cost effective and operable manner. A company needs an affordable, easy to implement solution which caters for a business solution, a service differential, risk mitigation, enhanced control, governance and scalability."

For example, often when signing up to a hosted service, the infrastructure will be governed, accredited and independently tested, managed and scrutinised.

The level of security will be published and the participant will have comfort in service levels being met and avenues of recourse being available.

But Sheppard highlights that by automating and relying upon proven, best-of-breed technologies and know-how, the industry participant will be subscribing to robust, cutting-edge technology.

Emerging technologies like distributed ledger technology (DLT), with full data traceability built into it, and artificial intelligence (AI) can help reduce operational risk. For example, AI can drive 'smart' reconciliations which reduces manual processing and operational risk.

Meenaghan argues the promise of DLT is not here yet. But in an ideal world, processing transactions via a distributed ledger may help to ensure that securities and cash are moved between participants instantly and without friction.

Additionally, checks could be added to ensure the seller actually has the stock available and the buyer has the cash available to settle the transaction.

"If that could be achieved, you could move to an instant settlement process rather than T+2. Foreign exchange could work in the same way; a rate is agreed and the two currencies are swapped instantly. There is a little way to go with DLT but if the current limitations with some emerging technologies could be overcome, then they could help to substantially reduce operational risk," says Meenaghan.

The settlement cycle

Some industry participants believe moving from the T+2 settlement cycle (two business days after the transaction date) to T+1 and even T+0 will reduce systemic and operational risks.

This topic was particularly brought under the spotlight in January when Robinhood had to restrict trading in stocks including Gamestop because of the volatility caused by retail traders. Vladimir Tenev, CEO of Robinhood, believes the existing two-day period to settle trades

exposes investors and the industry to unnecessary risk, which is ripe for change.

Sionic supports the belief that shortening the settlement cycle to T+1 is a business process issue more than a technology advancement issue. The proprietary technology developed by individual firms along with today's vendor solutions can support the move to T+1. However, real-time gross settlement or the migration to T+0 would require significant technology rewrites as well as wholesale business process changes.

Weighing in on this, Broadridge's Smith highlights that firms using T+1 will, in the process of the transition, simplify and modernise their technology, and will realise reduced operational risk benefits. However, he adds "firms that are late to the game and have not invested well in advance will find themselves scrambling to catch up, and may come up with band-aid solutions to comply".

"These stop-gap measures can increase risk; some will only find out the hard way. It is critical that firms start planning now for the inevitable and at least understand how they will be impacted," Smith says.

Meenaghan adds: "The Central Securities Depositories Regulation (CSDR) is on the horizon, so the imperative to settle all transactions on time will now take on a greater importance. There has always been a strong desire to settle all transactions on time, but soon there will be penalties for trades in EU central securities depositories (CSDs) that settle late."

Many industry participants rely on custodian or agent fail reports to deal with issues, but that is too late in the process.

According to Meenaghan, more attention to unmatched trades or unrecognised trades that have been alleged against companies is required, and there are several services that will allow clients to get these more real-time, rather than the current once a day report that most custodians send. Using these services to handle exceptions will become paramount from 1 February 2022.

The future of operational risk

There are a number of strategies, such as implementing enhanced technology (like DLT), that will play an important role for the future of operational risk.

Sheppard says the future of asset servicing operational risk needs to focus on enhancing business value, promoting proactive control and providing governance cost effectively through security, resilience and compliance.

Industry experts note that the conversation is changing from the top down to a mindset focused on making risky processes (such as corporate actions) as secure and as efficient as possible.

Sheppard highlights the importance of enabling automated processing of administrative tasks and aligning experienced small- and medium-sized enterprises to deal with the edge cases of an event and its options while giving due care and attention to decision support, entitlement optimisation, market claims and taxation — all differentials and healthy facts when it comes to profit, reputation and growth.

He says the steps to get there now "require less investment in time, budget and attention as my firm has done much of the hard work".

Also looking to the future, Smith muses: "It is easy to say the future looks bright, but this might be unwise optimism. While traditional risks are being controlled, new ones are emerging."

"We do not understand fully what risk is represented in new technologies. We already see the rough shape of what risk can look like through privacy breaches and ransomware hold-ups that have begun to appear."

From Sionic's perspective, Byrne believes that in the years ahead, as the adoption of cloud-based operating platforms progresses, data utilities will evolve beyond the parameters defined today and a movement toward a more collaborative approach to data management and risk management across the industry.

"Embedded deep into the fabric of the rapidly evolving post-trade support model are the intricacies of tomorrow's risk management solutions. We believe employing tools and systems that are data-driven, collaborative, agile, and sustainable will deliver the client centric value proposition firms strive for," concludes Byrne.

Pooling together resources in a regulated and secure way via the cloud will ultimately support an array of business models, business growth, and business functions which may well be the most pivotal step toward reducing risk. ■