Key Takeaways from NeuGroup's 2019 H1 Asia Treasury Peer Group Meeting

NeuGroup Insights

AsiaTPG members discussed treasury's role in M&A integration, risks to finance posed by humans, cybercrime, getting money out of China, RPA best practices and more at their spring meeting in Singapore.

Easing the M&A Integration Process: Treasury's Role

A checklist to help treasury teams manage issues before and after a merger deal closes.

Mergers and acquisitions present multinational corporations with a multitude of integration challenges, many involving treasury. So it helps organizations to have a systematic approach to managing issues including financing, banking and personnel when one company absorbs another. That was among the takeaways from a recent presentation at the spring meeting of NeuGroup's **Asia Treasury Peer Group** in Singapore. Here are some of the key areas and actions highlighted by one AsiaTPG member, who divided the topic into three parts: prior to day one of the combined company, day one, and the first 100 days.

Prior to day one: Hedging. The presenter identified hedging the purchase price as essential in funding cross-border deals. He said that using FX options, including collars, can help protect against swings in FX rates during periods that can be as long as eight months. Yes, management might object to paying the premium, as it did once in the presenter's career (at another company) during a multibillion-dollar deal. In that case the premium cost $10 million. That's high, but a lot less than the $100 million swing in the cost between the deal's announcement and closing date. Lesson learned.

Prior to day one: Tax and legal. Deciding which legal entities will survive a merger is part of the critical focus on exploiting synergies as two companies integrate. But changing legal entity names can take a long time in some Asian countries. The presenter also warned of problems and inefficiencies if tax and legal teams are brought into the integration discussion too late in the game. And service level agreements (SLAs) and transitional service agreements (TSAs) need to be in place to ensure audit compliance.

Prior to day one: Banking. Working capital bank credit facilities and related guarantees must be prepared and discussions with banking partners should begin before the deal closes, again with the goal of exploring synergies between the two companies. Updating bank account signatories can take longer than you think, and the presenter said there are two options: Add names first and clean up the list later, or wait until there's clarity and do a one-time setup. Just be aware of any signatories who are leaving the combined company.

Day one: Communication. The goal on the first day of the new company's life is for top management (including the CFO and the treasurer), department heads and regional leads to reach out to all stakeholders to welcome them, share company policies, schedule introductory meetings and establish parent company guarantees and support for credit facilities.

The first 100 days: Make a bank implementation plan. Here are some of the key responsibilities for teams tasked with starting discussions with banks about integrating the financial institutions used by the acquiring company with those engaged by the acquired company, some of which may overlap.

- Validate data: Make lists of bank accounts, bank signers, pooling structures and facilities limits.
- Update bank signers on these accounts.
- Update bank portal authorizers on these accounts.
- Update system administrators on the e-banking portals.
- Decide whether to integrate different e-banking portal IDs under a single corporate ID.
- Review pricing grids and harmonize bank fees.

The first 100 days: A consent letter from the acquired company. Due to bank secrecy laws, some banks will not release data of the acquired company to the acquirer's treasury team.

The argument is that the acquirer's treasury team has not been appointed by each of the acquired company's directors as authorized individuals on the bank accounts. The work-around is for the acquired company to issue a letter of consent to the banks allowing them to provide the data to the acquirer's treasury team.

The first 100 days: More stuff to do. Other items on the checklist include giving concrete instructions to any consulting firms hired to help with the integration. And internally, finance needs to check every working group to identify "treasury touchpoints." There's also agreeing on which systems to retain or adopt, setting an organizational structure, aligning policies and identifying "quick wins."

People issues. Many of the personnel issues that surface before, during and after mergers require treasury to answer questions. Here are some outlined by the presenter:

1. Who does what in terms of process? Is there a business continuity plan?

2. Do we have the right resources for the takeover to work in terms of competency and bandwidth? Do we have the integration expertise?

3. Who is leaving the combined company, will knowledge be lost, and who is taking over? How do we communicate this information?

4. How fast should integration take place to avoid disruptions to the business?

Avoid pitfalls. Here are some recommendations to help treasury make integration smoother:

1. Keep in mind that the acquired company may have some unique processes like manual signatories in certain cases.

2. Stay organized during the M&A integration, especially with old and new information. Retain access to legacy systems, repositories of data and knowledge learned.

3. Beware of prepayment penalties when the acquirer decides to prepay the target's more expensive debt.

4. Regarding FX, ensure the lines are in place, consider terminating existing trades and review the hedging strategy.

5. Ask, "Who needs money now?" as you review intercompany loans, credit facilities and pool structures.

Ask for help. Because many treasury departments are not staffed to handle complex integration projects, it's essential for treasurers to seek support from other teams. This may mean delaying nonessential work done by treasury for other departments and enlisting other teams to complete tasks usually done by treasury that have fixed deadlines. If necessary, consider hiring temporary staff.

People as a Risk

Regional treasurers in Asia contemplate the elimination of people from treasury operations.

"There is no problem in treasury that cannot be solved with better coding." That provocative statement raised a few eyebrows at the Asia Treasury Peer Group meeting. The member who said it, paraphrasing a leading proponent of digital transformation of treasury, clarified that it applies more to treasury operations than treasury's role in business support. But still.

Advantages to automating treasury ops. There are essentially three main advantages to coding treasury processes for greater automation:

1. **Cost reduction and greater productivity.** Bots licensed for $8,000-$10,000 per year that work 24/7/365 might reduce the cost and boost the productivity of certain treasury operations dramatically. With all the focus on scaling treasury to support growing business mandates, supplanting people with robotic process automation (RPA) can seem unavoidable.

2. **Employee engagement through technology.** The ongoing advancement in RPA and other forms of automation suggest that a lot of issues in treasury operations involving transaction processing, capturing and managing data, and creating forecasts and reports can be solved by coders. Coding automation into workflows also frees up people to interact with people who run the business processes and better support them with finance. Most importantly, however, the automation of mundane tasks that shifts work to more valuable human interaction keeps employees engaged and motivated.

3. **Greater cybersecurity and fraud mitigation.** People represent the most significant cyber-risk. A cybersecurity expert from a global bank with a center of excellence in Singapore noted that the largest proportion of cyberevents still exploit human vulnerabilities by convincing people to do things they shouldn't (see below). The best way to secure treasury, therefore, is to eliminate people from processes, especially involving payments. "It's far more secure to embed proper controls in an automated, straight-through process than to subject payment workflows to human failures," he noted.

Eliminate the easy theft. Most cyberevents consist of business emails that convince people to change payment instructions, give up information or click on something that installs malware. It's far easier for hackers to send an authentic looking and sounding email that fits facts and circumstances and convinces someone to circumvent normal processes and procedures than it is to hack into a secure system. This is why cybersecurity experts emphasize automation. Code is less vulnerable to an email with new payment instructions or the need for an emergency wire, especially if the identity verification controls are coded into the process.

Leave sophisticated hacker risks to others. Preventing hacking of secure systems is probably beyond treasury's ability to manage. The level of sophistication of crime syndicates and state actors with abilities to compromise secure enterprise systems, without convincing humans to circumvent security, brings the risk mitigation squarely into the realm of the information security teams of the enterprise and its partners. This is another reason why cybersecurity experts emphasize the people problem.

Check the need for a people control point? Eliminating people as a control point on straight-through processes is likely to be difficult for some treasurers to accept. Indeed, having a human being eyeballing automated payment files before releasing them to the bank feels safer to me. But I'm far more concerned about giving up on the need for human judgment in risk management activities.

Be smart. It still seems prudent to have checks and balances on automatic execution of outputs from a risk control model, for instance. Moreover, I believe people should still have an override switch on machines, which may still be compromised, poorly coded or otherwise far from infallible. People are a risk—but so are machines.

The Pressing Need for Cyberincident Response Plans

Painful lessons teach treasurers in Asia that humans—not technology—pose the greatest risks to data security.

Relentless cyberattacks and growing awareness of their potentially disastrous consequences have raised the pressure on treasury teams to take more action to mitigate the damage done by phishing scams in which bad actors impersonate trusted contacts, by malware used to obtain data and extort ransom, and by other forms of hacking. This awareness means multinationals can no longer avoid the need to adopt cyberincident response plans to deal with the reality that humans within organizations pose significant risks to the security of data and financial assets.

Those conclusions and other takeaways emerged at the **Asia Treasury Peer Group** meeting, where members shared some of their hard-learned lessons and an expert from a leading international bank outlined some of the risks and prudent countermeasures.

Business email compromise (BEC). Members described incidents underscoring the risks posed by employees, suppliers, customers and cloud service providers who fail to recognize emails often designed to facilitate a fraudulent payment. Here's a hypothetical example based on several cases discussed at the meeting: A former employee of a key supplier convinces a member's shared service center team to update payment account information just before a large delivery. Two days later, the supplier calls looking for the payment. A rapid investigation shows that the money went to the wrong account. The banks involved are contacted immediately. But thanks to vastly improving payment systems, the money has already been transferred to another jurisdiction with no cross-border judicial assistance. The money is gone and recovery unlikely.

Battling BEC. The expert's presentation advises mitigating BEC risk by developing a process that can potentially detect the registration of malicious look-alike internet domain names used by cybercriminals. But realize that if a vendor's email is compromised, fake messages may come from the correct domain. So be wary of any requests made by email and confirm all changes in payment instructions verbally.

The best defense. The expert argued that because people are the weakest point in guarding against cybercriminals, the best defense is to remove people and manual processes and use technology to automate controls and payment systems. While it might seem that hackers stand a better chance of foiling technology-based processes, the expert said it is harder to hack robust technology than it is to entrap humans who are using manual means to make and receive payments.

The bottom line. Far too many companies have not prepared a risk management plan whose effectiveness is regularly tested. Every organization's incident response plan should be grounded on these five basic concepts:

1. **Identify**. Know who poses risks to security and what methods they use, including phishing and malware.
2. **Protect**. Attack your employees to find weak links; get independent assessments; implement controls.
3. **Detect.** You will be attacked; to minimize damage, detection is more important than prevention.
4. **Respond.** Engage in scenario planning, conducting tabletop drills to simulate emergencies.
5. **Recover.** Learn the best methods to a) reduce the chances of repeated incidents and b) recover assets.

Critical questions. Treasury teams bolstering their cybersecurity must ask if they have:

- Prepared a risk management plan based on a realistic scenario?
- Established with IT and compliance departments effective policies and procedures?
- Ensured that policies and procedures remain adequate and cover financial information such as payments instructions?
- Checked that spam filters are turned on, protection software is active, and data backups are fully effective?
- Verified that the identity of staff with significant delegation of authority is protected?
- Tested all aspects of their defenses?

What to Know Before Jumping on the Bot Bandwagon

Asia finance professionals discuss lessons learned in employing robotic process automation.

Finance teams at multinational corporations have, by now, heard a lot about the benefits of using robotic process automation (RPA) technology to help handle high-volume, repetitive tasks as the business pursues growth and scale. While some companies are well down the road of adopting RPA, others are just starting to consider it or have it on their to-do list. That spectrum of experience formed the backdrop at recent meetings of the Asia CFOs' Peer Group and **Asia Treasury Peer Group,** where members discussed their journeys in exploring and implementing RPA.

RPA is tactical, not a replacement for ERP. RPA should be used as a tactical tool to enhance automating cumbersome processes. One member used this analogy to describe the role of RPA in her company's technology strategy: "If an ERP is like a subway network, then RPA is there to help in the last mile of the commute, like a shuttle bus service or a bike-share service." One member talked about her company's ERP implementation project and how RPA was used in data migration from the old legacy system to the new ERP system as part of the tedious phase of this project implementation.

Redesign business processes. Do not underestimate the importance of redesigning business processes before implementing RPA. If you use a robot to execute a process as humans would do it, the results will likely be suboptimal, and fail to leverage the full technology capabilities of the wider system infrastructure. To avoid such an outcome, one member's company spent 18 months to redesign business processes in preparation for a robust RPA rollout.

Where to locate RPA teams. Several members said they have a centralized team within the region that focuses on RPA projects company-wide. For one member, the driver was to have this centralized RPA project team in Hong Kong, where the company has its regional management office. That way, decisions on prioritizing the various RPA-related projects benefit from having regional management input and more resources from the bench strength of a regional office.

Consultant considerations. For another member, the critical factor in locating the regional RPA project team was being able to work closely with an external consulting firm in Shang-

hai that had expertise to cover projects for the region and offered the most cost-efficient service. And while you can start RPA projects by using external consulting firms that provide experience and know-how, one member recommended building RPA development skills internally so that your team becomes self-sufficient and can expand and maintain all RPA activities.

Progress report. This member started the RPA journey in 2016 with their first group of robots with the assistance of RPA vendors and a consulting firm executing on implementation. Today, they have their own internal automation center of excellence team, which evaluates business requirements for RPA and develops RPA solutions. They use 20 RPA licenses to operate over 500 bot programs every month and have downsized average RPA development time to 10 hours of programming per bot.

Start small and scale up when ready. With each RPA software application license costing about $10,000 annually, the barrier to entry is low and you don't have to consider a heavy capital expenditure investment. The recommendation from several members is to start small RPA projects as a proof of concept, focusing on easy cases with quantifiable justification for RPA; then progress from these quick wins to expand RPA deployment in targeted areas while establishing a framework and methodology for an efficient RPA rollout as a proof of ability. That's followed ultimately by a proof-of-value phase in which you're driving operation transformation with enterprise-wide implementation of automation initiatives.

Find your bot comfort level. Bots can be programmed to do any repetitive task that is logically sequenced. The bigger hurdle for humans is deciding what tasks we are willing to let go of and delegate to a bot. Members discussed their bot comfort level at the recent meetings. A few use bots for FX trading execution, with one using them for both execution and FX settlement. That led to a question on how to ensure adequate controls when RPA is used to execute financial transactions such as FX trades, revealing that some members only felt at ease with bots doing internal reporting tasks, like creating management reports that draw on information from various systems. Others are comfortable using bots to prepare tax filing reports and for central bank reporting. In this discussion, one member highlighted that her company uses an artificial intelligence (AI) tool to negotiate and administer legal contracts, which sparked surprise from others. We'll look into that subject in greater depth at future meetings and in upcoming articles.

Easing Cross-Border Fund Flows Out of China

MNCs with trapped cash in China are always evaluating channels for getting money out.

Where exactly US-China relations are headed is impossible to say—one big reason many investors are very uneasy. But for multinationals, it's safe to say that the best way to get money out of China is to diversify your fund-flow channels; it's a takeaway that comes up again and again.

Multiple structures for multiple channels. With fresh guidance on cross-border flows out of China as the backdrop, a global bank's China transaction banking head told participants at the recent **Asia Treasury Peer Group** meeting that having multiple structures will allow corporates to take maximum advantage of both official regulatory changes and unofficial window guidance. These structures include in-country and cross-border pooling, cross-border sweeping arrangements, centralized cross-border payments (aka payment factories using POBO/ROBO and virtual accounts) and outbound/inbound intercompany loan programs.

Prepare to tweak and change. Given that official regulatory changes and changes to unofficial guidance happen fairly often, you need to be prepared to tweak your use of channels and/or clean up cash management structures so that your cash outflows are as fluid as possible. One cleanup example cited involved ensuring that all entities—not just some—are in the cash pool to share the quota to the maximum level. That said, if you have structures set up under a previous regulatory methodology that are optimal for you because of a bigger quota capacity, then you might want to keep separate arrangements for specific legal entities. As one member said, "I am kind of glad we have not committed to any structure yet, so I don't need to keep changing it."

Understand the concepts. If you're not fluent in all the latest guidance, it can quickly sound complicated. So before getting too confused, most treasury professionals should start with

the basics. Simply stated, there are several fund-flow channels, then there is a separate track in each channel for foreign currency flows, mainly USD, in and out of China (governed by the State Administration of Foreign Exchange, SAFE) and RMB flows in and out of the country (governed by the People's Bank of China, PBOC).

Competition in the channels. The latest SAFE regulation in mid-March gives MNCs an enlarged quota of up to 2x total equity for centralized foreign debt (incoming flow to China) and a quota of 30% of total equity for centralized offshore loans (outgoing flow from China), resulting in more interest payments out of China going forward. SAFE has also simplified the quota registration process to a one-time effort, streamlined supporting documents for foreign debt FX transactions (digitized), and allowed for the removal of a previously required header account for the leading China entity in the structure.

The hope is that the new SAFE regs will prompt the PBOC to follow suit with its own easing of channel restrictions. The knock-on effects, of course, are made more complex by the local regulators and other government authorities (including tax authorities), who may have their own channel tracks and guidance on fund flows. For example, a simplification of a header account structure may work for one channel, but not necessarily the rest until everyone is on the same page.

Still a balancing act. At the end of the day, fund flows out of China must take into account the key performance indicators (KPIs) that all channel arbiters (banks, regulators, government authorities) have to balance incentives to bring foreign investment in with a demonstrated ability that profits earned can be taken out—at some point—while maintaining control of RMB and USD balance of payments at each level.