On Tuesday, 21st March IACT's Women in Treasury Pillar held a roundtable at Kellogg's Head Office to discuss the various risks facing Treasurers. This roundtable comprised senior treasury leaders including Smurfit Kappa, Jazz Pharmaceutical, Xerox, Kellogg and others.

The first risk considered by the group was **Counterparty risk**. In light of recent bank failures including SVB and Credit Suisse, the group said there is a strong focus on liquidity and counterparty risk within their respective companies. Treasury teams are dealing with large volumes of bank accounts, and bank counterparties, which can pose an operational challenge for cash management. There were examples given of discovering bank accounts opened within the business without Treasury's knowledge and inheriting bank relationships through M&A activity. Treasury policies should set out bank limits and give Treasury sole responsibility for opening and closing bank accounts.

Bank credit ratings and CDS are used to proactively monitor the credit worthiness of banks and will inform where funds are place, although it was noted these often lag prevailing conditions. Additionally, participants rely on regular conversations with their banking relationship teams and peers.

Bank account sweeps are a valuable tool both for liquidity and in managing counterparty risk where accounts are required in certain countries or with non-core banks.

Participants have been utilising money market funds to ensure ready access to cash for working capital purposes and to give diversification. On the funding side, it was noted that the current market volatility is having an impact on issuing commercial paper and tenors have tightened in to overnight bringing **funding risk**. The group discussed the need to manage the relationships within an RCF to ensure the other banks will step up if one of the banks in the facility fails and in terms of managing expectations around ancillary business to have confidence the facility commitment will be renewed.

Risk of **fraud** is another byproduct of the recent banking crisis. Treasurers were concerned that their businesses could be targeted by criminals purporting to be Suppliers updating their SSIs. The importance of verifying any new instructions through a call back etc. and to reinforce the correct procedures within the company was discussed.

Different approaches on **FX management** were noted. Some companies delegate responsibility for FX identification to the operating companies with execution undertaken centrally, whereas others managed FX risk centrally within the treasury team. A common challenge was getting the buy in of the business in managing and identifying currency risk. Often the FX policy will stipulate how currency risk should be managed, including procurement contracts, posting of gains & losses etc., but affiliates will adhere to it to different degrees. The group agreed regular education and training sessions were a critical tool in helping the business understand the value of hedging and what is needed from them. Sometimes framing in terms of EPS will help translate the Treasury view. It is always useful to have a CFO who will reinforce the policy, but Treasury needs to stay connected to the business to understand the commercial flows. The risks of human error and poor quality of information were called out. This led the conversation to the importance of automation and technology in the management of FX risk. Some companies have linked their ERP and TMS to a dealing platform which in turn returns details of the executed trades for posting. Various operational challenges of Central Bank rates and accounting rates were also discussed.

Rotations within Treasury and allowing rotations from the business were generally encouraged by attendees to promote cross training and a broader understanding of Treasury. However, some participants noted teams were thinly resourced which left little time to build capabilities at an analyst/manager level. The current difficulty in filling Treasury positions was called out as a significant **operational risk**.