KPMG

Treasury 2025

What needs to be done now already

Corporate Treasury

2025 still seems to be long way off. If you think back, though, how the world has evolved as far as technology is concerned in the last 10 years, you will likely do a double take. And if you then think of the increase in speed with which change is happening, you will quickly realize that we will be in for a hair-raising trip in the ten years to come. Treasury Management also has to start anticipating changes instead of chasing developments in the company and its markets. Indeed, Treasury, being responsible for managing cash flows and financial risk, plays an essential and across-the-board role in a company. This was also highlighted, among others, in the "Position Paper for the Definition of Treasury" issued in June 2017 by the Association of German Treasurers. So it is time to step up to bat and assume responsibility by making the right decisions now to best contribute to the company's future success.

Speaking of which, let's quickly look back on how Treasury Management operated ten years ago. Ten years ago, i.e. in 2007, Treasury was much more decentralized. Group companies were able to act much more independently, as Treasury at headquarters often lacked the necessary transparency to exert any meaningful influence. Data was neither collected to be centrally analyzed nor were any measures taken at Group level. Instead, each group company with Treasury activities independently drew conclusions and defined measures in most areas. The main reasons for this was that it was technically difficult to integrate the group companies into the central Treasury department.
So from a technical vantage point, Treasury these days looks starkly different. Especially treasury systems endowed with a comprehensive set of functions have turned into integrating platforms that use apps available in the market to perform special tasks. So today, for many Treasuries central data storage is quite real rather than a future vision, or at least it is for the most important Treasury processes. It is also clear that this path leads to a further integration of treasury data and the use of this data for decision-finding processes, for instance for risk management purposes.

So what are the reasons that force Treasury to stay ahead of the game already now in order to be ready for 2025? External influences (for instance, due to geopolitical power shifts or terrorism, economical shifts, such as Brexit) change market access, something that is especially important for financial markets. Shortened product cycles and transformed business models, the sale or acquisition

of business areas all influence internal processes - also in regard to financing and risk management. But is any of this new? No. All of the above has been bandied about for some time now and it is clear that Treasury must have the right tools to mitigate or handle these aspects and must be able to use these tools flexibly. So what are these tools and what can be done already today? This article wants to elucidate this by picking out the following four aspects:

- Automation of standard processes
- Digitalization of decision-finding processes
- Embedded compliance
- Performance as a quality indicator

Currently, Treasuries are discussing many new technologies. First implementations, such as the issuance of promissory notes using Blockchain technology have already appeared. However, it is not yet clear which technology will be widely accepted and how it will be used by Treasury. Despite this uncertainty, it is already clear now that the right activities should be initiated today to properly position Treasury for the challenges that lie ahead. What these activities are will be discussed below.

Automation of standard processes

The terms most seen in this regard are "straight-through processing", "management by exception" and autonomous systems or "smart contracts". Just think of the processes of FX exposures/liquidity planning, bank statement processing or the release of OCI during hedge accounting. There are many other examples. These processes involve a media switch (e.g. the manual export of portfolio lists in order to prepare a report), manual adjustments (e.g. data conversions) and account adjustments, all of which are part of the daily business of many treasury departments – and this to no mean degree! Such work blocks resources (in the form of staff and expertise) that could be used elsewhere, such as with the implementation of new technologies and the preparation of financial strategies. We think that with the advent of Treasury 2025 many of these processes will be completely automated, that exceptions will be handled according to pre-defined processes and that freed-up staff will be able to dedicate time to more strategic tasks. But in order to be ready for this, the fundamentals have to be defined already now. One of the ways is to identify the areas that take up many resources by analyzing processes and methods, and to eliminate these one by one. This will only happen through the standardization of processes and the elimination of exception-to-policy cases.

Digitalization of decision-finding processes

Everyone is talking about the real-time connectivity of relevant information, system-based decision-finding processes based on comprehensive data and self-learning systems. For instance, if we look at FX management, there are already now corporations that have parametrized rule-based decision-making to define hedging transactions. Exception-to-policy cases, such as the hedging of dividends in foreign currencies or the financing of a project, remain complex and still require manually prepared analyses. However, in order to prepare for system-based decisions also for such complex transactions in Treasury 2025, care has to be taken that complete, system-based exposures are available in real time and that clear rules for given specifics have been defined. Exception-to-policy decisions will be replaced with a system consisting of simulations and scenario-based decision-making, which will also increase reliability for a consistent implementation.

Increased efficiency, the proper allocation of resources and improved decision-making reliability will be the biggest enhancements of the aspects presented above – but with this, we will still be far off from the end of our journey to Treasury 2025. Stay tuned and be sure to take a look at our next newsletter with the second part of this article, "Treasury 2025 – What needs to be done already now".

KPMG

MiFID II: The clock is ticking! (Un)certainty regarding the implementation at corporates

Corporate Treasury

The new EU financial market regulation MiFID II will enter into force in less than six months.[1] Unlike with the previous MiFID, which was only indirectly relevant to Corporate treasuries, these may now also be directly affected by the so-called "secondary activities exemption" as of 3 January 2018.

Transactions in goods and commodities in the spotlight

A fundamental change for non-banks arises from the fact that, in the future, all trading activities with commodity derivatives as well as emission certificates (including derivatives thereof) would fall within the scope of MiFID II and, as a consequence, be subject to authorization. It is essential to understand that trading activity means any transaction involving one of the above products – regardless of whether they are traded on an exchange or OTC. As a result of these amendments, corporates will be widely affected by MiFID II – contrary to securities companies, where a trading book is still required in order to be subject to its regulations.

However, in order not to impose a licensing procedure (including capital requirements) on corporates using commodity derivatives in their ordinary course of business or which engage only in a very limited amount of proprietary trading, MiFID II provides for the so-called secondary activity exemption. Accordingly, companies falling within the scope of application must notify their national supervisory authority – e.g.in Germany, BaFin – of such a secondary activity.

MiFID II does not further specify the notification itself, which is why it is expected that national supervisory authorities will issue implementing ordinances. However, it already seems clear that there will be only a short form without accompanying documentation. The latter then needs to be submitted to the national regulator only upon request. In the future, the regulator needs to be notified within the first quarter of a calendar year. However, the first notification is subject to a rather hard to understand deviation. According to ESMA Q&A, a notification must already be made by 3 January 2018. In view of the fact that the rule still needs to be implemented and that the observation period will always be made up of the past three years, this could be quite challenging.

Whether a secondary activity is present has to be determined in a multi-stage test defined in the MiFID II as well as in the Regulatory Technical Standard 20. In the so-called **market size test**, a company must first set its own non-privileged trading activity in relation to the overall market. Transactions which have been concluded successfully and demonstrably for risk hedging are considered to be privileged and are therefore not taken into account. In principle, companies can make use of the already existing processes of the European Market Infrastructure Regulation (EMIR); however, they need to remember that MiFID II does not only apply to OTC contracts. This means that at least all transactions concluded at trading venues must also be included.

The overall market size as a denominator in the market size test is still a particular challenge for numerous goods. This has to be specified as an exogenous variable by the regulator or the trading venues, respectively. As the directive requires that all derivatives – including contracts concluded bilaterally without the use of a trading venue – must be taken into account, many of the requirements still undefined. Only on 6 July, ESMA published an opinion how the market size of individual categories of commodities have to be determined, which may serve as a first guide.

As a second step, a test must be carried out relating to the group's main activity. Two methods are available:

i. ***Trade-related test:*** This puts the company's own non-privileged trading activity in relation to the group's total trading activity (including privileged transactions).
ii. ***Capital-based test:*** 15% of each net exposures and 3% of the gross exposures (in each case multiplied by the price of the commodity derivative, the emission certificate or the derivatives thereof) held by a company are compared with the capital employed for the Group's main activity. The latter corresponds to the sum of the Group's assets less its current liabilities as set out in the Group's consolidated financial statements.

All of the tests must be based on the previous three years.

For companies that do not allow speculative trading in commodity derivatives or emission certificates, the question arises to what extent they could forego a calculation. The regulation itself does not make a clear statement on this topic; however, it seems at least possible to forego a complex calculation. This would probably be the case if the numerator would always amount to zero. Even if such a course is chosen, companies are nevertheless advised to prepare a comprehensive qualitative documentation demonstrating the privileged status of all transactions in case of a potential request by the national regulator.

As a conclusion, all companies (even those with only a small amount of trading in commodity derivatives and emission certificates, including derivatives thereof) will have to take action on 3 January 2018. On the one hand, the time remaining for implementing the test calculations is running out, and on the other hand, there are still many uncertainties that often arise from current market trends and industry practices.

The third trading venue

A further amendment to the MiFID II deals with the expansion of the EU trading facilities to so-called organized trading facilities (OTF). In addition to the regulated market and the multilateral trading facility (MTF), this puts a further trading venue within the scope of the regulation.

An OTF is characterized as a multilateral system, on which a multitude of supply and demand meet, but which is not a regulated market or an MTF. A key distinguishing feature here is that, unlike on an MTF, supply and demand is matched in a discretionary way. The information provided by the BaFin, among others, currently suggests that contrary to the fears of many corporates, trading platforms such as FXall or 360T are not deemed OTFs because they are not multilateral in both directions because only the company in question acts as a buyer.

The amendment of the MiFID II on this point can lead to changes in the scope of application of both EMIR and the Market Abuse Regulation (MAR), both of which refer to MiFID II's definition of trading venues. Since there will be no generally available list of OTFs (unlike regulated markets and MTFs), a final definition may crystallize only in the course of time as the interaction of users and platform operators develop.

KPMG

The SWIFT Customer Security Program

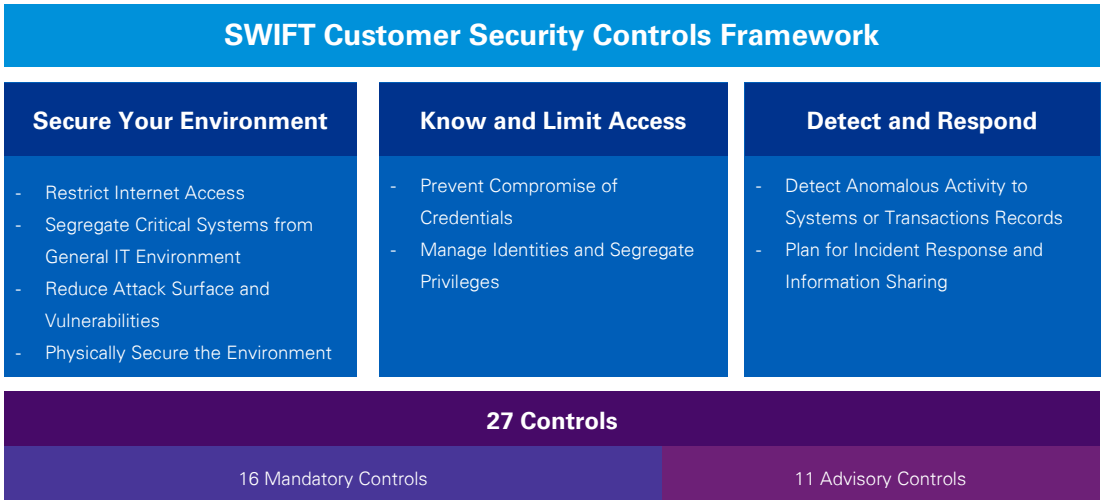
An initiative to prevent security risk in payment transactions

Corporate Treasury

SWIFT, mainly known for its network used for the standardized exchange of messages and transactions between affiliated financial institutions and companies, now also offers a multitude of products for handling payment transactions to thousands of industrial customers worldwide. In recent years, however, SWIFT has also registered increased attacks by hackers on the infrastructure of its users in recent years. The central bank of Bangladesh is the most prominent example with a loss of USD 81 million (originally, a multi-billion loss was rumored). Turkish Akbank and Ecuadorian Banco Del Austro also suffered damages to the tune of millions. There have also been other incidents that were never publicized for fear of a loss of reputation.

In response to the increasing attacks on the local SWIFT infrastructure of its customers, SWIFT has now launched its Customer Security Program (CSP). The aim of this initiative, already presented at the Sibos conference at the end of 2016 and published in April 2017, is to support SWIFT users in combating payment fraud. On the one hand, the program aims at providing more security on the customer side with technical improvements and introducing an appropriate audit framework. On the other hand, the information exchange within the SWIFT community is to be expanded.

The CSP's core component is the Customer Security Controls Framework shown in the diagram. The framework formulates a total of 27 controls consisting of 3 main objectives – "Secure Your Environment", "Know and Limit Access" and "Detect and Respond" – and 8 security principles. Of these controls, 16 are mandatory for all SWIFT users, whether they are financial service providers or corporates. Users are encouraged to make use of the 11 additional controls as well. For users who use SWIFT Service Bureaus or receive access via their system manufacturer instead of using a local SWIFT infrastructure will be subject to a slightly abbreviated version with 11 binding and 9 optional controls. Such controls include, for instance, IT security measures, access policies, software integrity measures or training concepts. The SWIFT security controls are based on international security standards such as those issued by the National Institute of Standards and Technology (NIST), the Payment Card Industry Data Security Standard (PCI DSS) and the ISO / IEC 27002 standard for information security control mechanisms.



To ensure compliance with the framework, SWIFT has developed an attestation and compliance process. In a first step, SWIFT expects all users, regardless of whether they are connected directly (for example through Alliance Lite2) or indirectly (e.g. through a SWIFT Service Bureau), to carry out an initial self-assessment regarding compliance with the controls. All users must communicate these results to SWIFT by the end of 2017 at the latest. The CSP will then formally enter into force on 1 January 2018; all SWIFT participants will have to reconfirm their conformity with the requirements on an annual basis. Swift will reserve the right to inform the authorities and/or the user's business partners if the user does not reconfirm or fulfill the requirements. A user can reconfirm in three different ways: self-attestation, self-inspection through an internal audit or inspection by a third-party (e.g. by an external auditor, such as KPMG). Regardless of the choice of the verification method, SWIFT will check the compliance of the controls with internal and external audits on a sample basis. In addition, participants can make available their own CSP data to selected business partners via the SWIFT network, using a dedicated process for the approval or request of CSP data, thus promoting their reputation. This increases the transparency within the SWIFT network and allows users to make risk-oriented decisions regarding the choice of their counterparties.

Due to the complexity of these CSP controls, we recommend starting to implement the new requirements earlier rather than later/already now. A good way to start is by clarifying important strategic questions, covering all aspects, from the usefulness of implementing the optional controls to the choice and conceptualization of the appropriate reconfirmation procedure, to the evaluation of the publication option within the network.

The initial assessment is also a good moment to analyze your existing security structures and any identified gaps relating to the CSP. A next step should be the application of appropriate measures to eliminate the gaps in comparison to the framework's requirements before communicating the assessment's results to SWIFT as the last step. it is essential to establish an adequate process to monitor compliance with the controls for the annual reconfirmation, especially if you choose to do it with a self-assessment.

The challenges surrounding SWIFT CSP should therefore be seen as an opportunity to think about a comprehensive security solution for payment operations that goes beyond implementing the CSP and includes processes and governance as well as the IT infrastructure outside SWIFT. And this is exactly what SWIFT CSP aims to achieve: increased security.