The importance of specialised standard software for MAD/MAR compliance.

Experience and insights from three years of practical use.

Finding the whole in the detail and vice versa./Satellite/Waterarea, place unknown.

MAR II/MAD – The EU Market Abuse Regulation has created a uniform legal framework and catalogue of criminal law for the prohibition of market manipulation and insider trading since 2016. Moreover, financial institutions have been obliged to take active and proactive measures in order to avoid these criminal offences in their own backyard. The amendments pose significant challenges for the financial industry, especially the banking sector, and their IT systems. Traditional methods for monitoring securities compliance are no longer effective here – therefore, new procedures have to be implemented. Almost three years later, it is time to take stock of the success of MAD/MAR and of the current market developments.

The burst of the real estate bubble in the USA resulted in a rapid increase of the interest for interbank financial loans and in a strong decline of the trust in the financial world and its players. The crisis peaked when the major US bank Lehman Brothers crashed in September 2008, entailing enormous economic and reputational damage which probably has not been repaired to this day. The consequences were not limited to the US, but soon reached Europe as well. In the aftermath of the crisis, it was revealed that there had been faulty risk assessment regarding complex financial products, countless violations of rules of conduct and criminal offences in the area of market and benchmark manipulation. Since the public had become increasingly critical of the financial industry, numerous rules were adopted or tightened on a national and international level in order to guarantee the financial sector's more effective operation in the future.

FIRST MEASURES

Long before the financial crisis of 2008, measures had been taken on a national and international level in order to avoid market abuse and manipulation, albeit in a comparatively limited framework. The Council of the European Community, for instance, published a directive for the coordination of provisions regarding insider trading as early as 1989. It is quite surprising that insider trading had not been prohibited in some member countries of the EC at that time.

Like in many other industries, the attitude towards ethically questionable methods has changed considerably in the financial sector.

In 2003, the EU published the directive 2003/6/EC on insider dealing and market manipulation (market abuse), the first big step towards a strict and uniform EU-wide regulation.

Germany took a first crucial step by publishing the MaH (Minimum Requirements for the Conduct of Trading Activities of Banks). In 2005, MaComp (Minimum Requirements for Compliance) and MaRisk (Minimum Requirements for Risk Management), which are, among others, based on MiFID (Markets in Financial Instruments Directive), WpHG (Securities Supervision Act) and KWG (Credit System Act), set new standards which would soon be applied to union-wide regulations.

In 2007, the Austrian Financial Market Authority (FMA) published the Standard Compliance Code, which significantly extended former provisions regarding insider trading and the regulation of employee transactions and which took measures against market abuse.

The obvious approach to avoid regulatory arbitrage was to create a uniform legal framework within the EU in order to eliminate discrepancies resulting from the respective national law.

FIRST STEPS TOWARDS AUTOMATED MONITORING

The entry into force of tightened provisions regarding securities compliance did not only lead to organisational changes within banks, but also to corresponding adjustments of the IT systems. Partly, these new regulations were paid little attention in the beginning. The new requirements were met with limited resources and an accordingly low level of automated support. Extensions of the IT systems were usually minimum solutions; Excel sheets and manually generated additional records were and partly still are common practice.

For example, restricted lists were kept manually and confidentiality areas were defined on a purely organisational basis. Therefore, the new rules hardly manifested themselves in the affected IT systems. There was no talk of automatic monitoring of affected restricted list items, not to mention a targeted check with IT support in combination with confidentiality areas.

Another interesting topic is the check of large orders, which is hardly conceivable without IT support due to its complexity. Here, data providers and IT system developers were faced with big challenges. How are large orders defined? Who provides information on daily trading volumes for individual instruments and for every exchange? For which period does the average trading volume have to be calculated and which percentage of the average exchange transaction represents a large order? Do the checks only have to consider individual transactions or several transactions within one securities account or even transactions of one person who has several securities accounts?

The processing systems needed to provide corresponding functionalities for all of these issues while the interfaces had to be enhanced in accordance with the market and the affected surrounding systems had to be adjusted. The first step was to extend existing systems using a monolithic approach which was often applied at that time. The limitations encountered during the implementation were partly of a technical nature, the lack of resources led to solutions which were not very sophisticated and did not apply to multiple areas.

WHICH REQUIREMENTS DOES MAD IMPOSE?

Since the directive against market abuse entered into force in 2003, the financial world has undergone significant changes to which MAD II/MAR reacted. Basically, the triggers for these changes were the same as in MiFID II: new financial instruments with a high level of complexity, technological developments, actors who operate across markets and new trading centres outside established exchanges were major keywords.

The EU's new directives were a reaction to the increasing diversity of trading systems in use and financial instruments with growing complexity. Apart from the directives' extended validity, the vehemence in the fight against market manipulation and insider trading is remarkable. With a certain gravity, both of these acts become criminal offences, which are punished according to a EU-wide minimum standard that also includes several years of imprisonment. The fine can amount to at least the triple amount of the profit gained by the abuse or a minimum of 15% of the company's revenue. The sentence of detention for insider trading and market manipulation can be up to five years. Tight regulations for monitoring employees and their compliance with laws are adopted for companies which operate in the financial market.

As mentioned at the beginning, the directive's extension is not only limited to the penalty range but also concerns the scope and the provisions' validity.

It includes the monitoring of OTC transactions as well as multilateral and organised trading facilities (MTFs and OTFs) which are increasingly used. Additionally, these issues are dealt with across markets, trading centres and products („cross-market", „cross-venue" and „cross-product").

The regulatory authorities are heavily focusing on financial instruments which depend on other instruments. Especially the combination of retaining a leverage product and manipulating the underlying instruments can produce significant advantages even with „small" manipulative steps which hardly arouse suspicion.

Moreover, not only transactions which were actually settled on the market are to be checked, but also transactions that were not carried out, since any attempt of manipulation, instigation or complicity constitutes a criminal offence.

This poses a difficult challenge for compliance officers in a financial institution. With the implementation of MAD II/MAR, the rules for securities compliance, which used to be comparatively basic, have become a highly complex undertaking which is not only difficult to represent in terms of organisation and IT, but which can also entail grave legal consequences.

WHAT DO THE NEW REQUIREMENTS OF MAD II/MAR MEAN FOR THE IT?

The monitoring and reporting of suspicious transactions and orders, also known under the abbreviation STOR (suspicious transaction and order report), is one of the elements of MAD II/MAR which would be most suitable for full automation via software. Transactions and orders are to be checked from diverse perspectives. It should be noted that the number of suspicious transactions found by the system should not exceed a quantity that is manageable. It is a fact that an automated screening is able to find suspicious transactions; nevertheless in most cases, the responsibility to classify the transaction as suspicious resides with the compliance employee in charge. If suspicious cases are reported automatically to the regulatory authority without prior assessment, this may constitute the same risk factor as not reporting actual suspicions.

Tools for checking money laundering transactions, fraud suspicions, embargos or sanctions have become a standard, especially in the area of payment transaction processing. The IT landscape is even more heterogeneous in the area of capital market transactions. Until now, only transactions which were actually settled and their relation to participating individuals (defined, for instance, through affiliations to confidentiality areas, restricted lists etc.) have been checked according to the old regulations. This issue can be solved in a comparatively simple manner by using a data pool and a fully automated evaluation of said pool.

MAD II/MAR now requires transactions/orders to be considered in connection with other transactions/orders and it requires the identification of conspicuities from these insights. This calls for a significantly different approach for which the „simple" search for combinations of instruments and persons will not suffice. Instead, a transaction needs to be evaluated in the context of numerous other transactions, frequently according to „soft" criteria such as „unusual volume".

The use of automated monitoring is a clear requirement in the regulations. However, the question which level of automation is intended and which procedures are to be used remains. The following overview outlines the spectrum of requirements for a corresponding software solution.

The new functional requirements include among others:

DIRECTORS' DEALINGS

This applies not only to manager transactions themselves; transactions of persons in close relationships (e.g. spouses) need to be monitored as well.

TRANSACTIONS WHICH SEND MISLEADING SIGNALS TO THE MARKET, E.G.

Transactions without a change of economic property.

Orders which are placed without the intention to actually settle them, e.g. by setting unrealistic limits or cancelling them instantly.

Transactions performed at reference times which can lead to significantly different fixed prices and which are reversed after calculating the price.

TRANSACTIONS WHICH ARE ONLY CARRIED OUT DUE TO UNDISCLOSED (INSIDER) INFORMATION

Unusual concentration of transactions in certain instruments, e.g. before announcing an ad hoc report, before a reorganisation or an annual general meeting.

Unusual concentration of transactions in instruments which are related through an employee of a confidentially area or through a key account manager who is in contact with insiders or has access to insider information.

Sudden, unusual concentration of transactions in instruments with low market volume.

Transactions regarding ad hoc reports.

The range of possible suspicious cases can be continued indefinitely. Overall, MAD/MAR can be divided into a high double-digit number of rule categories which must be noted and monitored. Each of these categories can contain numerous queries which must be applied or data constellations which are to be checked. Furthermore, the individual rules must not be considered in isolation – a combination of conspicuities can lead to a suspected case, which once again increases the complexity of the rules to be observed.

Existing processing systems can only partly be extended by the new requirements as they are designed for the mere processing of transactions and not so much for the subsequent checking of orders and transactions which have already been performed. Other analytical activities cannot be integrated into such systems in a reasonable way due to technical reasons such as a transaction-oriented database design.

Therefore, it seems obvious to use an independent compliance software with analytical capabilities. In terms of the functional scope and the methods which the software uses to search for suspicious transactions, we are convinced that an analysis of the potential market manipulation scenario which can be expected realistically should be performed first.

An extreme example is the ban of benchmark manipulation, which clearly aims at the activities associated with the Libor scandal. Now, the question arises in which institutions a manipulation of this kind might be possible at all. As a matter of fact, the manipulation of large benchmarks, Blue Chip prices etc. is only possible if extremely high amounts of capital are invested. Therefore, only a small minority of market participants would even be capable of this form of manipulation. For many institutions, this risk is merely of an academic nature. In fact, there have not been any more spectacular cases in this respect after the „big" scandals about the Libor and the introduction of MAD/MAR. One might accredit this to the deterring effects of the new legal situation, but it might also be possible that benchmark manipulation is seen as an exotic offence which may now be subject to time-consuming checks even though there is not actually a large number of attempts in this regard.

Other procedures, such as the manipulation of securities with low turnovers and prices or the slight manipulation of underlying instruments to make profit with leverage products, are also possible with little capital and sometimes other methods, which is why they can be observed much more frequently.

After a risk assessment, it can be decided which level of expenditure is reasonable and which method should be used to search for a solution. Obviously, the result for an institution concentrating heavily on own-account trading or investment banking will be different than for an institution dealing with conservative retail transactions.

Systems which use technologies and methods from the area of fraud detection (e.g. adaptive systems or algorithms for pattern recognition) provide an interesting perspective for organisations with business activities which have a high risk of manipulation and insider trading. However, even several years after the implementation of MAD/MAR, such systems are still not uncontroversial. Particularly the question of traceability and liability for mistakes has led to the fact that adaptive systems are still being used for supporting traditional systems and processes rather than for independent analyses.

Small and medium-sized financial institutions are therefore often well-advised to stick to a rule-based solution. If the user can parameterise the validation rules himself, the expenditure spent in a company's daily operation is low and the resulting benefits are high. Moreover, a suitable and clean controlling organisation can be presented to the supervisory authority. The ability to describe to an auditor in a fast and clear manner which controlling mechanisms are currently implemented and what exactly they are searching for is an advantage not to be underestimated. Of course, a system must therefore not hide these rules in a black box, but must disclose them to the technically adept observer (even without knowledge of a programming language).

Depending on the business model and the organisation of a financial institution, meeting non-functional requirements such as multi-client institution capability, different operation models etc. plays a vital role.

A basic requirement for the compliance software is audit compliance. Different user profiles for organisations with divided labour, journal logging for all activities as well as the representation and monitoring of historical data are indispensable.

Apart from these considerations, a crucial aspect arises after some time and experience with the new compliance rules: the cost factor. A software solution for ensuring securities compliance does not only have to filter suspected cases, it must also deliver as few so-called false positives (i.e. cases wrongly classified as infringement) as possible and guide the user efficiently through the remaining cases.

Good user experience with overview dialogs is therefore essential. The software must be designed in a way that allows the user to see all suspected cases immediately and in a reliable manner and that guarantees timely processing. Based on its customers' feedback, SDS has tremendously improved its software in the latest releases in this area, including a revised and redesigned web interface. At first glance, this may look like a gimmick, but it can actually do much more: The processing times and hence the compliance costs can be reduced significantly through this optimisation without the need to compromise on the quality of analyses, quite the opposite: Based on user experience in the field of MAD/MAR, we have been able to put the final touches to our software in order to make it simpler and clearer for the users to recognise and track the crucial cases. Not only can the costs for compliance be reduced by focussing on the critical cases, but also, higher-quality controlling mechanisms can be implemented.

SUMMARY

The Market Abuse Regulation put the IT of involved financial institutions under close scrutiny. Master data systems had to be adjusted, operative systems extended by detailed data and validation systems developed or acquired. Even if no completely established control system was required for the introduction of MAD/MAR, proven and adjusted systems which can reliably detect market abuse must be presented now. On the other hand, the number of false positives must stay within reason and the preparation of information must take place in a manner which ensures that the operational costs and risks remain minimal.

With the product SDS CCONFORM, SDS offers a rule-based solution for monitoring securities and derivative transactions with the following advantages:

Highly automatised processes

Automated analyses and checks, ex-ante and ex-post, online, via batch etc.

Data import and maintenance via interface, manual enrichment possible

Integrated workflow with extensive exception handling

Integrated case management:

- Documentation of the entire life cycle
- Traceability via history and consistent journal logging

Predefined template rules

- Selection and definition of individual rule sets
- Simple adjustment of template rules to individual requirements

Easy to use, fast and easy to parameterise

Sophisticated multi-client institution capability, can easily be integrated into standard environments

Conformity to typical industry standards in terms of access control, traceability, data security, operation of data processing centres etc.

JOACHIM BOBIK

Product Manager
Mobil: +43 676 88 241 5480
E-Mail: joachim.bobik@sds.at

Working with SDS

SDS is continuously setting digital standards in financial market operations, regulations and compliance solutions for the international financial industry. The comprehensive SDS portfolio covers state of the future products and services for all customer and market related processes, ranging from global securities and derivate processing, regulatory, tax and compliance automation, solution-based consulting, professional testing services to managed services.

More than 3,000 financial institutions worldwide with over 10,000 users in about 80+ countries trust in SDS and its sustainable business values. With our proven industry experience of over 4 decades, we have become a highly trusted and equally reliable partner of renowned financial institutions all over the world. SDS is Member of Deutsche Telekom, one of the world's leading providers of information and communications technology. www.sds.

SDS

Software Daten Service Gesellschaft m.b.H.
T-Center, Rennweg 97-99
1030 Wien, Österreich
E-Mail: marketing@sds.at
www.sds.at