

## How to ensure that the markets are futureproof?

Association of Futures Markets, 9<sup>th</sup> of October 2024

By: Hanzo van Beusekom, member of the Executive Board at Autoriteit Financiële Markten

Dear attendees good to see you all,

AFM meets AFM... Interesting! Although of course we wear different hats. Your mandate is to promote and encourage the establishment of new derivate markets, while 'my' AFM- as a conduct regulator- pays attention to ensure that the markets – old and new – operate in a fair and orderly manner.

I know that not all of you are based in Europe, but I hope you will forgive me for focusing primarily European markets. After all, the AFM is the Dutch Authority for Financial Markets.

I have been asked to look into the future. Challenging. After all, it is notoriously difficult to make predictions, especially regarding the future.

In many ways the future is already here: anyone who visits our headquarters at the Vijzelgracht in Amsterdam will see data-analysts, IT-specialists and an entire AI-team. Nowadays technology and technological developments are key. Not only to capital markets participants, but also to those tasked with supervising these markets.

And this technology is constantly evolving. The development of IT, the development of cloud-based exchanges and clearing services is truly an international game.

International finance and financial infrastructure are very much connected.

- We are in the same boat across Europe and the global capital markets,
- We are confronted with the same challenges and
- We must look for solutions together.

In fact, if you see the financial sector a computer system, we are connected to each other as circuit boards in a large financial server. And in this financial server we still depend on each other. Problems within one part of the computer system are likely to roll through. An IT-outage or cyberattack in the one country or on one financial institution potentially will impact many others.

For us, it is crystal clear. We really need to work closely together to mitigate technological and other risks in the of the financial markets. Only together we can we strive for a level playing field and ensure the markets are future-proof.

## **The legislation is tech-neutral. (But not all the risks have been addressed by legislation)**

Many laws and regulations have been introduced to address risks. Let's have a look at MiFID. The important point: MiFID was written "tech-neutral". This to prevent the regulation constantly needing to follow the latest in tech-innovation.

Cloud-based computing is one of those changes which has grown during the past decade.

We must not forget that although open outcry has almost disappeared as did most tangible trading floors, risks related to financial markets have not gone away. They just manifest in a different form.

Where, for instance, business continuity planning previously was access to physical computers, backups, and building, nowadays it involves ensuring uninterrupted access to a digital trading environment.

## **You can outsource parts of the operation, but not the associated responsibility.**

In practice, cloud-based solutions are a form of outsourcing of the IT infrastructure (hardware and/or software) to a third party.

This third party provides a flexible and scalable IT infrastructure solution which can easily be adjusted upon – in your case – the trading venues or clearing service provider's request. This means more computing power, storage capacity, and more flexibility.

When it comes to the outsourcing of critical processes, we note that, at least in Europe, there is already a regulatory framework in place which is to be considered by financial market participants.

MiFID and subsequently in MiFID II with more detail, provide a broad outline in terms of requirements and expectations with respect to the outsourcing process as well as the monitoring and control of processes and services that have been outsourced.

For authorized financial market participants, the emphasis should be on being in control of services and processes that have been outsourced to a third party. The entity that is authorized to operate a trading venue or provide clearing services ultimately bears responsibility for the services that they provide also in case related business processes have partially been outsourced to a third party. This responsibility can never be outsourced!

## **Work together to innovate. Within the legal framework and with an eye for the risks.**

Our expectations regarding cloud-based exchanges and clearing services are no different from any other form of outsourcing of critical business processes of financial market participants.

In that sense regulation is technology neutral. As market supervisor we try to look through the technological innovation to assess to what extent the financial market participant meets the applicable regulatory requirements. We ask ourselves whether the fair and orderly functioning

of the capital markets is at (higher) risk if the proposed technological innovation is be implemented.

As a relatively new industry, cloud service providers should take responsibility to identify and make transparent how risks involved with cloud-based solutions are effectively mitigated.

This includes transparency regarding the operation of data centers in terms of robustness and resilience, but also regarding risk management and corporate governance. Keep in mind that by hosting and servicing critical financial markets, cloud service providers have become an integral part of the capital markets landscape.

### **Be aware of changes to the regulatory environment, adjust services accordingly.**

As some of you all know, mid-January DORA will come into effect. DORA includes detailed requirements in relation to the outsourcing of critical IT-services. DORA will be applicable to EU financial market participants and as such to all third-party IT service providers which provide services to those financial market participants.

Thanks to DORA, regulators gain more insight into the concentration of cloud services. The register of information helps us to map all third parties to whom ICT services are outsourced. In addition, it helps us to identify the critical third-party providers (CTPP) where the greatest concentration risks occur. DORA offers parties as ESMA, EBA, EIOPA the opportunity to monitor these critical service providers. For these critical service providers, it is important that sufficient measures are taken to guarantee the availability, integrity, and confidentiality of their ICT systems.

And to be well able to fulfill the needs of regulated entities such as trading venues and clearing service providers, cloud service providers themselves should have a thorough understanding of the regulatory framework and the relevant requirements that apply to financial market participants when it comes to outsourcing of IT-services.

This is where cloud service providers should stand out. By offering a compliant flexible and scalable IT-environment, by being transparent on the specific risks that their business is prone to and by sharing their mitigating actions.

### **Insufficient attention to risks from the industry on many occasions lead to a regulatory push back.**

Although regulation covers many risks financial market participants are facing, by no means it will addresses all the potential risks in your business. Market developments are often one step ahead of rules and regulations. And then, it is up to you, up to the industry to introduce best practices for services provided which are not already covered by the regulatory framework.

But I hope you realize that the moment will come that regulations will unfold. In many cases legislators take industry best practices as starting point when developing new regulations. By having already developed and implemented best practices, the potential gap with future legislation applicable to cloud-based services is likely to be minimized. Only together we can we strive for a level playing field and a truly integrated capital market and ensure the markets

are future-proof. We need to have open lines of communication between markets, governments, and regulators to keep moving forward together. One cannot do without the other.

As mentioned, most regulation is tech-neutral and as market supervisor we have an open mind when it comes to innovations. We do note however that those innovations should at a minimum meet the high standards that already apply.

This means that in case of outsourcing of IT-infrastructure the envisaged setup should have the same or higher standards in comparison with the existing situation. Financial market participants' desire to have a more efficient and possibly less expensive operation should not be at the expense of the robustness of the capital markets.

When it comes to cloud-based solutions we could imagine that certain risks will be mitigated when making use of such solution. One could think of the risk that a financial market participant would reach the limit of its technological capacity. A cloud-based solution could be a mitigating factor in the sense that it allows for the financial market participant to add extra system capacity relatively easily if the situation would ask for this.

Cloud based solutions in my view are by no means to be regarded as the holy grail. Apart from the risks involved with outsourcing of critical services, cloud-based solutions in itself might add risks. Given the rather limited number of cloud-based service providers, one could think of possible concentration risks that can arise in case multiple financial market participants would opt for a cloud-based solution from the same cloud service provider. This means that business-critical functionalities of multiple financial institutions are invested in one cloud provider. A disruption at such a provider will therefore affect all these institutions, which can cause significant damage.

At all times cloud-based exchanges and clearing service providers should have sufficient knowledge and skills to be able to monitor and control outsourced activities and to assess whether the service level is in line with expectations. Thereto the outsourcing entity needs to be fully aware of the risks involved with the outsourced activity and should the outsourcing entity be able to determine whether these risks have sufficiently been mitigated.

Digitalization of capital markets, market innovations and increased cross-border activity have significantly changed our capital markets. Change will be a constant.

We bear a shared responsibility to reduce operational and other risk in the capital markets. Often risks do not disappear after a technological innovation, they just take on a different form. When it comes to outsourcing of services to a third party, the emphasis for financial market participants should be being in control of relevant risks. The responsibility they bear can never be outsourced!

Cloud service providers could benefit from further developing their thinking by creating best practices on how to empower regulated clients from a risk control perspective.

Now you have a window of opportunity to show that you hold the safety and stability of the financial sector in high regard. Handle that well.

Be strict with yourself during this period. Think very carefully about the consequences for the sector, for society. And it certainly can't hurt to ask yourself the question 'what will the regulator think of this' :-).

And if you can't solve that problem yourself... Feel free to contact us. I can ensure you that our coffee is up to standards. But not only that. The fact is: if you want to innovate, dialogue with the regulator is important. We are in favor of sensible financial innovation: We're curious to learn about your innovations, we're open to discuss your dilemma's and for sure I would like to hear how you keep the risks under control.

Thank you for your attention.