ÖSTERREICHISCHE
FMA · FINANZMARKTAUFSICHT

Digitalisation in the Austrian Financial Market

Call for Input: Findings

April 2022

FMA

TABLE OF CONTENTS

The masculine form is used throughout this report to assist with the readability of the report. Such personal nouns should be considered as being gender-neutral. It should in particular be noted that all formulations relating to persons apply equally to women and men. The legal basis remains unaffected by this report. No rights and obligations extending over and above the provisions of the law can be derived from this document. Despite every care having been taken in the preparation and research of this report, the FMA is unable to assume any liability for the correctness and completeness of data and content contained in this report.

INTRODUCTION

The FMA's Analysis on Digitalisation in the Austrian Financial Market

Digital transformation is fundamentally changing the financial market's framework conditions, brining new opportunities, but also difficulties regarding legal interpretation and risks. In addition, supervisory tools are being placed under particular scrutiny. The FMA is therefore interested in remaining on the ball in relation to digitalisation and correctly appraising the drivers, trends and potential future developments. In 2021, we therefore again conducted our analysis on digitalisation in the Austrian financial market. Thanks to practically complete market coverage across almost all sectors of the financial market and a high level of involvement of supervised entities, we have been able to gain the latest insights about the current status of digitalisation as well as areas in which digital technologies are deployed in the Austrian financial market.

In order to initiate broader discussion and to intensify the dialogue regarding the implications of digitalisation, the FMA additionally invited stakeholders – the customers of supervised entities, the bodies representing their respective interests, sectoral associations as well as the interested public – to scrutinise the findings and conclusions contained in the Report on Digitalisation in the Austrian Financial Market critically and to submit their own experiences, perspectives and approaches for finding solutions.

Findings from the Call for Input

A broad range of stakeholders responded to this Call for Input and submitted statements in February 2022, in some cases of a very comprehensive nature, in response to the questions that the FMA had formulated as guidance at the end of every chapter in the report.

- The participating stakeholders generally also shared and supported the FMA's conclusions regarding the implications of digitalisation.
- Some opinions also contained supplementary remarks and additional practical examples (e.g. on data protection issues, about handling of liability for risks associated with digitalisation, and risks arising from a merely fleeting and unrecorded communication in pushing social media).
- Several stakeholders raised legal policy suggestions and proposals *de lege ferenda* (in this way it is proposed that care should be taken to ensure that underlying algorithms used in digitalisation are discrimination-free and that an analogue infrastructure shall be required to be maintained, so that there is no transformation of services towards exclusive digitalisation).

The FMA expresses its thanks for the comprehensive opinions received and will feed this valuable input into its strategic planning as well as defining its priorities for supervision.

I. STRATEGIES

In which areas do you expect disruptive developments in the medium- to long-term? What are the decisive opportunities and threats from digitalisation for the Austrian financial market? What are the success factors for exploiting digital transformation optimally for the further development of business models in the individual sectors within the financial market? What is the expectation regarding the role of the supervisor? These were a selection of the questions that the FMA asked in its Call for Input.

The participating stakeholders in the Call for Input by and large echoed the FMA's conclusions about the implications of digitalisation, while also adding the following views:

Overall, the impact of digitalisation on the financial market is to be considered to be positive. Digitalisation benefits innovations and supports financial market participants in understanding customers better, and also tailoring business models as well as products to the needs of their customers.

- From the stakeholders' perspectives the impact of digitalisation are not exclusively limited to increases in efficiency and cost savings. New competitors and new business models will force existing sectors to embrace **innovation and agility**. **Market shares will change completely** as a result of digital transformation.
- Digitalisation will have a particularly strong influence on **less advice-intensive products and services**: in particular in payment transactions it is reckoned that digitalisation will continue to cause a strong change in processes. Lending business involving smaller amounts are also increasingly being affected as well as transaction processes and securities business. It is expected that the customer and distribution areas will be conducted between the analogue and digital world. As a result new service areas will emerge, while old ones disappear. In this regard, it remains important that there is the possibility to make contact for such situations requiring advice.
- It is viewed critically IT departments are one of the principle drivers of transformation. There is a fear that **digitalisation is only advancing due to technology** and in so doing does not adequately reflect the requirements of the market.
- A proposal is made to focus on the opportunities arising from digitalisation, rather than primarily on the risks. This comes out of the perspective that **risk-averse companies encounter more difficulties in transformation** and are therefore more easily "conquered" by market participants from outside the sector or from abroad.
- **Employees** also feel the impact of digitalisation in the sense that skill requirements also change significantly. Increasing digitalisation would also have an impact in the form of successive reductions in staff numbers. One stakeholder expressed a desire for a more detailed examination of this aspect.

No disruption is expected within the next three years to supervised entities' core business. However they remain convinced that the changes observed over the next five years will be closer to disruption than evolution.

- Major changes have hitherto failed to materialise, or had **already** been adopted by the financial industry **as the state of the art.** "Creeping" change is therefore more probable: only the way in which (existing) projects are operated and offered will be further digitalised, in order to make them more accessible to the customer. The transformation of existing products into the digital era is considered to be a relevant challenge by several stakeholders.

- A further challenge results from the **increasing number of cooperations**, which lead to a stronger networking of financial market participants with one another, as well as with participants from outside the financial market. The emergence of ecosystems is seen as a given as a result of the increase in cooperations. Such cooperations might **prove disruptive** in that an established ecosystem could attract numerous customers, retain them, and therefore could completely change the market.
- While digitalisation is driven by the entry of new digital competitors, less disruptive developments are nevertheless expected due to their cooperative design. One stakeholder fears in this context that for many groups in the population, such rapid changes in technology occur **too quickly and with too little involvement for them.**
- In the medium- to long-term, **disruptive development** is anticipated in the areas of securities management, payment transactions, instant loans and embedded finance. A rapid and agile regulatory framework is also expected to bring about a profound change in the area of crypto assets, whose importance will continue to grow.
- Too a certain degree, it is felt that **complex regulations** in the Austrian market **impede disruptive developments**.

Barriers to digitalisation are not only observed in connection with regulation, but also with regard to the corporate culture and the IT landscape.

- The following aspects were raised regarding **regulatory impediments** for digitalisation:
  - the lack of homogeneity of regulation both at EU and national level (in this regard different rights, obligations and approaches are mentioned in the conclusion of various financial products or services);
  - many legal requirements relate to obsolete technologies (e.g. the Telecommunications Act (TKG; Telekommunikationsgesetz));
  - unharmonised national and international interfaces;
  - the trend towards the “know your customers principle” in regulation is viewed critically and from the perspective of several stakeholders should be a job for the authorities.
- The **organisation of an entity** (in this regard, an expert at management board level seems appropriate) and the **corporate culture** (here, it seems important that transformation is accompanied by change management and culture management) are also seen as significant hurdles to digitalisation.
- However, others consider the largest risk or barrier is that **trends** in relation to digitalisation **are not recognised (in time)**. “Best practices” that have been established over decades are also considered as impediments. Similarly, how renewal was handled in the past should not be used as a blueprint.
- Heavily fragmented and outdated **IT landscape** and key infrastructure are described as an impediment for digitalisation. Solutions and rules for corresponding adaptive interfaces and simplified possibilities for connection (e.g. APIs) are urged. It should also be possible to reach the customer simply and securely outside of the institution’s own application universe.
- **Customer behaviour** is not viewed as an impediment, but in more as a challenge. From a customer perspective **fraud cases** were addressed. Fraud methods are becoming ever more sophisticated and even vigilant consumers are increasingly unable to see through them. The consequences are still borne by the customers (e.g. for dubious or even fraudulent investment platforms).

Decisive factors for the success of digitalisation range from the ongoing adaptation of the corporate strategy, creating the necessary technological basis, through to ensuring sufficient know-how in the form of personnel resources.

- Successful transformation depends on the appreciation of the fact that corporate culture and organisational structures must adapt to the dynamic market environment (the **corporate strategy** vision and the accompanying implementation and continual adaptation). It is important to understand the elementary rather than mere passing importance of transformation. While it is necessary to transform traditional core business, innovation must also be used for the further development of the business model. This is viewed as being critical for protecting and expanding a company's market position.
- A **need to focus** also appears important, as decisive success factors often simultaneously represent bottleneck factors. Critical success factors should therefore be identified in order to then start digitalisation with precisely these.
- Once the strategy has been finalised, the corresponding technological basis should then also be formed. This also includes adapting the **IT infrastructure** or better usage of data. In this way, transactions can be simplified and advisory processes digitalised or optimised using AI. IT should focus on success factors in this area, instead of sticking to standard services.
- Ongoing development and the integration of good ideas (e.g. via cooperations with tech companies) is seen as helpful for successful digitalisation. It is crucial for success that sufficient **know-how** is available in terms of personnel **at the various managerial levels** for the challenges ahead. In this context, "generalists and visionaries" as well as including a "Chief Digital Officer" at management board level are considered important factors in the implementation.
- Suitably **qualified personnel** and continual training are also cited as decisive factors for success. In addition, the importance of **involving employees** as well as representatives of their interests is pointed out.

It is expected that the **new digital competitors** will push the incumbent entities towards ongoing further development. The increase in product and service diversity is viewed positively, but consideration should be given to groups of the population for whom technological changes may be occurring too rapidly.

- The implications of new digital competitors entering the financial market are viewed as positive, since
  - they assist incumbent entities to master digital transformation by means of cooperations;
  - doing so drives new developments while increasing the range of products and services of market participants.
- Rapid changes in technology occurring too quickly and with too little participation for many groups of the population are viewed negatively.
- New market participants often lack the necessary technical and legal expertise and experience. **Regulatory issues** – which pose major challenges even for BigTechs – are also seen as a barrier to market entry for new digital competitors. Consequently, new competitors look for **individual business areas** that are easier to "get up to speed with" from a technical and regulatory point of view.

New market participants and incumbent market players are not only competitors, but frequently mutually complement one another through cooperation. Substantial increases are being observed in such cooperations.

- FinTech/InsurTech sector start-ups known as “digital competitors” are primarily viewed as **cooperation partners** for established market participants.
  - Many new players look to cooperate with established players, to be able to profit from their access to the market.
  - Established entities look for partnerships with new players to profit from their innovative strength.
- The downside of cooperative relationships is that any efficiency, price or expense benefits are not passed onto consumers.
- Non-industry companies (especially "BigTechs") taking over start-ups to enter the market are seen as **competitors**. Companies that have already secured a share in financial services, e.g. Alphabet/Google, should be mentioned here.
- The following business areas are mentioned as ones in which new players could play a significant role within the next three years: payment services, instant loans, securities transactions/advice in certain segments, debit and credit card business, crypto asset managers, microcredits and cash loans.
  - Credit institutions as a whole are not seen as being threatened; however, they are exposed to a multitude of smaller, specialised new market participants. Especially smaller credit institutions set up as universal banks with a broad range of services are therefore face particular challenges.
  - It is also neglected that insurance companies are threatened with competition from within their own company, as re-insurers are among the main financiers of the start-up scene and have established many cooperations with FinTechs/InsurTechs.

The transformation during the process of digitalisation should be accompanied by the supervisor from the perspective of the stakeholders. The supervisor’s role in particular is seen as ensuring a level playing field. In this context, on the one hand the timely clarification of the regulatory framework is important in order to ensure the necessary stability. On the other hand, it is essential that the FMA acts in an agile manner and on a cross-sector basis.

Expectations regarding the role of the supervisor affect several areas:

- The supervisors should ensure a **level playing field**. In so doing, it would be important
  - to have a holistic overview of the **entire financial market** and to ensure a level playing field for all market participants,
  - that the supervisor anticipates **new interdependencies** in the risk view,
  - that the FMA actively accompanies **harmonisation within the EU**, in particular addressing unharmonised national and international interfaces and "open insurance" in order to prevent the existing uncontrolled growth from continuing in Europe,
  - to also create equal opportunities in Europe in purchasing and using digital tools (e.g. software, cloud solutions); for example, data protection is regulated differently in detail.
- The importance of the timely **clarification of the regulatory framework** is highlighted in order to avoid too much development in undefined directions. Accordingly, necessary stability in the form of consistent interpretation over a longer period of time should at least be created in the regulatory area, for what is an inherently volatile environment.

- Transformation during the course of digitalisation also requires supervisory authorities to **act in a more agile and iterative manner.**
  - The supervisor should strive for **dialogue with social partners** with regard to the far-reaching structural change in the banking sector, especially regarding the development of sustainable business models. Collective consumer protection should be performed in an active and comprehensive manner, and attention also paid to the overall resilience of entities with regard to digitalisation.
  - Binding regulations would be required about **liability issues** in human-machine communication or in the usage of decision-making algorithms. The FMA should pay greater attention to the issue of delineation regarding liability issues in the future.
  - One of the central issues should be the impact of the Austrian financial market's digital transformation on **financial market stability**.
- Finally, it is important to ensure the supervisory authority's own further development or **building up its own digital competence** to be able to keep pace with the rapid development, and to attach a greater role to the structure and qualification of the employees. With regard to the increasing number of social engineering attacks, there should be a stronger push regarding raising awareness and sensitivity.

II. PRODUCT DESIGN

What impediments make the development of new digital financial products more difficult? Do you share the FMA's assessment about the opportunities and threats associated with their impact on banking or insurance business? What specific positive and negative developments regarding "digital" financial products can be observed from your perspective? What duties should the FMA perform in relation to the protection of investors, insured persons and creditors with regard to "digital" financial products? These were a few of the questions that the FMA asked in its Call for Input.

The participating stakeholders by and large confirm the FMA's estimation about the effects of digitalisation on the product landscape as well as adding the following remarks:

A consensus essentially exists about there being no current need for further regulatory requirements. It is important unequal treatment does not stand in the way of fair competition and a level playing field for all market participants.

- Existing regulations should be **harmonised** and **simplified** instead of expanding regulatory requirements.
- Formal requirements that **cannot be performed digitally** and which prevent processes in customer service from being carried out digitally from end-to-end, are viewed as being problematic, for example:
  - handwritten signatures being required for a signature specimen sheet,
  - the fact that only the customer themselves are able to provide certain information that is require to be in handwritten form (e.g. tax self-disclosure), thereby forcing the continuing existence of physical processes, in turn preventing such processes from being carried out digitally.
- It is important that the regulatory framework is transposed **into national law** in all essential areas, to avoid having to contest minor amendments every time at EBA level.
- Another aspect is the **unequal treatment** between credit institutions and FinTechs. The PSD 2 RTS is cited as a specific example. PSD 2 placed a strict obligation on credit institutions to implement strong customer authentication (SCA) by 14.09.2019. Immediately after that date, the supervisory authority conducted inspections at credit institutions to ensure correct implementation. In contrast, other financial service providers in the e-commerce and card sectors were granted extensions and transition periods. This led, from the user's point of view, to credit institutions falling behind considerably in terms of user-friendliness. Therefore, in the future, greater attention should be paid to the equal regulation of all market participants for similar transactions.
- One stakeholder demands that digital processes and algorithms should be given separate treatment as "audit material".

Impediments to digitalisation are considered not only to exist due to the regulatory environment, but also as a result of the partially fragmented and out-of-date IT environment, and its acceptance by customers:

- The regulatory impediments to digitalisation include existing regulations that are no longer up to date, such as
  - requirements that individual authorised signatories must provide original signatures on printed specimen signature sheets,
  - the fact that the conclusion of digital products cannot be completed "seamlessly", "without media discontinuity" and without delays,

- the difficulty of implementing the General Data Protection Regulation (GDPR) in practice and the fact that data protection in Austria is very narrowly defined compared to the frameworks of European competitors,
- the compulsion to implement ever stricter risk avoidance approaches, which restrict the possibilities for developing new digital financial products,
- the lack of regulatory parity with large providers such as Google and Amazon (e.g. in terms of anti-money laundering regulations and ZaDiG).

- The partly old and sluggish core infrastructure and **IT infrastructure** of capital and financial market as a whole continues to be seen as an impediment to digitalisation. In this case, solutions and specifications for corresponding adaptive interfaces and simplified connection options (APIs) are needed.
- Another impediment is seen in the existing customer structure or **customer acceptance**, since considerable numbers of customers still want direct on-site customer support. Such hurdles should be overcome by a simple design and low complexity. A standardised, simplified and legally secure procedure for customer verification could assist in this instance.

Increasing transparency of products and better customer service are perceived especially as positive developments. Cost savings are also frequently mentioned.

- The **increasing transparency and simplicity** of products as well as innovations that provide the customer with **better service** and increase "consumer convenience" (keyword "around the clock") are highlighted positively.
- Increased use of digitalisation also enables faster adjustments to the business model and a broader range of products.
- Process automation leads to **cost savings**; outsourcings, which can be used through more intensive cooperation with third-party providers, also limit costs. A new/larger offer also leads to a better cost ratio.
- An increase in the level of innovation and exchanging of ideas can be observed.

The mere “digitalisation” of existing products as well as modular products in conjunction with “advice-free” products continues to be considered in a negative light.

- Efforts to simply make existing products **“digital-only”** are considered in a negative light. Digital transformation should have a different appearance. Individual customer solutions and needs-oriented advice would be pushed back as a result.
- **Modular products** are also viewed critically, for which the total amount for all the selected components is ultimately significantly more expensive than existing products that cover all components. This is particularly to be viewed in a critical light **in relation to “advice-free” offerings**. Similar risks are also seen in the topic of "embedded insurance", insofar as useless or unneeded insurance or financial products are offered to the end customer in a non-transparent manner.
- The average consumer is also seen as a risk – due to their lack of financial education – since they need good advice, which should be supported.
- The need for increased IT security is accompanied by **increased IT costs**.
- Splitting the value chain entails risks, especially in the case of high **dependency on external service providers**.
- Personal contact with the customer and customer loyalty are reduced, resulting in entities becoming interchangeable.
- An increase in market participants (from other industries) is expected. The lack of regulatory level playing field is feared to place entities at a disadvantage.

- One stakeholder discusses the critical aspects of digitalised financial products cited by the FMA in detail (e.g. the risk that apparent correlations are created or parameters are used that are not entirely within the customer's control) and the question is raised about the real added value of technology-driven innovations for the customer.

Expectations regarding the role of the supervisor: while there are calls for the supervisor to perform the same tasks as for "analogue" financial products, others also welcome such , amendments to laws are also welcomed.

- On the one hand, the risks of digital products should be perceived, examined and, if necessary, objected to in the interest of **consumer protection**. Against this background, an almost complete digitalisation of business models should not also take place without taking into account the wishes and needs of many consumers. On the other hand, the risk of "financial exclusion" exists. Fraudulent activities in the financial market should continue to be pursued and prevented in a consequent manner, in order to provide comprehensive protection for consumers.
- A **level playing field** should however also be ensured – based on the principle of "same activity, same risk, same rules". The financial centre as a whole should thus be considered and suitable framework conditions created in this regard. **Legal certainty** and a stable foundation are also seen to be imperative.
- A supervisory framework in the sense of an **iterative and agile** approach is requested, which adequately reflects the various speeds of development of the financial market.
- There is a general **need for discourse**.
  - The principle should be "the same price for the same risks". In particular, in the case of insurance companies, it is quite possible, in addition to a risk-appropriate, fair and affordable "base price", that a discount should be justified and possible for those who actively live more risk-consciously and actively avoiding risks.
  - It is also noted that the market should not always be required to address every under every eventuality. Possibly, the state should also be called upon to bear any "super risks" that may exist, or to collectively distribute such risks across the population as a whole.
  - Analogous to internal models reviews, review processes should also exist in relation to digitalisation to ensure that discriminatory and/or decision parameters are not used that infringe in data protection terms. Technical standards should be drawn up, for example, for robo advice that should be reviewed on an ex ante basis as well as ad hoc ex post audits.
  - The supervisor's pioneering role with regard to the discourse on ethical boundaries is viewed as somewhat questionable. This should be primarily be politics' and society's role. The supervisor should only initiate and moderate necessary discussions in this regard.

III. DISTRIBUTION / CUSTOMER INTERFACE

What duties should the FMA perform with regard to the protection of investors, insured persons and creditors in relation to the digitalisation of the interfaces to the customers? Do impediments exist in Austria that hinder digital communications? What specific positive as well as negative developments regarding "digital" distribution can be observed from your perspective? These were a few of the questions that the FMA asked in the Call for Input.

The stakeholders participating in the Call for Input supplemented the FMA's perspective with the following statements:

There is a generally unanimous feeling that **regulatory standards** do not yet reflect digital transformation adequately. Pleas are made for the advisory and conclusion process to be simpler and faster for all parties involved – taking place without media discontinuity and waiting times. Interaction with the customer should be allowed to correspond with standards that are technically possible nowadays. In the cases of automated processes, however, it must be ensured that the underlying parameters are transparent, comprehensible and non-discriminatory.

- **The same rules** are desired for both online and physical interfaces. This includes information and documentation requirements, as well as obligations for the prevention of money laundering and the checking and verification of identity when concluding a contract.
- With regard to digital communication, the importance of consumers' **freedom of choice** regarding the forms of communication is also emphasised. For example, it is considered positively in the insurance sector, for example, that electronic communications must be explicitly agreed to and arranged by means of a separate declaration. Customers should neither be de facto forced to use technology-based solutions, nor forced to for cost reasons. Consent being required must be presented transparently for customers, and not be allowed to negatively influence usability. Minimum standards and consent requirements are proposed for the implementation of the previous two points, which are geared towards implementability.
- In the cases of automated processes, it is necessary to ensure that underlying parameters are **transparent, comprehensible and non-discriminatory**. Specifically, for example, algorithms that are used in robo advice might constitute a "black box", with rules needed for their use. In this context, the following are mentioned: rights to receive information, the obligation to explain, the obligation to label, inspection and examination by experts, as well as rules and technical standards.
- Furthermore, the regulation of comparison portals and distribution platforms would also appear to make sense: it should be apparent to the customer about the relationship that exists between the operator and the product provider, about which fees and commissions are passed onto the operator and, for example, the criteria used for drawing up the ranking shown. Furthermore, there should also be rules for addressing conflicts of interest for comparison portals and distribution platforms.
- In addition to regulation, which could be an impediment to digital communication, the lack of nationwide **high-speed internet** is also highlighted. It is difficult to inform customers via all channels in a transparent and timely manner about the prescribed record-keeping obligations.

Greater interaction with customers is seen **positively** with regard to digital distribution. Communications can be maintained even in crisis situations. The acceptance of digital structures has also increased significantly.

Complex offerings without any form of advice as well as modular products, for which the total cost of all components is ultimately significantly more expensive when selected than for existing products covering all components, are viewed **negatively**.

The **expectations of the supervisor** are complex and cover the following suggestions:

- The product landscape is becoming more uneven as a result of digitalisation. Consequently, there is an **increased demand for advice**. The selling of financial services without advice might have the consequence of an overly hasty and ill-considered purchase being made. In any case, scepticism prevails about complex offerings without any form of advice. There is a risk of a wrong choice being made.
- The promotion of **social media** is also viewed critically, doing so carries the risk of communication of a fleeting and incomprehensible nature. There are fears about network marketing, in which the structured sales principle could lead to mass losses, as illustrated by past investment scandals. This is another reason why comprehensive and competent advice by qualified staff members is essential in the financial sector.
- It is also proposed that where **algorithms** are used that they should be submitted to the supervisor, to be able to evaluate the observance of conduct rules and that they are non-discriminatory. After all, investors are barely able to assess and evaluate the quality of robo advice programmes as well as their underlying parameters.
- The **maintaining of banking secrecy and data protection requirements** poses a particular challenge for all interfaces and should be subject to special inspections by the supervisor. The same rules should apply for the digital interfaces to the customer as for offline interfaces. This also applies for information and documentation obligations as well as the “know your customer process”.
- It is warned that clear rules don’t exist regarding the eID and that adequate standards don’t exist (such as in the case of ich.app vs ID Austria). Furthermore, video identity verification shows technical weaknesses and a lack of customer acceptance. Bank-Ident procedures were not able to be used by banks. Foto-ID procedures have still not been approved. Regarding digital signatures, acceptance of the digital signature for the land register (Grundbuch) is also seen as an urgent necessity.
- The supervisor should contribute towards a **harmonised level playing field in the EU**, e.g. in relation to video-based identification. The continuing lack of a level playing field is viewed critically in particular in relation to the disclosure obligations that apply to online banks.
- The regulation of **comparison portals** appears sensible. It should be apparent to the customer about the relationship that exists between the operator and the product provider, which fees and commissions are passed onto the operator and the criteria used for drawing up the ranking shown. With regard to the ranking of products, it is also stated that it is not possible to guarantee the independence of digital distribution platforms. Furthermore, there should also be rules for addressing conflicts of interest for comparison portals and distribution platforms.

IV. ASSET MANAGEMENT

From your perspective, what duties should the FMA perform with regard to digitalisation in asset management? What impediments exist to automate the asset management processes and to facilitate the extension of alternative technologies like AI, deep learning and machine learning? During the consultation, the following input was received about these issues:

The **advantages** of digitalisation in the field of asset management are considered in relation to the potential to reduce costs and in increasing efficiency as well as in reducing operational risks. Automation is however also associated with various **disadvantages**: the possibility for manual intervention must remain. Furthermore, it would be dangerous if a provider with a significant market share were able to transfer capital investments by means of an automatic trigger, and thereby would be able to influence the market. Furthermore, some stakeholders view the investment trend towards crypto investments negatively.

A lack of know-how and the prevailing data landscape were identified as an impediment for automation.

- It is considered **positive** that many product solutions (e.g. robo advisors) already exist that can make fully automated investment decisions.
  - It has proven useful that complex advisory processes and the associated regulatory requirements can be processed in a quick and simple manner. Digitalisation also helps to combat manual data manipulation as the principle source of errors.
  - Perception of AI systems for more targeted research and the development of blockchain technology is also positive.
  - Although automated processes are considered beneficial, manual intervention must also be possible. In this regard, a stakeholder advises about the use of machine learning in a specific use case: underlying market allocations are calculated so that allocation decisions are not supported by traditional fundamental analysis, but by means of quantitative analysis using machine learning. However their implementation in specific transaction decisions explicitly remains the responsibility of the fund manager.
- **Impediments** for automating asset management processes are considered to be due to:
  - a lack of know-how in individual entities and lack of a standardised training and education programme in the banking sector,
  - the prevailing data landscape (data is often held in a large number of different systems, and is often not “cleansed” and “consolidated”; a broad data basis and history are however essential for data science techniques; furthermore no legal guidelines exist that cover the accessing and processing of data).

The **expectations for supervision** also cover various issues in this area:

- The suggestion is made that **automated** and often risk-based **asset management** ("Robo Advisory" or "WealthTech") should be addressed separately and explicitly in the digitalisation study. This is justified by the fact there are already over 100 providers throughout Europe, a few of which have assets under management of more than EUR 1 billion. While this is useful in terms of cost efficiency and convenience, on the other hand this may be dangerous if a provider obtains a significant market share and transfers capital investments (ETFs, shares) on a large scale due to an automatic trigger, thereby strongly influencing the market.

- There is also the opinion that the supervisory authority should play the role of an **auditing instance** of digital and automated processes (e.g. RPA), especially in the mid- and back-office departments.
  - Regulatory measures for dealing with automated order processes are also considered necessary.
  - An institutional framework for the overarching control and monitoring of artificial intelligence in Austria should monitor compliance with rules, measures and the distribution of competencies (AI governance).
  - There should be regulatory requirements in the area of control and monitoring of **data providers**, in the case that they fall under the supervision of the FMA.
- In addition, the supervisory authority should be an ad-hoc **provider of information** on current developments and a **sparring partner** for a national dialogue on the topic of digitalisation.
- The promotion of **education and training** in the area of digitalisation is desired, as users need IT understanding in dealing with alternative technologies.

V. IT INFRASTRUCTURE

What duties should the FMA perform in relation to the IT systems used in the Austrian financial market? What specific regulatory standards are necessary in relation to the use of IT systems in the financial sector? What positive and negative aspects exist for IT security in relation to the increasing concentration of the financial market towards only a small number of IT providers? Are the material advantages and potential disadvantages of agile approaches duly captured? What specific positive as well as negative developments regarding IT systems in individual sectors can be observed?

During the consultation the following input was received about these issues in particular:

The financial market's increasing **concentration on a small number of IT providers** is both advantageous and disadvantageous:

- A positive aspect is that widespread use could raise the level of IT security in the application and thus also among users. In addition it results in a **reduction in costs** as well as a **simplification of the cooperation**. Furthermore more staff and money could be invested into IT security centres than would be possible in the case of a decentralised structure in smaller units.
- The disadvantage, however, is that centralised systems or providers are a considerably more attractive target for potential attackers, and therefore the probability of an attack also rises. In the event that a compromise and outages occur, the consequence would be a large number of customers being impacted and thus, under certain circumstances, also **far-reaching systemic effects** on entities in the financial sector. Where several financial services providers are affected, then the coordination of a harmonised reaction is both complex and difficult. The reduced possibility for controlling large service providers is also viewed disadvantageously.

With regard to **IT systems**, as well as positive developments, increases in cyber risks and concentration risks have also been observed. Financial market participants should be aware of these risks.

- There is strong growth in the **trend towards agile development**. The uses of agile methods brings many simplifications, but also some risks. In addition, this also intensified by cloud services and the associated networking of applications. As a consequence the risk for overall functionality increases. However, in many areas, the deployment of agile methods is only possible to a limited extent. Due to open banking platforms becoming more widespread, agile methods are increasingly able to be used, and therefore demonstrate their strengths and benefits.
- **Cyber risks** are increasing. Measures taken in entities should therefore be reviewed and adapted.
- The focus on a few large providers leads to **concentration risks** often not being recognised as such and therefore not treated accordingly. Large providers often only offer full functionality of their products when they are operated in their cloud. This is usually associated with concessions in the technical implementation of the network connection and little readiness for special requests.
- The **modernisation of IT systems** towards open banking platforms is a gradual process; the replacement of existing systems is sometimes delayed. Due to the complexity and size of existing systems, this causes enormous costs and takes several years. An investment backlog therefore builds up.

Regarding the **role of the regulator and the supervisor,** the following comments were made with regard to this area:

- The supervisory authority should **certify** the conformity of IT systems with the Austrian legal basis. An analysis and evaluation of IT systems should therefore be carried out regarding their suitability for use in the financial market, as well as a listing of IT systems that are suitable for use in the financial market. The aspects used for the evaluation of IT systems (encryption, logging, IT security, user administration, historisation, ...) should be included in regulatory requirements. An increasingly detailed audit of IT systems/processes should therefore take place.
- **Increasing awareness** in entities is also considered important with regard to the audit security of the systems. The supervisor should monitor this both theoretically (documentation reviews) as well as practically (on-site inspection). Banks in particular should be made aware of the risks of global value creation chains.
- The topic of **Business Continuity Management** (BCM) is also highlighted. In this regard, minimum BCM requirements are desired from the supervisory authority.
- Nowadays, IT systems are largely redundantly designed – but this is not the case for the **staff** who are supposed to operate these systems due to cost pressure and the limited availability of competent employees. Therefore, it is desirable to increase awareness in the relevant ministries for corresponding initiatives.
- Specific regulatory guidelines in the form of **requirements for the minimum staffing of IT departments** would be welcome. In addition, they would like to see Europe-wide regulation/limitation in the area of concentration risks by large IT service providers..

VI. IT INTERDEPENDIENCIES

What duties should the FMA perform in relation to the interdependencies between supervised entities and IT service providers? In which form should such tasks be undertaken? What specific regulatory standards are still necessary in relation to the interdependencies in the Austrian financial market? What positive and negative developments can be observed in individual sectors regarding interdependency with IT service providers?

The stakeholders add the following input to the aspects mentioned in the Digitalisation Study:

With regard to the increasing interdependency with IT service providers, it is considered important that the FMA keeps track of the interdependencies and where concentrations of critical services exist that critical service providers are monitored regarding their business continuity.

- The following developments are viewed **positively**:
  - The fact that IT service providers come from a common sector is seen positively, as there is then the advantage that security guidelines can be demanded and implemented in a coordinated manner.
  - The active exchange of information is also seen positively.
  - The increased use of innovative standard software from the market instead of in-house developments and outsourcing of "standard services" is also beneficial.
- In contrast, the increasing risk (e.g. cyber fraud) as well as the increasing effort to meet regulatory requirements is viewed **negatively**.
- One stakeholder notes that it is not yet clear whether a homogeneous landscape and a market concentration in IT systems make the goal of uniform interfaces easier or more difficult.

The **expectation of the supervisor** also covers various remarks in this area:

- It is suggested to **update the service provider list** with regard to an overview of important service providers and sub-service providers.
- The FMA should also take over the **coordination of pooled audits** or inspections of service providers by supervised entities. Ín this context, the acceptance of the outcomes of pooled audits at least as a basis for the individual audits to be carried out by the supervised entities is essential.
- The FMA should also maintain an **overview of the interdependencies** from the outsourcing and re-outsourcing reported by the supervised entities. In the case of concentrations of critical services for the financial market, these service providers should be monitored with regard to their business continuity.
- In addition to the importance of having an overall view of interdependencies, the standardisation of certifications is also mentioned as a task that should be performed by the supervisory authority. In connection with regulatory requirements, the creation of transparency with regard to interconnections and dependencies is desired, as well as the prevention of monopolies. It is also noted that due to the spread of ecosystems, the increase in interconnectedness of IT systems will also be cross-sectoral. This raises the question of **cross-sectoral** (IT) **regulation** and supervision.
- The current regulatory requirements are considered to be largely sufficient. A **specification** of the requirements for dealing with widespread service providers (e.g. MS 365, AWS, Azure as well as A1, Drei as suppliers of data connections) is considered desirable.

VII. DIGITAL TECHNOLOGIES

Based on your personal experiences or your estimation should other digital technologies or opportunities for deployment be considered in the observation of the implications of digitalisation on the Austrian financial market? What lack of legal clarity are associated with the deployment of new technologies from your perspective? Do you share the FMA's opinion in relation to the opportunities and threats of the individual technologies? Which additional material risks could also be relevant from your perspective for the individual sectors in the future? What is your expectation with regard to the role of the supervisor in the individual sectors of the financial market?

The participating stakeholders in the Call for Input by and large echo the FMA's conclusions about the implications of digitalisation, while also adding the following views:

By and large, the assessment of the opportunities and risks of the individual technologies is shared, and supplemented with a few comments.

The pressure of global players on the financial market as well as potential concentrations among individual cloud service providers are viewed as additional material risks.

- Great potential is seen in the better use of one's own data with **Big Data**. In many areas, data quality must meet regulatory requirements down to the level of individual data records. Therefore, no statistically significant data quality problems should occur in Big Data.
- A few stakeholders felt that **robotics** is unsuitable for process automation in the long term.
  - It should only be used where service interfaces are not possible, meaning that robotics should only be seen as an intermediate step towards service integration. Instead, service-oriented integrations beyond entity boundaries should be strived for.
  - Application APIs can also be addressed using robotics, in order to access data. This provides some assistance regarding the complexity of access.
- In the field of **machine learning**, the subcategory of Decision Intelligence in particular could be highlighted. It is also noted that machine learning and the problem surrounding black box effects might lead to explanation problems or false bias.
- **Open source software** is apparently safer than dedicated software and should (be allowed to) be treated and used accordingly.
- One stakeholder sees increased opportunities for deploying new technologies, especially in the area of compliance (keyword "know your transaction").
- It is also noted that the "ethically problematic conclusions" mentioned by the FMA in the digitalisation study could be dealt with in greater detail, as these are presumably not yet widely present among market participants.
- The inherent **technical risk** (processes without the involvement of/review by a human being) is also added as a material risk.
- The **pressure created by global players** in the financial market (i.e. global tech giants like Google, Apple, Amazon) is described as another material risk: If they were to expand their services, there would be a risk that their presence would cut into banks' business lines.
- Potential **concentrations** among individual cloud service providers, which increase the concentration risk, are mentioned as an additional risk.

Legal uncertainties in connection with new digital technologies relate primarily to cloud services and outsourcing.

The **expectations of the supervisor** in this respect are also primarily directed at the harmonisation of regulatory framework conditions.

- **Equal regulatory conditions** should exist for all market participants (banks, FinTechs, BigTechs). Currently, banks in particular are subject to very strong regulation, whereas BigTechs are hardly covered. Moreover, the expectation of the supervisory authorities is for the supervisory authority to generally act in a **technology-neutral manner** with regard to the essential regulatory objectives, but also to take into account the specificities of the respective service (and type of service provision).
- **Using cloud services** is associated with relinquishing complete control over data. Large providers would stipulate legal arrangements without any possibility of adjustments. This is already associated with extremely high regulatory costs (outsourcing). In parallel, the conditions resulting from the GDPR and the problematic links to America (Schrems ruling) create additional major hurdles. Greater clarity is needed on these aspects.
- Legal uncertainty is also seen in the areas of **machine learning** and **big data**: a risk of discriminatory processes exists in this area. Digitalisation will only be able to create added value if designed and regulated without discrimination.
- Greater clarity regarding the **use of crypto technologies** is also desirable. Supervision should ensure a legal framework for digital currencies.
- Frequent **changes in product design**, the type of communication and term (e.g. digital products with "on" and "off" mode) make many contractual or civil law changes necessary. In addition, there would be a risk of liability risks being presented detrimentally towards consumers.
- It is emphasised that the supervisory authority should be equipped with sufficient resources to be able to take an active role in the digital transformation of the Austrian financial market.

VIII. CYBER RISKS

Using which measures or initiatives might be FMA be specifically able to contribute to increasing cyber security in the financial market? Which cyber threat scenarios could be particularly relevant in the future for the Austrian financial market? Which core areas of IT security should be strengthened by undertakings in the Austrian financial markets as a priority? Should further measures be deployed by undertakings to defend against cyber attacks in the future? From your perspective is there a balanced level of threats between the different sectors of the financial market, or are some areas particularly highly exposed? What lack of legal clarity, opportunities and threats do you see in relation to cyber insurance? These were a few of the questions that the FMA asked in its Call for Input.

The participating stakeholders in the Call for Input by and large echoed the FMA's conclusions regarding cyber risks, while also adding the following views:

Hacking attacks on sensitive data are recognised as particularly relevant **cyber threat scenarios** for the Austrian financial market. Other threats include: cyber fraud, attacks on electronic payment systems, attacks via the supply chain, attacks on supply chains, attacks on end consumers, state-motivated attacks, attacks using "artificial intelligence", follow-up attacks during the course of a blackout, brute force attacks and exposed and hitherto unknown vulnerabilities (along the same lines as Log4J).

Cyber attacks as a result of social engineering are being observed more frequently: in the case of retail depositors a higher increase in cases of fraud (investment fraud, sale/purchase fraud, identity theft, phishing, debit card fraud, theft of digital wallets, credit fraud, threats and coercion as well as call bots). In this process, technical security measures do not need to be circumvented by the hackers, as the financial services customer has been instrumentalised.

- In general, the skill set required for cyber attacks is decreasing and the **quality of the attacks is increasing**. Better language proficiency and well-crafted fake pages convey a reassuringly seductive correctness. At the same time, the complexity of digitalisation is increasing so that it is no longer comprehensible for individuals. The threat increases with the nature and scope of data processed as well as the transactions and potential impact. The broader the financial service is set up, the greater the threat. The online offerings of banking institutions and the possibility to initiate payments quickly are obvious targets for phishing attacks.
- The area of **user awareness should be strengthened as a priority** to improve IT security. In addition to all technical measures regarding internet security, awareness training for staff members is also an important factor. Furthermore, greater priority should be placed on actual cyber resilience across all departments of entities. IT security is not exclusively dependent on technical parameters. Cyber attacks instead also require smooth interaction between technical departments, corporate communications and the legal department.
- In addition, greater consideration should be given to information security in IT procurement. The establishment of systems for rapid reaction and prevention (e.g. SIEM-SOC) is also mentioned.
- In any case, entities should take **additional measures in the future to defend themselves** against cyber attacks.
  - In addition to various exercises and technical tests, the availability of the necessary quantitative and qualitative resources as well as trained processes in the event of an emergency should also be considered. Activities for testing and improving technical and organisational security measures in terms of scope, timeliness and effectiveness should be intensified.
  - It is also important to call for a comparable level to in-house security from service providers and subcontractors to ensure that no security vulnerabilities arise.

The following comments were made with regard to cyber risks in relation to **expectations in terms of supervision**:

- The FMA should consider an **exchange of information and experience** – in particular in relation to DORA. Consideration of initiatives for determining whether basic competences should be required in **education and training**. In the case of outsourcing and cooperation, the problem exists that service providers are still encountering high security requirements.
- Nevertheless, existing regulatory requirements are by and large considered to be adequate. They should be used to create **better transparency** for the management bodies by **making the maturity level more quantifiable**. The overall maturity assessment should not hide general weaknesses in some critical areas.
- For uniform transparency and to improve cyber security, the FMA could initiate some kind of "**FMA FinCoop Ready**" certification or self-certification based on the known legal and regulatory requirements for financial service providers.
- Inspections should take place with specific focuses with regard to the current threat situation, and also include **active attack simulations**.
- Establishing **Finanz-CERT** (a computer emergency response team for the financial sector), which has been considered several times, would be welcomed.
- Regarding the difficulty of reviewing cyber security measures, it is suggested to at least prescribe **general principles for proper data processing**, and then to check on a case-by-case basis whether and how these are adhered to.
- One stakeholder notes that this topic should only be regulated jointly with other affected areas and ideally also at a higher level in the EU.

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
API	Application Programming Interface
BCM	Business Continuity Management
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
e.g.	for example
etc.	et cetera
ETF	Exchange Traded Fund
EU	European Union
GDPR	General Data Protection Regulation
PSD	Payment Services Directive
RPA	Robotic Process Automation
RTS	Regulatory Technical Standards
SIEM	Security Information and Event Management
SOC	Security Operations Center
ZaDiG	(Austrian) Payment Services Act