ÖSTERREICHISCHE
FMA · FINANZMARKTAUFSICHT

DIGITALISATION IN THE AUSTRIAN FINANCIAL MARKET 2021

TABLE OF CONTENTS

INTRODUCTION

Digital transformation is changing the framework in the financial market, creating new issues about legal interpretation and risks for supervised entities while also putting existing supervisory tools to the test.

In 2021, the Austrian Financial Market Authority (FMA) is therefore continuing its analysis on digitalisation in the Austrian financial market. This report serves as a preliminary stock take, which specifically depicts the current status of digitalisation of the Austrian financial market and areas in which digital technologies are deployed. Furthermore, we also want provide an assessment in a concise form about drivers, trends and potential future developments. By doing so, we hope to create a sound basis for us, the FMA, to remain on the ball with regard to digitalisation, and to be able to correctly assess developments.

Risks represent the FMA's focus of attention in so doing. This report therefore examines digitalisation in the Austrian financial market predominantly from a risk-based perspective. In so doing we adhere strictly to the principle of technological neutrality: the FMA does not supervise any technologies, but instead primarily focuses on risks. Equal risks require equally high supervisory requirements, irrespective of whether they arise from digital or analogue business models or processes. The underlying study behind this report assists the FMA in being able to assess the risks of digitalisation in an appropriate and timely manner.

We conducted a comprehensive data collection exercise in the Austrian financial market as a basis for this report, in order to obtain new insights into opportunities, trends and risks associated with digitalisation. We received responses from supervised entities from all[1] market sectors during the summer of 2021. In almost all sectors of the financial market, we were also able to achieve near 100% market coverage:

Participants by sector:

- 32 insurance undertakings (IUs)[2]
- 8 Pensionskassen (PKs)
- 8 Occupational provision funds (OPFs)
- 49 (explicit) or 440 (implicit) credit institutions (CIs)
- 6 payment institutions (PIs)

[1] *Due to the low number of participants from the sectors for market infrastructures and virtual asset providers, the results from both of these sectors have not been included in this report, in order to prevent conclusions being drawn about individual undertakings.*
[2] *Insurance undertakings falling under the Solvency II regime.*

- 79 Investment service providers and investment firms (IFs) - comprising 64 investment firms and 15 investment service providers
- 23 management companies (MCs) (investment management companies, real estate investment management companies, alternative investment fund managers (AIFMs)
- 2 virtual asset service providers (VASPs)
- 3 market infrastructures (MIs)

We believe that this very high market coverage has again allowed us, in 2021, to form the most comprehensive and most detailed basis of data and information that is currently available on the topic of digitalisation in the Austrian financial market.

CALL FOR INPUT

This report should also be used as a springboard for launching a broader discussion about digitalisation in the Austrian financial market and intensifying dialogue within the Austrian financial market about the implications of digitalisation in financial services. Your input is therefore particularly important.

We therefore invite you, our stakeholders – supervised entities, investors, savers, insurance policyholders and consumers, public sector institutions and the interested public – to critically scrutinize the findings and conclusions sketched in this report, and to enrich your own perspectives, experiences and approaches to solutions. Several questions have been formulated at the end of every chapter in this report to serve as guidance.
Input about the report may be sent informally by e-mail to digitalisierung@fma.gv.at. The closing date for submissions is 28.02.2022. We will be happy to include your input and consider it in the FMA's strategic planning or in determining priorities for supervision.

STRUCTURE OF THE REPORT

The report is broken down into the following parts:

- The **strategies** of the supervised entities in relation to digitalisation (Chapter 1),
- **new business models:** new ecosystems, new digitalisation-driven products, new customer interfaces and the deployment of digital technologies in individual business processes (Chapters 2 to 4),
- **new digital technologies:** proliferation of technologies used in the financial market, their associated opportunities and threats as well as practical examples (Chapter 7),
- **new risks:** changes in IT infrastructure and cyber risks (Chapters 5 to 11 excluding Chapter 7).

Based on research findings about international, European and national initiatives about digitalisation in the financial market and the results of the surveys conducted in individual sectors and based on other observations from ongoing supervision potential implications of digitalisation have been identified in the individual sectors for the FMA's supervisory activities, and potential courses of action for the FMA derived accordingly.

Note:

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.

EXECUTIVE SUMMARY

In summary, it was possible to glean the following material facts and trends from the study for the Austrian financial market:

1. **Strategies / Governance:** the need for external support in the ICT area in the form of advice, outsourcing and ad hoc assignments will increase; the delineation between the processes and services that are relevant to the core business and the procurement of other services (mere delegations) is becoming ever more complicated. IT skills are becoming more significant for key functions in addition their actual expert competences.

   The expectations of supervised entities with regard to BigTech and FinTech start-ups have changed since 2018: established financial market participants currently believe that the likelihood of BigTechs entering their markets is currently substantially less probable than was the case in 2018. In contrast, the significance of FinTech / InsurTech start-ups is increasing, which is not only expressed due to their increasingly being perceived as competitors, but also due to their intensified co-operation.
2. **Products / New Business Models:** the product landscape is adapting to the new digital opportunities. At the forefront are technology-driven innovations, in which traditional products and services are being migrated to new technologies. While new types of products have been launched since 2018 to an increasing extent, as a rule they are still only being launched on partial or experimental basis.
3. **Distribution:** supervised entities are increasingly conducting their direct contact to customers via digital channels (e.g. social media, chats, video conferences), especially in the pre-sales area. Conventional sales channels are increasingly losing their importance due to the use of digital distribution platforms, comparison portals and robo advice. A strong increase has been detected in particular in the usage of video conferencing and social media since 2018; the former has intensified because of the COVID-19 pandemic, while the latter has also increased due to among other reasons pressure from competition in relation to the acquisition of new customers.
4. **Technologies:** despite the increasing proliferation of crypto assets, supervised entities are currently barely investing in this segment. This applies both regarding their own assets, as well as for customer deposits. To date, blockchain technology has been unable to establish itself as a basis for new products or services due to outstanding regulatory issues. This might change in the medium-term, due to new legislation such as the Markets in Crypto-Assets Regulation (MiCA). The significance of cloud services has in any case increased since 2018.

5. **IT applications:** The trend is towards consolidated standardised software that can be deployed for as long as possible thanks to updates. As a result, the diversity of providers may fall in the long-term and a concentration may emerge with only several large software developers.
6. **Interconnectedness / ICT Security:** The degree of interconnectedness of the financial sector with service providers is increasing due to digitalisation. The IT risk of supervised entities is therefore increasingly shifting towards the interface to third parties (co-operation partners, IT service providers). However, at the same time the quality of proprietary IT security measures of supervised entities is increasing. This has also been shown by the Cyber and Cloud Maturity Level Assessments developed by the FMA, which for the first time permit a view into the cyber resilience of the Austrian financial market. With regard to the cyber threats that are constantly becoming more developed as well as the increasing digital demands of customers, ICT security requires constant adjustments of security measures.

The FMA conducts its digitalisation studies as the increasing use of new information and communication technologies as well as the knock-on changes in business models that they effect are of great significance for supervisory activities both in terms of the product landscape and in the interaction with customers.

From the results of this digitalisation study, is has been possible to identify the following particularly relevant thematic areas in relation to supervisory activities:

- external provision of ICT services, especially by way of outsourcing, and the associated risks,
- the identification of new channels of contagion and concentration risks,
- the interactions between supervised and unsupervised market participants as well as exact delineation of the scope of transaction requiring a licence especially in group structures,
- the requirements for management board members and key function holders when applying digital business models,
- the comparable safeguarding of customer interests for digital as well as traditional forms of distribution and communications,
- the monitoring of the further development of crypto assets as an instrument for investment, and
- the intensification of the monitoring of cyber risks and deriving suitable supervisory steps.

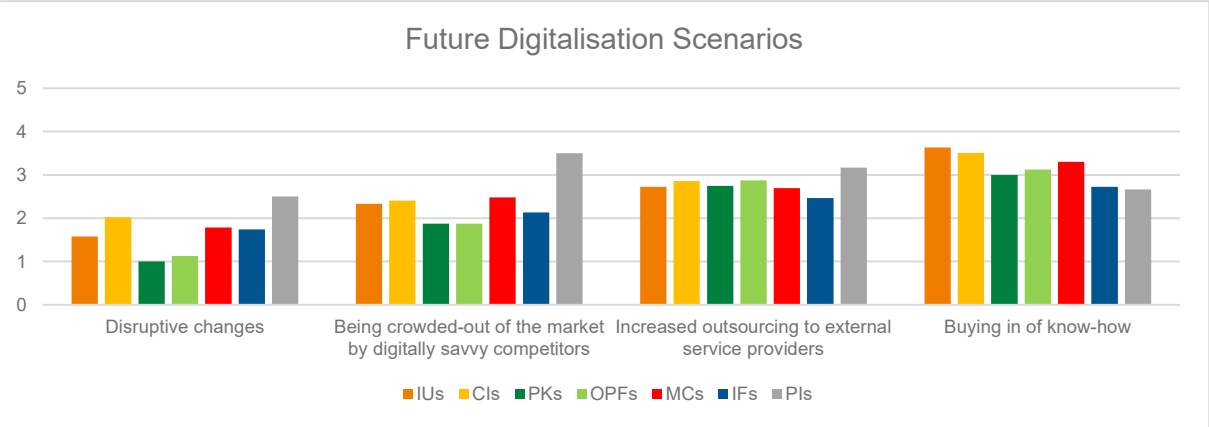
The results of the study show that the measures taken by the FMA to date are going in the right direction. Specific additional strategic and operational steps are being taken that also take into consideration the feedback of participating undertakings or other stakeholders.

1 STRATEGIES

1.1 EXPECTED FUTURE SCENARIOS

In aggregate form, the undertakings present in the Austrian financial market expect an ongoing continuation of digitalisation trends to date. There is an increased need for external support in the form of advice, outsourcings or ad hoc assignments.
The more digital-based the business model, the higher the expectations are of disruptive development.

The expectations of the Austrian financial market regarding potential future scenarios have not noticeably changed since the last version of the FMA Digitalisation Study in 2018,[3] as is also shown in the following chart using a numerical scale from 1 ("very unlikely") to 5 ("very likely") regarding the estimations of supervised entities:



The predictions between the individual sectors are largely homogeneous:

- The most probably future scenario overall is an increased need for external support in the form of advice, outsourcings or ad hoc assignments.
  The tendencies regarding the commissioning of external service providers however vary strongly from one entity to another. Outsourcings driven by digitalisation are still estimated by significantly less than half of the supervised entities as "very likely" or "fairly likely". While such outsourcings may increase efficiency, at the same time they may also have implications regarding the ability of providing complex services in-house as well as for the issues of IT security as well as concentration risks.

[3] *FMA, Digitalisation in the Austrian Financial Market – Status Quo, Outlook and Call for Input, June 2019.*

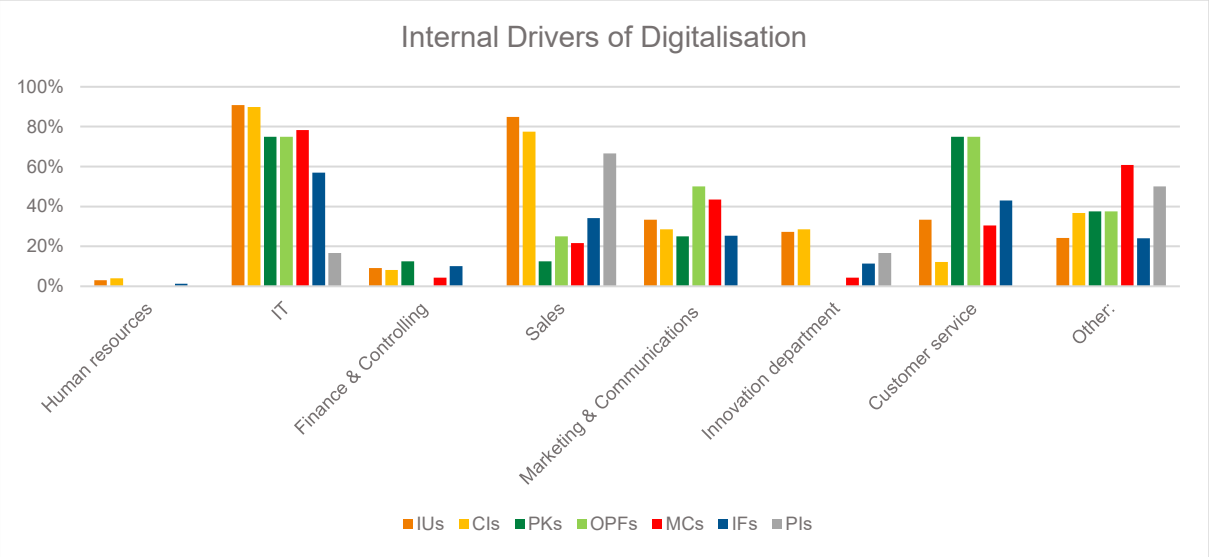
- Revolutionary or disruptive changes are consider to be more likely than average by payment institutions (PIs) and virtual asset service providers (VASPs), which reflects the comparatively high dynamism in these relevant new and digitalisation-based market segments. In contrast, Pensionskassen (PKs) and occupational provision funds (OPFs) particularly categorically exclude the possibility of disruption and crowding-out effects, which can be explained directly by the respective business models of such undertakings.

1.2 DRIVERS OF DIGITALISATION

The **IT Department** remains the principle driver of digitalisation in the undertaking itself in almost all sectors. This shows that internal technical know-how is an important component of digital innovation despite the frequent existence of outsourcings and that IT departments in many entities have a role that extends far beyond mere technical administration.
At the same time, **directly customer-facing departments** (sales, customer service, marketing and communications) are perceived as an important motor for digitalisation. The focus of entities on this area points to a certain competitive pressure in relation to digital contact with customers. Modern communications channels play a decisive role, both in marketing products and services as well as in cementing existing customer relationships.

- **IT** (IUs 91%, CIs 90%, OPFs 75%, management companies (MCs) [KAGs, ImmoKAGs, AIFMs] 78% and IFs/ISPs 57%) is the most important internal driver of digitalisation in companies in almost all financial sectors. With the exception of only payment institutions, more than 50% of entities in every sector stated that the IT department was a principle internal driver of digitalisation.
- At the same time, **Sales and Customer Service** are perceived as an important motor for digitalisation. Around 80% of IUs and CIs list sales as a key element in this regard, in the case of PKs and OPFs customer service occupies this place based on business models for around 75% each. Since customer communications or the provision of advisory services in the individual sectors are subject to specific rules under supervisory law, it is essential for the FMA to keep pace with them in order to remain true to its supervisory mandate.
- Finance & Controlling and Human Resources, in contrast, only have minimal acknowledgement as being drivers of digitalisation. Human Resources and Finance departments are clearly viewed as less of a driving force regarding innovations for increasing efficiency in administrative fields.

- In the meantime, over 20% of CIs and IUs have a separate **department for digital innovation**; this figure has increased since the 2018 edition of the FMA Digitalisation Study.

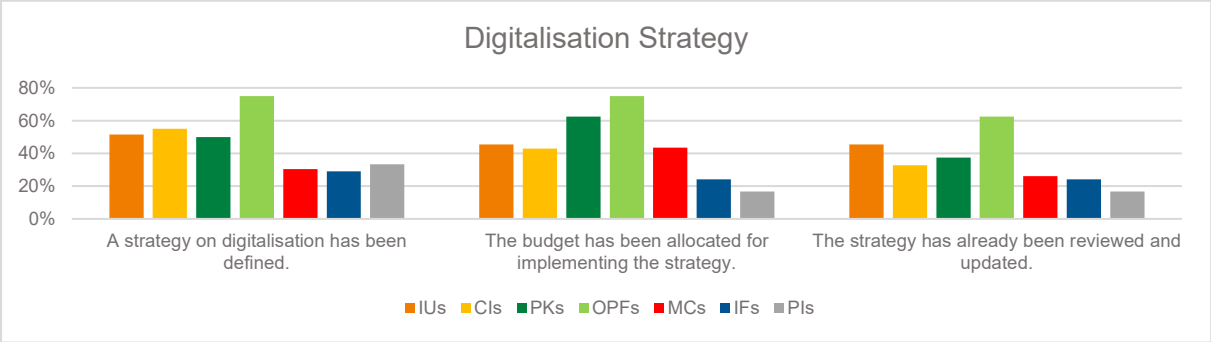


1.3 DIGITALISATION STRATEGY

In the meantime, almost all supervised entities have at least partially integrated digitalisation into their strategy. Three years ago, the picture was a completely different one: digitalisation was part of their strategy for only 20% of entities. Progress in the field of digitalisation has therefore developed into an essential objective of supervised entities in Austria in the course of recent years.

There are however large differences between the individual financial sectors:

- Only slightly more than one-quarter (29%) of IFs have fully defined an explicit digitalisation strategy. In addition, around two-thirds of MCs and PIs have only partially integrated digitalisation into their strategy.
- In contrast, the greatest advances are been observed for PKs and OPFs, which in 2018 did not yet attach so much importance to aligning their strategy with digitalisation in view of the structural differences in their business models. Around three-quarters (75%) of OPFs have fully defined an explicit digitalisation strategy.



Considered across the various industries, almost half (44%) of the supervised entities therefore twice as many as in 2018, have fully underpinned their target vision and digitalisation strategy with measurable targets and budget (24% of IFs, 63% of PKs, 45% of IUs, 43% of CIs, 43 % of MCs, 17% of PIs and 75% of OPFs).

Of the remaining entities, in the meantime almost all have at least implicitly or in some sub-areas defined a digitalisation strategy or dedicated budget to it.

With regard to digitalisation strategies, it is not possible to establish a clear connection with the other questions; such a strategy therefore does not seem to be a mandatory prerequisite for innovation and digitalisation, although where one is present it is a clear symbol for the management's commitment to this issue.

1.4 OPPORTUNITIES ARISING FROM DIGITALISATION

Gains in efficiency and greater customer proximity are observed across practically all sectors as being the greatest opportunities arising from digitalisation.

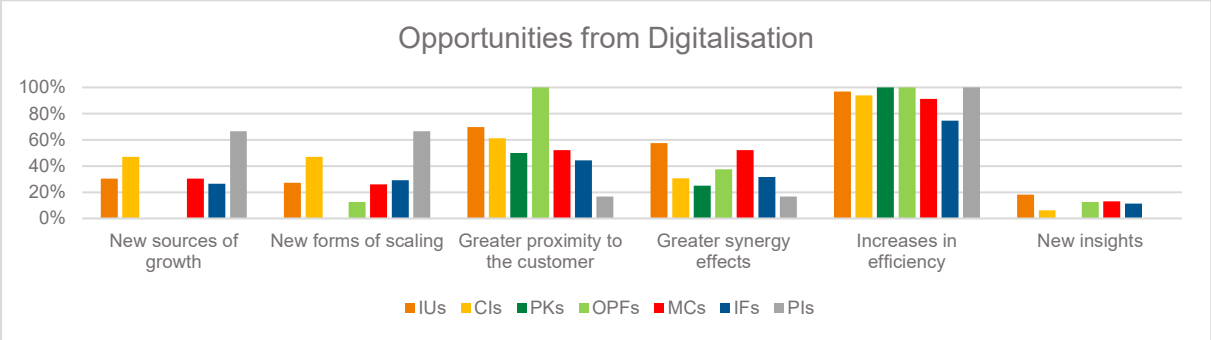
Overall, supervised entities see varying options for the deployment of digital technologies and in so doing focus most strongly on increasing efficiency in existing processes. The entities' internal focus currently also predominantly lies in the potential attached to digitalisation. Improvements are therefore expected that are incremental rather than revolutionary in nature:

- All sectors view **improved efficiency** as the significant potential for digitalisation. The range of estimations lies between 100% (PKs, OPFs, PIs) and 75% (IFs).
- New sources of growth and forms of scaling are still hoped for by 47% of CIs, whereas such hopes only apply for around 30% (IUs, MCs, IFs) or not at all (PKs, OPFs, MIs) for other sectors. The PIs

is an outlier, with this being the case for over 50%. Only a few individual entities are expecting new insights (e.g. In the field of Big Data Analytics) independent of the financial market sector.

- The possibility to achieve greater proximity to the customer by means of digital media, is classified as being a significant benefit. In line with the estimation of distribution and customer care being a driver of digitalisation, more than 50% of supervised entities classify it as a significant opportunity, with approx. 70% of IUs or even 100% of OPFs viewing it as such.
- Although in the case of internal drivers of digitalisation primarily customer-facing divisions feature prominently, to a certain extent, synergy effects are also perceived as even more significant opportunities.

The following chart contains an overview of the results by sector:

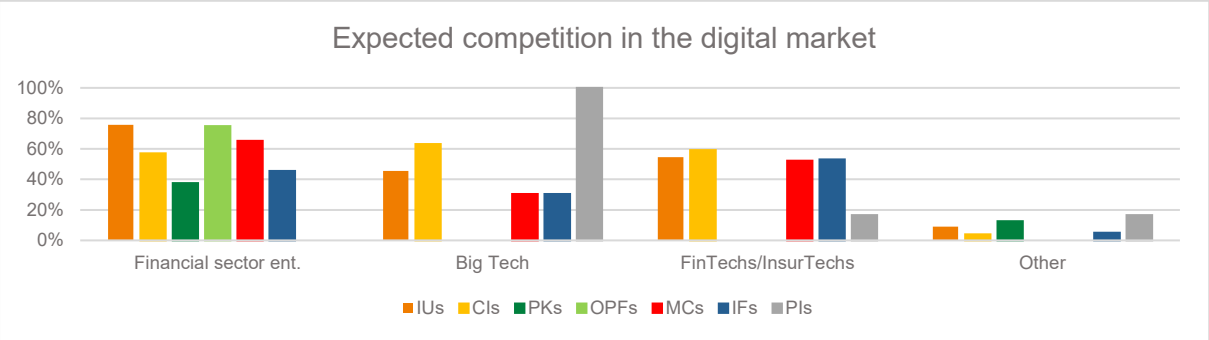


The overall picture and the aforementioned observations are relatively similar to the results of the study in 2018. In a few sectors there have however been certain dislocations, for example the opportunity for greater proximity to the customer as classified as being more relevant than the opportunity for increased efficiency.

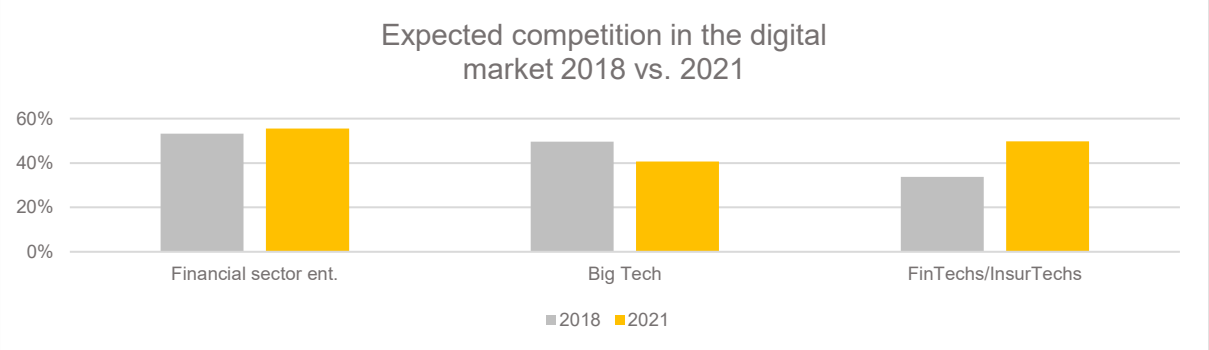
1.5 DIGITAL COMPETITION

Most supervised entities continue to view established financial market participants as their largest competitors. However, there are strong sector-specific variations. These can be attributed to the economic and regulatory differences in the business segments that make the market entry of different competitors more or less probable from the perspective of the entities.

While PIs, VASPs and CIs estimate the potential competition from BigTechs as the highest, IUs and MCs expect the stiffest competition to come from other entities in their sector. Only IFs perceive FinTechs as their largest competitors. PKs and OPFs generally see little competition in the digital market for their business model, and therefore only respectively view other PKs or OPFs as potential rivals.



Viewed holistically, entities' expectations have especially changed regarding BigTech and FinTech start-ups since 2018:



The supervised entities currently consider it as significantly less probable than back in 2018 that BigTech entities will aggressively enter their markets. This might be because such a scenario, with the exception of a few experiments, has not yet been largely realised. In this context, the Bank for International Settlements[4] analysed the possibility of BigTechs taking a dominant position in the market, which might primarily arise based on their records from e-commerce and social media. Customers' readiness also to purchase insurance products from BigTechs also appears to have increased dramatically during the Corona pandemic.[5]

In contrast, supervised entities increasingly perceive FinTech-/InsurTech- start-ups as potential competitors.

At the same time, the number of co-operations with such players is also growing. Both factors point to a growing significance of start-ups for the financial market. This impression is also due to several entities that were originally characterised as "start-ups", having obtained licences for financial services and have been successful in the market.

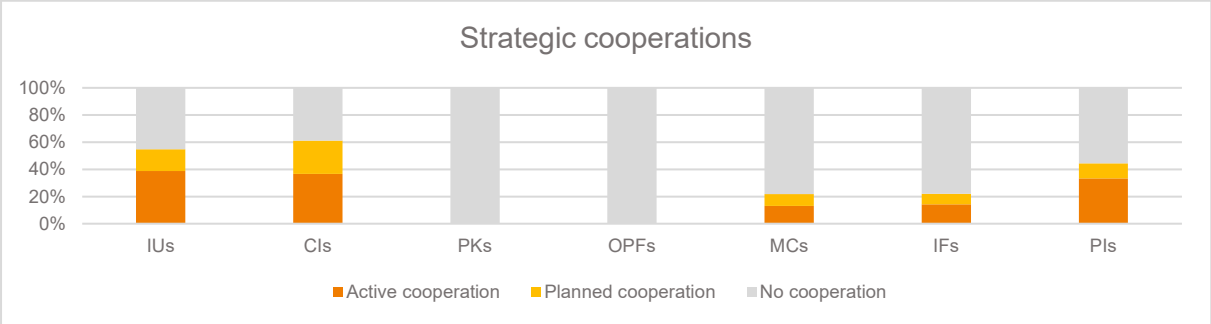
1.6 CO-OPERATIONS WITH FINTECHS/INSURTECHS

The trend of entering into co-operations with FinTech-/InsurTech start-ups is continuing on a constant basis. By doing so such entities have been able to establish themselves in a few digital niches.

- VASPs, IUs, CIs and PIs in particular are cooperating with FinTechs/InsurTechs. This correlates with the fear of PIs, VASPs, banks and insurers that Google, Amazon et al. could enter the financial market as digital newcomers with new products and services.
- In contrast, PKs, OPFs and MIs have not entered into any strategic co-operations with FinTechs to date.

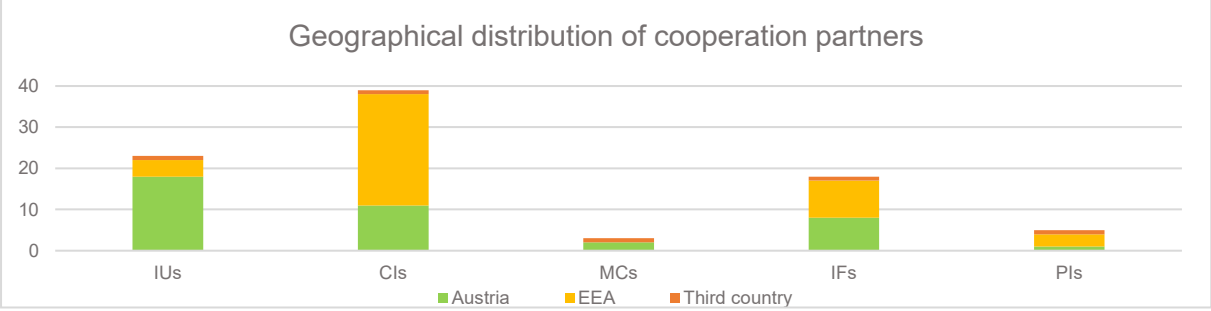
Irrespective of the fear of some supervised entities that FinTechs/InsurTechs could in the future become competitors, the Austrian financial market assumes that the number of co-operations will also increase in the next three years. By 2024, more than half of CIs and IUs want to cooperate with at least one FinTech/InsurTech.

[4] Cf. BIS Bulletin no. 45, https://www.bis.org/publ/bisbull45.pdf.
[5] More than 50 % of customers would be prepared to purchase insurance policies from Google et al. See the World Insurance Report 2021, https://worldinsurancereport.com.



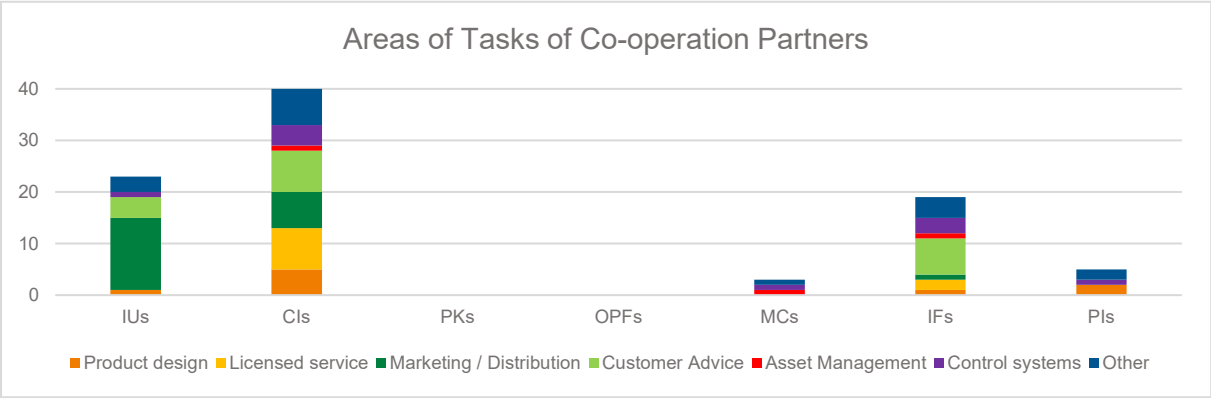
Looking at the geographical distribution of the co-operations with start-ups, there is a difference between the sectors:

- while IUs primarily cooperate with Austrian entities,
- CIs and IFs (as well as MCs, VASPs and PIs to a far lesser extent) cooperate predominantly with foreign start-ups, or at least from other EEA countries.



With regards to areas of tasks in which co-operations with start-ups are made use of, it has been determined that

- for IUs the focus is on processes and tools in relation to customer support and sales,
- while a larger diversity in the fields of co-operation is observable in other sectors: in addition to customer-related issues, start-ups in these sectors are also partially integrated into the licensed service itself and in control systems.



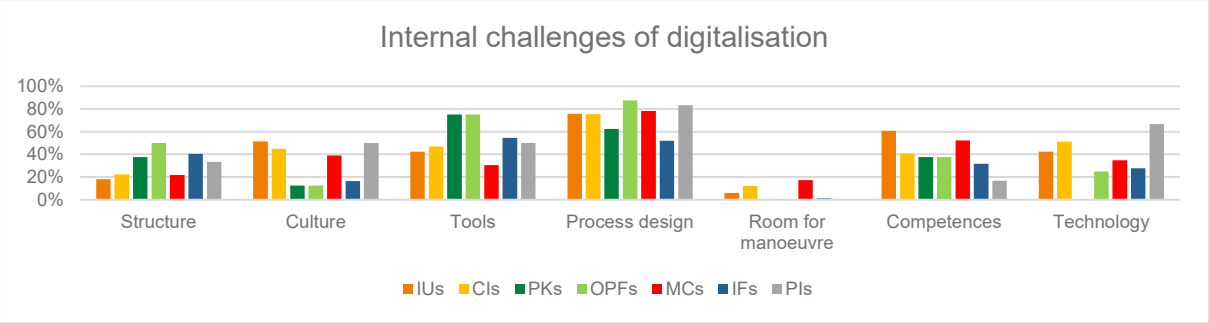
Overall, start-ups are establishing themselves as part of the Austrian financial market. In doing so, co-operations with licensed entities are a logical step in overcome regulatory know-how-based or financial hurdles to entry. At the same time, new players introduce new technologies and creative, digital approaches into the market.

The FinTechs/InsurTechs scene becomes an additional area of relevance for supervision for the FMA, which already operates a regulatory sandbox for certain co-operation models.

1.7 CHALLENGES IN IMPLEMENTATION

The increasing digitalisation of tradition business models also comes with numerous challenges and is associated with internal and external impediments. Which impediments are identified does not exclusively depend on the sector, but also strongly depends on the individual entity in questions, and thereafter dictates how digitalisation is advanced further:

- The largest challenge for increasingly digital or hybrid workflows is considered relatively unanimously to lie in **process design**. This is also understandable, as software-automated implementation of a workflow often requires process design to be defined and described in a highly formalised manner, which sometimes did not yet exist.
- Adequate **staffing and technical resources** (competences and tools) are viewed across all sectors in practical terms as significant challenges, in the case of digital ventures within the entity.
- Around half of the insurers (52%), payment institutions (50%) and banks (45%) view the necessary adaptation of **corporate culture** as a particular challenge.
- Room for manoeuvre within the entity is generally not considered as a problem.

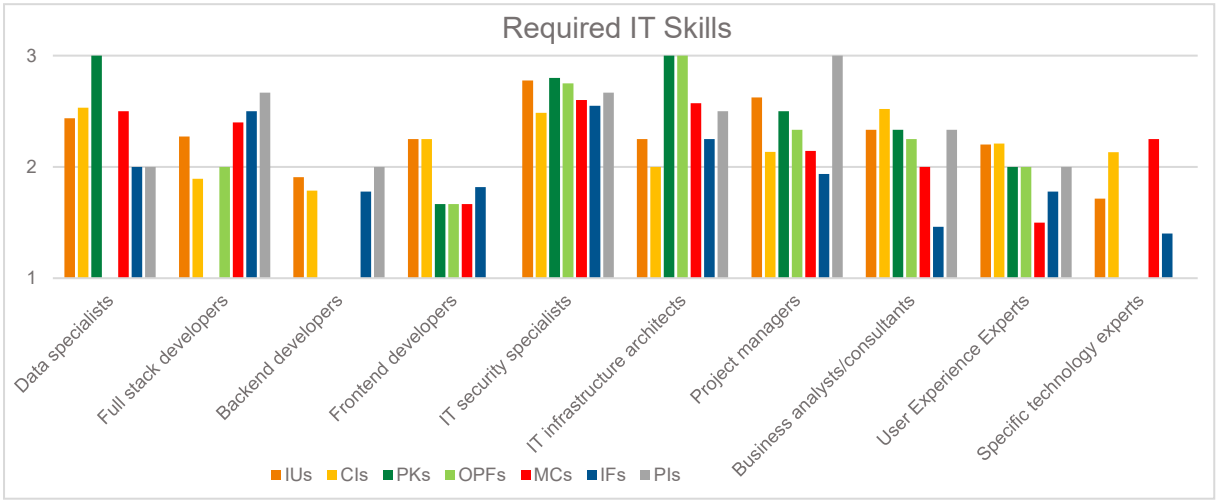


1.8 IT KNOW-HOW SOUGHT AFTER

New opportunities and possibilities may arise from advancing digitalisation that require specialised IT competences in light of the issue of increasing competitive pressure. The digitalisation study shows that a need exists in a broad field of disciplines. The following trends have been detected in the financial market, with certain sector-specific variations:

- All sectors are primarily interested in extending capacities in the field of **IT security**.
- There is a trend towards assigning greater relevance to management and analyst positions with a technical affinity that the field of activity of out-and-out software development.
- With regard to IT development itself, it emerges that greater importance is attached to an expansion of **generalists** (full stack developers) compared to the expansion of know-how in the area of front-end or back-end developers.
- In particular in the case of IUs, CIs, PKs, MCs and MIs expansion of know-how is planned regarding the structuring and analysis of data.

In the following chart, the results are placed in order from 1 (little relevance) to 3 (very relevant):

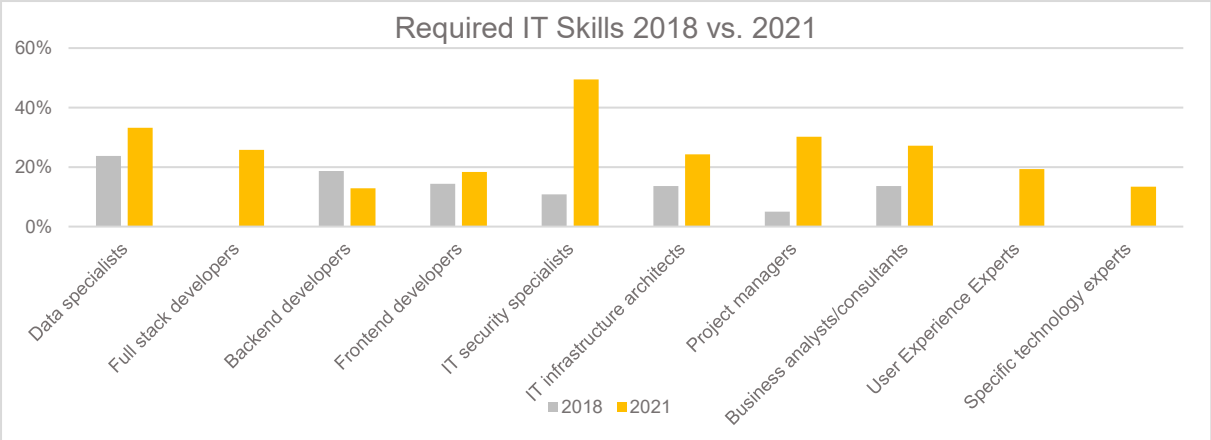


Compared to 2018, the first impression already shows that supervised entities want to further extend their IT competences even more. Furthermore, a few priorities have changed significantly:

- In 2018 purely technical skills were still the focal point.
- There has been a particularly marked increase in the **need for project managers and analysts**, who have the necessary technically understanding to manage and support digital ventures.

- The strongest weighting is with regard to the topic of **IT security**, which was still of moderate importance in 2018 and now, considered relevant by around 50% of the companies, occupies by far the top position.

This follows the corresponding graphical overview for this comparison, although it should be noted that the areas *full stack developers, user experience experts* and *specific technology experts* did not exist in the 2018 survey and therefore no data is available for them:



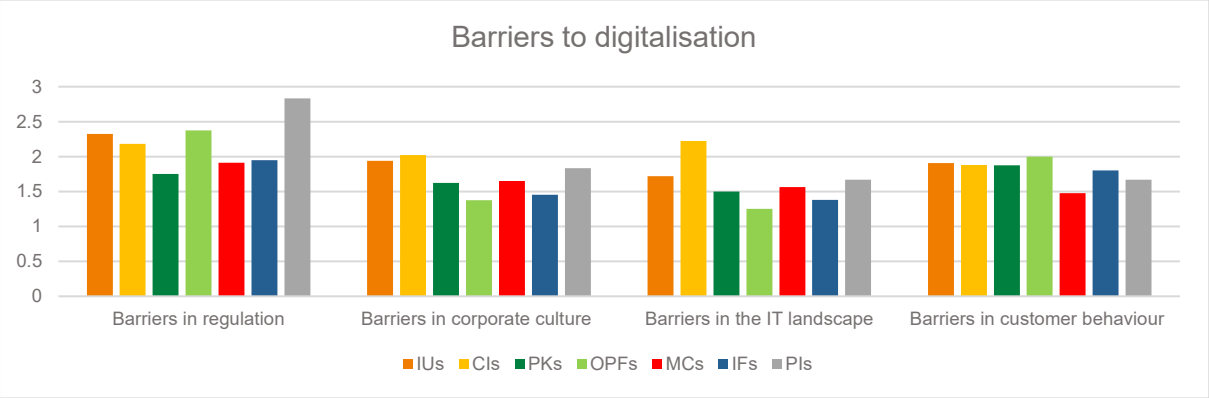
- From the supervisor's point of view, the massively increased requirement for IT security in particular catches the eye. This illustrates a **strongly increased awareness about the growing threat of cyber attacks about the supervised entities**. On the flipside, there also however appears to be a certain lack of available sufficiently qualified staff, which might make it more difficult for entities to implement their IT security-related projects in a timely manner, especially since appropriately qualified personnel are also sought in other sectors. [6]
- It is also apparent in some areas at least that many entities want to strengthen their **in-house capabilities**. Doing so may ensure that there is a certain degree of independence from external service providers, and helps to prevent concentration risks. However, since financial market participants also have to compete with exactly these companies for skilled workers, demand for in the relevant vocational groups will probably remain higher in the future than the available supply in the labour market, making it difficult to fill such positions.

[6] *In relation to this problem see also e.g. Der Standard, 6.4.2021, Firmen fehlen mehr als 24.000 IT-Fachkräfte - Digitalisierung - derStandard.at › Karriere*

1.9 BARRIERS TO DIGITALISATION

The relevance of the different categories of barriers in relation to digitalisation were classified by the supervised entities using a scale from 1 (not relevant) to 3 (very relevant):

- In most sectors, **regulation** was the area with the largest barriers to digitalisation. This is particularly strongly prevalent among PIs, MIs, OPFs and IUs. The principle factors in particular relate to rules about signatures signed by hand, the priority afforded to paper form, the rules that are in part difficult to achieve in relation to electronic transmission as well as only dictating digitalisation trends too late.
- Barriers for digitalisation that originate in **customer behaviour** are also relevant. In this regard, the entities above all report about customers having an inadequate digital competence, which is an obstacle for digital solutions, as well as a somewhat wait-and-see attitude of certain customer groups towards digitalised processes.
- With the exception of the banking sector and VASPs, greater importance is attached to the barriers to digitalisation in the **corporate culture** than to the obstacles that relate to the internal IT landscape (outdated IT landscape, insufficient financial resources for research and development, low flexibility, etc. are mentioned here).



The following sector-specific barriers to digitalisation are mentioned:

- **IUs** also see difficulties as part of progress in relation to digitalisation in the extensive information obligations, such as in online sales, as well as in the shortage of skilled workers in the digitalisation environment.
- For **CIs** the lack of focus in the “securities” business field is an obstacle for modern core banking systems.

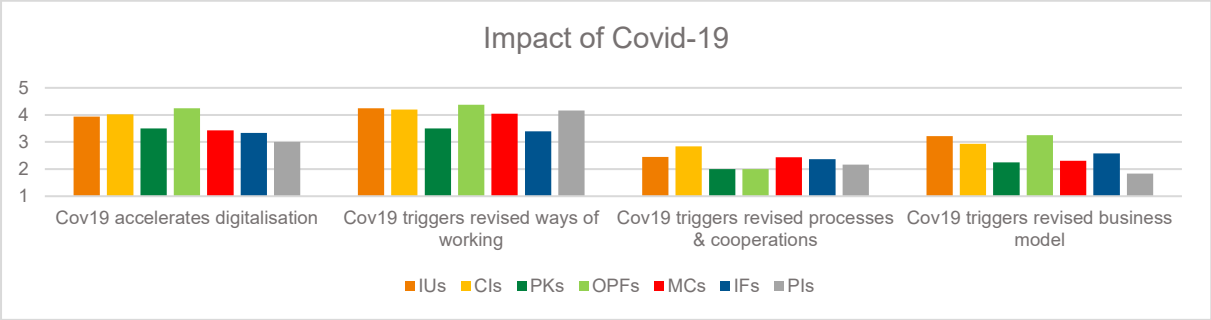
- **OPFs** mentioned in the survey about the lack of regulatory priority towards electronic rather than paper form, and consider there to be a certain need to act in this field.
- **MCs** see the high demands placed on IT business partners as an obstacle that stands in the way of digitalisation efforts.
- **IFs** report about the lack of flexibility of their business partners.

1.10 IMPACT OF THE COVID-19 PANDEMIC

The sudden outbreak of the COVID-19 pandemic and the subsequent restrictions on physical mobility have led to large-scale changes in the financial sector. On the one hand, customer contact is standard in many business models, on the other hand, processes at the supervised entities were predominantly based on staff physically working at the workplace. That the impact of protective measures, lockdowns, quarantine and cases of illness has not been considerably more noticeable is due to a large extent to the digitalisation in the Austrian financial market.

The supervised entities have identified the following impact of the COVID-19 pandemic:

1. The Austrian financial market views the most important implication of the COVID-19 pandemic was the changed framework conditions gave rise to the long-term re-evaluation of internal working methods. For example, permanent digital workplaces could be created. This would be linked to the possible greater flexibility of working hours or the reduction of working spaces.
2. COVID-19 has led to a general acceleration of the deployment of digital technologies as a **driver of digitalisation** in all sectors of the financial market.
3. In contrast, supervised entities are less likely to see COVID-19 as a reason to re-evaluate future working processes and co-operations in the long term. Considerations regarding the extension of outsourcings and co-operations with external service providers are therefore based on other motivations.
4. A further potential consequence of COVID-19 is the re-evaluation of the licensed **business model**. Supervised entities – especially IUs, OPFs and CIs – are occupied with potential adaptations of digital services or the adaptation of communications and sales strategies.



From the supervisor's perspective, COVID-19 has accelerated existing development towards electronic customer communication, with regulatory issues having gained additional relevance in this regard.

Furthermore, the increased usage of digital media and means of communication as well as the widespread deployment of remote working ("teleworking") have created issues that have needed to be taken into account in entities' IT security plans.

Finally, COVID-19 has also further developed the working methods of the FMA itself in order to cope with the switch to working from home, while also not losing proximity to the financial market even without physical meetings, and to be able to continue to carry out supervisory activities.

1.11 SUMMARY AND ACTION AREAS FOR THE FMA

The 2021 version of the digitalisation study and the comparison with the findings from 2018 confirm that there is a **technology-driven transformation of the Austrian financial market**. The entities that are active in the Austrian financial market are also aware of this and therefore more frequently include digitalisation-related agendas in their planning and strategy.

Accordingly, the responses in the chapter "Strategy" show an increasing change, varying in intensity but nonetheless clearly recognisable, from a wait-and-see attitude to an active engagement with digital topics by the decision-makers of the supervised entities.

This development is particularly underpinned by the following results of the survey:

- Intentions regarding further outsourcing and making use of advisory services on digital issues will continue further in the entities' estimation (see the section on Expected Future Scenarios).
- Many approaches regarding more efficient digitalised processes and improved customer proximity using new methods of communication are already being used practically, however the potential for improvement in these areas continues to be classified as high (see the section on Opportunities arising from digitalisation).

- In addition to the competitive pressure from other licensed entities some financial market players classify start-ups as potential future competitors (see the section on Digital competition).
- Entities are increasingly looking for qualified staff members with digital skills, with demand for IT security specialists having increased most strongly by quite a margin (see the section on Sought-after IT Know-How).
- The number of co-operations with start-ups is increasing constantly, and in some sectors there is also an emphasis on cross-border co-operation (see the section on Strategic Co-operations).
- The general development towards digitalisation was accelerated further due to COVID-19 (see the section on the Impact on COVID-19).

The FMA has already taken various steps to accompany such developments and to integrate them into its supervisory approach. From the trends identified in this study, indications show that the following strategic areas in particular will need to be addressed in the future:

Actively accompanying digital transformation in the Austrian financial market; actively communicating the rules of the game.

- The structure of the value creation chain is changing with (partial) services increasingly being provided by service providers or co-operation partners. These interconnected dependencies may create various risks for entities, such as concentration risks and interruptions in the digital value creation chain.
- The involvement of start-ups as well as new business models and platforms may also be accompanied by implications for sales practices and the licensed business operations as a whole.

Allowing new interdependencies to flow into ongoing supervision and risk classification:

- The business models of supervised entities are changing as a result of the co-operation with FinTechs / InsurTechs. The FMA must adjust itself to a higher level of complexity and allow such new interdependencies to flow into its risk perspectives in relation to entities and the financial market as a whole.
- Dependence on external service providers as well as the supply structures and concentration risks must accordingly increasingly be taken into account by the supervisor in the future.

Adapting the FinTech Point of Contact and the Sandbox constantly to the market's requirements and regulation:

- Furthermore, new innovative providers are entering the Austrian financial market in the form of FinTechs and InsurTechs, also create new opportunities for established supervised entities. Business models can be overhauled and more efficiently designed by such co-operations throughout the entire value-creation chain. FinTech/InsurTech business models may also be offered by undertakings that neither hold a licence nor are subject to supervision. It is frequently not easy to delineate which approach applies, so the FMA therefore considers it its task to provide support to FinTechs/InsurTechs in clarifying what is possible. The FMA established the **FinTech Point of Contact** as the central entry point for questions that are relevant in relation to supervisory law, which constantly has to adjust its information to the market's requirements and regulation.
    - On 01.09.2020 Article 23a FMABG on the "Regulatory Sandbox" entered into force, obliging the FMA to establish such a sandbox:
    - FinTechs looking to obtain a licence, as well as entities that already holding licences, and their financial innovations are prepared for supervision within the sandbox by an intensive dialogue with the FMA. The implications under supervisory law of FinTech models may be tested with a conditional licence.
    - Sandbox means supervision: the sandbox is intended for participants that already have a licence or which wish to obtain one during the course of the sandbox procedure. A co-operation with technical services is possible, but may not only consist of sandbox participants.
    - There is no exemption from regulatory requirements and no "lightweight licence", but the principle of proportionality applies.
    - During the test phase, additional conditions and restrictions may even be imposed under which services may even be provided to customers.
    - It is possible to clarify in advance about the requirement to hold a licence, be registered or to produce a prospectus in the FinTech Point of Contact (as an innovation hub).
    - The maximum period that a project may remain in the sandbox is 2 years.

The FMA's sandbox commenced its operations promptly and work is ongoing across the various supervisory departments to solve the challenges arising from new types of business models. Three entities have already submitted an application to be admitted to the sandbox (to do so it is not necessary to have legal representation). The submitted business models in particular involve services in relation to crypto assets/tokenised securities for innovative forms of investment in securities for retail investors.

Promoting and demanding of developing general knowledge in the areas of finance (financial literacy) and digital technologies (digital literacy):

- It is still not possible to rule out disruptive developments from either technological or structural developments. While supervised entities themselves consider revolutionary changes as rather unlikely, nonetheless, in 2018 start-ups were still viewed far less frequently as important players; similarly the awareness for cyber risks has increased significantly, and new technologies are being adapted more quickly than a few years ago. This highlights the necessity for the FMA to continue to keep abreast of new trends with awareness and understanding, in order to be able to anticipate changes in the financial markets.

1.12 CONSULTATION ON STRATEGIES

- How do you estimate the impact of digitalisation on the financial market?
- Do you share the view of the financial market participants that disruptive transformations (i.e. the fundamental principle of the core business being replaced) is unlike to occur in the financial market within the next three years?
- In which areas do you expect disruptive developments in the medium- to long-term?
- From your perspective, what factors are decisive for the success of the entities active in the financial market to use digital transformation optimally for developing their own business model further?
- In what areas do you think that barriers to digitalisation exist?
- How do you assess the implications of the entry of new digital competitors into the financial market? In which business areas do you assess that the new players will become materially significant within the next three years? What developments do you expect regarding the relationship of established players and new players?
- Do the risks and opportunities identified by the FMA correspond to your perspectives, or what material deviations exist from your experience?
- What is your expectation with regard to the role of the supervisor in the digital transformation of the Austrian financial market?

2 PRODUCT DESIGN

Digitalisation is a catalyst for new products and services. Customer behaviour is changing with regard to access to services that must be possible at any time, from any location via different channels. The increasing networking of devices, households and infrastructures furthermore creates new demands on the design of products and services.

2.1 BANKING PRODUCTS

The results of the FMA's digitalisation survey show that banks in Austria classify digitalisation as a very relevant issue, and are willing to take measures to exploit this development for themselves. At the same time, the opportunity of profiting from new technical capabilities is appreciated, and the risk of falling behind the competition recognised in regard to this issue. The latter aspect is further emphasised by the expectation that the competition in the future will no longer solely be with other credit institutions. Those banks surveyed continue to hold the view that large technology companies (e.g. Google, Amazon) as well as financial services providers might attempt to tap the market with their own products.[7] Digitalisation's greatest influence on product design is seen to be in having a better understanding about the customer by having more data about them and more points of interactions as well as due to automation and saving in terms of resources.

2.1.1 TECHNOLOGY-DRIVEN PRODUCT INNOVATIONS

Internet of Things	■ The Internet of Things (IoT) allows classical banking services to be connected to existing **digital voice-activated assistants**. Such products (at least in Austria) are not yet widespread, and currently only available with simple functions ■ A significant technological trend that is currently being observed is **voice-controlled interaction without manual input** ("the age of air").[8] It is safe to assume that digitalisation will also be reflected in this area at product level.
Artificial Intelligence (AI)	■ Automatic image recognition ■ **Online opening of an account**: new customers can be identified using video-chat, in co-operation with external providers ("Opening of an account from the comfort of your couch").[9]

[7] *For further information, see: Bank for International Settlements, July 2021, https://www.bis.org/publ/bppdf/bispap117.pdf.*
[8] *Erste Bank, 6.7.2017, https://www.erstegroup.com/de/news-media/news-views/2017/07/06/kuenstliche-intelligenz-spracherkennung-fintech; https://www.santander.com/csgs/Satellite/CFWCSancomQP01/en_GB/Corporate/Press-room/Santander-News/2018/04/12/Santander-launches-the-first-blockchain-based-international-money-transfer-service-across-four-countries-.html.*
[9] *Der Standard, 23.1.2017, https://derstandard.at/2000051355606/Per-Selfie-zum-Konto-Banken-machen-mit-Video-Identifizierung-ernst.*

	■ **Photo transfers**: a few banks offer the option in co-operation with a FinTech to make a credit transfer by taking a photograph of the relevant data.
Machine learning	■ Banks use machine learning in particular in relation to the personalisation and improvement of their products.
Blockchain-based applications	■ At product level such applications are currently not particularly widespread; and from a customer perspective crypto assets are the most prominent example for blockchain-based applications ■ Individual banks have already started projects that are based on the Blockchain, i.a. The issuance of borrower's note loans.[10]

2.1.2 NEW TYPES OF PRODUCTS

New technologies also allow new niches and products to be created (for example, almost all Austrian banks offer e.g. instant credit transfers by means of transfers of funds via smartphones [Zoin], a product of Payment Services Austria: once the Zoin app has been registered, a digital wallet is used and money sent directly to contacts stored in the phone (also to other banks).[11]

Two new products are now subject to clear regulations with the entry into force of the Payment Services Act 2018 (ZaDiG 2018):

- account information services, which allow a comprehensive and consolidated statement about payment accounts; and
- payment initiation services, with which payments may be triggered using third-party providers.

In the future, both of these innovative services or products will be offered by banks as well as by third-party providers. Third-party providers wanting to offer such types of services must be licensed by the FMA, or in the case of account information service providers registered.

Furthermore, a trend is emerged in the area of asset management. Robo-Advisor-Tools, which lead to the conclusion of asset management, open up entry to this kind of product with low initially invested sums (from EUR 5,000) and low ongoing payments (from EUR 100 per month).

2.2 INSURANCE PRODUCTS

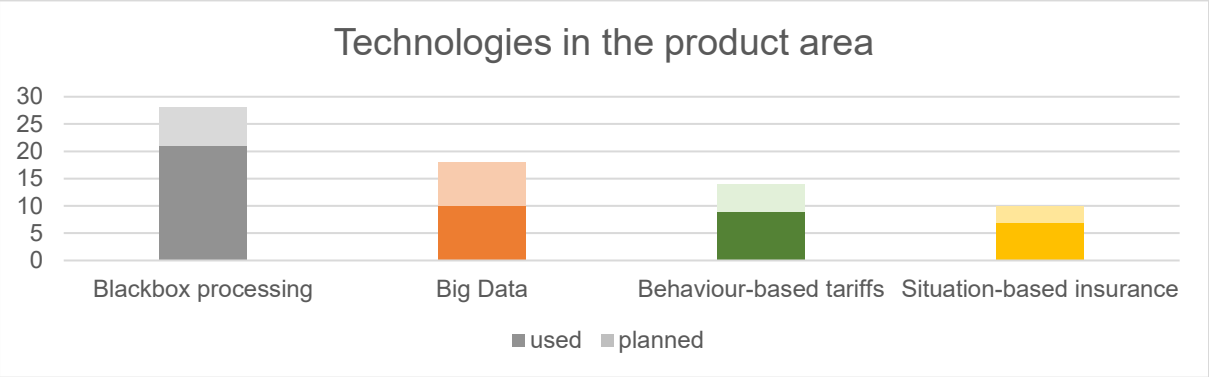
The use of digital technologies also influences the product landscape. In one case, traditional insurance products are now being converted to new technologies. On the other hand, the

[10] *Cf. https://www.erstegroup.com/de/schuldscheindarlehen.*

[11] *Der Standard, 20.9.2017, Zoin: Sofortüberweisung als Feature zum Geldtransfer über Smartphones, https://derstandard.at/2000064349794/Zoin-Sofortueberweisung-als-Feature-zum-Geldtransfer-ueber-Smartphones.*

technologies themselves are leading to new insurance products that in some cases are being launched experimentally.

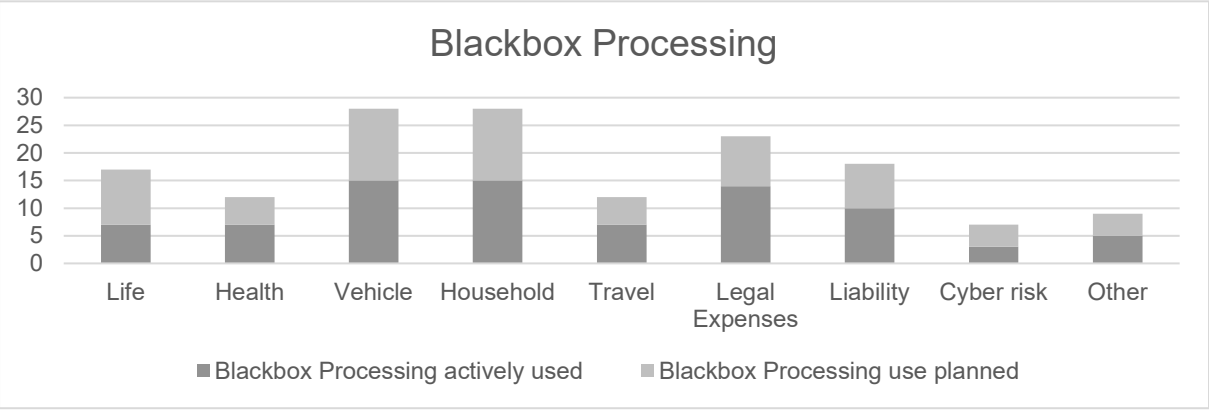
The most frequently used technologies by Austrian IUs in this regard are black box processing (85%) and Big Data analyses (55%). Behaviour-based tariffs (42%) as well as situational insurance (30%) are also offered by IUs or are in the planning stage.



2.2.1 BLACK BOX PROCESSING

Black box processing describes the fully automatic processing of business processes, with workflows being conducted more efficiently and the processing quality of standardised procedures can be increased without the necessity of interaction by the user. In all of the insurance classes black box processing is already being used and its use intended to be extended further in the course of the next three years.

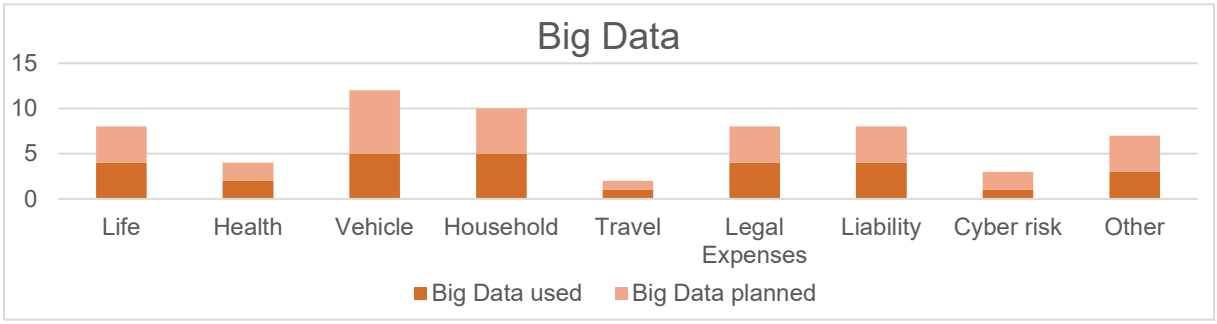
- Black box processing systems are most frequently used in motor and household insurance (in 15 IUs respectively), and in legal protection and health insurance.
- However, half of the liability insurers and a third of life insurance providers are already using black box processing to optimise standardised processes.



2.2.2 USING OF BIG DATA

By analysing large volumes of data, risks can be analysed in real time on the basis of individual behaviour. The estimation of risks will become an increasingly exact process in the future, and consequently the calculation of premiums will be far more individually tailored. Big Data is therefore also becoming increasingly significant in the insurance sector.

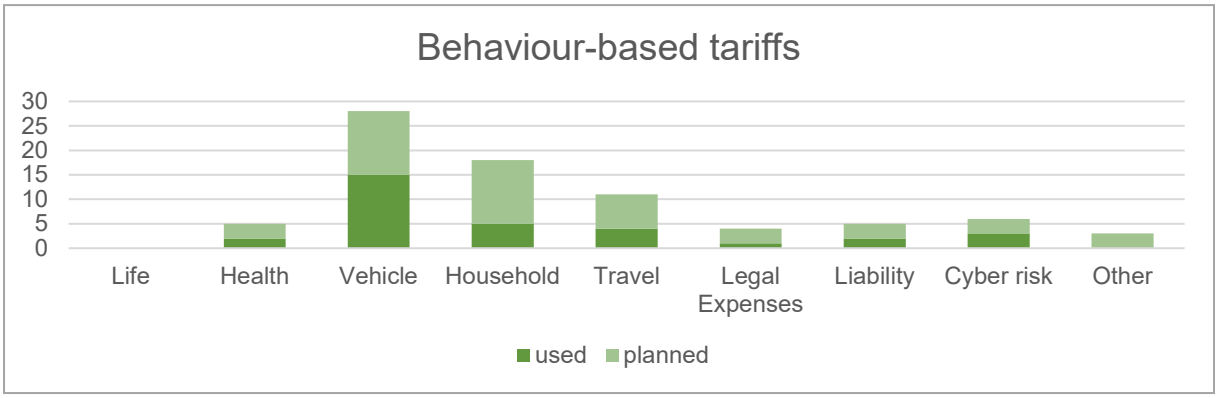
- Big Data was already used by IUs in all of the insurance classes surveyed. Most frequently in the areas of motor insurance, household insurance, legal protection, life insurance and liability.
- Many IUs plan to extend their use of Big Data by 2024.



2.2.3 BEHAVIOUR-BASED PRODUCTS

Big Data applications also enable the implementation of behaviour-based products:

- **Smart Homes:** detailed data about behaviour, environmental data, or claims data are used for calculations for household insurance that are correlated with one another thereby allowing more valid conclusions to be drawn that with blanket data.
- **Usage driven insurance**: insurance companies base their offer on usage behaviour, such as driving behaviour and the kilometres driven by the insured person (telematic tariffs).
- **Pay as you live:** insures may actively support their customers to live healthily using additional offers (e.g. fitness trackers that provide information about their daily exercise), and thereby increasing their presence.



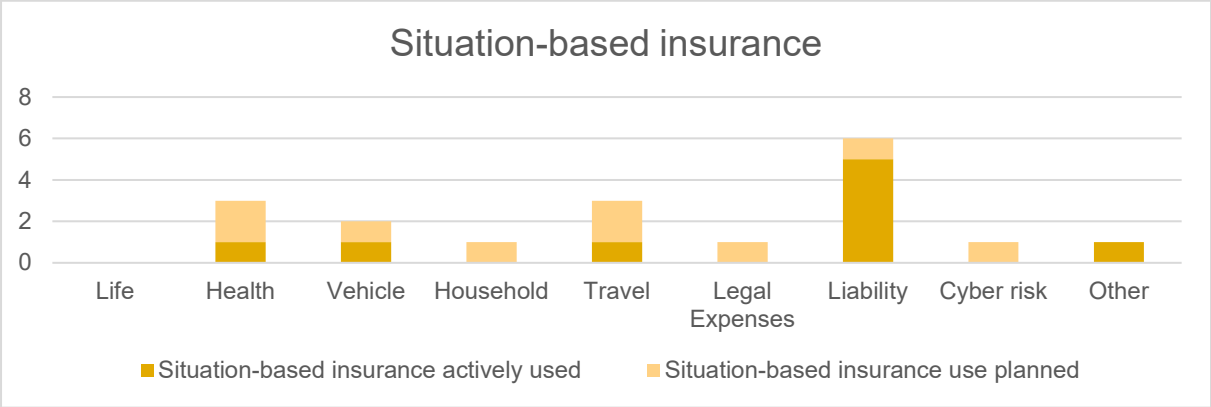
- Behaviour-based tariffs to date have primarily been used in Austria in the area of **motor insurance**. Half of the IUs (15 IUs) already offer behaviour-based tariffs in this insurance class. A further 13 (13 IUs) additionally plan to extend their range of such tariffs or to incorporate them in their product portfolio.
- Behaviour-based tariffs are also seen as a topic for the future regarding **household insurance**. Especially with regard to the current developments regarding smart homes and the associated sources of data, 40% of IUs (13 IUs) are planning to use or extend their range of products in this area.
- IUs believe there is a certain degree of potential in the future in relation to **travel insurance**. In this area a tripling of the number of providers of insurance solutions is planned by 2024 (currently 4 IUs, extension of tariffs planned by 7 IUs).

2.2.4 SITUATION-BASED INSURANCE COVER

In the case of insurance "on demand" customers are able to activate and deactivate their insurance cover for the cases captured in an app from their smartphone, and therefore can determine the duration of cover themselves. IUs' product landscape will move away from standardised tariffs and modules towards more strongly individually tailored and situation-based insurance cover.

Situation-based insurance cover has to date only been offered by comparatively few IUs up until now. The classes of travel insurance, health insurance, accident insurance and liability insurance are the main areas of application for this innovative form of insurance.

- In the liability insurance class, currently 12% of IUs (also planned by 1 further IU) offer situation-based insurance solutions. In the classes health insurance, travel insurance and motor insurance it is only possible to date to conclude such situation-based insurance cover at one IU in each instance.
- Examples of currently offered products are short-term health insurance for travel purposes, short-term liability cover for event organisers as well as the possibility to temporarily extend the geographical validity of insurance coverage in the customer portal.



2.2.5 PARAMETRIC INSURANCE

In the case of parametric insurance contracts, provisions are technically mapped on the basis of a blockchain in such a way that contract clauses can be partially or completely executed independently. The need to check whether and for what amount a claim has arisen for the insured person becomes obsolete as the agreed amount automatically becomes payable, as soon as a certain parametric trigger has been achieved. Triggers may include certain amounts of precipitation, a certain level being reached, or wind or earthquake strength at an agreed measuring station. In the further, corporate risks that were hitherto unable to be insured against may be insured against (e.g. operating interruptions without preceding material damage, cyber risks, product recalls as well as risks due to weather damage or energy prices).

Opportunities	■ Damage checks are not necessary ■ High potential for automation, efficient risk transfer ■ New areas capable of being insured (e.g. intangible assets) ■ Low administrative costs and low costs to settle the claim ■ Better evidence in cases of fraud, and simpler pricing
Threats	■ Availability of data constitutes an enormous challenge. Technical advancements (remote sensing and Big Data) may yield improvements in this regard

2.2.6 COMMUNITY BASED INSURANCE

Community-based insurance goes all the way back to the origins of the insurance industry, where certain community groups such as families or village communities provided mutual assistance to one another in the event of claims. The innovation lies in the fact that such types of insurance can be conducted through other channels in the era of computers and mobile phones.

With the help of digital possibilities (P2P) persons can be drawn together to form small groups. Damages for amounts that are less than the amount of the excess are split among the collective. Only in cases of larger damage amounts does the protection in the insurance policy take effect.

Opportunities	■ Modern technologies and the "Internet of Things" may facilitate access to insurance cover. ■ A no claims bonus creates positive incentives against committing insurance fraud while also saving costs.
Threats	■ Adverse selection of insurance risks ■ Regulatory "grey area" ■ Competent and financially sound carrier undertakings must exist

2.2.7 PRODUCTS BASED ON THE SHARING ECONOMY

The term "the sharing economy" is an umbrella term covering enterprises, business models, platforms and practices that permit the shared usage of resources that are partially or fully unused. Making use of goods or services over sharing economy platforms, is not a new trend, but the innovation relates to the type of service provided, i.e. using digital platforms that permit the matching of supply and demand particularly quickly based on the underlying technology.[12]

The increasing significance of business models from the sharing economy may lead to insurance benefits increasingly being attached to usage and far less to the ownership relationship of goods.

Opportunities	■ New insurance products
Threats	■ Misuse and consequently other risk profiles ■ It is unclear in which form customers and sharing platforms bear risks ■ Complex issues arising with regard to insurance law ■ Processes for claims processing may become more complex

[12] *Cf. for example Lloyds und Deloitte (2018), Squaring risk in the sharing age: How the collaborative economy is reshaping insurance products; which is critical of US health insurance regarding so-called health sharing ministries It Looks Like Health Insurance, but It's Not. 'Just Trust God,' Buyers Are Told. - The New York Times (nytimes.com).*

2.2.8 CYBER INSURANCE

The flipside of digitalisation is an increase in cyber risks. It is not possible to exclude cyber incidents fully even in the case of conscientious cyber risk management. This potential, which also includes assistance services for protecting against or treating cyber incidents, faces new challenges, for example, due to limited available data bases for calculating premiums and due to increased, changing cyber-attacks, which are also caused by the COVID 19 environment. Accumulation risks, arising from cyber-attacks that affect many insured persons at the same time, must also be taken into account.[13]

Cyber insurance products are not standardised products, and no separate insurance class exists for them. The respective scope of coverage of a cyber insurance policy may vary. Cyber risks are often covered by liability or legal protection insurance policies.[14]

Opportunities	■ Risk awareness ■ Large potential both by providing protection against cyber-attacks as well as providing support in the event of a successful cyber-attack: the shift to the home office, the professionalization of attackers and the daily reports on this are increasing awareness of the possible effects of risks. Furthermore, data protection rules are also driving demand for cyber insurance policies. The size of the global cyber insurance market was estimated as around USD 5 bn in 2019, and is projected to grow to around USD 29 bn in 2026.[15]
Threats	■ Calculation of premiums is difficult due to the lack of experience with claims as well as the rapidly changing environment

In Austria, 11 IUs explicitly offer cyber risk cover.[16] Just under three quarters of these providers thereby make use of reinsurance to reduce their risks.

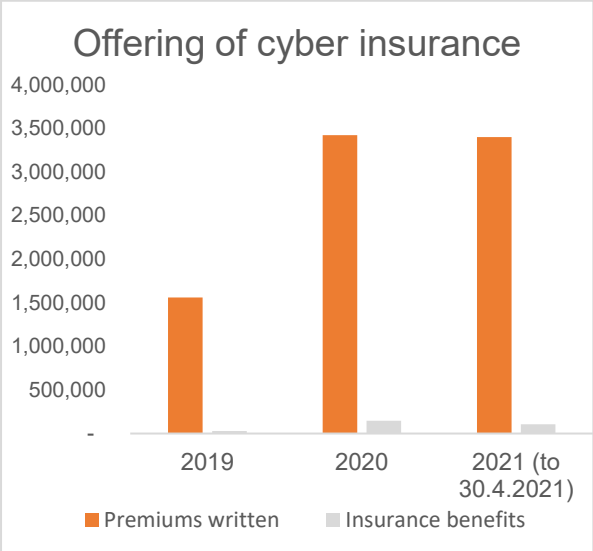
The cyber insurance premiums written by Austrian IUs in 2020 stood at around EUR 3.4 mn. This is more than doubled compared to 2019. Despite the large increase, the proportion of the cyber insurance market compared with the overall premium volume in 2020 of Euro 19 bn remains very low.

[13] *Premiums and the scope of coverage are currently being reevaluated by IUs due to an increase in the number of cyber incidents or a better understanding of risk profiles. Cf. Insurance Business America, ‚Dysfunctional' cyber insurance market puts pressure on brokers, 8.3.2021; United States Government Accountability Office, Report to Congressional Committees, Cyber Insurance – Insurers and policyholders face challenges in an evolving market, May 2021.*

[14] *See also EIOPA, EIOPA Strategy on cyber underwriting, 2020.*

[15] *Allied Market Research, Cyber Insurance Market Outlook - 2026, accessed on 07.09.2021.*

[16] *Cf. e.g. VersicherungsJournal.at, "Dramatische Marktverhärtung in der Cyberversicherung", 2.9.2021.*



While benefits from cyber insurance products have increased by half per insured event from 2019 to 2020; they are currently still at a management level of approx. EUR 148,000 in 2020.

The premium sum, for cyber insurance products concluded with supervised entities, stood at approx. EUR 42 million in 2020. The majority can be allocated to the sector of credit institutions (banks).

- The premium sum for 2020 has increase by approx. 6% compared to the previous year; an increase by 8% is expected for 2021.
- In comparison, the received insurance benefits in 2020 stood at EUR 5 million.

2.2.9 CRYPTO ASSETS POLICIES

The need for insurance coverage is increasing in light of hacker attacks and gradual regulation of crypto assets.[17] In this respect, demand for insurance against "cryptocurrency fraud" is growing globally. Insurers in the USA and Japan in particularly have been launching crypto assets policies for several years now.

Opportunities	■ New insurance products ■ Increasing of risk awareness ■ Better evaluation and estimation of risks
Threats	■ The size of risks arising from "cryptocurrencies" are very difficult to estimate[18]

[17] *Cf. e.g. The theft of around half a billion dollars from the Japanese exchange Coincheck, BBC, 27.01.2018, Coincheck: World's biggest ever digital currency 'theft' - BBC News; see also the incident in August 2021 Hackers return $260 mln to cryptocurrency platform after massive theft | Reuters.*

[18] *Cf. ENISA Opinion Paper on Cryptocurrencies in the EU (europa.eu) such as: AML issues, tax issues, illicit activities, energy used causing impact on climate change.*

2.3 SUMMARY AND ACTION AREAS FOR THE FMA

Digital transformation requires a stable foundation and legal clarity

- The lack of legal clarity regarding the classification under supervisory law and possibilities in relation to digital transformation in product design must still be identified further and overcome. This also affects
  - the weighting between the costs for a more far-reaching differentiation of premiums and the associated benefit that can be achieved by doing so by avoiding an anti-selection;
  - the assessment about what room for manoeuvre exists on a permanent basis for the progression of the individual underwriting principle of equivalence and allows an associated ever more fine differentiation in premiums.

Technological neutrality does not exclude regulation

- The supervisor generally has a neutral positioning towards innovation and technological developments. The possibility is not however excluded of new regulations being published for certain innovations (e.g. in relation to “ethical” boundaries of digitalisation).

Product innovations require transparency

- Digitalisation not only heralds innovative products, but to some extent also brings more complex products. To counteract the customers’ increased need for information and to make customers aware about the information requirements for providers and sensitive thematic areas, the FMA must continue to push its consumer information.

Stimulating legal or socio-political debate in the case of the threat of financial exclusion

- In the insurance industry, individually calculable premiums may massively threaten the insurance principle of equalisation of risks: good risks may become cheaper to insure against, while in contrast bad risks would become more expensive to insure. In extreme cases, individual risk-adjusted premiums could become prohibitively high.
- Consequently the question arises about the extent of the existence of the danger in the future, that bad risks will no longer be insurable – with the threat therefore of partial market failure (Effects on financial inclusion and exclusion).

2.4 CONSULTATION ON PRODUCT DESIGN

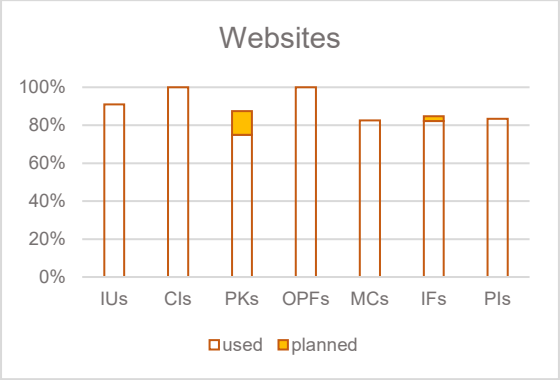
- From your perspective, what duties should the FMA perform in relation to the protection of investors, insured persons and creditors with regard to “digital” financial products?
- What specific regulatory standards are still necessary due to the digitalisation of the financial sector?
- From your perspective, what impediments exist in Austria that hamper the development of new digital financial products?
- Do you share the FMA’s assessment about the opportunities and threats associated with their impact on banking or insurance?
- What specific positive and negative developments regarding “digital” financial products can be observed from your perspective?

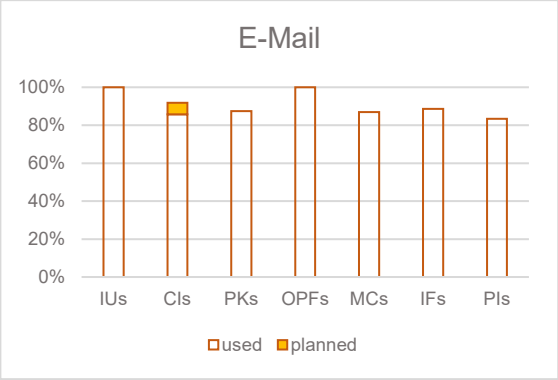
3 SALES / CUSTOMER INTERFACE

3.1 TRENDS OBSERVED IN THE VARIOUS CHANNELS OF COMMUNICATION

As shown in conjunction with the strategies, the improvement of and intensifying of customer contact is one of the main drivers of digitalisation in the Austrian financial market. In the competition to conclude contracts, it is advantageous to be able to contact customers over as many potential channels as possible, while electronic customer contact is intended to increase efficiency and contribute towards stronger customer retention. Accordingly, many supervised entities have invested in extending their digital communications channels. Ultimately, the pandemic has also accelerated digitalisation. The trends in this regard can be summarised as follows:

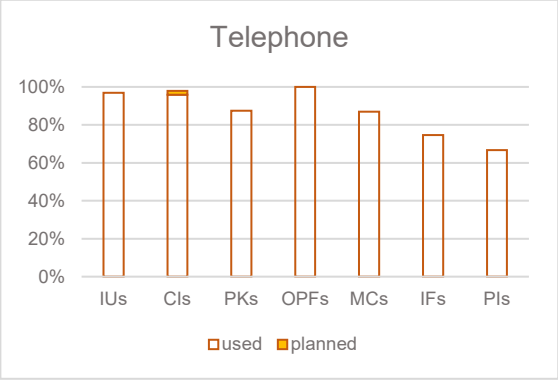
Classical channels of communication like websites, e-mail and telephone continue to belong to the standard repertoire of all sectors of the financial market.



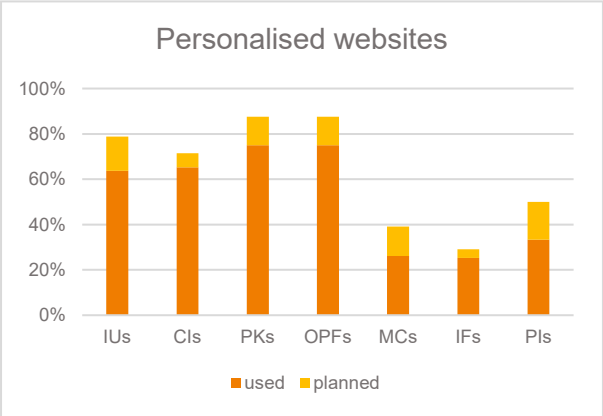


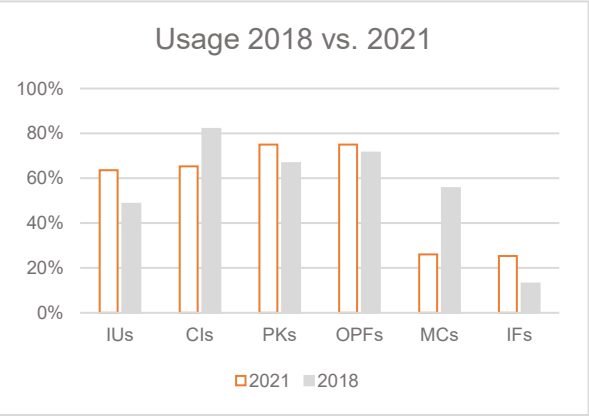
Exceptions only arise based on the entities' business models.

In a few cases (such as in the case of VASPs) such channels are consciously not used.



Personalised websites (e.g. customer portals) are already showing a high level of proliferation, and are intended to be even more frequently used in all sectors in the coming three years:

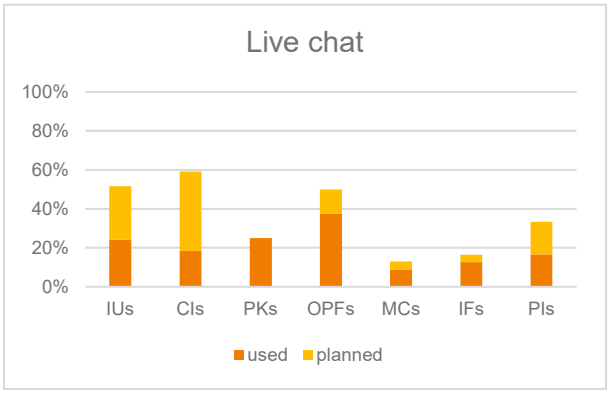


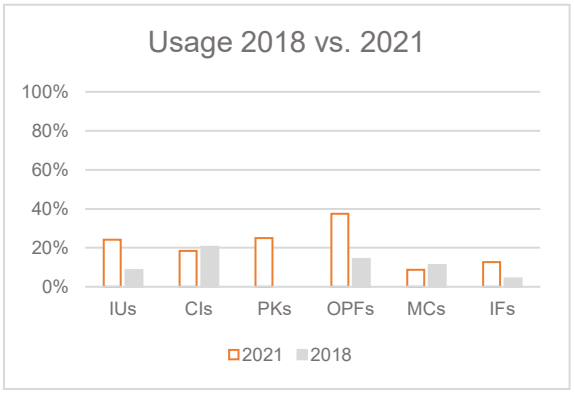


Usage of and the general trend about the usage of customer portals varies strongly by financial market sector. The proliferation of personalised websites has increased significantly among IUs (currently 64%) and OPFs (100%). Digital customer portals may lead to an increased interaction by the customer with the company. The possibility to look at a contract and see how it is performing or to make changes directly at any time may increase attractiveness for customers. Declining trends can be observed for CIs and MCs, although this will be partly due to the expansion of the group of participants in the 2021 edition of the Digitisation Study in these two sectors to include special institutions.

It should be borne in mind that setting up customer portals is a comparatively complicated means of communication. Such a solution must be implemented internally or externally by software developers and then tailored to the entity's website and IT infrastructure. From an IT security perspective it must be well secured, since it constitutes a potential source of attack and must be constantly updated and maintained. Since portals are not deployable for every business model, it is therefore easily explainable that this tool will not establish itself in every entity, or in individual cases in hand prototypes will also be discontinued.

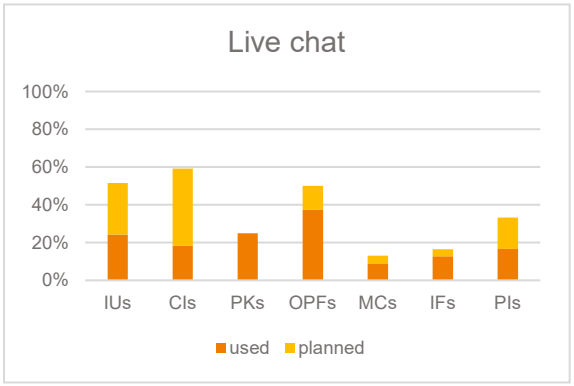
Live chat solutions, where text messages are exchanged with customers in real time have been used increasingly frequently in the last three years, and are expected to be rolled out further in the coming three years. In 2024, around half of IUs, CIs and OPFs want to use them.

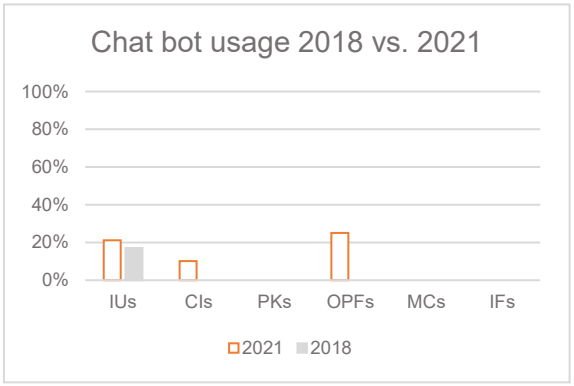




In 2018, this option was only used by a few entities and since then has established itself in a number of IUs, PKs and OPFs. IUs and CIs are planning a concerted further roll-out in the next three years. However, this claim was also stated in a number of cases by IUs and CIs three years ago. That many entities have plans in this regard, but that they have only been implemented by a few during the course of the COVID-19 pandemic may indicate that while added value is seen in live chat tools, they are not however given such a high priority for implements as other technologies.

Chatbots were only used in the insurance sector in 2018. Using the live chat option, the potential also increases to assist customer communication by automated means using chatbots:





According to a study conducted in Austria, Germany and Switzerland in 2021 on chatbots[19], 63 % of those surveyed responded that they had already interacted with a chatbot. In doing so, they prefer to type rather than speak, i.e. the interaction was more frequently with a chatbot than with a voicebot. From the user's perspective, reachability and rapid, uncomplicated assistance was viewed positively. The experiences to date of users with bots have been predominant positive ones. One in five could imagine completely concluding a contract – from pre-advice through to the purchasing process – via a chatbot.

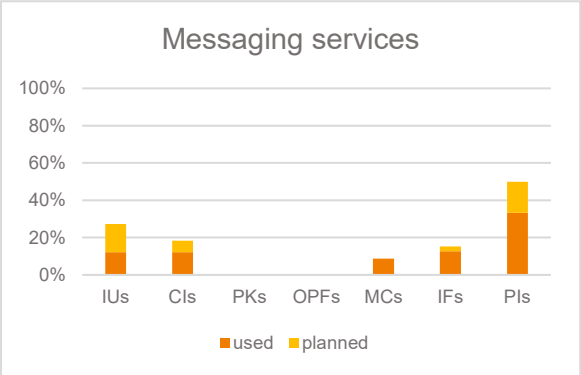
[19] *https://page.aiaibot.com/de/chatbot-studie*.

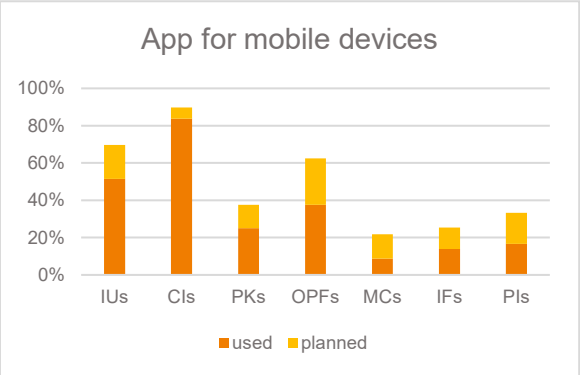
As was the case with the live chat tools, IUs and CIs are also planning to use chatbots more strongly in the future. Several conclusions can be drawn from this:

- A certain degree of potential is seen for chatbots, although their operational uptake is currently not occurring as quickly as was originally planned.
- As was the case with live chat tools, from the use of which a chatbot depends, their implementation does not appear to be the highest priority.
- Most entities that plan to make use of live chat tools, are simultaneously planning to automate them using chatbots. The added value of chat programs therefore depends strongly on the extent to which they can be automated.

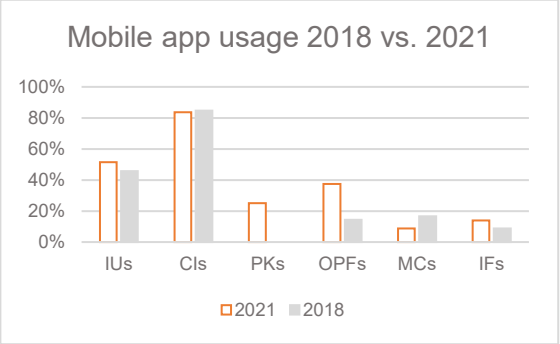
Where chatbots are used to advise customers, legal challenges might also arise. Due to the restrictions of the technology itself and this additional aspect, future implementations in this field depend very much on which entities succeed in finding clearly delineated and definable use cases for the bot.

Communication via mobile devices by means of **messaging services** or other apps were already relatively broadly deployed by IUs and CIs in 2018. PKs and OPFs in particular have subsequently followed suit:

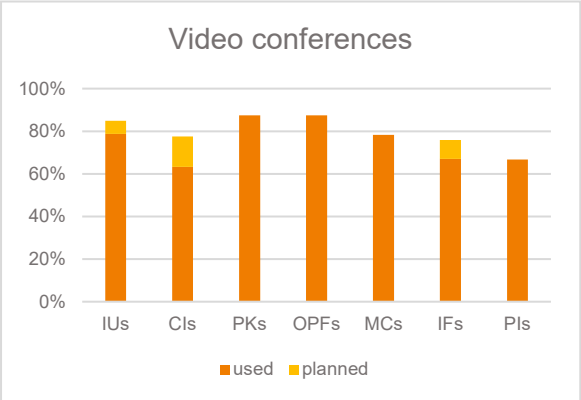


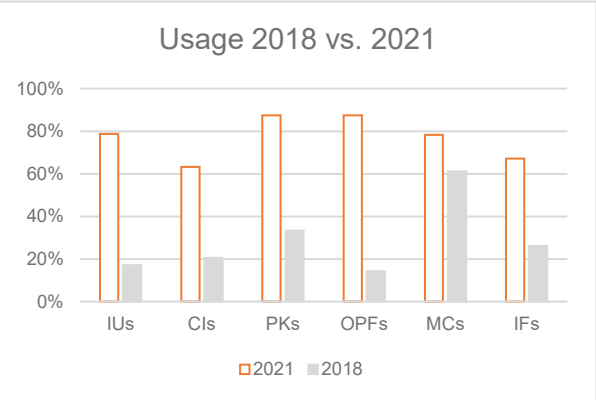


Since the usage of apps has not increased noticeably at IUs and CIs during the period of the COVID-19 pandemic, it may be assumed that most entities in these sectors view there to be an added value in such communications channels are already making use of them.
PKs and OPFs have not yet reached this peak, so it is therefore expected that the usage of messaging services and mobile apps will still increase in the future.

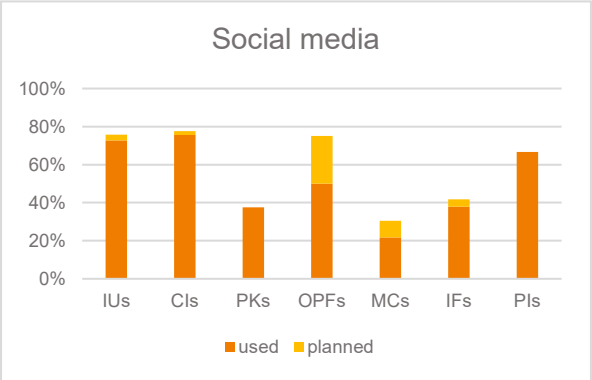


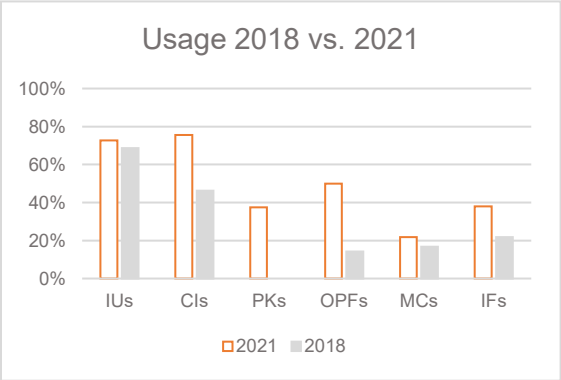
In contrast, no clear trend has emerged yet for MCs and IFs. While several entities are planning to make use of such tools, there has been little movement in this regard in the last three years. In the short- to medium-term, mobile communications channels will therefore not be developed across the board by these sectors.
The strongest upwards tend in the last three years in all sectors has been witness by **video conferencing**. During lockdowns, in many cases, they have replaced direct customer contact. While other channels of communication are often new approaches that are chosen in addition to address specific customer segments better, or for conduct processes more efficiently, video conferences were used to keep day-to-day business up and running. Since such tools have established themselves for both internal and external communication, it is to be assumed that they will continue to be used to a similar extent.





Social media platforms are also clearly playing a larger role in relation to customer communications than they did three years ago:

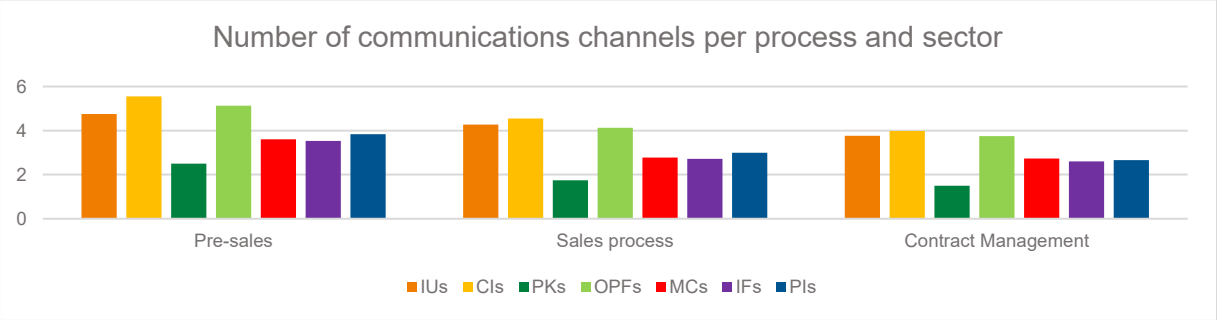




- With the exception of the insurance sector, which was already making substantial used of social media in 2018, the use of such networks by entities has increased significantly. Apart from plans among OPFs and MCs a certain saturation effect already appears to have occurred, and in the medium term the level of use is stagnating at a high level.
- Social media is in particular being used for the acquisition of new customers (see Section 3.2). A driver of the strongly increased presence of entities in the relevant networks may potentially be attributable back to a certain competitive pressure. A presence on social media nowadays is considered as standard for many entities. No entity wants to be one of the few that are not represented, especially since the effort required for maintaining the social media accounts as a rule is manageable.

3.2 DIGITAL COMMUNICATION IN BUSINESS PROCESSES

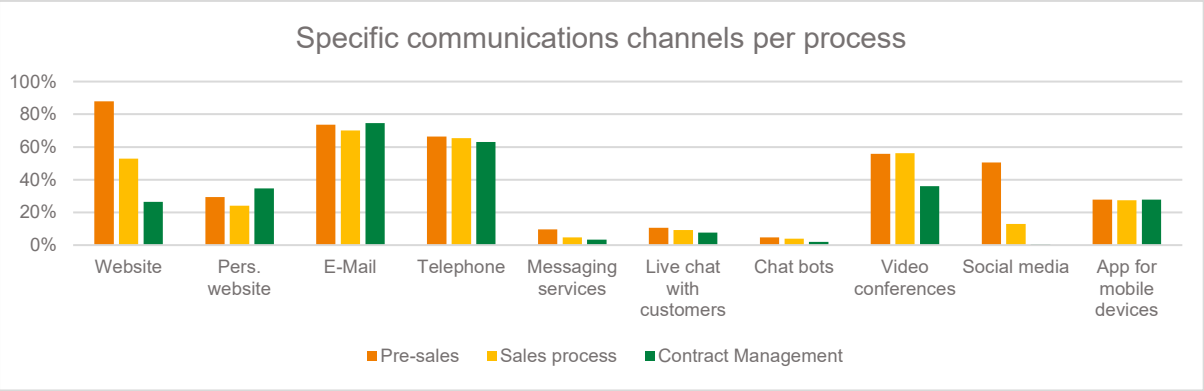
Generally, entities make more use of **means of communication in the pre-sales area than in the sale process itself**, with it being used least in relation to contract management. This may point to a certain competitive pressure in acquiring new customers, however, means of communication also differ from one another with regard to their inherent properties, and are variably well-suited for various purposes.



In the area of communications channels that are used, there are clear differences arising from the technical characteristics of the means of communication.

- Websites and social media networks are particularly suitable for imparting a limited amount of information to a broad target audience quickly, which naturally predestines them for the area of pre-sales.
- In contrast, personalised websites (customer portals) are particularly well-suited for the administration of existing contractual relationships.

The following illustrations shows the proportion of usage of the channels of communication by process aggregated for all financial market segments:



Overall, entities use more channels for pre-sales or marketing than for contacting existing customers, although such channels usually require less effort to operate.

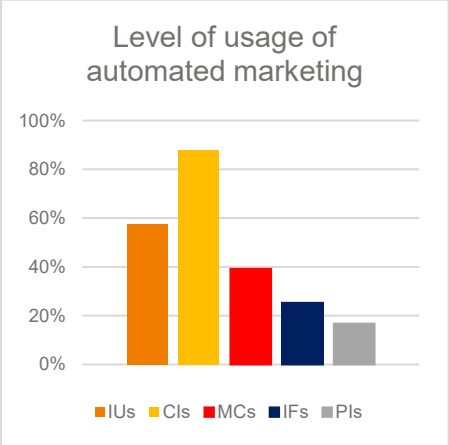
The sales process is of particular relevance for the FMA, as depending on the relevant financial market segment, special rules under supervisory law must be observed.

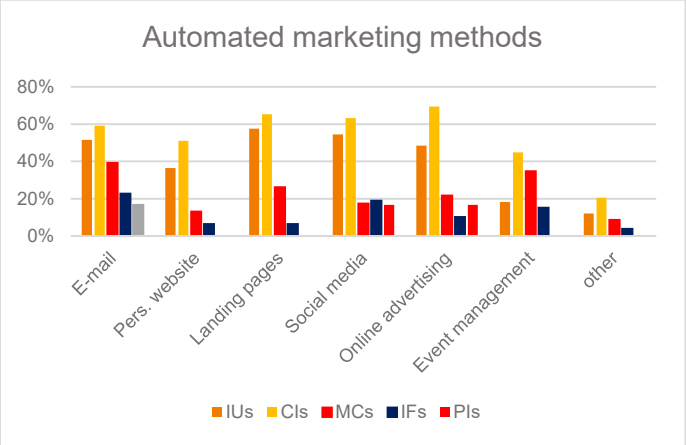
Despite their varying weightings, practically all of the channels that were asked about are used in all processes, which highlights the necessity for the supervisor to keep up with new technologies and to apply existing rules in a dynamic context.

3.3 AUTOMATED MARKETING

Software-based methods for automating sales and marketing processes are being used increasingly more frequently by supervised entities. Starting with e-mail newsletters through to advertising campaigns in search engines and social media there are numerous possibility to increase the range of your own marketing – and therefore the number of potential new customers – and to make the advertising process more efficient. Entities were specifically asked about their use of automated marketing processes in the following categories (no data was collected in the sectors PKs, OPFs and MIs, due to business models not being based on direct retail marketing):

- E-mail campaigns (automated newsletters etc.)
- Personalised websites (personalised offering in the customer portal)
- Personalised landing pages based on customer-behaviour
- Social media (targeted advertising based on customer data)
- Online advertising (campaigns in search machines etc.)
- Event management (automated invitations/reminders)





Automated marketing is primarily used by CIs (88%), followed by IUs (58%) and MCs (39%). IFs (25%) and PIs (17%) also partially used this form of marketing.

Similarly as in the area of pre-sales channels of communication, different methods are used in parallel in entities in order to achieve as broad reach as possible. The most frequently automated marketing methods in this case are **online advertising** (e.g. Google-Ads as part of advertising

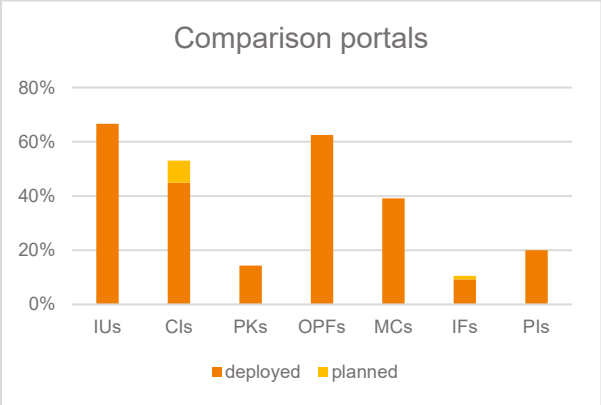
campaigns), **landing pages** (web pages that relate to a campaign), **social media** (e.g. advertising with tracking options via YouTube, Instagram, Facebook or similar services) and **e-mail** (e.g. newsletters, initial information about product innovations, birthday wishes).

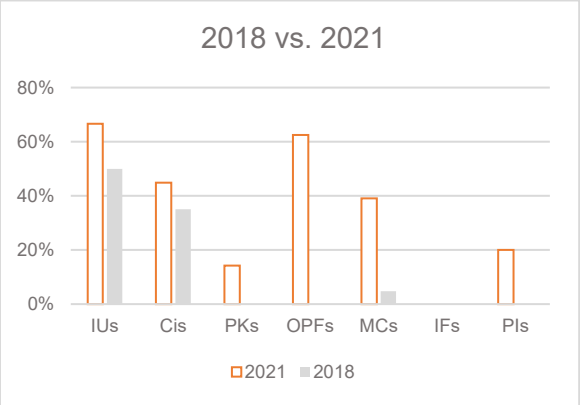
There is a somewhat lesser focus on **personalised web pages** (e.g. For directly addressing customers with bonus offers) or **event management** (e.g. annual customer events). In addition to the categories that could be selected, responses to the survey mention that in game ads, premium calculators with the option to conclude a policy online as well as SMSes reminding customers about appointments or sending them birthday greetings, to achieve greater reach as well as to create customer loyalty.

Due to these methods already being decidedly widespread among CIs, it is expected that IUs and AMCs in particular will continue to extend the possibilities for automated marketing in the coming years. Especially in the pre-sales area, recognisable competitive pressure exists within the sectors, thereby strongly incentivising making use of new marketing methods as soon as they have gained a certain spread among the peers.

3.4 COMPARISON PORTALS

Comparison portals have increased in significance, with comparison portals having emerged across all sectors as a pre-sales tool, whereas in 2018 only IUs and CIs listed their products on such portals.

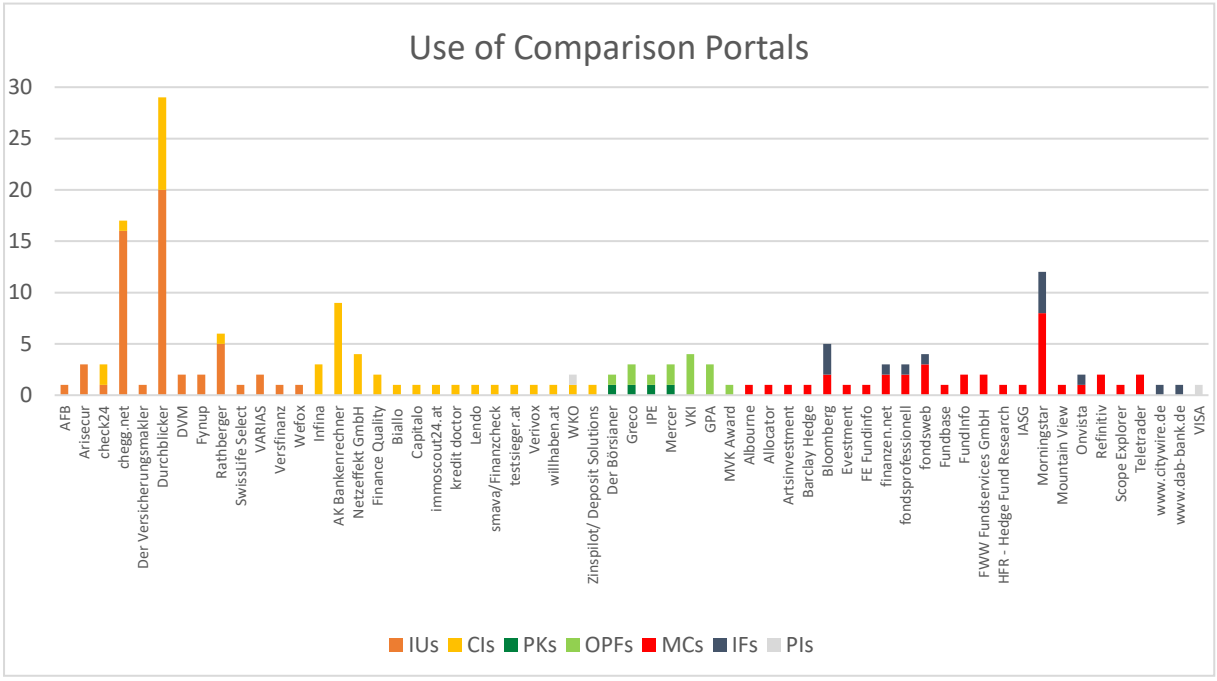




A essential factor behind this is potentially the intense competition between entities in the area of pre-sales. Potential customers and service providers are able to quickly inform themselves about services and products using comparison portals and in the course of this are often already close to concluding a contract. The pressure of listing your own products in comparison portals is particularly large in the case that competitors are already doing so.

- IUs focus in particular in terms of comparison portals on “Durchblicker.at”, “chegg.net” and “Rathberger”.

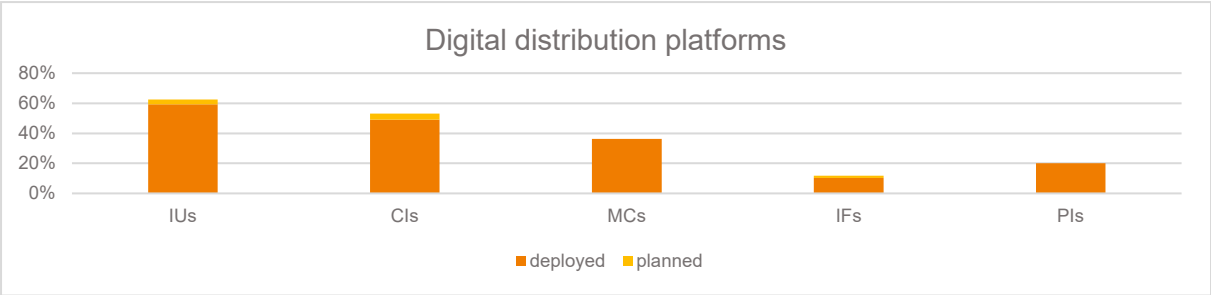
- CIs are predominantly also active on “Durchblicker.at” and the Austrian Chamber of Labour’s “Bankenrechner” comparison portal.
- PKs and OPFs are listed on the comparison portals of the VKI (consumer protection organisation) and the GPA (trade union for private salaried employees) as well as “Greco” or “Mercer”.
- For the sectors of MCs and IFs, financial information companies like Morningstar and Bloomberg play the largest role in terms of comparison options.



The FMA already analysed the practices of individual comparison portals in the Austrian insurance market in 2020 in the insurance sector, and issued an information brochure. The brochure provides practical tips about what to look out for in terms of how up-to-date the content is, the independence of portals, the brokerage commission, the ranking of the selected products and advice. A checklist contains hints about what to look out for prior to the conclusion of the contract.

3.5 DIGITAL DISTRIBUTION PLATFORMS

Digital transformation simplifies and promotes the use of digital distribution platforms. Digital distribution platforms are used to a similar extent as comparison portals (IUs 59%, CIs 49%, MCs 36%, IFs 10%, PIs 20%). Due to their conceptual proximity to comparison portals, a several development may be assumed here: on the one hand, it illustrates the advancement of digital development, especially in the distribution process; on the other hand, such developments also highlight the growing importance of co-operations and partnerships between supervised entities and digital service providers.



Supervised entities use numerous different distribution platforms. Across all sectors, however, by far the largest share of users is accounted for by "Durchblicker.at" and entities' proprietary web pages/customer portals. The following distribution platforms are most frequently used:

IUs	■ Durchblicker ■ Arisecur ■ chegg.net ■ Clark ■ fynup ■ Klickmal ■ Together
CIs	■ Durchblicker ■ Google ■ immoscout24 ■ Bing ■ Netzeffekt GmbH
MCs	■ Clearstream ■ Cominvest

Currently the proportion of sales through comparison portals and distribution platforms in most entities in percent is in the single digit percentage range or less. However, further growth may be expected in the next few years. As the use of comparison portals increases, the requirement for fairness and transparency of such providers also increases implicitly. The regulatory requirements

that apply in the individual segments of the financial market, should also be considered for such (comparatively new) forms of distribution.

3.6 SUMMARY AND ACTION AREAS FOR THE FMA

The FMA must be able to assess Implications under supervisory law observed for the digital technologies that to date have only been used scarcely or only used in a few sectors (comparison portals, social media, chat bots):

Three rough groups of technologies have emerged from the results of the survey:

- **Established means of communication** (e.g. websites, telephony, e-mail, video conferences, apps for mobile devices) already being used by a broad majority of the supervised entities.
- **Growth groups** (e.g. social media, comparison portals) have already achieved a certain degree of prevalence in the financial market, and will be used even more in the future. It therefore appears that such channel of communications will soon be considered as standard.
- **Marginal groups** (e.g. live chat, chat bots) are barely used, or are only used in a few sectors. Some undertakings are planning to introduce such technologies, and they will therefore within the foreseeable future play a more significant role.

Digital transformation requires a stable foundation and legal clarity

- A lack of legal clarity regarded its classification under supervisory law and the possibilities of practical implementation especially with regard to
    - The question of approval requirements within the electronic conclusion of contracts and electronic communication,
    - The evaluation of opportunities for influencing the ordering in a comparison portal (e.g. with regard to potential conflicts of interest) in 2020 the FMA already conducted analysis about the practices of comparison portals in the Austrian insurance sector and determined that the level of detail of the information requested from the user varies greatly),
    - The evaluation of which technologies satisfy the requirements for a durable medium or which requirements can be placed on fully or partially automated advice systems and advice algorithms.

The FMA should therefore work in these areas towards ensuring greater legal clarity and where applicable communicate its positions or expectations in order to minimise legal risks as far as possible and to create a level playing field.

3.7 CONSULTATION ON DISTRIBUTION

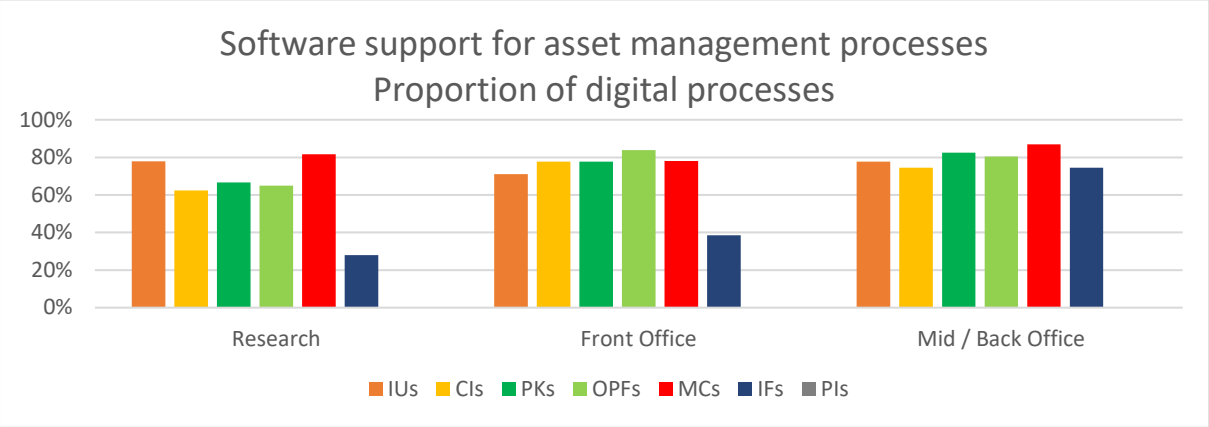
- What duties should the FMA perform with regard to the protection of investors, insured persons and creditors in relation to the digitalisation of the interfaces to the customers?
- In which form should such tasks be undertaken?
- What specific regulatory standards are still necessary due to the digitalisation of the financial sector?
- From your perspective, what 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?

4 ASSET MANAGEMENT

Digital information technologies have already penetrated into asset management for a long time. Digitalisation in asset management relates both to the IT systems of market participants as well as the financial instruments e.g. in the shape of new forms of investments or investment classes. To evaluate how the information technologies are taken into account in supervision and regulation of supervised entities, their deployment was investigated and analysed based on the individual steps in the investment process.

4.1 IT SYSTEMS IN ASSET MANAGEMENT

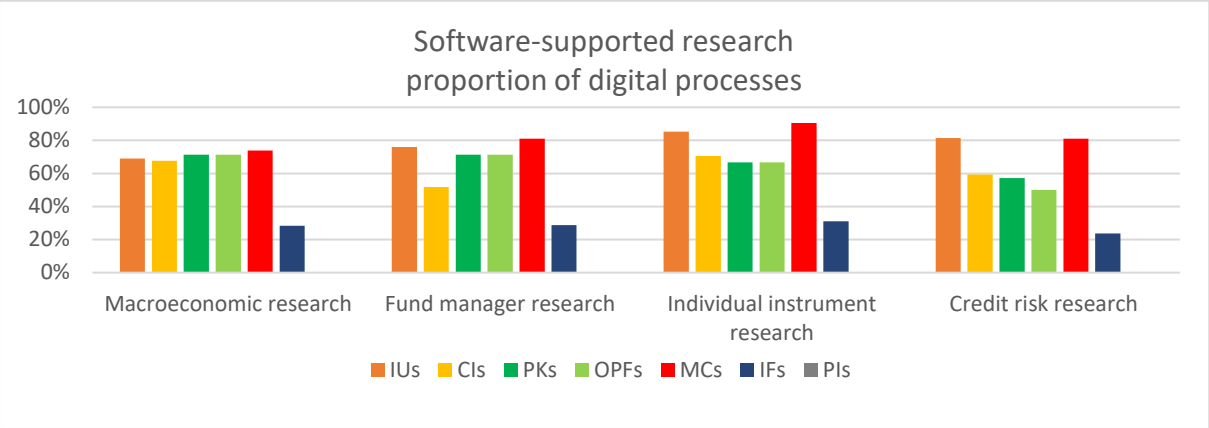
IT systems are deployed in practical all processes in asset management. The different shares of digital or non-digital processes in the individual sectors is affected by the sector-specific differences in business models.



In particular, the size of the company, the resources deployed, as well as the degree of centralisation of investment are relevant for the level of digitalisation in asset management processes. Regulatory requirements also play a role in this case.

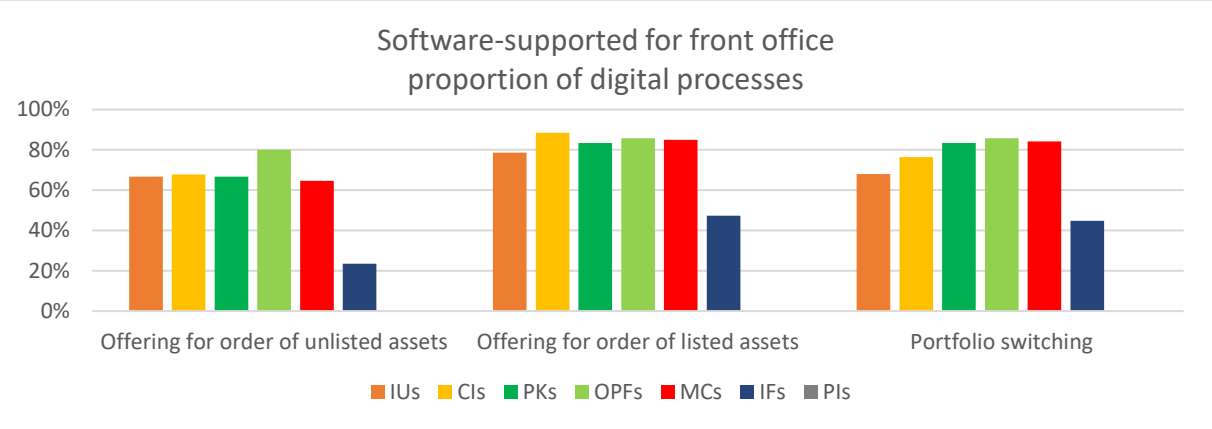
4.1.1 RESEARCH

Prior to every investment decision a comprehensive data analysis is performed, e.g. regarding the selection of external managers or investments in individual titles. There is also a large wealth of information to be evaluated in relation to ongoing due diligence (e.g. key balance sheet data, performance), documented and monitored.



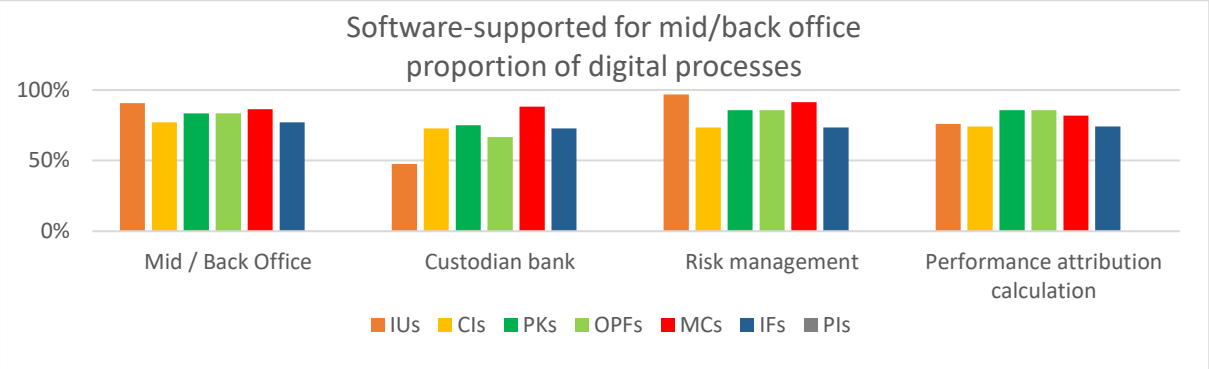
4.1.2 FRONT OFFICE

Following research conducted in relation to due diligence, the implementation of investment decisions takes place in portfolio management, with it being possible to differentiate between different procedural steps in relation to the use of IT systems:

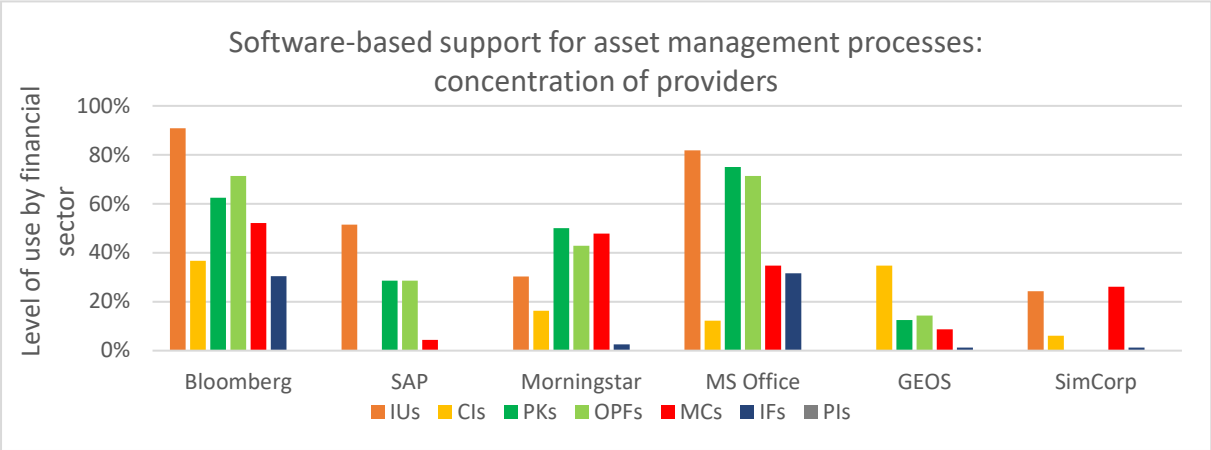


4.1.3 MID / BACK OFFICE

Once the investment decision has taken place and the order made, the securities orders are duly executed and books or the documentation in relation to unlisted assets stored accordingly. The mid and back office functions also include the interface to the custodian bank, ongoing risk management and performance attribution analysis.



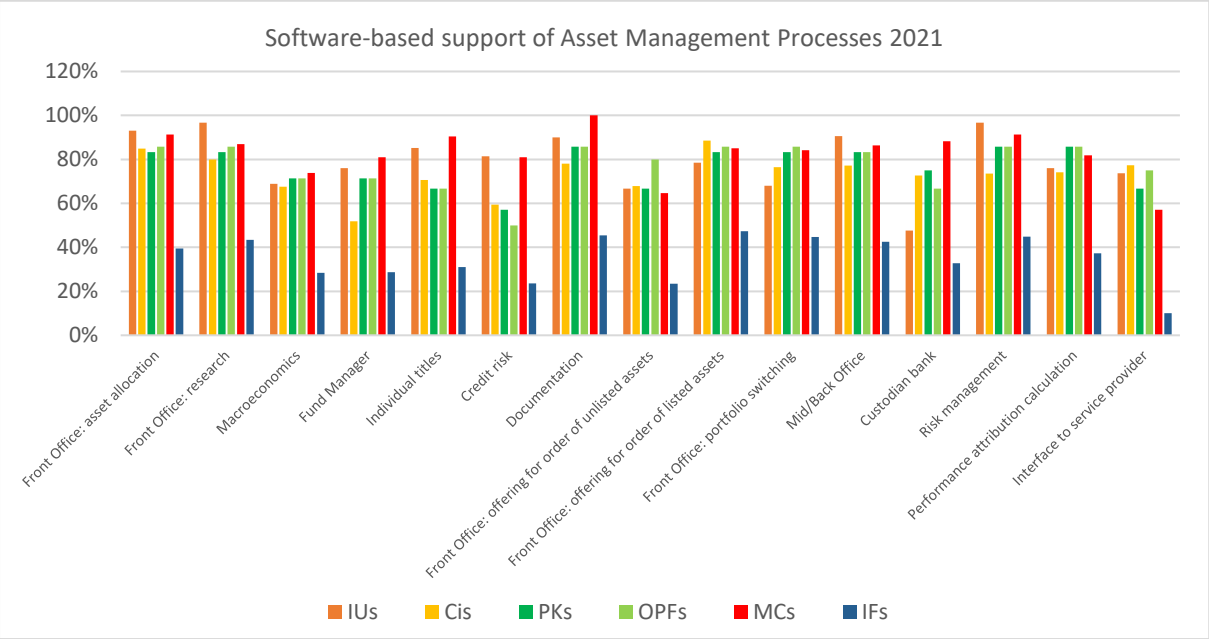
The following information and portfolio management systems are the mostly widely used ones in asset management: Bloomberg, SAP, Morningstar, MS Office, GEOS (SDS) and SimCorp:



4.1.4 SOFTWARE-BASED SUPPORT FOR ASSET MANAGEMENT PROCESSES

The comparison of the usage data about software solutions in the supervised entities' asset management processes against those from 2018 shows that the share of software-based support has stagnated around the same level or even fallen slightly depending on the category of the entity and the scope of application.

- IUs have increased software-based support for asset management processes slightly in some areas (research, documentation, offering for order of unlisted assets, custodian banking, and performance attributes) whereas it has remained at the approximately the same level in the remaining parts of the process.
- CIs have extended software-based support in most sub-processes and have comparatively achieved the largest increase.
- With the exception of the sub-processes "documentation of investment decisions" and "custodian banking" the share of software-based processes have fallen slightly in the area of PKs.
- In the case of MCs and OPFs, the proportion was already high in 2018, with a further increase only being determined in isolated cases, for example in the area of documentation. The trend in most areas, however, is a slight decrease. However, a change in the composition and number of entities surveyed must be taken into account compared to 2018.
- In the case of IFs, software-based assistance has also fallen proportionally in the majority of the sub-processes (with the exceptions being "credit risk" and offering for order of unlisted assets).



4.2 NEW INVESTMENT FORMS AND CRYPTO ASSETS

In light of the dynamic in the area of crypto assets and taking into consideration influencing factors such as increasing cost pressure, the low interest environment and the search for yield-bearing investments, the issue arises to what extent new forms of investments are being used. The current study shows that the supervised entities continue to remain reserved regarding the use of blockchain technology and services in virtual currencies:

As a % of the total portfolio		*IUs*	*CIs*	*PKs*	*OPFs*	*MCs*	*IFs*
Participation in FinTechs	Direct current	<0.1 / <1	0.02 – 0.2	-	-	-	-
	planned	-	-	-	-	-	-
	Indirect current	0.0005 – <1	0.17	-	-	-	-
	planned	-	-	-	0.015	-	-
Crypto assets	Direct current	-	0 – 0.036	-	-	-	-
	planned	-	-	-	-	-	-
	Indirect current	-	-	-	-	-	-
	planned	-	0.012	-	-	0.0157	0.001 - 2

- No IU provides services in virtual currencies. From an investment perspective, five IUs are planning a minor participations in FinTechs/InsurTechs, of which three already hold participations of less than 1% of the total portfolio in own shares, and are not planning any notable increase. Indirect investments in crypto assets through funds, of 0.0003%, also only make up a negligible proportion and are generally concentrated in ETFs that do not invest in blockchain technology itself, but instead merely grant access to this ecosystem.
- Only one CI surveyed currently indirectly invests in crypto assets (0.012% of portfolio) and is planning to extent its investments in this area (0.036-0.055%). Three CIs hold participations in FinTechs/InsurTechs of around 0.02-0.2% of the total portfolio.
- PKs are even more reserved in this area: none of the PKs provided services in connection with virtual currencies or plans to make direct investments in new investment forms. Indirect fund investments in assets in the crypto environment are low, and are restricted to hardware and software providers in the blockchain environment.
- Virtual currencies are currently also not actively used in OPFs. One OPF currently has a proportion of 0.015% of the portfolio indirectly invested in FinTechs/InsurTechs.
- One supervised MC currently has invested in crypto assets (approx. 0.015% of the total portfolio, owned by third parties). In this sector, there are also no services of any kind provided in connection with virtual currencies.
- One IF is planning a low (0-1% of portfolio) in crypto assets, with two IFs having invested to a low extent in crypto assets. A further IF is planning an investment in FinTechs/InsurTechs owned by third parties (customer deposits).
- Two IFs provide services in virtual currencies. Furthermore, one entity has a participation in crypto assets to the extent of 0.5% of the portfolio.

4.3 SUMMARY AND ACTION AREAS FOR THE FMA

In an environment with a high level of IT penetration automation processes are gaining in significance

- There is generally a strong penetration of IT systems among the supervised entities in the asset management sector. This is particularly strongly prevalent in the case of insurance undertakings, management companies, investment firms and occupational provision funds.
- Software-based automation processes are still increasingly gaining in terms of significance. Regarding cost pressure for asset managers, process automation by means of Robotic Process Automation (RPA) is also becoming ever more attractive for asset management companies. The greatest potential in efficiency terms for RPAs remains in mid and back office areas.

Monitoring the Expansion of Alternative Technologies:

It is not possible to detect a strong trend regarding the expansion of alternative technologies, such as AI, Deep Learning and Machine Learning. Such results do not mean that new technologies do not play any role in asset management, but special software applications are already being deployed throughout the entire process chain.

Manual manipulation of data constitutes a potential source of errors. Therefore the level of digitalisation should also be included in the evaluation of the observance of the prudent person principle in investment.

- How the IT systems deployed in asset management are fixed within the company's internal IT landscape, and whether or by whom a review is conducted prior to the execution of an order, is also significance in relation to the internal investment limits.
- As a rule, electronic data capture is also a condition of the capturing of assets in the risk management.

As a rule, the financial market data information systems deployed and the interfaces both externally and internally within the undertakings in some sectors are also decisive with regard to the correct calculation of own funds requirements.

- A main problem in relation to the valuation of the assets are exchange-listed, but nonetheless not particularly liquid, investments in bonds. Although the market value identified in financial market data systems does not necessarily reflect the actual realisable disposal value, alternative valuation methods are largely also based on market data (e.g. interest rates and interest rate curves, implied volatilities).

- Since asset valuation directly influences the solvency situation and as bonds are the most important asset class in a few sectors, financial market data information systems are particularly important[20]. The following issues should be considered in the inspections by the supervisory authority.
  - What financial market data information systems are used?
  - How are the software licences defined?
  - How and in which IT systems are alternative valuation methods deployed? For which asset classes?
  - What adjustments are made "manually" to market data in the valuation for the solvency balance?
  - How are the interfaces with external service providers designed?

Monitoring of investments in new investment forms:

- One of the most significant issues for new investment forms is their allocation in the balance sheet in terms of their classification as assets. The high volatility of virtual currencies and in certain circumstances their prompt settlement provide circumstantial evidence for being allocated as short-term assets.
- In relation to investment in blockchain issuances clarity should be obtained to what extent such issuances fulfil requirements in relation to their location.
- With regard to the frequently indirect form of investment in investment funds it must be clarified, whether and how institutional investors invest in funds with new investment forms and which investment processes and risk management requirements are applied for this purpose.
- Since the valuations of growth companies are often priced in accordance with the high growth rates, the selected valuation approaches for FinTech start-ups may be applied as an element for the valuation of the investment with regard to the prudent person principle.

[20] *Article 10 of the Level 2 Regulation (EU) 2015/35, in 2017 more than a quarter of all IU assets were valued using alternative valuation methods.*

4.4 CONSULTATION ON ASSET MANAGEMENT

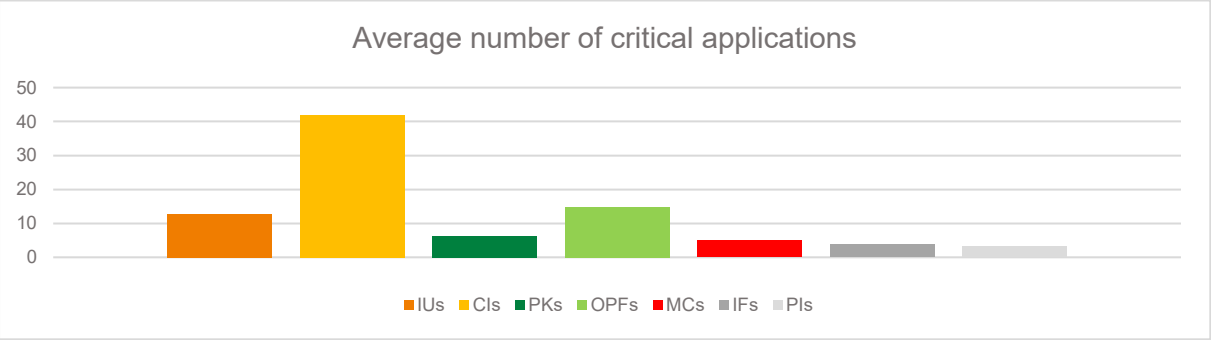
- From your perspective, what duties should the FMA perform with regard to digitalisation in asset management?
- What specific regulatory standards are still necessary due to the digitalisation of the financial sector?
- What impediments exist in Austria for automating asset management processes and simplifying the expansion of alternative technologies such as AI, deep learning and machine learning?
- What specific positive as well as negative developments regarding the digitalisation of investment can be observed?

5 IT INFRASTRUCTURE

5.1 IT SYSTEMS LANDSCAPE IN THE AUSTRIAN FINANCIAL MARKET

The players in the Austrian Financial Market use **more than 3,000** (3,087) **IT applications** to support their critical business.

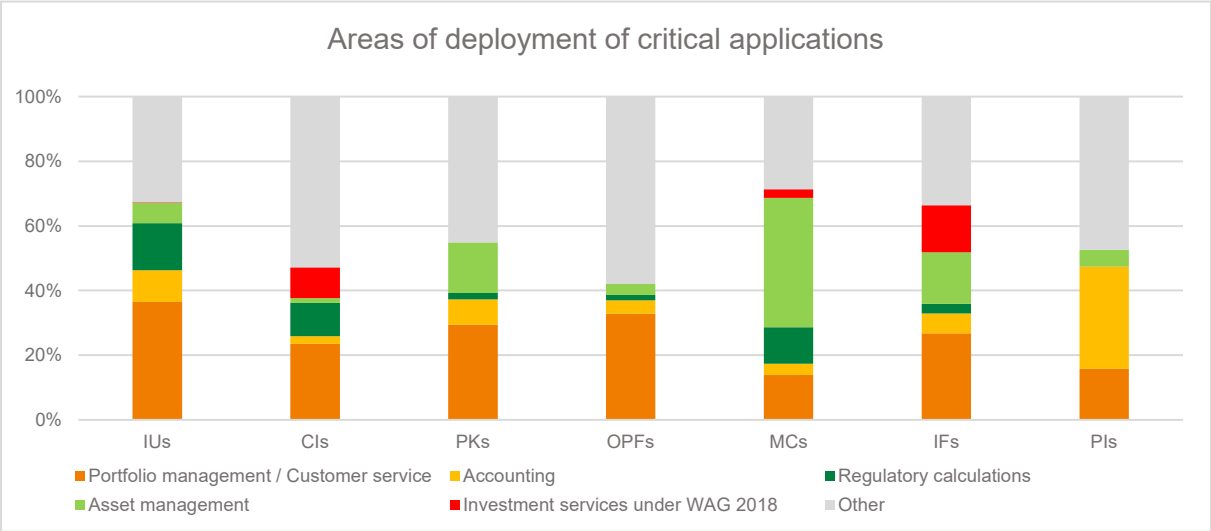
With 42 individual systems on average, in the area of end user applications, the most critical applications by a considerable margin are used **in CIs**, with as many as several hundred applications being used in large institutions in some cases. The underlying software infrastructure behind the applications (e.g. operating systems, virtualisation solutions) as well as applications that are not critical for the core business are not considered.



The business model as well as the entity's IT strategy in particular are **drivers** for the number of applications deployed:

- A few of the financial market sectors, such as the banking sector, inherently cover a comparably broad field of activities in accordance with their **business model**, while others are more strongly specialised, as is the case for example of out-and-out payment service providers or VASPs. In addition, depending on their business segment, special regulatory conditions must be observed, such as the prevention of money laundering or terrorist financing.
- The **IT strategy** with regard to the system landscape, irrespective of whether planned or "grown" is also reflected in the outcomes. In a few entities, parts of their business activities are outsourced, thereby reducing the number of applications that are used in-house. Furthermore, a low number of applications may point to the use of strongly integrated, multifunctional applications, while other entities support their processes with a large number of smaller applications and the relevant interfaces to one another.

The difference in business models is also reflected in the **areas of deployment** of the IT applications used:



- Systems for direct **portfolio management or customer advice** make up between 14% (MCs) and 37% (IUs) of the critical applications depending on the sector.
- **Asset Management** is an area, especially in the case of MCs (40%) as well as PKs and IFs (16% each), in which a significant proportion of the critical software solutions are deployed.
- Applications for **regulatory calculations** constitute a meaningful proportion of critical software solutions in particular in the case of IUs (15%), MCs (11%) and CIs (10%).

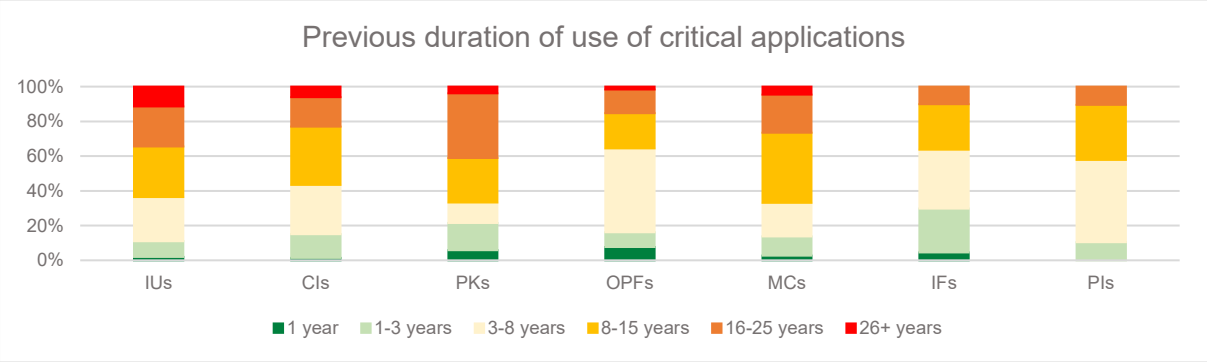
Entities' "miscellaneous" applications cover collaboration systems (simultaneous editing of documents), communications systems, money laundering checks/KYC, fraud checks, bank transaction systems, document management systems, and personnel management.

5.2 LIFECYCLE OF THE DEPLOYED IT SYSTEMS

The future sustainability of the IT infrastructure in the Austrian financial market depends on several factors. One of them is the **operating life of the IT systems used.** An out-of-date IT landscape

- is a source of **operational risks** (maintenance licences expire, new requirements become increasingly difficult to meet, while key employments leaving the company or retiring reduces the available know how about old software),
- may be particularly vulnerable with regard to cyber risks,
- cause **increased costs** for maintenance, further development and potential replacement, and
- sometimes requires relatively **complex software projects** to replace them.

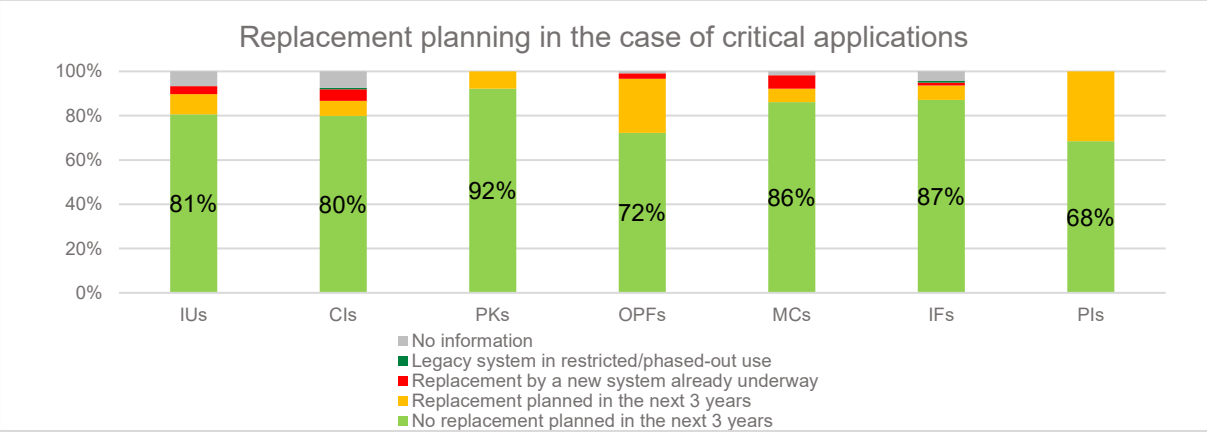
In most sectors of the financial market, IT applications are sometimes used for decades.



- In **IUs** approximately 34% of the applications have been in use for at least 16 years, with 11% even being used for 26 years.
- **CIs** have the second highest number proportion (6%) of systems that have been in use for 26+ years, while 17% of systems have been in use for between 16 and 25 years.
- In the case of **PKs** on the one hand, 41% is a relatively high proportion of systems that have been in use for 16+ years, while on the other hand 22% of the critical applications were only commissioned within the last three years.
- The software landscape of **OPFs** was renewed comparatively more frequently, with approx. 64% of the critical applications having been deployed for 8 years or shorter.
- In the case of **MCs** 27% of the critical applications have been deployed for 16+ years, while 19% of the applications have been deployed for between 3 and 8 years.

- **VASP**s are a segment of the financial market that overall are relatively young, a fact that is also reflected by the length of use of the software (75% used for 3 years or shorter).
- **IFs** have put a relatively high proportion of their critical applications, 30%, into operation within the last three years, while only 10% of the applications are older than 16 years old, and none are older than 26 years old.
- Software solutions with a very balanced age structure are being used by **PIs**: only 11% of the critical applications have been in operation for more than 16 years, with the same amount operational for under 3 years.

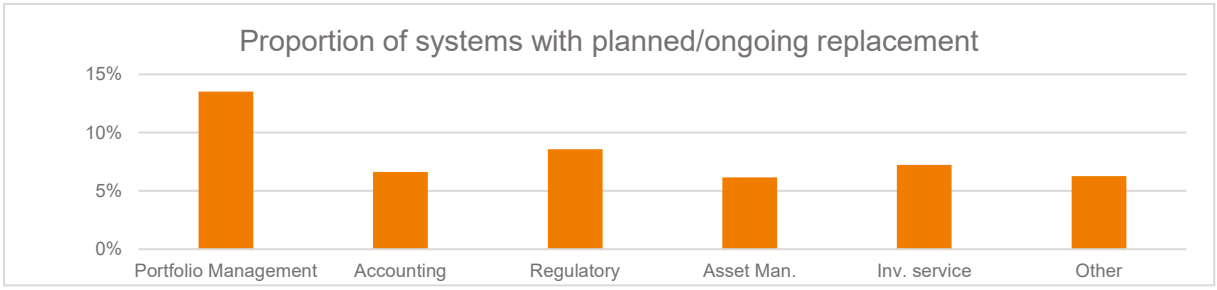
The life-cycle status of critical applications shall not however be allowed to be reduced to the out-and-out age of the systems deployed. The FMA has therefore also investigated **entities' replacement planning** for the individual systems. From this, a significantly more homogeneous picture emerges between the sectors, and **a clear tendency emerges to also use the available systems in the future.** In most financial market sectors, for 80% or more of the critical applications there is no planned replacement for at least the next three years. The only exceptions are among **OPFs** and **PIs** where the corresponding ratios are 72% and 68% respectively.



On this basis, it is possible to perform a **comparison between the introduction of systems that were conducted in the last three years** and the planned replacement of systems in the next three years, and in this way to deduce a rough indicator of how stable the system landscape it, and whether large overhauls have occurred or are planned:

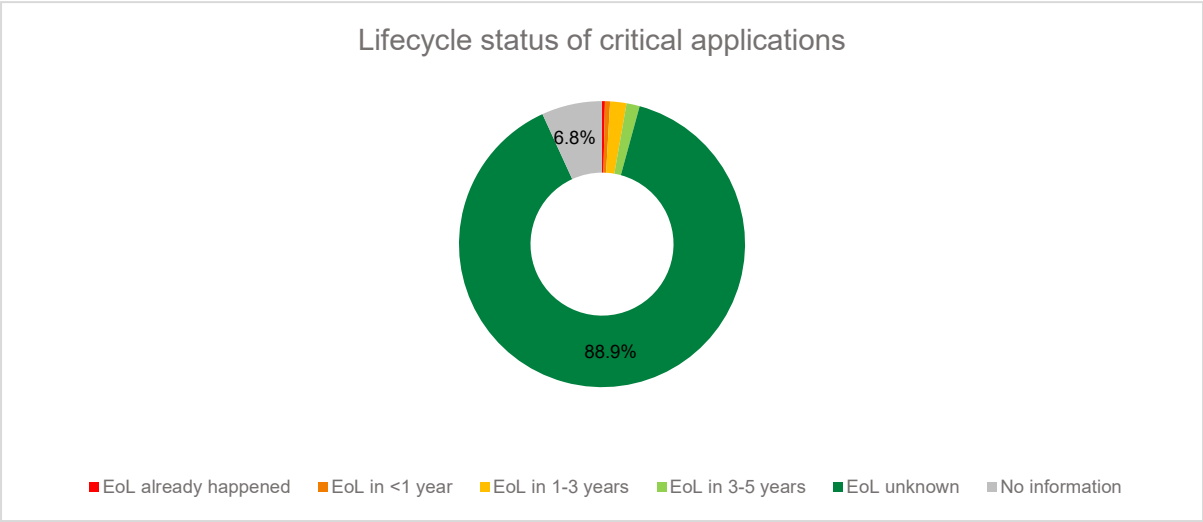
- In the case of **IUs, CIs, MCs** and **MIs** the number of applications that were introduced during the last three years roughly match the planned innovations during the next three years; this is an indicator for there being a relatively stable IT landscape in these sectors.
- **PKs** and **IFs** as planning significantly fewer system renewals in the next few years than they had already implemented in recent years, which is, among other things, a sign that there has been increased investment in new systems in these sectors that are now expected to remain in operation for a longer period of time.
- Similarly, **VASPs** have only set up their entire IT in the last few years and are not currently planning to renew their very young application landscape.
- In contrast, **OPFs** and **PI**s are planning to make significantly more renewals within three years than were made in the previous corresponding period, which indicated that a planned modernisation process is afoot for many core systems.

Proportion of critical applications by area of deployment, for which replacement is planned or ongoing:



On average, about 7% of the critical applications are currently in the process of being replaced. Only in the area of portfolio management or customer care is a renewal planned for about 14% of the applications. In the overall context of the findings of the study, this may be due to the fact, especially in this area that integration with new concepts (mobile applications, customer portals ...) is an important driver. Other application areas, such as accounting, on the other hand, are subject to much more stable requirements.

Ultimately, the **End-of-Life** date (EoL) of critical applications is relevant for assessing the future viability of IT systems. This refers to a point in time specified by the manufacturer/licensor of an application after which no further development of maintenance will take place. This therefore becomes a critical indicator for IT security and the adaptability of applications to new requirements. Usually, both are no longer given once EoL has occurred, although continued operation can be considered in certain cases and with the inclusion of additional security measures.



- In total, for approx. 89% of the critical applications there is no explicit end of support in sight. There are no strong deviations between the sectors of the financial market.
- For 0.3% of applications, EoL has already happened, and for 0.6% it is expected within a year.
- For 6.8% of applications there is no set EoL, so in this case a degree of uncertainty remains.

The consideration of the End-of-Life date for the critical IT systems used is important, since it should also be considered when using relatively old applications that provided they are maintained and developed further that they may continue to perform their purpose across decades.

Replacement planning and the proportion of software that may be considered as obsolete based on its EoL status **do not provide any indications of a systemic problem** in the financial sector. In a few sectors, measures were increasingly taken in recent years to renew applications, with some measures currently ongoing. Overall, the continuous renewal and maintenance of systems is keeping pace with their obsolescence.

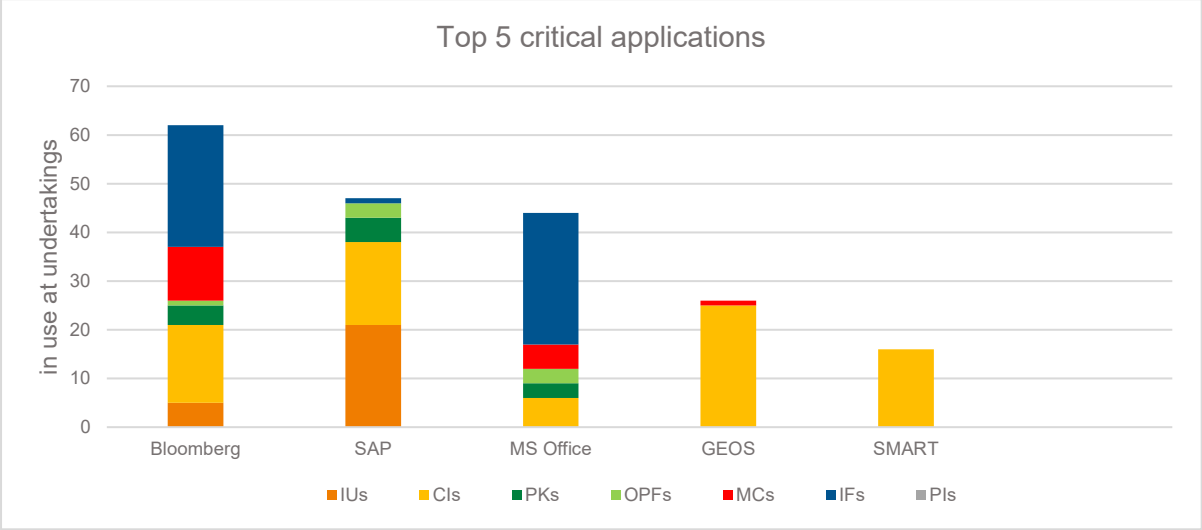
5.3 CONCENTRATIONS OF APPLICATIONS USED

There is a high diversity of systems across the market, but also within companies, also with regard to the large number of authoritative IT applications. Both proprietary software developments, but increasingly off-the-shelf solutions, are being used.

By deploying solutions from the large providers the software landscape for covering standard processes overall is becoming more harmonised.

The potential loss in flexibility for non-entity-specific applications is often accepted, since products from external providers have predefined data interfaces and cover several areas in the entity. This trend is also being demonstrated by the increased deployment of cloud services.

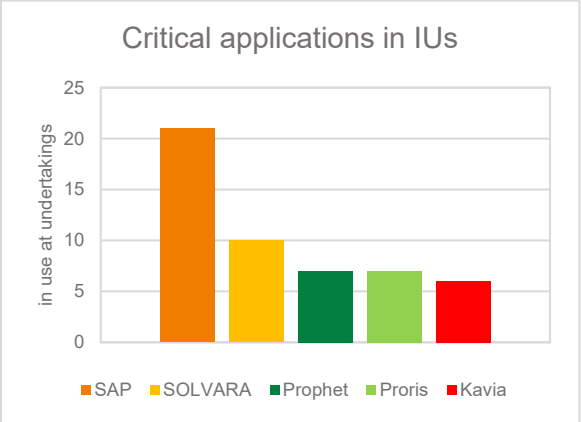
In order to identify concentration risks and obtain a better understanding of the IT landscape of the Austrian financial market sector, those applications have been identified which are most critical for maintaining the entities' business processes:

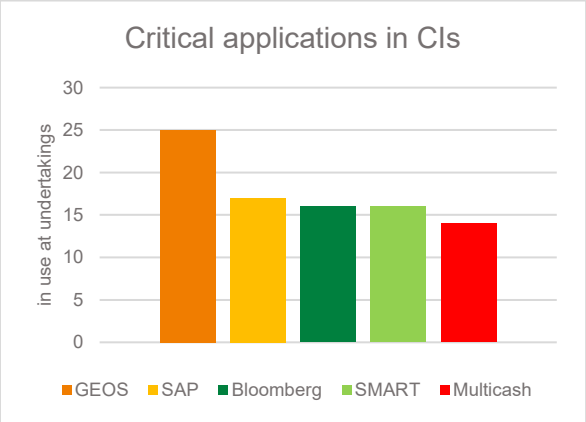


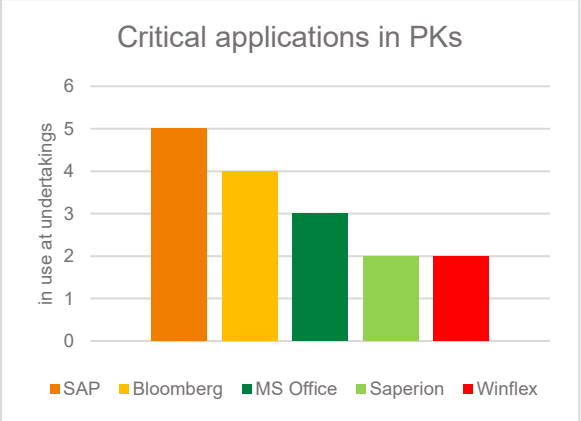
- The top three most frequently used applications in critical business processes are Bloomberg, SAP and Microsoft Office, which are well spread across almost all financial market sectors, and which are used in total by 62, 48 and 42 entities respectively.

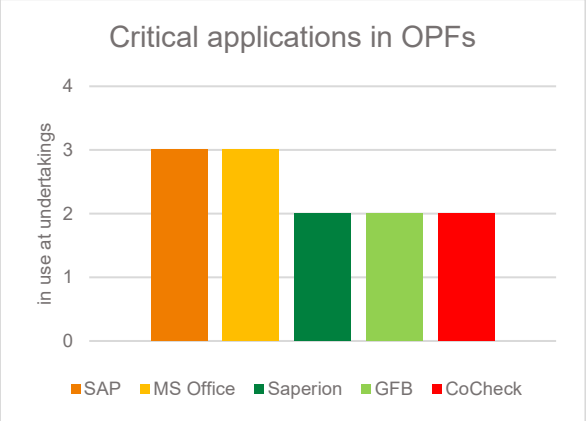
- In this ranking, from 4th place the list is largely dominated by CI-specific applications (GEOS and SMART in the top 5).
- It should be borne in mind when interpreting the results, that only those usages are covered for which the application is necessary for ensuring the maintenance of at least one critical business process.
- Only relatively few solutions are relevant across sectors.
- Within the individual sectors of the financial market there are however specialist applications with relatively high market shares. This analysis together with the analysis on the interdependency with IT service providers constituting a significant source of information for the FMA on the subject of concentration risks.

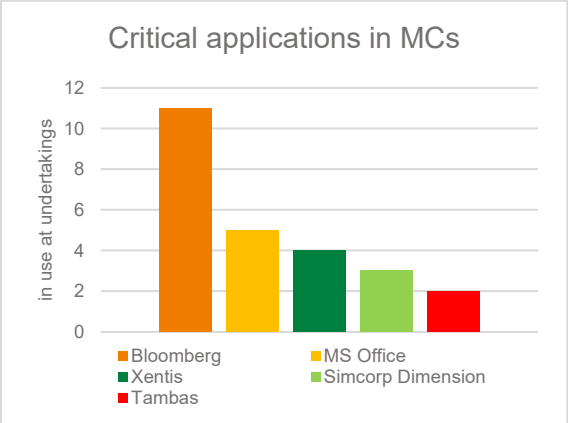
The following series of graphics show the most important applications by financial market sector (there are no separate diagrams for MIs, VASPs and PIs due to the marginal overlaps or low number of entities):

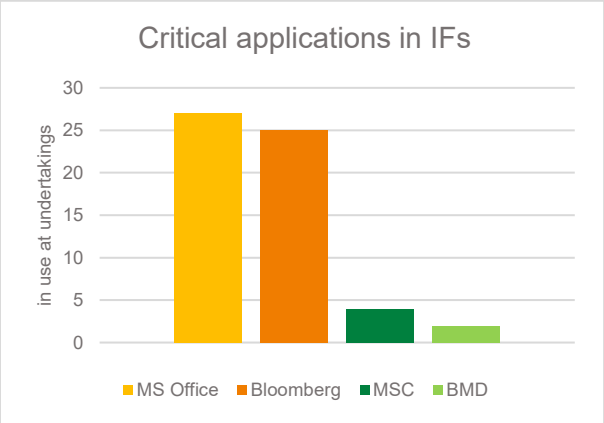












- **Bloomberg, SAP**, and to a certain extent **Microsoft Office**, constitute critical applications in several financial market sectors.
- The important places that follow are occupied by **sector-specific software**, which with one notable exception (Saperion among PKs and OPFs) is also only in the top 5 in a single sector.
- In addition to Bloomberg, SAP and Microsoft Office there are several specific applications that are comparatively widespread in individual sectors. This applies especially significantly to CIs. In the case of IFs on the other hand, this general trend is not discernible.

5.4 SUMMARY AND ACTION AREAS FOR THE FMA

The outcomes of the study are accompanied by the following implications for the FMA:

- The players in the Austrian financial market make use of **a large number of IT applications** for assisting with their critical business processes. In the area of end user applications alone, on average almost 15 critical applications are used per entity, with the details varying significantly by financial sector.
- Regarding the age structure and up-to-dateness of the applications that are used it was not possible to identify any indication that would point to a systemic problem with out-of-date software. Critical applications remain **to some extent in use even for decades, however continuous updates are also performed,** and there are only very few systems in operation with a foreseeable end date for support.
- Bloomberg, SAP and Microsoft are important software suppliers for the Austrian market, and must be considered in any dependency analyses conducted. For individual sectors there are also a large number of smaller software products that are significant; while the failure of a supplier/licence supplier does not directly have the same effect as the disappearance of a critical

service provider, although a certain dependency on support and updates therefore nevertheless also exists.

As is also shown in the chapter on strategy regarding strategic co-operations, digitalisation aids an increasing interconnectedness of the players involved. The FMA must also observe and accompany such developments in the future, in order to fulfil its supervisory mandate. Reliable data on the IT systems used in the financial market sectors has become a relevant requirement for the supervisor:

- Concentration risks regarding individual externally sourced software solutions are to be considered as relevant for financial market stability, both in the event of product discontinuation, as well as in terms of IT security (see e.g. the attack via the Solar Winds Platform in 2020[21]).
- Buzzwords like "outdated IT landscapes" are also freely used in the media in conjunction with topics relating to digitalisation; reliable data allows the FMA to gain a more sophisticated view. An overview of the systems actually in use helps to better grasp current trends and not to be purely dependent on announcements that are partially driven by marketing.

5.5 CONSULTATION IN RELATION TO THE DEPLOYMENT OF IT SYSTEMS

- What duties should the FMA perform in relation to the IT systems used in the Austrian financial market? In which form should such tasks be undertaken?
- 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?

[21] *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor | Mandiant.*

6 IT INTERDEPENDENCIES

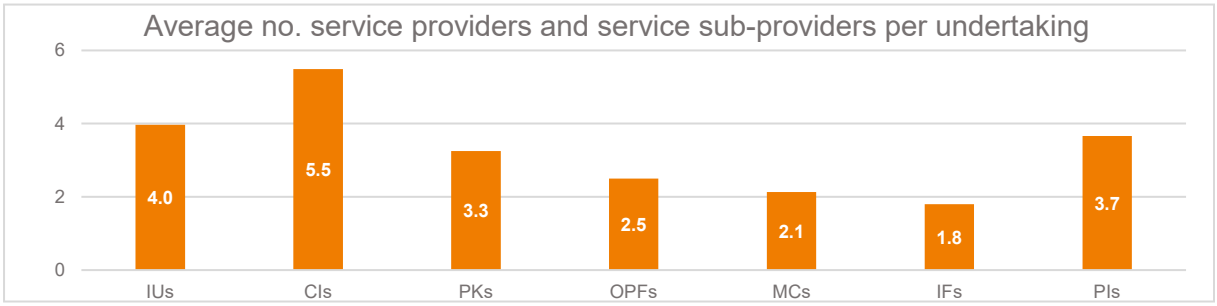
6.1 IT SERVICE PROVIDER LANDSCAPE

Digitalisation also favours the **advancing networking of players that are driving the economy**. In view of the constantly growing technical complexity, the **provision of critical services by IT service providers** is becoming increasingly important. This study therefore surveyed the use of IT service providers (SPs) and IT sub-service providers (SSPs; service providers of first level IT service providers). The survey was limited to those SPs and SSPs that are **necessary for maintaining critical business processes**. The service provider relationships that were surveyed were broken down into the following categories:

- Hardware (e.g. classic data centre services)
- Data connection (e.g. operator of a physical data connection between two locations)
- Network infrastructure (e.g. maintenance of routers and switches)
- Operating systems (e.g. administration of Microsoft/Linux devices)
- Databases (e.g. operation/maintenance of SQL databases or database servers)
- Middleware (e.g. provision of authentication services or APIs)
- Security services (e.g. firewall maintenance)
- Applications (e.g. hosting, operation or administration of end-user software)
- Other

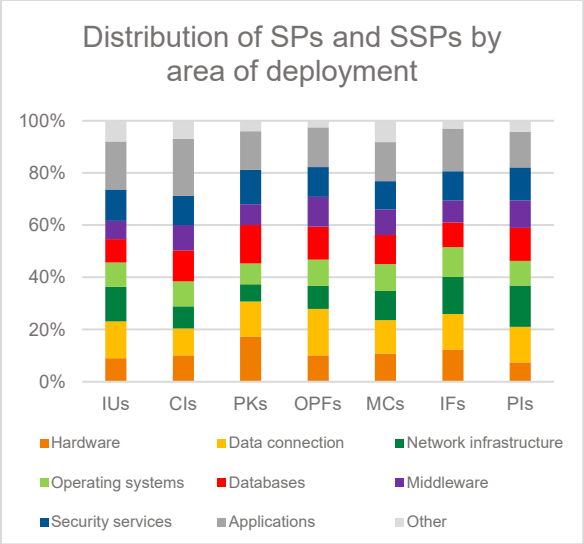
In addition, a distinction was made between internal and external service providers.

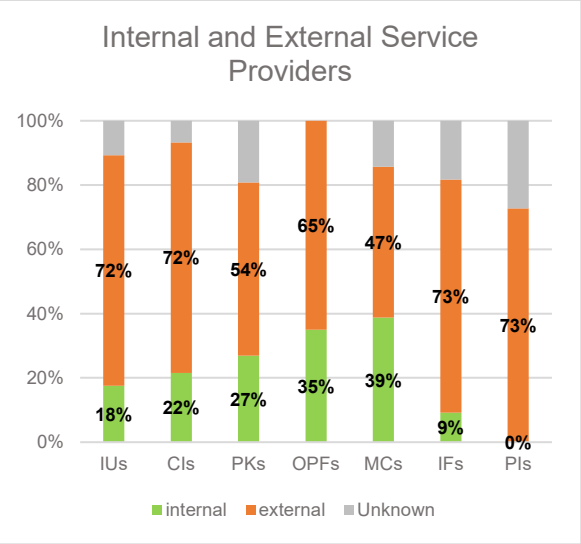
There are around 1,000 critical interdependencies with IT service providers and sub-service providers in the Austrian financial market (966 were identified in the study).



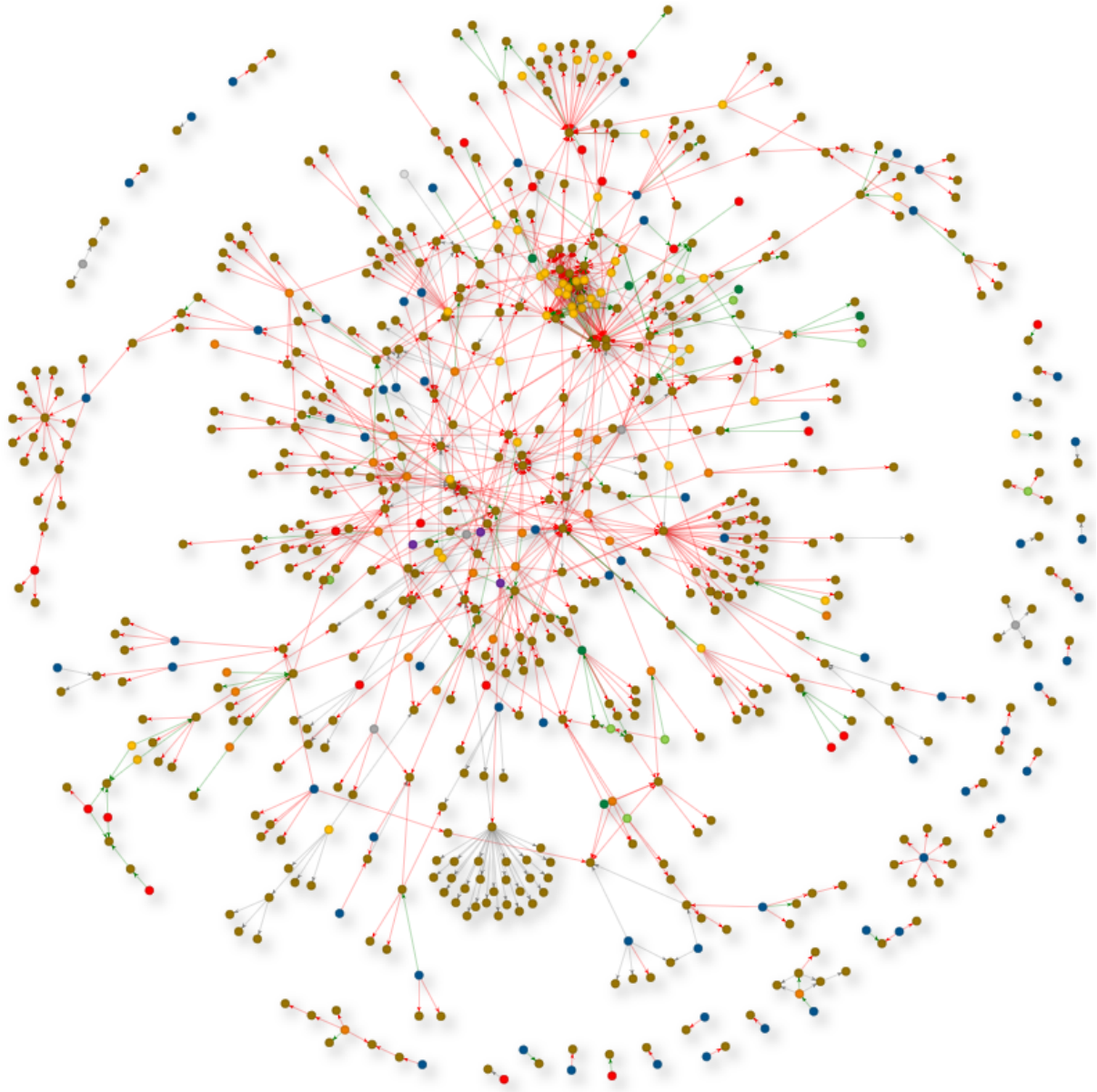
- On average, the entities in all financial market sectors are dependent on several SPs/SSPs.
- The range is from 5.5 SPs at CIs to 1.8 SPs at IFs; there is a close relationship here between the business model, complexity of the IT landscape and outsourcings.
- In general, there were more direct service providers reported than sub-service providers; this may be due in part to information gaps at the SSPs. At some SPs simultaneously service several supervised entities, this was able to be supplemented well by aggregating the corresponding SP reports.

The average number of SPs and SSPs used varies relatively strongly between the different sectors of the financial market; however, their distribution across areas of use is relatively comparable.
No particularly strong trends are observed here and service providers are used across all the areas surveyed. A majority of the SPs and SSPs across all sectors are of an external nature:





The interconnectedness of the IT service provider landscape in the Austrian financial market may be visualised as followed, taking into consideration all IT interconnections.



This representation illustrates the following characteristics of the IT service providers network:

- Although a number of smaller autarkic chains and 1:1 relationships exist, the majority of players involved form a large network.
- While local clusters can be observed, all areas of the financial market are however involved in the IT service provider network; there is no systematic separation between the service providers in the individual sectors.
- For a few service providers, clear concentrations can be identified; numerous entities would be affected by a problem or outage.

- IT service providers, particularly those with a central role, also tend to use sub-service providers for delivering critical aspects of their services.
- Although only one level of SPs was surveyed, in some cases very long chains of dependency emerged, meaning that the outage of an IT service provider might sometimes have an unexpected impact upon supervised entities via several intermediate stages.

6.2 SECTORAL DEPENDENCY NETWORKS

The complex landscape of interdependencies between supervised entities and IT service providers may be examined in greater detail in various dimensions. The following section extracts the sub-networks of the individual financial market sectors. The following colour codes were chosen:

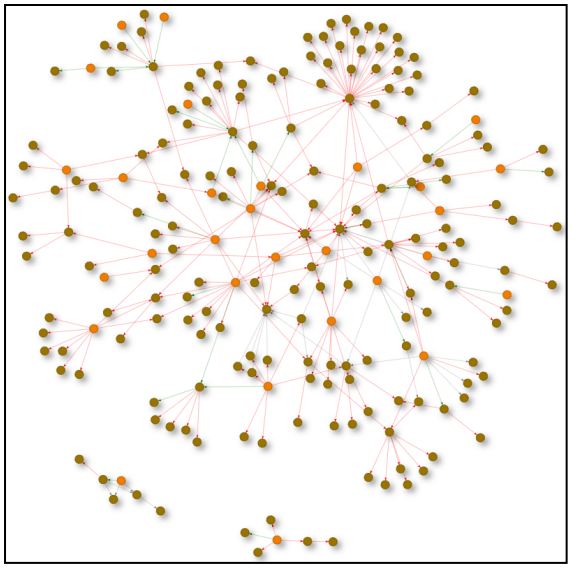
IUs dark orange	CIs light orange	PKs dark green	OPFs light green	MCs red	MIs violet	IFs blue	PIs grey

Due to the low quantity of associated service providers, VASPs were excluded.

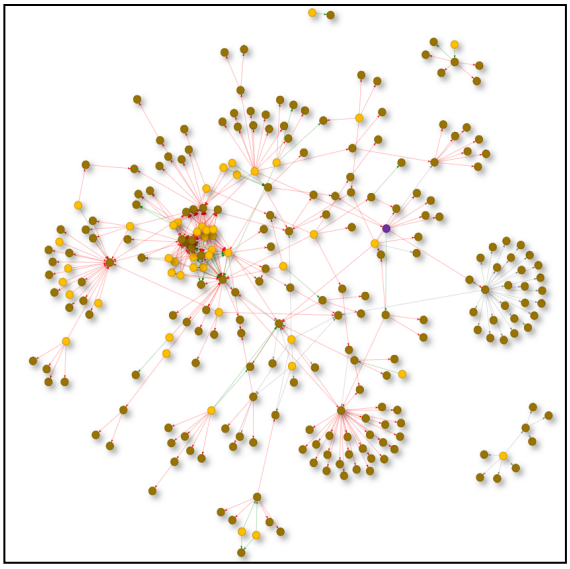
Out-and-out IT service providers, that are not entities supervised by the FMA, are marked by bronze points.

The connecting edges between the nodes of the network represent the service relationships and in the case of intra-group SPs are marked in green, while SPs external to the group are marked in red.

IUs

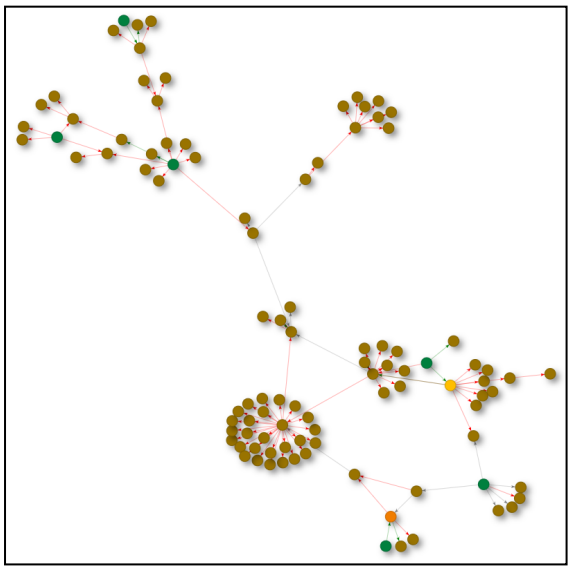


CIs

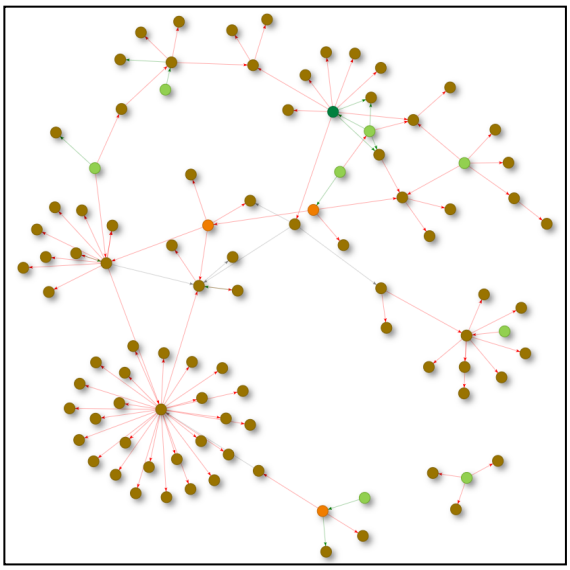


- The outsourcing network at **IUs** is generally characterised by **many small clusters** (often in connection with group associations) rather than concentration at individual SPs. However, most insurers are also linked via one or more SSPs to companies outside their group or via external service provider relationships, in some cases via longer dependency chains.
- On average **CIs** use the most SPs and SSPs in the groups of undertakings. The strong degree of interconnectedness of this sector in therefore not particularly surprising. What is striking, however, is a **small number of very large clusters**, some of which are explained by groups, but some of which also consist of fundamentally independent banks that use the same external SP in parallel. Furthermore, a very **large number of critical SSPs** were identified for a few SPs, which represents a possible starting point for further questions (see Section 6.5 Conclusion and fields of action of the FMA).

PKs

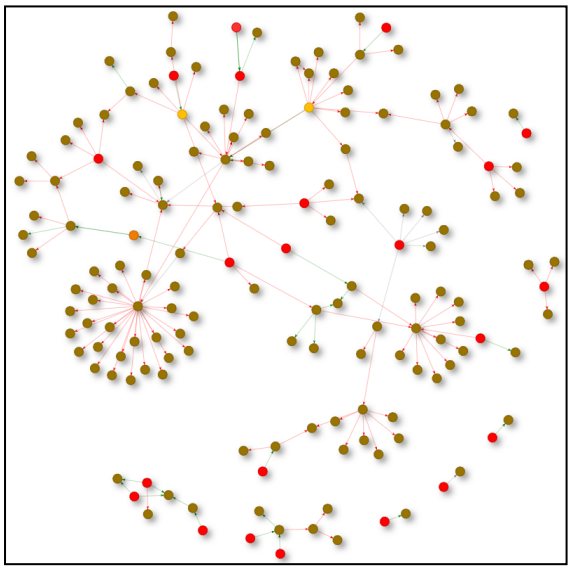


OPFs

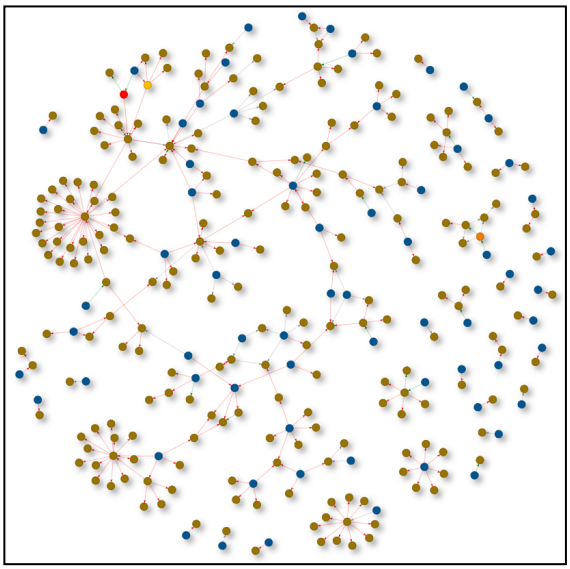


- **PK**s are less interconnected with each other via service providers than other sectors, with the same SP being used by two PKs remaining an exception. One IU and one CI are also integrated into the PK network as IT SPs. Despite the lesser degree of interconnectedness, **all PKs are linked via several jumps through SSPs**, this underlines the rapidly progressing linking of players in times of digitalisation: even entities that otherwise act independently of one another are linked again via some intermediate steps.
- A **complete but not particularly close linkage** via SPs and SSPs can also be observed for OPFs in a similar way to PKs. A comparatively large number of entities from outside the OPF's sector of the financial market, namely three IUs and one PK, are integrated into OPFs' service chains.

MCs



IFs

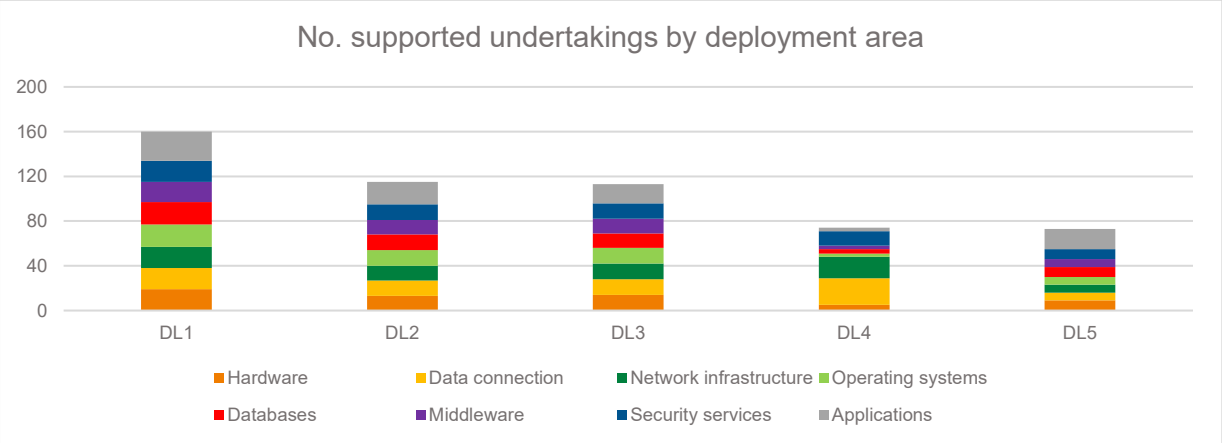


- The service provider relationships of MCs are **comparatively heterogeneous**, but tend to be **relatively distanced**. There are also several **small clusters** that are not connected to the rest of the network. In contrast, several cases exist of the parallel use of a service provider by two MCs. Two CIs, one IU as well as one MC are involved as SPs of MCs.
- **IFs** and their SPs/SSPs form a **relatively loose network with many non-connected clusters**, which also often consist of 1:1 relationships. The clear structural difference becomes apparent if this picture is compared with, for example, the network of IUs or CIs. This is probably due to the business model and the size of the IF. A closer look reveals that many IFs, especially smaller ones, also use smaller entities as SPs and often have all relevant services provided by a single IT company rather than spreading them between several companies.
- With the exception of two **PIs** that use a common service provider, these entities are **not directly connected** via their outsourcing chains, although they use a relatively large number of SPs.

Overall, there are clear sectoral differences in service provider dependencies. Both the average number of SPs and SSPs per supervised entity as well as the degree of interconnectedness and the structure of the clusters formed represent distinguishable characteristics here.
It is also clear that the failure of service providers in many sectors would affect multiple entities. If sub-services are also considered, then clear concentrations exist in every sector. Moreover, the illustrations in this section do not take into account the possible additional impacts on other financial segments.

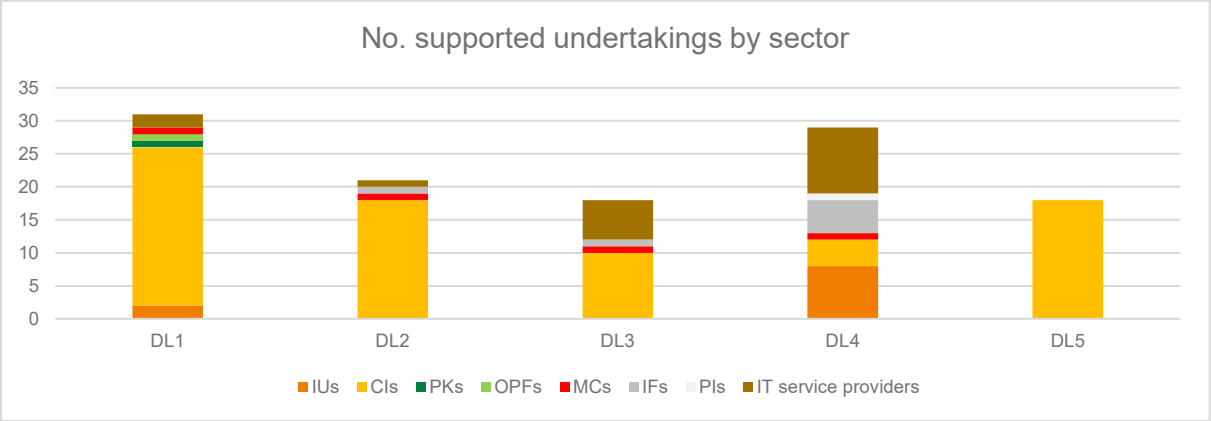
6.3 CONCENTRATION OF THE MOST IMPORTANT SERVICE PROVIDERS

It is not possible to determine the role of individual technology companies for individual financial sectors and the market as a whole based purely on quantitative criteria. An examination in several dimensions nevertheless can provide an insight into the position of some key service providers:
Regarding the **number of directly provided business-critical services** for supervised entities or other SPs of supervised entities, the relevance of individual players in the service provider network can be recognised in the following chart (the cascading number of entities for which these SPs constitute an SSP has not been included here and there is no weighting by balance sheet totals):



- These **large direct service providers are more generalists rather than specialists.** Apart from DL4 focussing on data connections and network infrastructure as well as a general tendency towards increased support at the application level, all types of services are offered to a similar extent; often also for the same entity in the form of extensive overall IT outsourcing.

In terms of the n**umber of entities supported by critical services** per sector, a **very high proportion of CIs** are observed for the top five service providers:

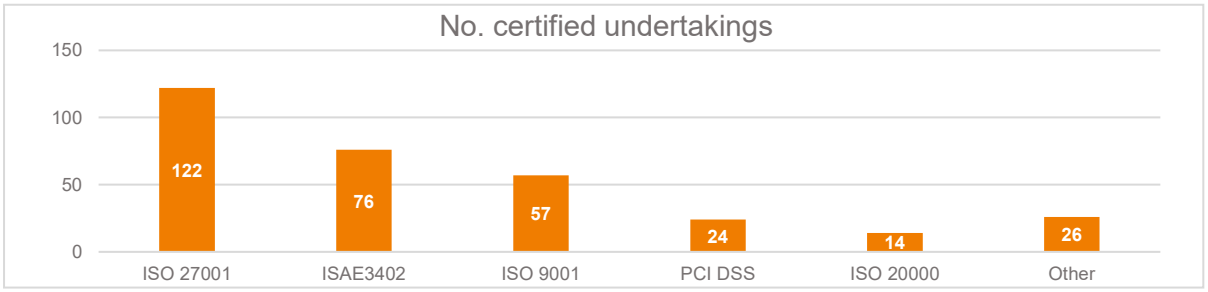


- DL5 is a service provider exclusively active in the banking sector. Only in the case of DL4 do CIs not represent the majority of the entities supported.
- This result is consistent with the sectoral networks examined in Section 6.2. **The banking sector forms the largest clusters in direct outsourcing, whereas other sectors are mostly only strongly networked via SSPs.** From the example of DL4, it is nevertheless noticeable that notable cross-sector dependencies on SPs exist, in particular in the field of specialised IT services.
- The analysis of the dependencies also permits the identification of **central sub-service providers**. In the case of the five SPs listed above, for example, DL1 makes use of 11, DL3 of 10, and DL4 of 3 known SSPs. Further links often emerge only after several steps in the service chain.
- The question of the extent to which a hypothetical failure of a sub-service provider can have an effect across several levels would have to be investigated further.

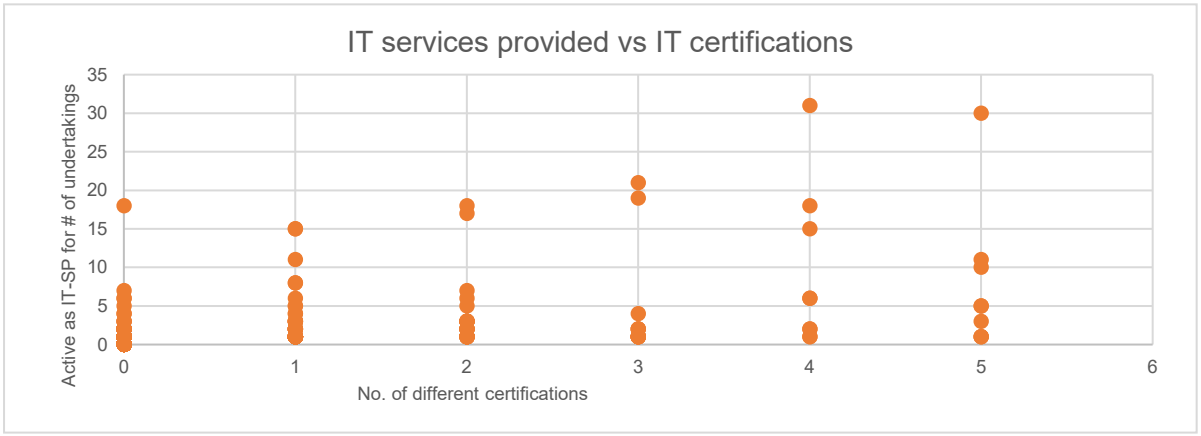
6.4 CERTIFICATIONS OF IT SERVICE PROVIDERS

Within the context of this study, the **IT-relevant certifications** of their service providers known to the supervised entities were also surveyed. The overall picture may sometimes contain gaps, since the SPs and SSPs themselves were not surveyed. This notwithstanding, an overall representative overview should nevertheless emerge, since knowledge is expected about the certifications of the entities' critical SPs as part of the corresponding assessment of risks.

Out of the 512 entities that provide services, 168, i.e. **one third of the IT service providers** (a figure that also includes some of the supervised entities that additionally act as IT SPs) **have relevant certifications**. A relatively large proportion of the 168 certified entities simultaneously hold several relevant certificates:



A certain correlation can be determined between the number of entities supported as IT SPs and the number of IT certificates held:



- While the trend is not strictly linear, certificates tend to be held by larger service providers.
- Overall, the number of SPs and SSPs that do not hold certifications, although they provide IT services to several entities, is relatively high.
- The question of whether and which certifications make sense for provision of a certain activity as a rule depends on the individual case-in-hand. The question nevertheless arises as to what the overall reasons are for this relatively low coverage, even in the case of relatively common standards, such as ISO 27001/9001, and whether the supervised entities hold up-to-date information about the certifications of their service providers.

6.5 SUMMARY AND ACTION AREAS FOR THE FMA

The comprehensive data show a high degree of interconnectedness between the individual financial market sectors with IT companies, as well as with each other:

- Strong sectoral differences can be observed, but an overwhelming proportion of regulated entities are interconnected to one another through SPs and SSPs, which are critical to the entities' business processes.
- In the most concentrated sectors, especially CIs, a large number of market participants are directly dependent without any intermediate steps on a few service providers for the delivery of their services.
- The information on IT SPs and SSPs allows for a better understanding of the IT landscape of supervised entities and thus a more informed and risk-based approach in ongoing supervision.
- Out-and-out IT companies are becoming increasingly significant for the financial market. With the available information, the FMA is able to identify key Austrian service providers and take them into account in a targeted manner in its supervisory activities.
- The EU regulation on digital operational resilience (DORA) aims at a supervisory regime for critical ICT service providers, which again calls for a comprehensive service provider map on a national basis.
- Where there are major incidents at IT SPs or SSPs, the FMA is able to identify a group of affected entities and categories of services quickly.

This study ultimately also provides the FMA with a starting point for further questions relevant to supervision:

- Due to the exponentially increasing number of entities with each step of the outsourcing chain that are dependent on a sub-service provider, it is important to be able to estimate the effects of the failure of a service provider on all potentially affected parties.
- The number of reported critical sub-service providers per IT service provider varies strongly in some cases: potential backgrounds for this variation would have to be determined.
- The heterogeneous use of certifications at IT service providers emphasises the question of when and for which entities these are useful, or what message a lack of such certificates at central IT companies may give off.

6.6 CONSULTATION ABOUT IT INTERDEPENDENCIES

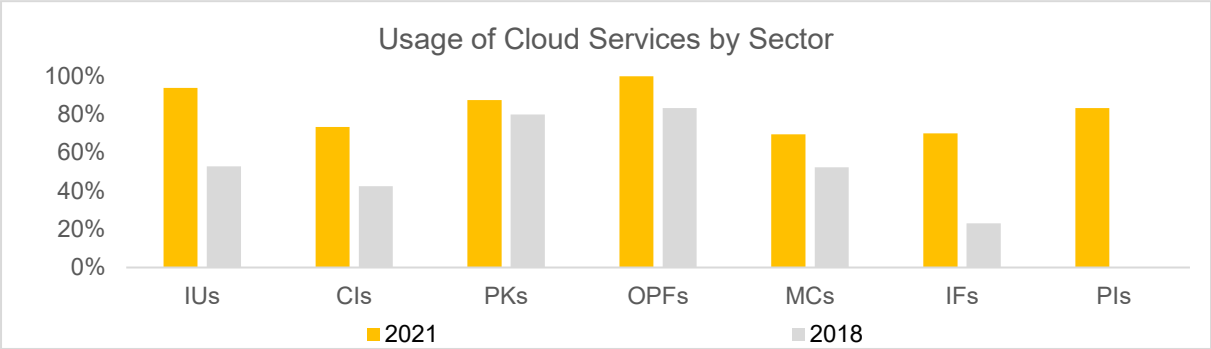
- What duties should the FMA perform in relation to the interdependencies between supervised entities and IT service providers?
- In which form should such tasks be undertaken?
- What specific regulatory standards are still necessary in relation to the interdependencies in the Austrian financial market?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

7 DIGITAL TECHNOLOGIES

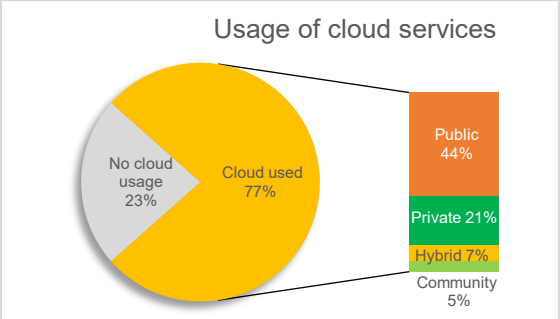
7.1 CLOUD SERVICES

Cloud services offer the **provision of IT infrastructure and IT services** as well as storage space, processing power or software applications available **as a service over the Internet**. Cloud services are not provided from a specific computer. Instead, the virtual processing cloud comprises of many computers that are networked to one another. Cloud services are accessed via a network. Users access the resource pool of the cloud, and the capacities they need dynamically allocated.

Cloud services have gained in importance in the Austrian financial market. Around three quarters of the supervised entities already use cloud services. In comparison, in 2018 around half of the supervised entities used such services. The expectation in 2018, of expected cloud services usage by more than 60% of market participants has therefore been clearly exceeded.



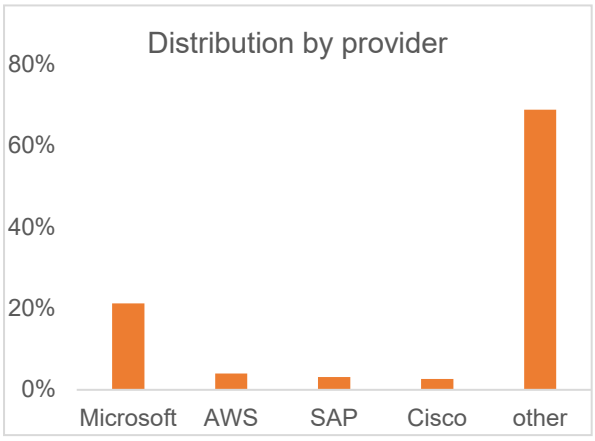
Cloud usage is most widespread among OPFs. Every OPF makes use of such services. IUs, PKs and PIs use clouds intensively. 94% of IUs, 88% of PKs and 83% of PIs make use of cloud services.



- Cloud services are already being used by approximately three-quarters of the supervised entities.
- Around three quarters of the entities using clouds use more than one cloud-based solution.
- Out of the different cloud provision model (public, private, hybrid and community) the use of public clouds dominates.

The most widely-used providers among Austria financial services providers as a proportion of the total number of cloud users are Microsoft, AWS, SAP and Cisco.

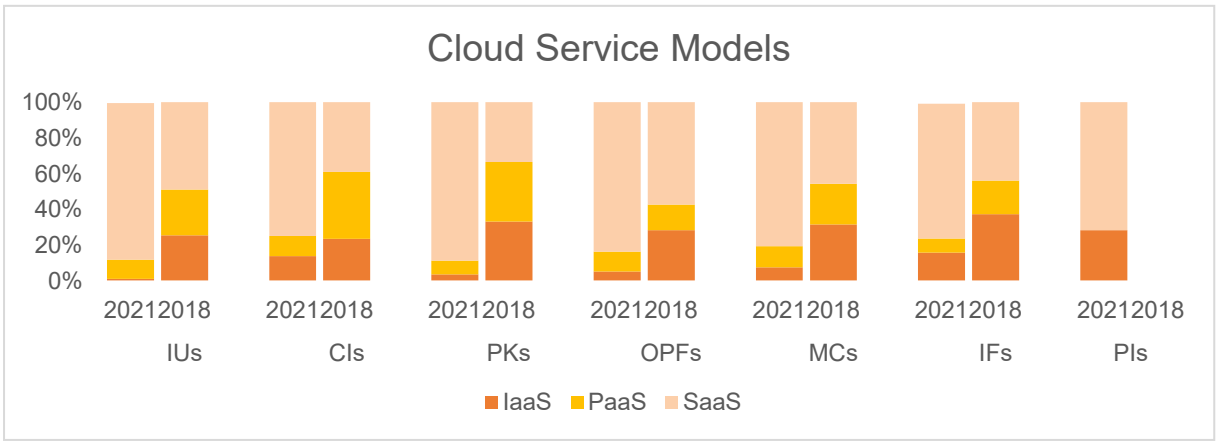
Out of the Austrian providers, for example, **ARZ** and **Fabasoft** are represented.



Microsoft continues to be widely used as a cloud service provider. For example, the Azure cloud platform is also used, in addition to MS Office 365. Microsoft's share has fallen from 34% in 2018 to 21% in the current year. Compared against to the previous edition of the digitalisation study, the share of other providers that are not among the four most used service providers has increased from 60% to 69%.

On average, 80% of all cloud services used by supervised entities can be allocated to the Software as a Service (SaaS) service model.

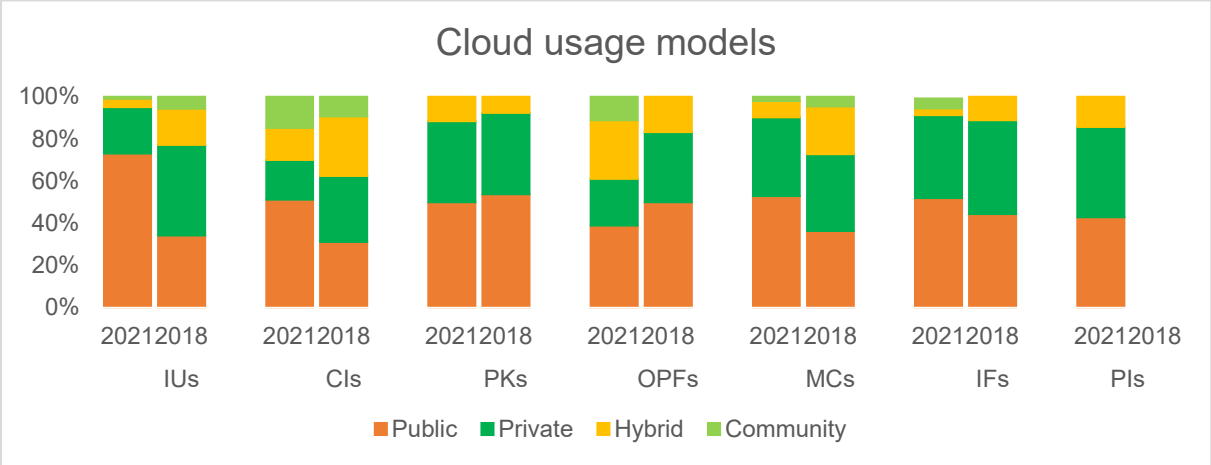
In 2018, the share attributable to SaaS models stood at approx. 45%. During the same observation period, the share of Infrastructure as a Service (IaaS) service models fell from 30% to 14%. The same trend can also be observed for Platform as a Service (PaaS) service models – in this case, it fell from 25% to 7%.



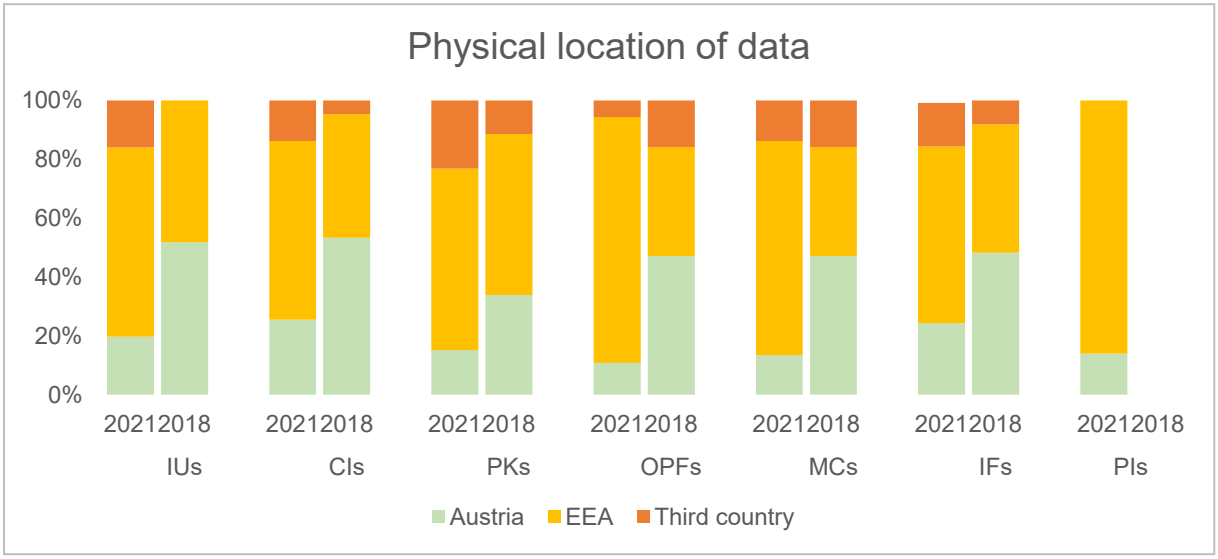
Half of the cloud services used are allocated to public clouds.

The use of public clouds has increased compared to 2018. At that time, around 40% of all cloud services used were such public clouds. This usage model now accounts for around half of all cloud services.

Meanwhile, the share of private clouds has decreased slightly: more precisely from around 38% to 34%. A similar trend is also observed regarding hybrid clouds, which account for around one tenth of the total in 2021. The significance of community clouds is very low, with a usage share of around 4%.

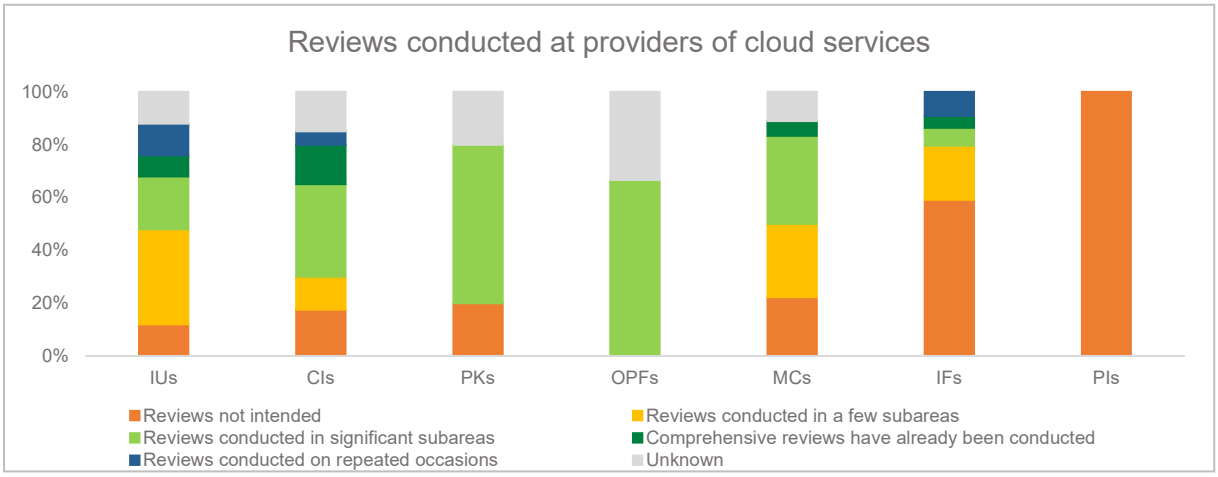


90% of all physical locations of data are in Austria and in other EEA countries. Compared with 2018 the proportion located in Austria has fallen from just under 50% to approx. 15% now.



Around half of all supervised entities that use cloud services, do not conduct any reviews of cloud service providers.

Given the complex risks of cloud services, it is important that cloud users are aware of the potential dangers. The digitalisation study shows that many supervised entities have yet to perform any kind of review of the cloud solution to check for any deficits:



- Around four out of ten entities using clouds do not conduct audits of cloud service providers. If the 10% of all cloud using entities that did not respond to this question were also not to perform such audits, then the result would be that half of all entities using cloud services is not planning any audits of cloud service providers from the outset. In particular, PIs, VASPs and IFs do not plan to conduct audits of cloud service providers.
- Around 4% of entities using cloud services have already completed comprehensive audits. A further 3% have already conducted such audits on multiple occasions. These comprehensive audit activities are accounted for entirely by IUs, CIs and to a lesser extent by IFs and MCs.

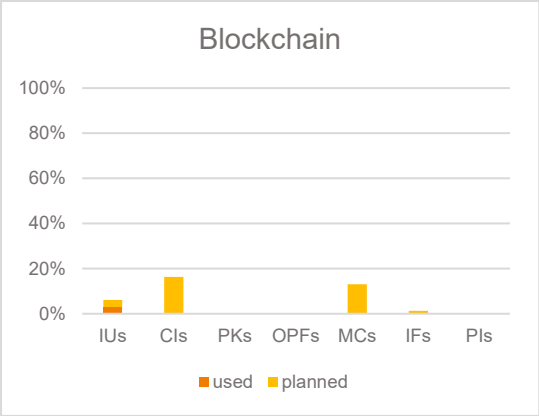
7.2 BLOCKCHAIN

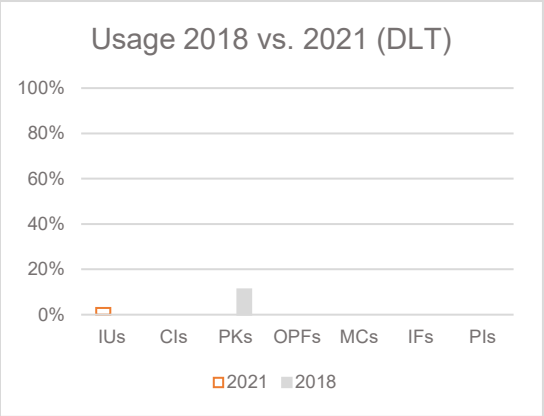
A blockchain is a cryptographically coded database (ledger) with a digital log that cannot be manipulated stores on a large number of decentralised computers. All different types of information (bookings, sale and purchase agreements) are consensually verified in the network. The blockchain is currently the most commonly used form of distributed ledger technology (DLT). Since these terms are often used synonymously, blockchain is hereafter used as a generic designation for the DLT.

Opportunities	■ May be used in many areas ■ May primarily be used in distributed non-hierarchical systems. ■ Potential high transparency and resistance against manipulation due to consensual verification ■ High failure resilience due to the distributed structure
Threats	■ Relative new and partially poorly understood technology ■ Decentralised structure prevents inherent applications with centralised control ■ Purely digital processability may lead to legal or technical risks ■ All of the data saved in the blockchain are public between the participants, which may have technical implications with regard to data protection

Current developments:

The opinion expressed in the last edition of the digitalisation survey in 2018 that blockchain technology would not find any broad use cases among the supervised entities in the medium-term, has been confirmed. While some supervised entities are planning to use the blockchain in the next three years, this technology is currently barely being used:





This does not mean, of course, that the blockchain is considered an irrelevant topic for the FMA or the financial market, however in the perception of the supervisory authority, the primary focus is on business models involving tokens or cryptocurrencies and their applications as payment instruments, investment objects etc. Regarding the technology itself, no other use cases have yet been established among the supervised entities.

However, this is probably more or a conceptual hurdle rather than a technical one. The distributed ledger, as the name implies, is primarily suited for decentralised systems. It may therefore be more difficult for an established entity, to integrate and monetise concepts that are technically fundamentally possible and interesting like e.g. peer-to-peer insurance or smart contracts into the existing business concept.

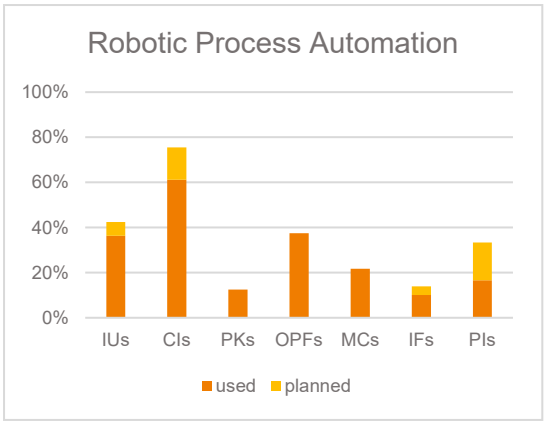
7.3 ROBOTIC PROCESS AUTOMATION

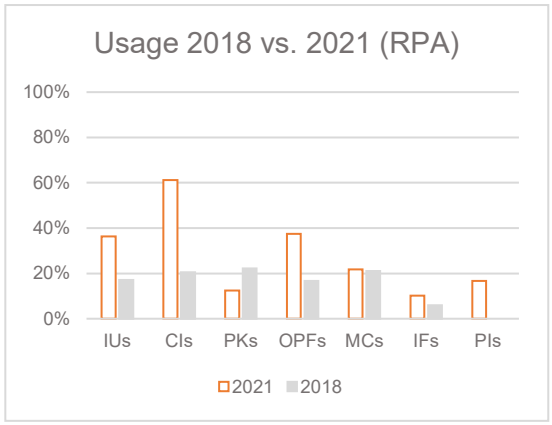
Robotic Process Automation (RPA) is an umbrella term for "bot" software, which can perform repetitive activities in software applications, e.g. by the pre-defined execution of keyboard entries and mouse movements. Typically, only a relatively simple decision-making logic is used, and by using the mouse pointer and keyboard, the program works in the same way as a human processor would.

Opportunities	■ easily and inexpensively implementable ■ does not require IT skills for operation and application ■ Compatible with practically every application without any need for adaptation
Threats	■ in the case of an amendment of one of the processes automated with RPAs, all bots running must consequently be adapted. ■ usually unsuitable for complex decisions ■ is frequently unable to access the underlying data for an application

Current developments:

The use of RPA has increased significantly in most sectors over the last three years and is already widespread, especially in CIs:





RPA is a method whose application is mostly considered as a temporary auxiliary solution or support for systems where you do not have the necessary direct access to the business logic and database

level of such systems. The possibility to implement rapidly appears to be the decisive factor for the usage of RPA, in order to achieve rapid gains in efficiency.

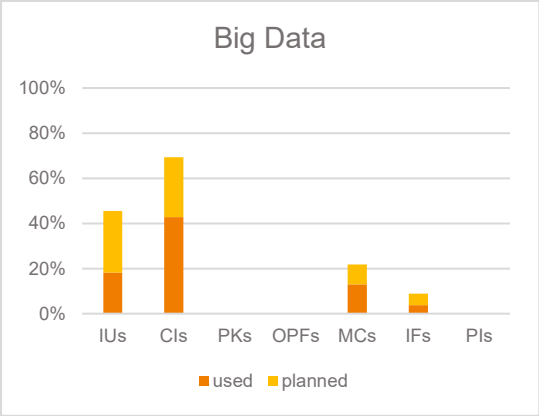
7.4 BIG DATA ANALYTICS

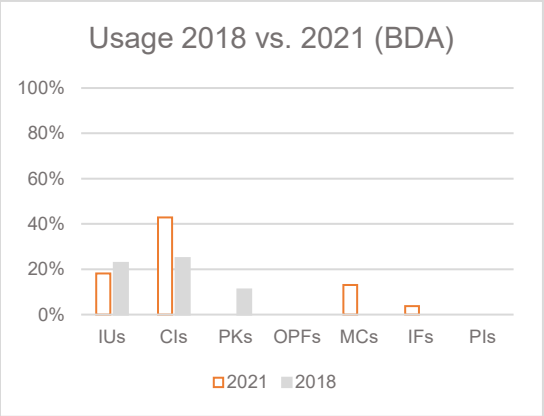
Big data is the designation for automated processing of large quantities of data (volume) in a narrow timeframe (velocity) from different sources (variety). There are numerous potential use cases for this technology in the financial sector (e.g. in marketing, fraud detection, creation of mathematical models, etc.).

Opportunities	■ More precise models may be constructed by analysing greater quantities of data. ■ Individual hedging requirements and probabilities of sales can be predicted more precisely using new data analytics methods. ■ Offers may therefore be better individually-tailored as a result. ■ Big data applications improve analysis processes in the prevention and combating of fraud, money laundering and terrorist financing. ■ Technologies line machine learning can only be realised using large amounts of data.
Threats	■ A lack of data quality or faulty models may distort results. ■ The high complexity of analysis models may lead to deteriorating transparency and traceability ■ Processing of large amounts of data also requires increased investment in infrastructure and processing power ■ Regularly running analyses of large data volumes can often not be repeated during live operation due to the resources required

Current developments:

While many entities show interest in big data analytics, the specific structure of corresponding databases and analytics systems seems to be an obstacle:





Over 40% of CIs now use Big Data, but use of this technology is largely stagnating in other sectors. In particular, CIs and IUs often plan to introduce corresponding tools. The comparatively high level of

use by CIs may sometimes be explained by the existence of large, structured data volumes in such entities, whereas other market participants first have to create corresponding structures.
Overall, there are potentially numerous valuable use cases for big data, especially in combination with machine learning. Accordingly, a possible future scenario is that entities with access to big data may be able to gain a competitive advantage from it. For the supervisor, the safeguarding of customer interests remains important.

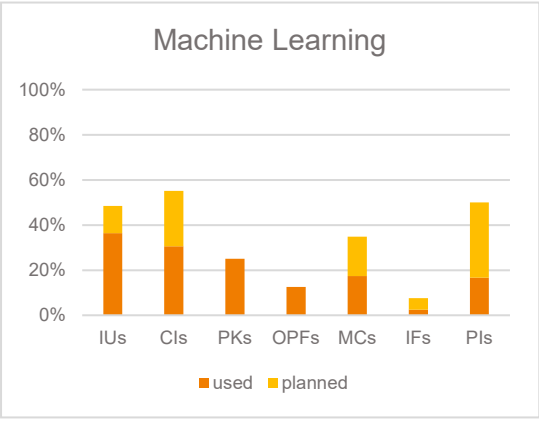
7.5 MACHINE LEARNING

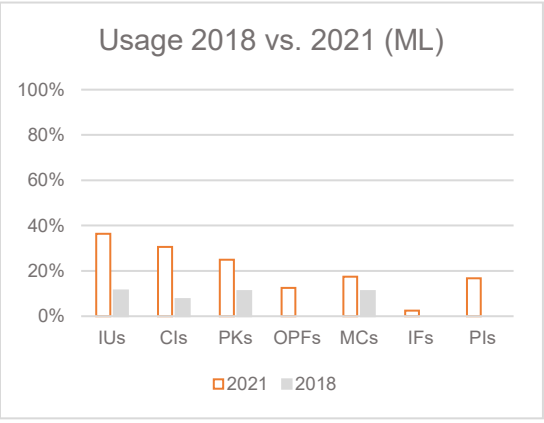
A field of informatics dealing with self-learning software. No solution algorithm is stipulated by the programmer, and the software itself looks for the suitable approach to a problem. This procedure is particularly suitable for interpreting and recognising patterns in large amounts of specific data.

Opportunities	■ large amounts of data can be automatically processed in a short time. ■ Very complex activities that may otherwise require an expert can be supported or taken over fully. A correctly calibrated and trained system is able to work very exactly and improves itself constantly based on new data. ■ Potential new and unknown relationships may be detected.
Threats	■ Problems with data quality or the statistical methodology may lead to imprecise results. ■ Complexity and the "black box" effect may impede transparency. ■ The system may also develop false stereotypes in an unnoticed manner as the result of incorrect learning (e.g. image recognition, recruiting tools).

Current developments:

The degree of use of machine learning has increased significantly in the last three years. While not all entities that had planned to do so have been able to implement corresponding projects, the technology has already been applied in over 20% of IUs, CIs and PKs:





Machine learning can be used to enable predictive analyses and identify new correlations in data. Overall, it has great potential as a tool, but is susceptible to methodological errors and problems in the data basis. Depending on the algorithm used, transparency can also be significantly limited. This results in some challenges for the supervisor: models must remain explainable and shall not be allowed to unintentionally lead to legally or ethically problematic conclusions.

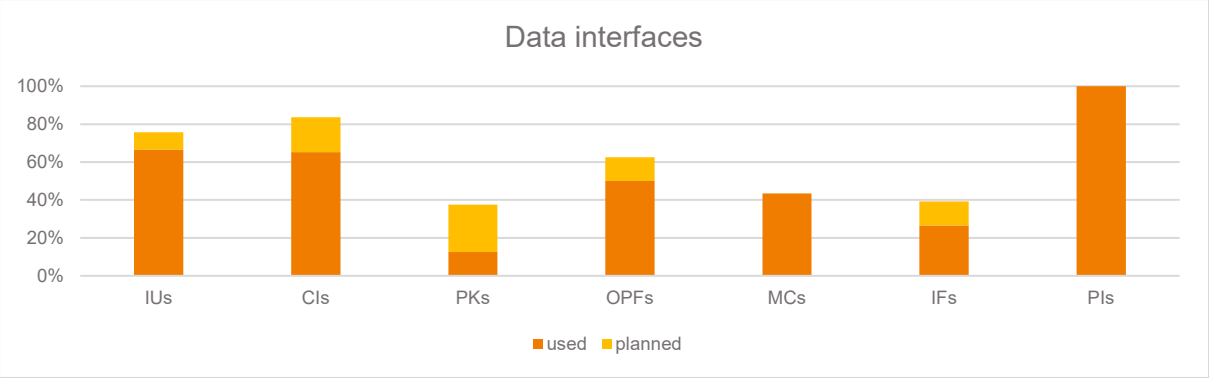
7.6 AUTOMATED DATA INTERFACES

Standardised interfaces (APIs) enable the automated exchange of data with third parties via predefined formats and transport channels. In this way, it is possible to integrate data from external providers and calculations into one's own systems on a regular basis. The possible use cases are far-reaching: capital market data, exchange of portfolio data with intermediaries or automated information channels about current IT risks.

Opportunities	■ External data providers can support big data analytics and machine learning implementations ■ An external supplier may be more cost-effective compared with an exclusively internal data collection ■ Correct data are the basis for the deployment of many complex IT systems
Threats	■ Every data interface is a potential route of entry for external IT security threats and therefore must be secured accordingly. ■ With regard to personal data, maintaining data protection is sometimes an additional challenge ■ Additional dependencies on external service providers

Current developments:

Many supervised entities already use automated data interfaces; among IUs, CIs, OPFs and PIs respectively the level of use is 50% or more. This is unsurprising, since modern IT systems are taking over an ever-increasing number of duties in entities, but can only deliver results that are as good as permitted by the data fed to them. For the FMA, this trend also underlines the growing complexity of the IT landscapes used by the supervised entities and the necessity of adequate IT security measures as well as monitoring of the service providers used.



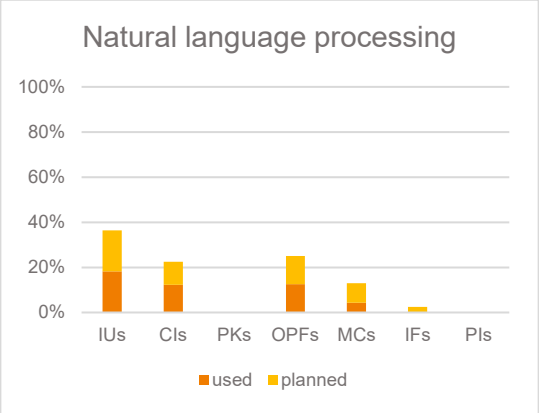
7.7 NATURAL LANGUAGE PROCESSING

Natural language processing (NLP) describes techniques and methods for the machine processing of natural language. The goal is direct communication between humans and computers using natural language (e.g. SIRI, ALEXA, etc.).

Opportunities	■ Efficiency gains through possible use in customer-related business ■ Conversion of speech into machine data enables interfaces to the entity's other IT systems
Threats	■ Technically still rather complex; Challenge relating to data protection and risk of misinterpretation when used in customer-related business

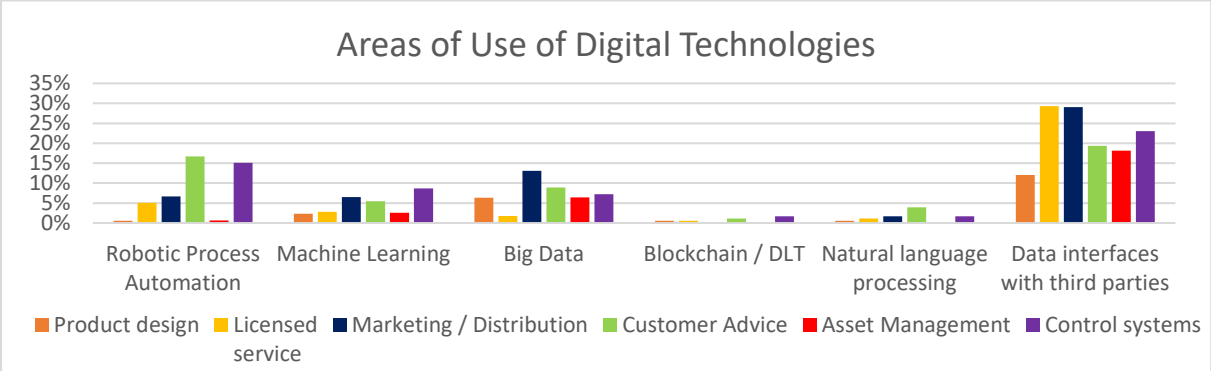
Current developments:

Natural language processing is a technology that has not yet found widespread use in the Austrian financial sector. A usage rate of 20% has not been reached in any market segment, even though it seems possible that this mark will be exceeded by IUs, CIs and OPFs due to planned implementations in the next three years. In this respect, this is one technological development whose use the FMA is currently observing with a wait-and-see attitude.



7.8 AREAS OF USE OF DIGITAL TECHNOLOGIES

In addition to the trends regarding usage of individual digital technologies in the sectors of the financial market, the current survey also allows an insight into the areas of use of such technologies. The following picture emerges:



Marketing/sales, customer service and regulatory control systems (e.g. risk management, compliance) are the **main areas of use of digital technologies.** This is consistent with the other findings of this digitalisation study, according to which

- the customer interface in the Austrian financial market is generally the location where digital technologies establish themselves most quickly;

- regulatory requirements as well as the possibility of reducing one's own costs, for example by means of fraud detection systems, are driving the use of new analytical methods in the control systems.

The following conclusions emerge in relation to the individual technologies:

- **Robotic Process Automation** is primarily used in customer care and control systems, where it is mostly used for the processing of repetitive forms, e.g. in creating and transferring data records into the actual analysis systems.
- **Machine learning** is used in marketing/sales and control systems. Customer analyses, e.g. for cross-selling and advanced fraud detection systems are two potential use cases.
- **Big Data Analytics** is closely related to this and is used accordingly in similar fields. In addition, this technology is used by some entities in asset management.
- **Blockchain technology** is hardly used overall; identifying specific use cases is the heart of the problem.
- **Natural Language Processing** is also not yet frequently used productively, but a trend is being observed, as also indicated by the characteristics of the technology, towards customer support.
- **Data interfaces** are a very versatile tool and are used by many entities in several areas simultaneously; heavy use is a clear indication of the increasing value of data in the context of digitalisation.

7.9 CONSULTATION ABOUT 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 digital 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?

8 ICT-RELATED INCIDENTS

While the intensified and networked use of digital opportunities, also driven by the COVID 19 pandemic, opens up new opportunities, it is also accompanied by increasing ICT risks.

For example, reported cybercrimes in Austria increased by 26% from 2019 to 2020.[22] The attack on the network of the Federal Ministry for European and International Affairs in 2020[23] is cited by the European Cyber Security Agency, ENISA, as one of the main incidents worldwide in the period January 2019 to April 2020.[24] This example illustrates that Austria is also within the radius of consideration of cyber criminals and that appropriate security measures must be taken.

In addition, the financial sector remains an attractive target for attackers.[25] This is in particular due to the "inherent monetary nature" of the financial services sector, as well as due to the increasing global level of interconnectedness. Successful cyber-attacks may proliferate quickly, and may therefore become a danger for financial market stability.

8.1 CYBER INCIDENTS

Harmonised cross-sector definitions and reporting obligations regarding ICT-related incidents have not yet been defined. This makes it more difficult to make comparisons within and between the sectors as well as to deduce findings.[26]

While payment service providers are required to report severe operational or security incidents to the FMA[27] that do or could influence the financial interests of the payment service users, such reporting obligations are still being drawn up in other sectors, or intended to be harmonised in the future. The proposal published by the European Commission in September 2020 for a Regulation on digital operational resilience for the financial sector (DORA)[28] also covered ICT-related definitions and cross-sector reporting about ICT-related incidents. The structure and contents of reporting regulations will however only be drawn up once the Regulation has entered into force.

The FMA's surveying of ICT-related incidents, differentiates between cyber incidents and other major operational or security incidents.

---

[22] *Federal Ministry of the Interior, Criminal Intelligence Service Austria, Cybercrime Report 2020, Situation report on the development of cybercrime (in German only), Vienna 2021, 26.*
[23] *Federal Chancellery, Cybersecurity Report for 2020, Vienna, 2021, 6.1 The BMEIA incident and its consequences across government*
[24] *ENISA, Main Incidents in the EU and worldwide – from January 2019 to April 2020, 4.*
[25] *Cf. e.g. FireEye Mandiant Services, M-Trends 2021, Special Report, 18.*
[26] *FMA, Digitalisation in the Austrian Financial Market, June 2019, VIII. A. Definition of Cyber Risks*
[27] *Cf. FMA, Reporting of major operational or security incidents in accordance with Article 86 ZaDiG 2018.*
[28] *Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, COM(2020) 595 final.*

The data collected by the FMA about cyber incidents is based upon potential or actual adverse impacts of an unplanned single event or a series of related events on the integrity, availability, confidentiality, continuity and or the authenticity of the financial products provided. The data was broken down by the type of attack.

8.1.1 NUMBER OF CYBER INCIDENTS

From 2019 to 2020, the **number of cyber incidents in supervised entities increased significantly more strongly than the general increase** in reported cyber-crimes in Austria. Even if these figures are not directly comparable with one another, they nevertheless represent an indication of the particular degree of exposure of supervised entities towards cyber attackers.

Austria	*Number of reported cybercrimes*[29]	*Number of cyber incidents at supervised entities*
2019 - 2020	+26%	+98%

The number of cyber incidents in supervised entities almost doubled from 2019 to 2020. The increase is therefore significantly higher than the number of reported cybercrimes in Austria, which increased by 26% during the same period

The figures about cyber incidents varies in some cases massively between the sectors. Currently cyber incidents are predominantly concentrated in the CI sector.[30]

[29] *Federal Ministry of the Interior, Criminal Intelligence Service Austria, Cybercrime Report 2020, Situation report on the development of cybercrime (in German only), Vienna 2021, 26.*

[30] *This is also apparent in the numbers of cyber incidents reported to the ECB. They increased by 54% from 2019 to 2020, although there were no significant impairments observed in the provision of banking services. Cf. ECB, Supervision Newsletter: IT and cyber risk: a constant challenge, 18.August 2021.*

8.1.2 MOST FREQUENT TYPES OF ATTACK

Phishing and malware have been the most frequent types of attack in supervised entity since 2019. In 2020 just under **90% of cyber incidents** could be attributed to these types of attack.

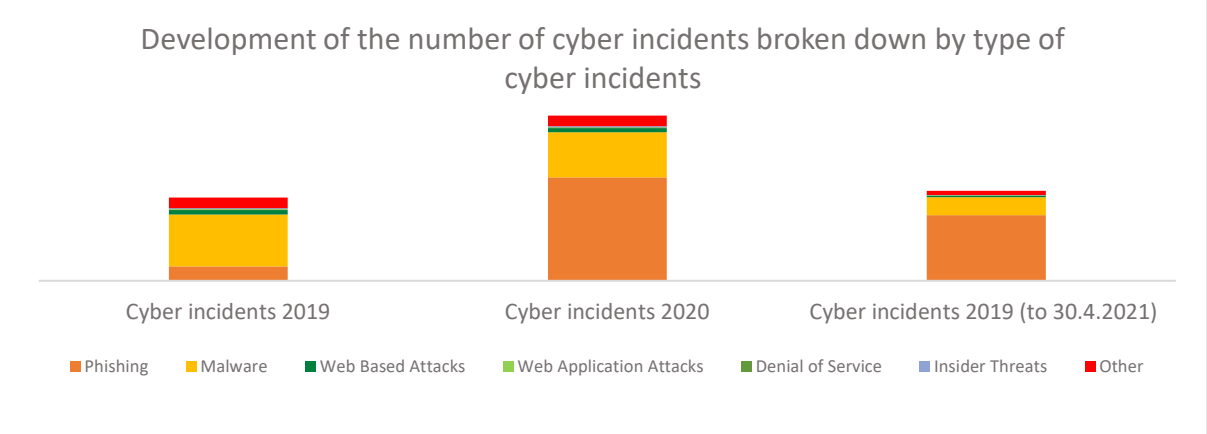
Top 5 types of attack 2020

Rank 2020	*Type of attack*	*Rank 2019*	*ENISA largest threats 2019-2020*[31]
1.	Phishing	2.	3.
2.	Malware	1.	1.
3.	Other	3.	-
4.	Web Based Attacks	4.	2.
5.	Denial of Service	11.	6.

In 2020 among the types of attack, Phishing was easily the most widely spread. Malware occupies 2nd place and is significantly ahead of the other types of attack.

ENISA recognises malware, web-based attacks and phishing as the three largest threads in 2019 to 2020.[32] Denial of Service is in 6th place in the ENISA rankings. Overall, a consistent picture emerges, in which the situation in the financial sector of Austrian financial institutions is generally in line with European situation.

By way of comparison, among the cyber incidents reports to the ECB in 2020, Denial of Service attacks ranked ahead of unauthorised access and phishing; subsequently followed by malicious scripting attacks and malware.[33]

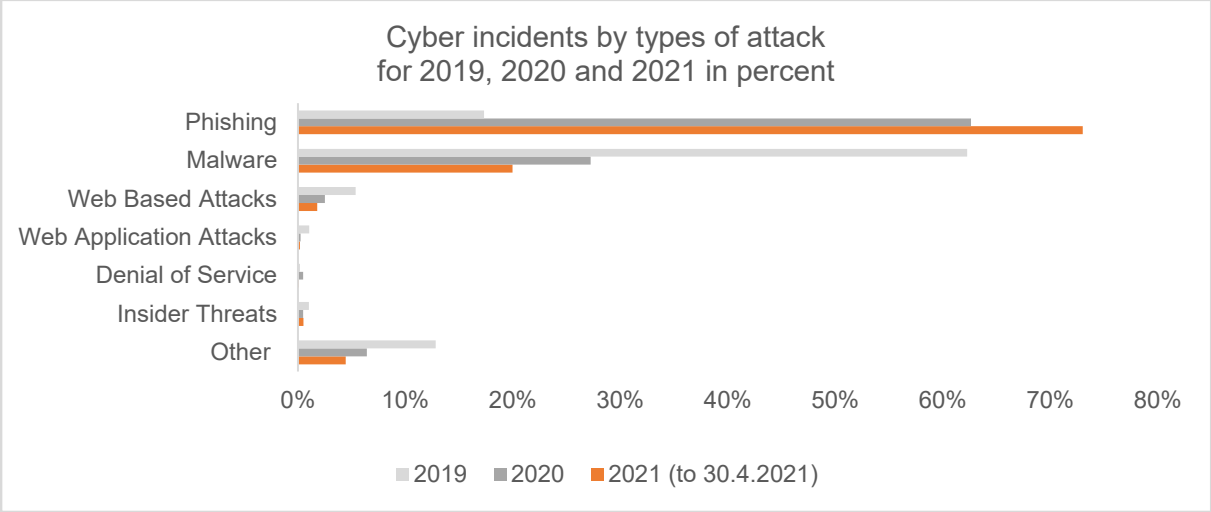


From January until the end of April 2021, phishing was also the most frequent type of attack.

[31] *ENISA: The Year in Review – from January 2019 to April 2020, ENISA Threat Landscape.*
[32] *ENISA: The Year in Review – from January 2019 to April 2020, ENISA Threat Landscape.*
[33] *ECB, Supervision Newsletter: IT and cyber risk: a constant challenge, 18.August 2021.*

During this period, almost three-quarters of all cyber incidents were attributable to this category. The top ranking can also be explained by the fact that phishing attacks are easily scalable. For example, phishing e-mails can rapidly be sent to multiple recipients.

In 2021, malware is in second place, with the following places being occupied by “other” followed by “web based attacks” and “insider threats”.



What are the most common types of attack?

Phishing	Customers’ or employees’ personal details (e.g. passwords or credit card numbers) are obtained by means of fake e-mails or websites.
Malware	Malicious software like viruses or Trojans is subsumed here.
Web Based Attacks	Web systems are compromised in order to divert their users or to start scripts (a sequence of commands) that initiate the downloading of malicious software.
Denial of Service	Systems are deliberately overloaded by a large number of requests.
Web Application Attacks	Attacks occur on the entity’s web applications of the underlying databases.
Insider Threats	Data breach or data theft by perpetrators within the company

8.1.3 FINANCIAL LOSSES

The largest proportion of losses since 2019 can be **traced back to phishing attacks**. As in the case of the number of cyber incidents, they also differentiate significantly between direct and indirect financial losses that occur in conjunction with cyber incidents both within and between the sectors. The main burden of stated losses are **sustained by credit institutions**.

- In total the **direct financial losses** associated with cyber incidents from 2019 to 2020 have fallen by ~80% and come to just under € 600,000 in 2020. The change in amount is generally attributable to the stated loss of a single entity in 2019. This illustrates also that cyber-risks that have been realised may be associated with significant financial impacts.
- **Indirect financial losses** may significantly exceed direct losses. Some entities estimate indirect losses based on the number of person days required. Other entities use potential reputational losses as a guide, which may also have an impact on the share price. Overall, the addition of data in this area is therefore only possible to a very limited extent.

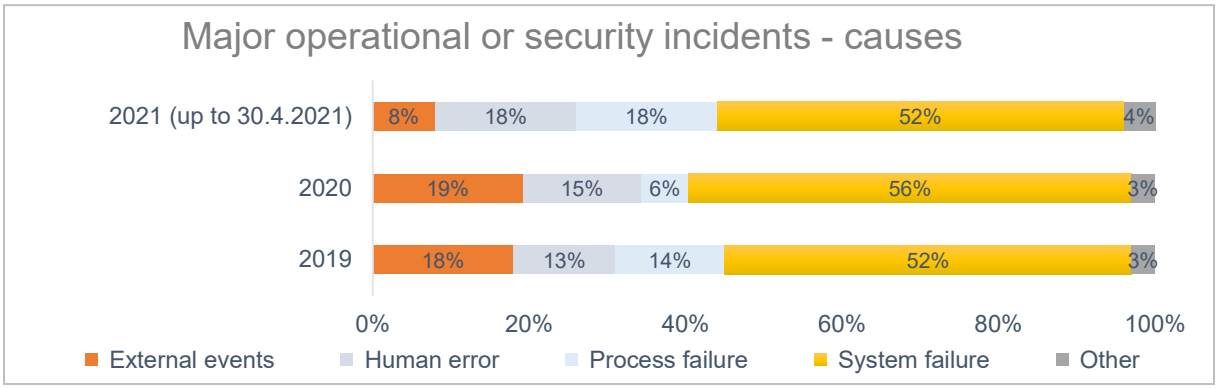
8.2 OTHER MAJOR OPERATIONAL OR SECURITY INCIDENTS

ICT-related incidents that are not subsumed under cyber incidents are stated as other major operational or security incidents.

The supervised entities were indirectly affected by major operational or security incidents **in around two-thirds of all cases affecting a service provider.** Most incidents were reported by CIs followed by IUs. The direct and indirect costs vary strongly by incident and in turn primarily affect credit institutions.

8.2.1 CAUSES

System errors are the most frequent cause of other major operational or security incidents according to the data collection that has been taking place since 2019.

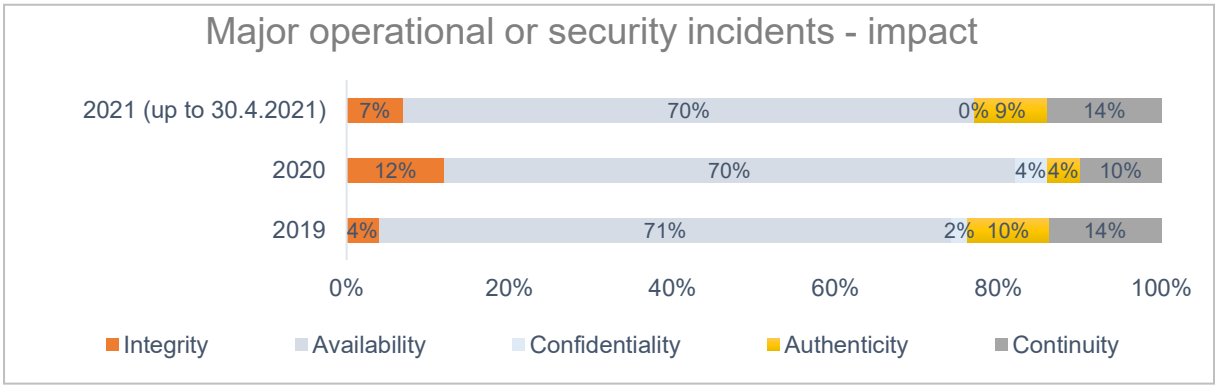


Major operational or security incidents may be caused by system errors, external events, process errors and/or by human error. FIs most frequently list system errors as the source.

While external events accounted for around one-fifth of all reports in 2019 and 2020, the comparable figure for the first four months of 2021 is just under one-tenth.

8.2.2 IMPACT

Major operational or security incidents most frequently impede targeted **availability**.



The protective goal of availability, i.e. the characteristic of being accessible and usable, has been affected by far the most since 2019.

Since 2019, approximately **70%** of all details about the impact have stated this category.

In contrast, such incidents have impacted confidentiality targets least of all.

What might the impact relate to?[34]

Availability	The property of being accessibly and usable.
Confidentiality	Information are not made accessible to unauthorised persons, public bodies or processes, or disclosed to them.
Integrity	Correctness and completeness
Continuity	The necessary processes, duties and assets for the provision of financial services, are fully accessible and functional on an acceptable pre-defined level.
Authenticity	A source is indeed what it claims to be.

[34] *The information is provided in accordance with the EIOPA Guidelines on information and communication technology security and governance, EIOPA-BoS-20/600 and the EBA Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2), EBA/GL/2017/10..*

9 POST-COVID-19 RELATED ICT RISKS

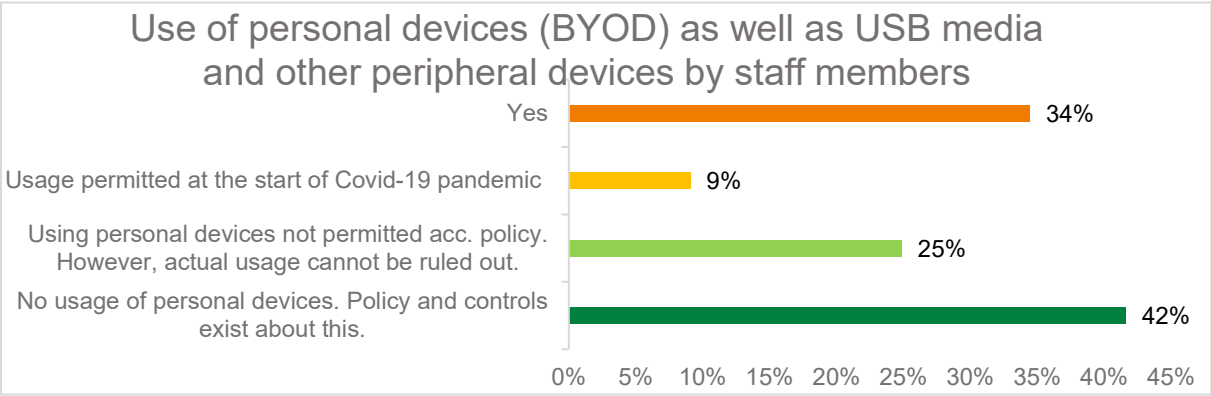
The FMA has analysed the risks in relation to returning to the physical workplace after the COVID-19 crisis in the form of analyses about using personal devices (BYOD), on the permissibility of personal applications (e.g. teleconferencing software), the redeployment of unmonitored IT systems as well as training about social engineering.

Overall, the supervised entities appear to have taken appropriate measures in order to also guarantee a return to the physical office with mitigated ICT risks.

9.1 USING PERSONAL DEVICES (BYOD)

The COVID-19 pandemic has effected unexpectedly quick and far-reaching changes to home offices. As a result, in part, the usage of personal devices (such as computers or mobile phones) and USB storage media or other peripheral devices was intensified. Unless adequate security measures are taken, new risks can arise from unknown attack targets and vulnerabilities. These arise from required updates not being carried out or from a lack of or insufficiently protected access to the devices. Among other things, there is also the possibility of infiltrating the corporate network with malware via such personal devices.

One third of supervised entities explicitly permit the use of personal devices (e.g. computers or mobile phones) as well as USB storage media and other peripheral devices, while at the same time providing for security measures.



In contrast, two thirds of supervised entities do not permit the usage of personal devices. This principle is also stated in a policy in four out of ten entities; in addition, compliance with the prohibition is also checked.

A quarter of entities have a policy that excludes such use, but are not able to exclude actual use occurring. Examples include the use of USB devices or the possibility of data being transferred using encrypted USB storage devices.

During the initial onset of the COVID-19 crisis, just under 10% of the supervised entities permitted use in conjunction with further security measures.

- The exclusion of personal devices is most prevalent in OPFs (three-quarters of all OPFs) and least prevalent in IUs (33%).
- The use of personal devices as well as USB storage media or other peripheral devices for work purposes is most widespread in IUs – and is permitted in around half of the IUs.

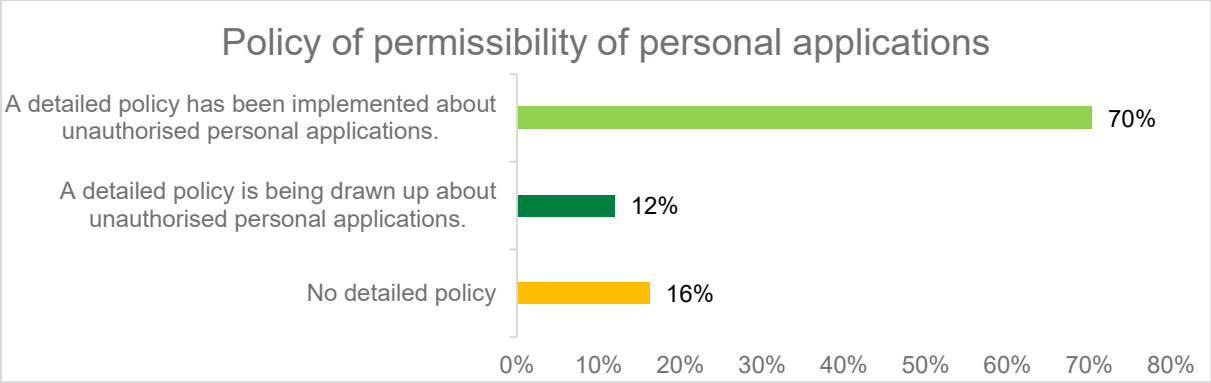
In the case of use of personal devices being permitted, the following technical and organisational security measures, for example, are also provided for in combination:

- MDM (Mobile Device Management): In an MDM, for example, all devices are inventoried and can be remotely configured and maintained. Remote deletions are also possible. Access to apps and websites can be regulated, e.g. excluded. The use of so-called containers, in which company data is separated from personal data, can also be included.
- Container solutions for mobile phones
- Technical prevention or controlling of USB use
- Using artificial intelligence to detect cyber threats
- Two or multi-factor authentication: During the authentication process, two or more proofs of identification must be provided. Factors of proof include knowledge, possession, inherence[35] or the location of the user.
- Access to a network from outside via a secure connection, via a Virtual Private Network (VPN).
- Encryption of connections between devices
- Use of virtualisations: Here, the user can work from his or her device on familiar application surfaces
- Installation of remote maintenance software or checking of security software on personal devices
- Preventing data downloads on private computers
- Operating procedures or guidelines on the use of personal devices
- Training to strengthen cyber security

[35] *This refers to biometric methods, such as a fingerprint.*

9.2 PERMISSIBILITY OF PERSONAL APPLICATIONS

Teleconferencing software, personal cloud backups, printer and other hardware drivers, video games and the use of social media may constitute possible examples of unauthorised applications in the work environment. Where IT security requirements are not observed, they may leave corporate IT vulnerable.

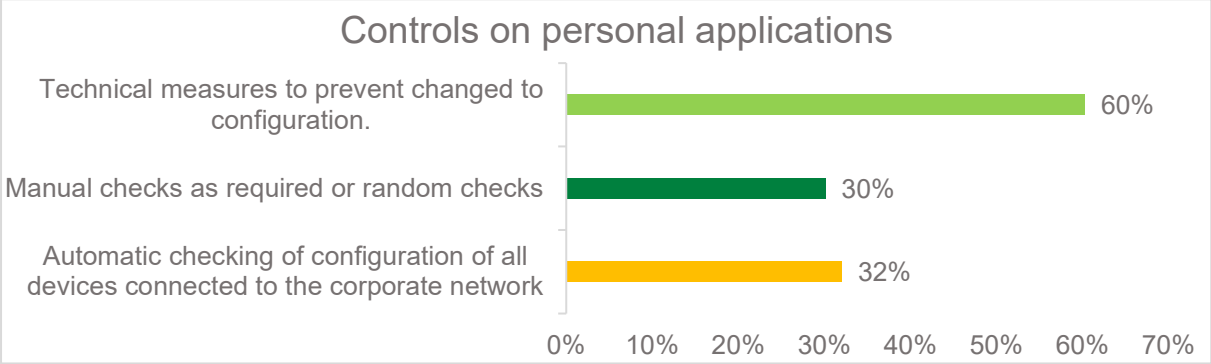


70% of the supervised entities have implemented a detailed policy on unauthorised personal applications. Such policies are more frequently in place in CIs, IUs, MCs and OPFs than the overall average.

While around 12% of FIs are currently developing such policies, 16% state that a detailed policy is not explicitly in place. In the latter cases, use of personal applications is almost universally prohibited based on guidelines or internal company standards or prevented by a security system.

Around 16% of supervised entities do not have an explicit policy on unauthorised personal applications; however, almost all of these entities exclude such uses by means of other internal company guidelines or prevent them from the outset by means of technical measures.

Supervised entities set the following controls with regard to unauthorised personal applications:



60% of FIs set technical measures to prevent configuration changes on official devices by users.

One third of all FIs automatically check the configuration of all devices connected to the company network.

In contrast, 30% of FIs randomly check configurations or on an ad hoc basis.

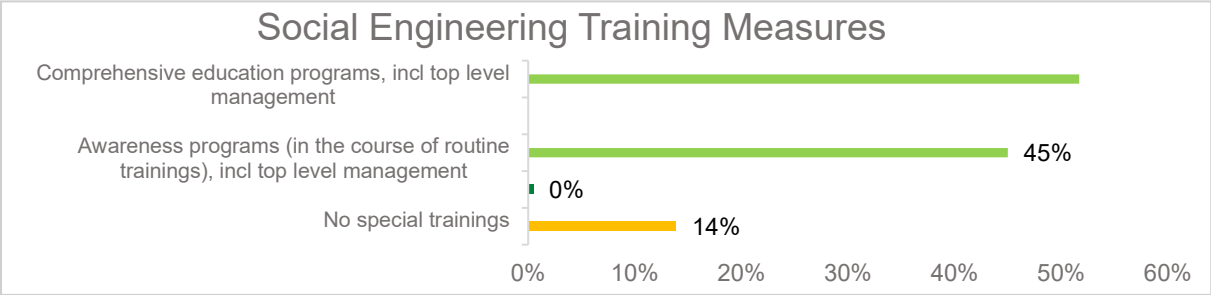
- User account control
- Principle of least privilege
- Controlled usage of administrator rights
- USB lock
- Prevention of downloads, mail transfers and file transfers by executable files
- Central management of version and patch statuses
- Vulnerability scans
- Port security
- Firewall
- Software blocking lists ("blacklists")
- Preventing the execution of unknown applications ("application whitelisting")
- Annual licence check based on the software found on the devices
- Automated recording of the software status on end devices and central storage
- Semi-automated, real-time analysis of security-relevant events (Security Information and Event Management, "SIEM" / User and Entity Behaviour Analytics, "UEBA")
- Fresh installation of the system following an incident

9.3 REDEPLOYMENT OF UNMONITORED IT SYSTEMS

As a rule, nearly all IT systems in supervised entities were/are online and monitored during the COVID-19 crisis. Only in exceptional cases were individual systems offline or unmonitored while remaining online. For example, it was not able to check the status of updates in isolated cases in home office mode. In these individual cases, prior to the physical return to the office, measures were taken, such as, for example, conducting a complete antivirus scan, or updating configurations and security patches.

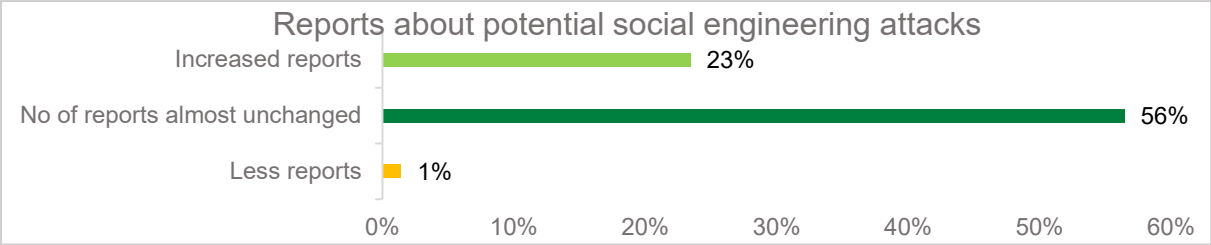
9.4 TRAINING ABOUT SOCIAL ENGINEERING

According to Europol, social engineering attacks increased significantly during the COVID-19 crisis, both in terms of their quantity as well as the level of sophistication.[36] Social engineering tries, using various means (e.g. phishing) to obtain specific information, or to motivate people to perform certain acts. ENISA recommends awareness campaigns, training measures and targeted penetration tests as precautionary measures.[37]



14% of supervised entities have not conducted special training measures about social engineering. In contrast, more than half of the supervised entities have conducted comprehensive training measures about this type of attack – including also for managerial staff. Moreover, awareness about social engineering was increased in routine training measures in 45% of entities.

Most supervised entities have conducted comprehensive training courses or measures for increasing awareness about the issue of social engineering at which managerial staff members have also participated. These measures have led to an increase in the number of potential cyber-attacks that have been reported.



Following training measures on social engineering, reports about potential attacks have increased in around a quarter of supervised entities.

At approx. 55% of supervised entities levels of reports hardly changed. A fall in the number of reports was only observed in one percent of entities.

[36] *Cf. e.g. Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020, 14.*
[37] *ENISA, What is "Social Engineering"? – Recommendations, retrieved on 7.9.2021.*

10 FMA CYBER MATURITY LEVEL ASSESSMENT

The FMA developed and deployed the FMA Cyber Maturity Level Assessment in the insurance sector in 2019 and also deployed it in the Pensionskassen sector in 2020. This tool allows the FMA to investigate the cyber resilience of supervised entities for risk classification purposes, and for preventive purposes to prepare entities for new regulatory rules in the area of ICT security (e.g. EIOPA Guidelines[38] of the European Commission's proposal on digital operational resilience for the financial sector [DORA][39]). Within the scope of the 2021 Digitalisation Study, OPFs, MCs, MIs, IFs and VASPs were also subjected to this assessment. This allows a first cross-sector comparison of cyber risk maturity.

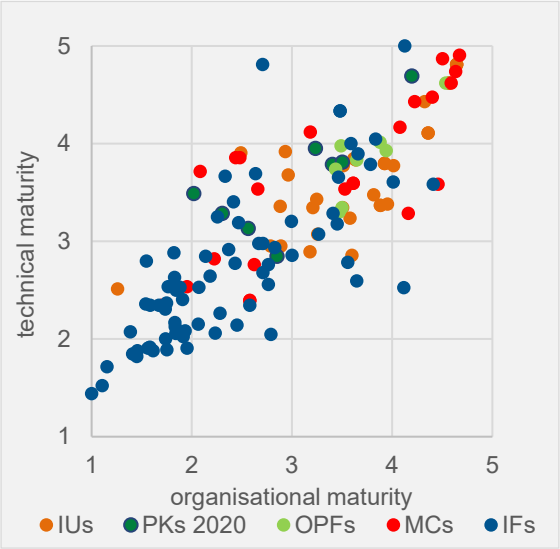
On the maturity scale from 1 to 5, where a higher degree of maturity goes hand in hand with a higher maturity in terms of age, the Austrian financial market (excluding in this case the banking sector) achieved an average overall maturity level of 3.2.

The average maturity level of 3.2 means that the Austrian financial market overall has taken the most essential precautions to ensure adequate ICT security. OPFs and IUs, with scores of 3.8 and 3.7, show the highest level of cyber maturity ahead of MCs, PKs and IFs.

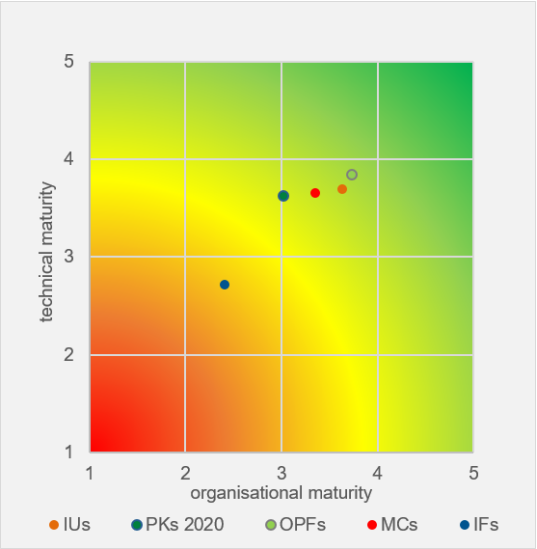
Overview	*IUs*	*PK 2020*	*OPFs*	*MCs*	*IFs*
Overall maturity	**3.7**	**3.3**	**3.8**	**3.5**	**2.6**
Organisational maturity	3.6	3.0	3.7	3.4	2.4
Technical maturity	3.7	3.6	3.8	3.7	2.7

[38] *EIOPA, Guidelines on information and communication technology security and governance, EIOPA-BoS-20/600.*
[39] *EC, Proposal for a Regulation on digital operational resilience for the financial sector, COM(2020) 595 final.*

Average degree of maturity per entity



Average degree of maturity by sector

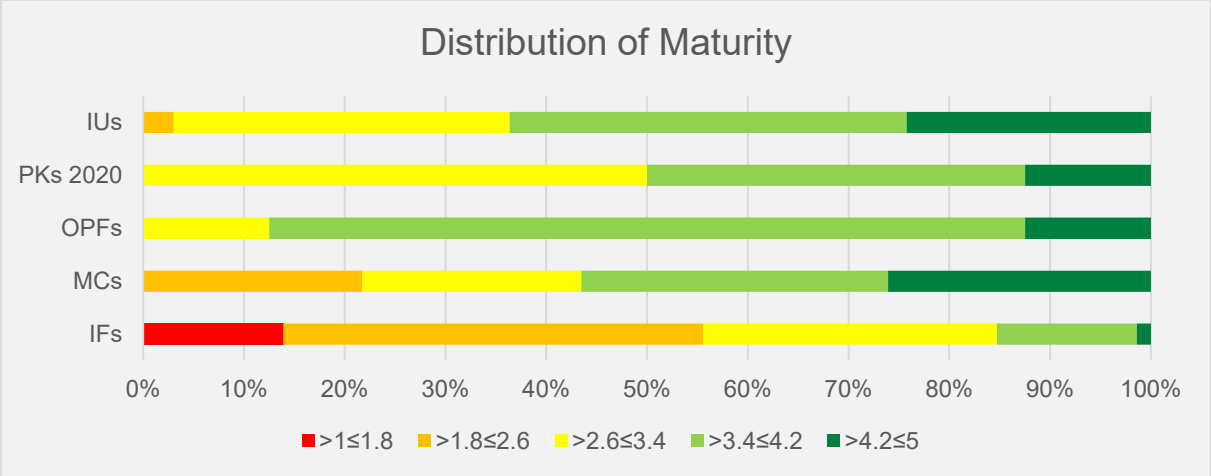


It is clearly apparent from the graphic above that it is not possible from the average maturity of the sector to determine the cyber maturity of individual entities. This assessment in any case requires consideration at the individual entity level.

- Among the second-placed IUs in the ranking, the average maturity level has increased from 3.1 for the first assessment conducted in this sector in 2019, to the current level of 3.7. In the first assessment, the organisational thematic areas achieved a lower average maturity level of 2.9 than the technical areas, which had a comparative value of 3.3. The measures taken and conspicuous features were discussed in the bilateral meetings with each individual IU following the assessment. The average organisational maturity level of 3.6 has got closer to the technical maturity level of 3.7, and is now almost at the same level.
- The Cyber Maturity Assessment was already carried out in 2020 in PKs and has been included here for comparison purposes. When interpreting the results, it should be borne in mind that PKs may have already taken further measures in the meantime.

Technical precautions for ICT security are on a higher level overall than organisational measures. High technical cyber maturity for example, can be attributed to IT outsourcing, where the IT service providers' specialised knowledge is tapped, at least in technical terms. The downside, besides a potentially high dependency on IT providers, may be the reduced awareness of setting organisational measures. It is also possible that IT departments are implementing security measures that have not yet been fully considered in the governance or controlling area.

Maturity distributions illustrate, based on a traffic light system, which company share of the specific sector has which maturity level: dark green, for example, shows the share of companies in the respective sector that achieves a high maturity level (greater than 4.2).



While around a quarter of MCs and IUs are in the dark green range, in contrast only the case for 1% of IFs and none of the VASPs. The red and orange bands – with average maturity levels of less than or equal to 2.6 – are currently mainly occupied by VASPs, IFs and MCs.

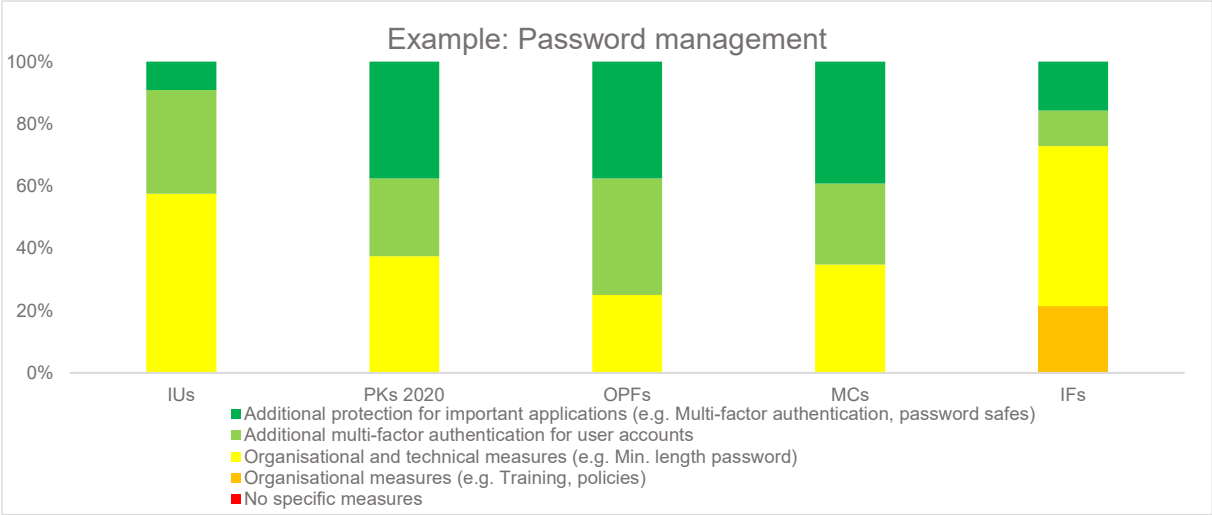
The correlation between the technical and organisational maturity levels averages 0.8: companies with a higher technical maturity level tend to have a higher organisational maturity level. Companies that intensively address cybersecurity issues do so holistically and not only in terms of setting technical measures.

In a ranking of the thirteen thematic areas, "authorisation concept" achieves the highest level of maturity overall. "Logging and monitoring" scores the lowest.

The overall average maturity levels per thematic area:

Thematic areas with a higher cyber maturity level than the overall maturity level average:

- The **authorisation concept** thematic area achieves the highest maturity level on average. In particular, password management to avoid weak passwords as well as overviews of user authorisations and the allocation of these according to the need-to-know principle are largely used as security measures.



- The authorisation concept is followed by **configurations & security settings** and **IT assets**. Virus scanners, for example, are installed as a matter of principle and their result messages are usually recorded centrally, and documented and handled in accordance with a predefined process. Software whitelisting, which only allows users to run predefined applications, is also widespread.

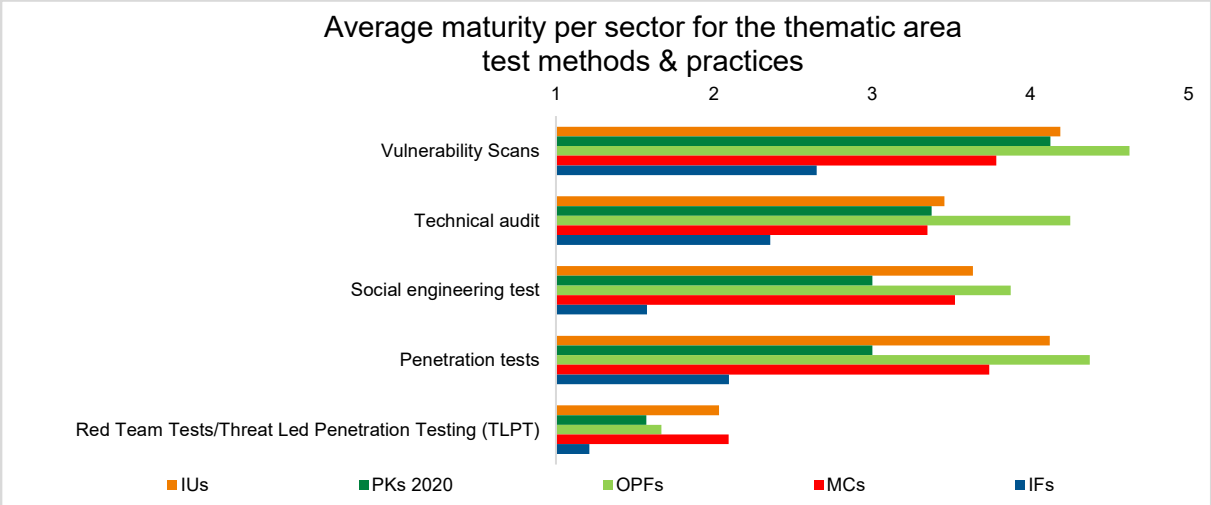
- In the category of **IT assets**, inventories of hardware and software assets are an important basis and prerequisite for security measures, such as complete vulnerability management. These inventory lists are partially automated.
- **Incident management** ranks fourth in the ranking of all thematic areas and at the same time achieves the highest average organisational cyber maturity. Processes to manage ICT-related incidents are generally defined and root cause investigations and remediation are also implemented, at least for serious incidents.
- In the next category, **Data Backup & Encryption**, backups of important data and configurations and their being stored separately from the company network are common security measures.
- With regard to the **cyber security strategy**, the promotion of awareness regarding cyber security is particularly important to the entities. This is done, for example, through appropriate staff training courses.
- This is followed by the technical thematic areas of **network security** and **vulnerability and patch management**. The systematic protection of external access to the corporate network and connections from within the company to the internet achieves the highest average level of maturity within the thematic area of network security. In Vulnerability Management & Patch Management, responsible persons for patch management are generally defined and patches rolled out at least monthly via patch management software.
- **Staff members** is the final thematic area, with a maturity level average for all sectors of 3.2, that is just above the average overall maturity level for all categories. Here, the definition of roles and responsibilities scores best. Conflicts of interest are also generally evaluated and addressed or mitigated where necessary.

Areas with room for improvement:

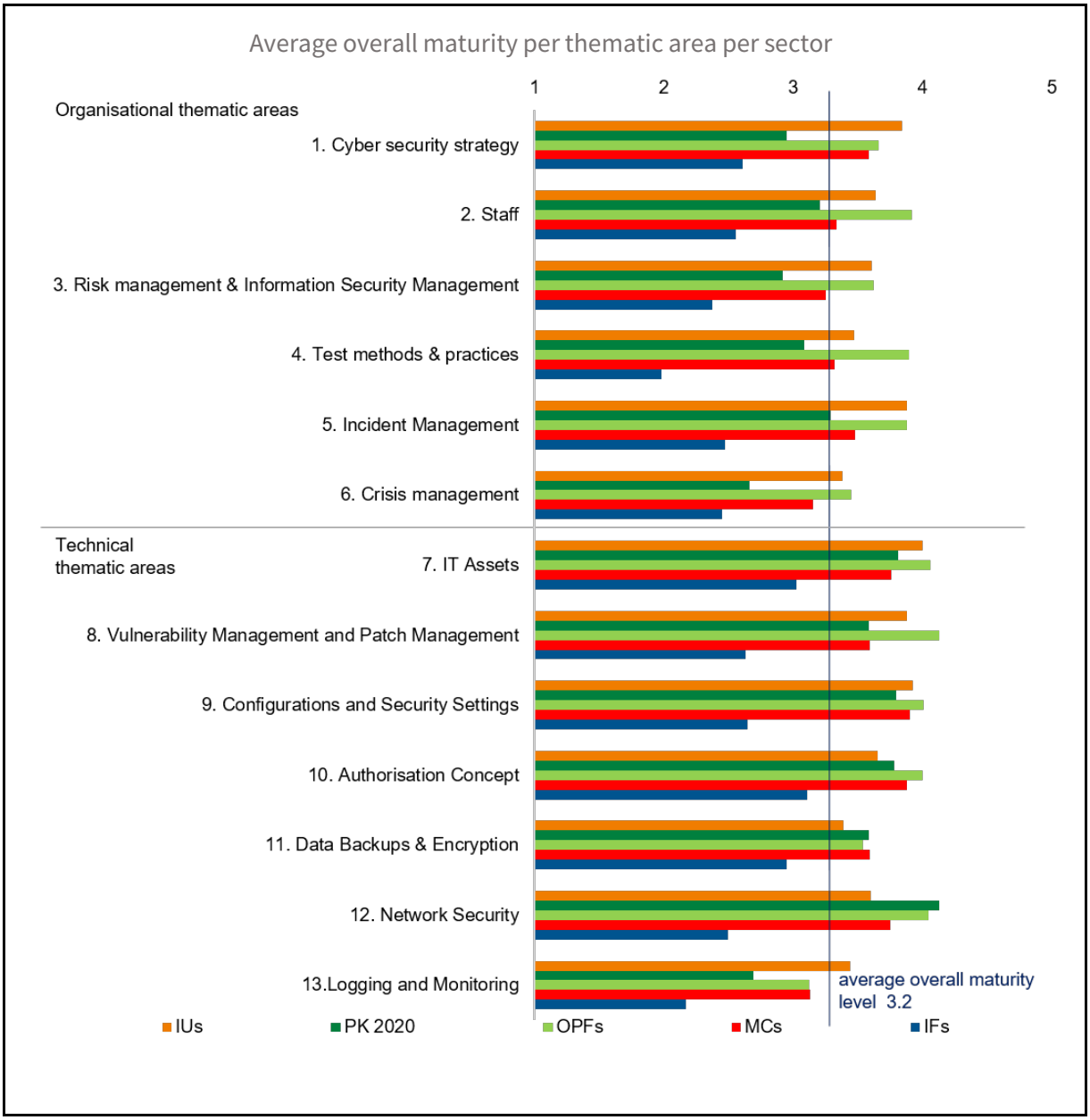
There is still particular room for improvement in the areas of risk management and information security management, testing methods and practices, emergency management, as well as logging and monitoring.

- Within the scope of risk management and information security management, information security agendas on average are handled at any rate by one organisational unit, with the establishment of an independent function being planned within the next year. Overall, there is particular room for improvement in the exchange of information about the respective cyber security framework with contractual partners.
- The question of Red Team Tests / Threat Led Penetration Testing (TLPT), in which a targeted, controlled attack on the "crown jewels" of the company is carried out using a wide variety of

methods, pushes the maturity level of the **Test Methods and Practices** category below the overall average maturity level. However, the FMA only expects significant entities with sufficient cyber maturity to perform such resource-intensive red team tests. With regard to the remaining test methods, vulnerability scans, for example, are generally carried out both on a regular as well as on an ad hoc basis in the entities.



- Emergency management has the lowest average cyber maturity of all organisational thematic areas. Above all, room for improvement exists in the selection and implementation of tests and more complex exercises for emergency management.
- In contrast to the technical thematic areas, which otherwise are above average, **logging and monitoring** is at the lower end of the cyber maturity spectrum. Generally, both the collection and monitoring of log data show potential for optimisation. The collection of log data is an important basis for recognising anomalies or deviations from usual events. The structured collection of relevant data therefore forms an important step for an effective monitoring system.


Average overall maturity per thematic area per sector
1
2
3
4
5
Organisational thematic areas
1. Cyber security strategy
2. Staff
3. Risk management & Information Security Management
4. Test methods & practices
5. Incident Management
6. Crisis management
Technical thematic areas
7. IT Assets
8. Vulnerability Management and Patch Management
9. Configurations and Security Settings
10. Authorisation Concept
11. Data Backups & Encryption
12. Network Security
13.Logging and Monitoring
average overall maturity level 3.2
IUs
PK 2020
OPFs
MCs
IFs

11 FMA CLOUD MATURITY LEVEL ASSESSMENT

The FMA Cloud Maturity Level Assessment enables a cross-sectoral comparison of cloud risk maturity levels.

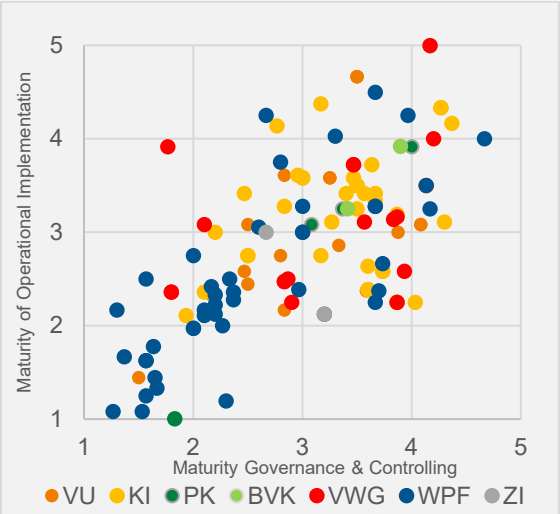
The development and objectives of the FMA Cloud Maturity Level Assessment are widely analogous to those of the Cyber Maturity Level Assessment.

The entities on the Austrian financial market were able to achieve an average maturity level of 3.1 overall. The provisions in the areas of Governance & Control and Operational Implementation respectively achieve an equally high maturity level. In a ranking of the thematic areas, migration takes first place overall. The greatest potential for improvement is in the area of ongoing monitoring.

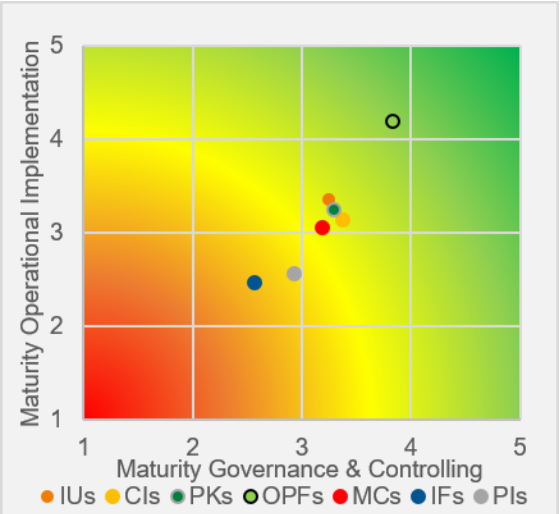
- In the FMA Cloud Maturity Level Assessment 2021, OPFs achieved the highest cloud maturity level on average – as they also did in the FMA Cyber Maturity Level Assessment. On the maturity scale from 1 to 5, where a higher maturity level goes hand in hand with a higher maturity, the maturity level of OPFs averages 4.0. IUs, MIs, PKs, CIs and MCs follow behind. These are followed at some distance by PI, VASPs and IFs.
- The cloud assessment was conducted for the first time for IUs in 2019. At that time, average cloud risk maturity level was 3.2, whereby the maturity level for the thematic areas Governance & Control with an average value of 2.8 was significantly below that for the thematic areas about Operational Implementation with a value of 3.5. In 2021, the overall maturity level increased marginally to 3.3 for this sector. This development is due to the increase in the maturity level for the Governance & Steering aggregation to an average value of 3.3.
- A Cloud Maturity Assessment was also rolled out in the PK sector back in 2020. Compared to this year's results, the average maturity levels increased on average for both the Governance & Steering thematic areas (+0.2 to 3.3) and those assigned to the Operational Implementation aggregation (+0.5 to 3.3). Overall, cloud maturity of PKs has increased from 2.9 to 3.3 from 2020 to 2021.

Overview	*IUs*	*CIs*	*PKs*	*OPFs*	*MCs*	*IFs*	*PIs*
Overall maturity	**3.3**	**3.2**	**3.3**	**4.0**	**3.1**	**2.5**	**2.7**
Maturity Governance & Management	3.3	3.4	3.3	3.8	3.2	2.6	2.9
Maturity - Operational Implementation	3.4	3.1	3.3	4.2	3.1	2.5	2.6

Average degree of maturity per entity

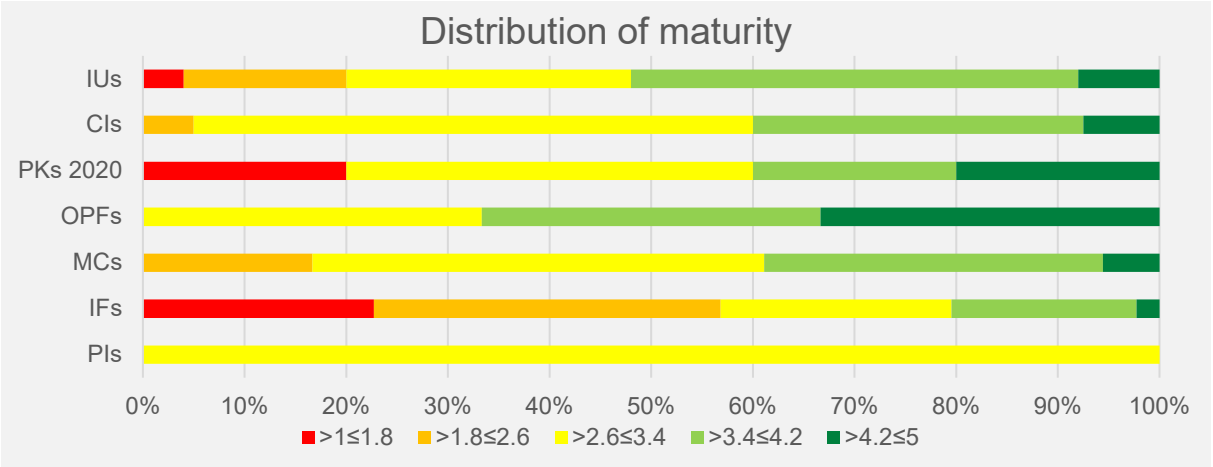


Average degree of maturity by sector



The measures in the area of Governance & Control and Operational Implementation have each achieved an equally high maturity level of 3.1.

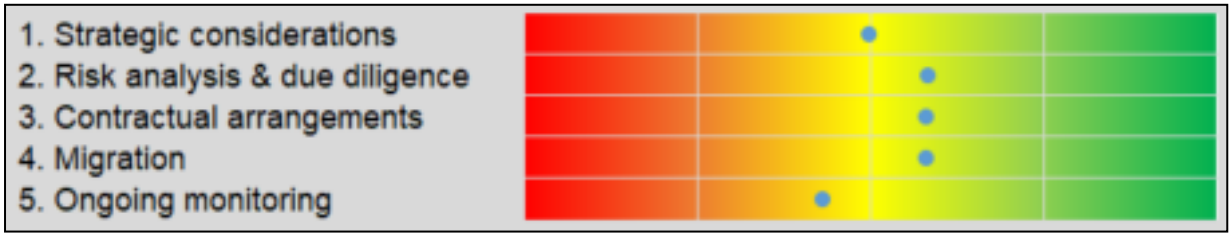
In all sectors apart from IUs and OPFs, maturity levels for governance & control exceed those for operational implementation. This is due in particular to the below-average cloud risk maturity level of ongoing monitoring/review, which is assigned to operational implementation.

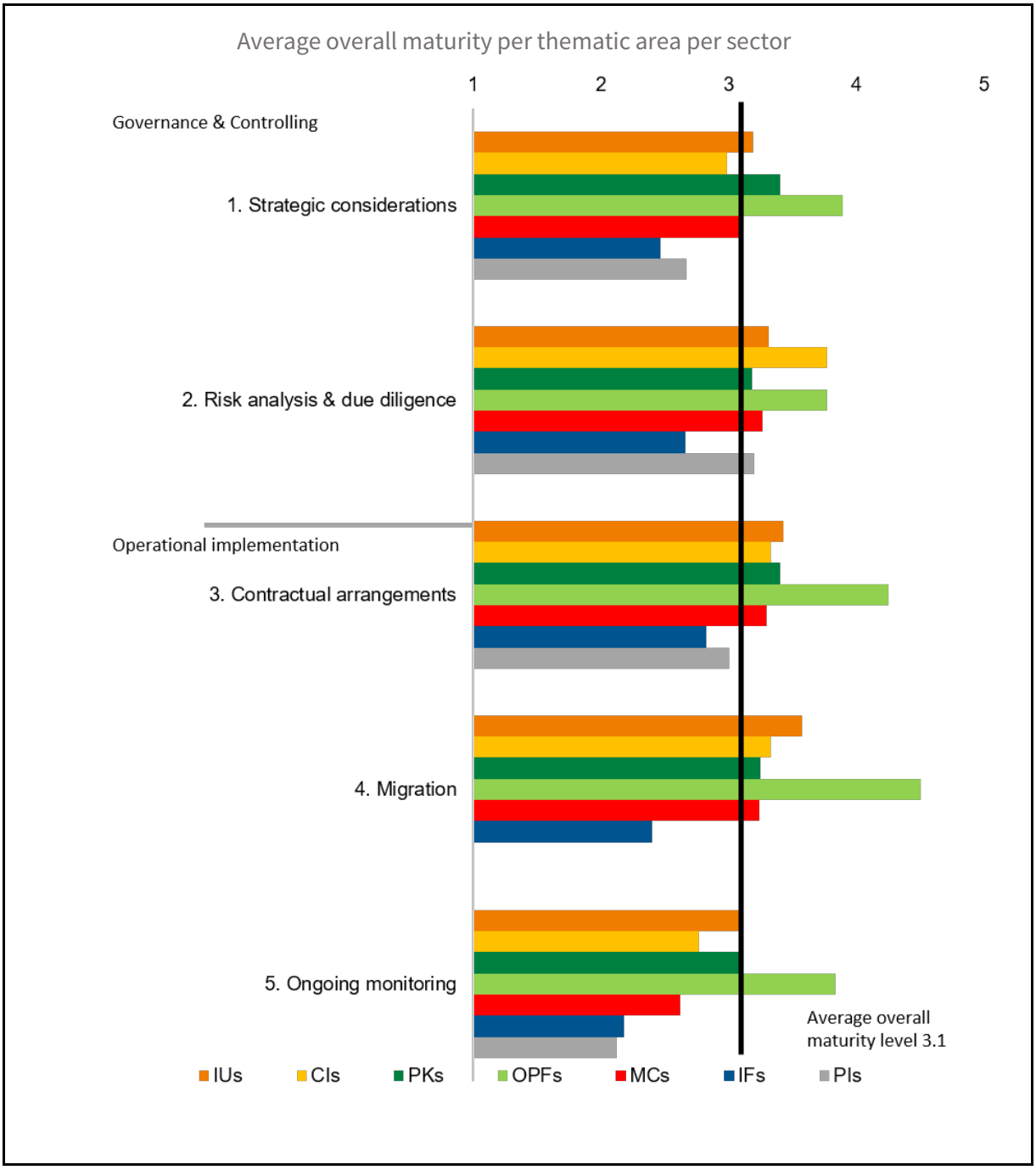


The graph about maturity distributions illustrates, based on a traffic light system, which market share of the specific sector has which maturity level: dark green, for example, shows the share of entities in the respective sector that achieves a high maturity level (greater than 4.2 and less than or equal to 5). The colour scale ranges from dark green through light green, yellow, orange to red, in descending order of cloud maturity.

For example, OPFs, IUs, CIs, PKs and MCs are mainly in the dark and light green ranges. IFs, PKs and IUs can be found in the red band.

The overall average maturity levels per thematic area:

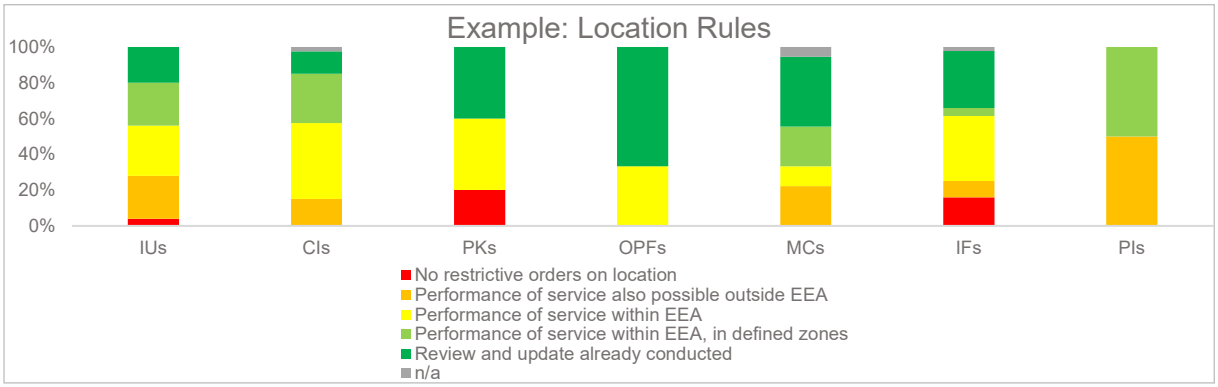




Thematic areas with a higher cyber maturity level than the overall maturity level average:

- On average, **Migration** occupies first place in the thematic areas ranking. Migration refers to the change towards using cloud services or switching to another cloud service provider. Errors can easily occur in this phase, which is why accompanying organisational and technical measures are important. Their specific design depends on the cloud services used or the type of data migration planned. The definition of roles and responsibilities for the migration, the planning of test and handover procedures and also a migration acceptance or the termination of the migration phase are generally provided for.

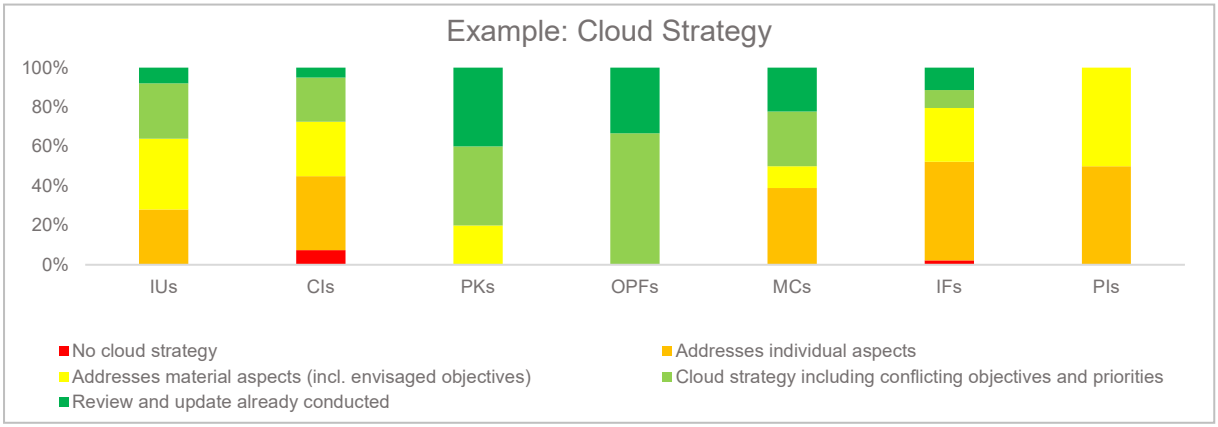
- When **drafting contracts** with cloud service providers, pre-formulated contract templates may be used. In particular, technical availability requirements as well as reporting and information requirements are generally specified in the contracts. The location of the service provision is usually limited to the EEA area.



- In the context of **risk analysis & due diligence**, assessments are made, for example, as to whether critical or important operational functions or activities are outsourced through cloud use. Specific measures for protecting data confidentiality have also been evaluated. Exit strategies are sometimes evaluated not only across the board, but also at the service level.

Areas with room for improvement:

- With regard to the category **strategic considerations**, a strategy for cloud use is usually available, in which the desired goals are also documented.



- **Ongoing monitoring/review** of cloud services shows the highest potential for taking strengthening measures overall. Currently, deviations from the agreed service level in particular are being investigated and follow-up measures agreed. The entities also use key figure analyses in some cases. Comprehensive audits of cloud service providers have only been carried out in isolated cases so far.

11.1 SUMMARY AND ACTION AREAS FOR THE FMA

New IT security and cyber risks emerge with increasing digitalisation. Cyberattacks have continually increased, in terms of both frequency and complexity, in recent years. From 2019 to 2020 alone, the number of cyber incidents in the supervised entities almost doubled. The Austrian financial market's cyber resilience has therefore become a fixed parameter of the FMA's risk-based supervision:

- The development of a common understanding on ICT topics was promoted by publishing a series of thematic FMA guides.
- Preparation for EU regulations in this respect have taken place, such as the EIOPA Guidelines on information and communication technology security and governance, which were actively co-drafted.
- The FMA is also working towards sector-specific, proportional requirements during the course of negotiations on the European Commission's Proposal for a Regulation on digital operational resilience for the financial sector (DORA).
- The FMA supports the supervised entities in strengthening their cyber and cloud maturity, for example by conducting FMA Maturity Level Assessments.
- In the insurance sector, these assessments are incorporated into the entities' risk scoring and also serve as a basis for the selection of on-site inspection activities.
- Supervisory instruments are being developed further on a constant basis. Currently, a pilot exercise is being planned for selected insurance entities to test their operational cyber resilience.

In particular, the other major operational or security incidents show that supervised entities are mostly indirectly affected through a service provider:

- The FMA is updating the interdependencies in the Austrian financial market. In 2019, a project was launched for this purpose to visualise these interconnections.
- These analyses have been extended and updated to also include sub-outsourcing in the considerations.

ICT security requires the implementation of continuous improvement processes due to ongoing technological developments and changes in the environment:

- The FMA meets this requirement, among other things, by further developing the FMA Cyber Maturity Level Assessment on an annual basis.
- Risks in connection with the physical return to work in the wake of the COVID 19 pandemic have also been evaluated.

11.2 CONSULTATION ON CYBER RISKS

- Using which additional measures or initiatives might be FMA be specifically able to contribute to increasing cyber security in the financial market?
- What specific regulatory standards are still necessary in relation to IT security in the financial market?
- Which cyber threat scenarios may be particularly relevant for the Austrian financial market in the future?
- Which core areas of IT security should be strengthened by undertakings in the Austrian financial market 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 specific developments are observable with regard to cyber-attacks?
- What lack of legal clarity, opportunities and threats do you see in relation to cyber insurance?

12 LIST OF ABBREVIATIONS

AI	Artificial Intelligence
AIFMs	Alternative Investment Fund Managers
API	Application Programming Interface
BWG	(Austrian) Banking Act
CI	credit institution
DLT	Distributed Ledger Technology
DOS	Denial of Service
e.g.	for example
EBA	European Banking Authority
EC	European Commission
EIOPA	European Insurance and Occupational Pensions Authority
ENISA	European Union Agency for Cybersecurity
ESMA	European Security Markets Authority
ETF	Exchange-Traded Fund
EU	European Union
FMABG	Financial Market Authority Act
FSB	Financial Stability Board
GDPR	General Data Protection Regulation
IaaS	Infrastructure as a Service
IAIS	International Association of Insurance Supervisors
IDD	Insurance Distribution Directive - Directive (EU) 2016/97
IFs	investment service providers and investment firms
IoT	Internet of Things
IUs	Insurance undertakings
KYC	Know your Customer
MCs	Management companies (investment management companies, real estate investment management companies, alternative investment fund managers (AIFMs))
MIs	market infrastructures
OPFs	Occupational provision funds
P2P	Peer-to-Peer

PaaS	Platform as a Service
PHI	Private health insurance
PKs	Pensionskassen
PSD	Payment Services Directive
RPA	Robotic Process Automation
SaaS	Software as a Service
SCR	Solvency Capital Requirement
SIs	significant institutions
SME	small and medium-sized enterprise
UK	United Kingdom
VAG	Insurance Supervision Act 2016
ZaDiG	(Austrian) Payment Services Act