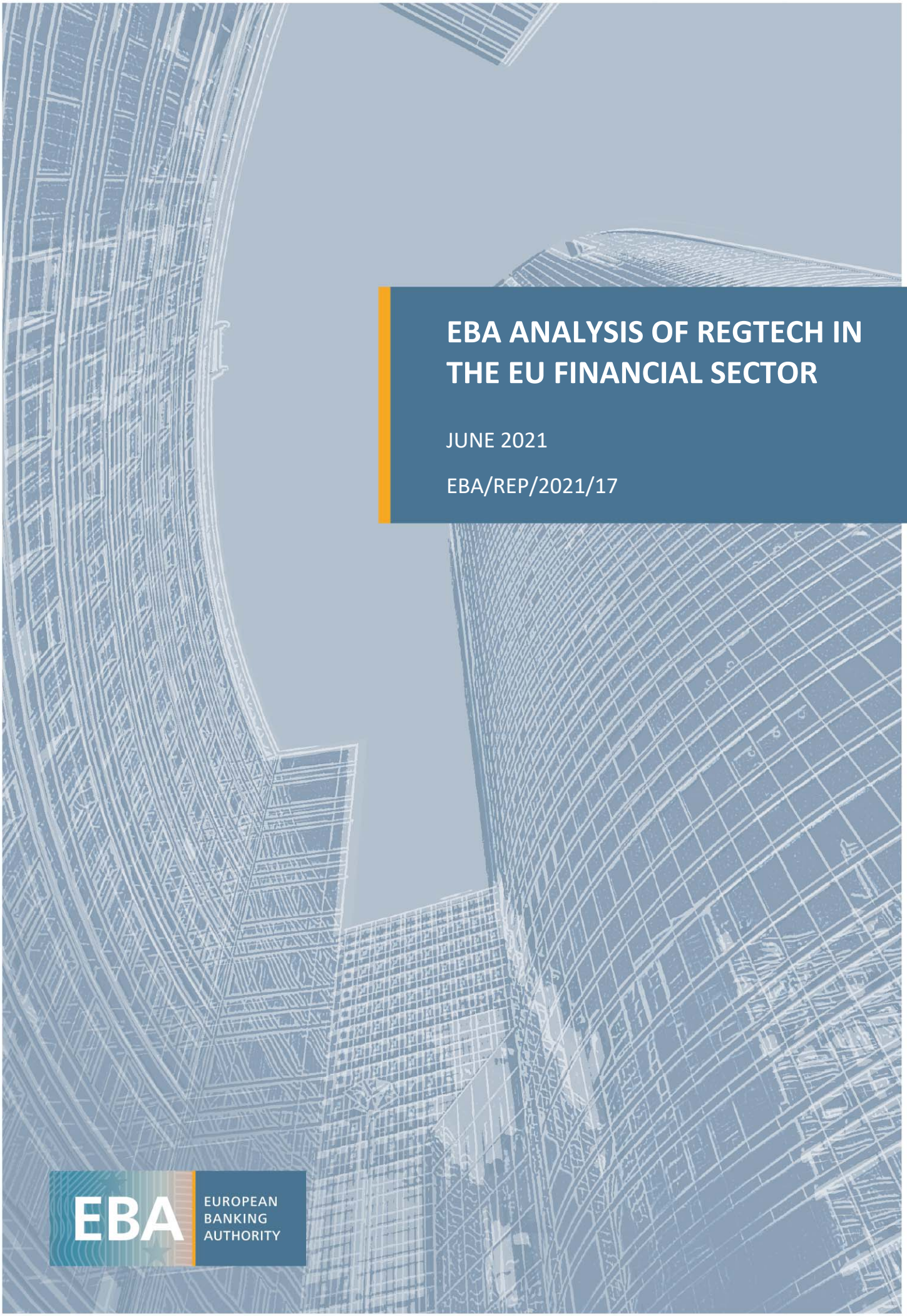


EBA ANALYSIS OF REGTECH IN THE EU FINANCIAL SECTOR

JUNE 2021

EBA/REP/2021/17

EBA EUROPEAN BANKING AUTHORITY

Contents

Abbreviations

AI	Artificial Intelligence
AML/CFT	Anti-Money-Laundering and Countering the Financing of Terrorism
API	Application Programming Interface
BTS	Binding Technical Standards
CCO	Chief Compliance Officer
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
COO	Chief Operating Officer
CRO	Chief Risk Officer
CWA	Creditworthiness Assessment
DLT	Distributed Ledger Technology
DPI	Distribution Point Identifier
EEA	European Economic Area
ECB	European Central Bank
ESAs	European Supervisory Authorities
E-money	Electronic Money
ETL	Extraction, Transformation and Load
FIUs	Financial Intelligence Units
GIS	Geographical Information System
ICT Security	Information & Communication Technology Security
KPI	Key Performance Indicator
KYC	Know Your Customer
KYE	Know Your Employee
LEI	Legal Entity Identifier
ML	Machine Learning
NLP	Natural Language Processing
POC	Proof-Of-Concept
PSD 2	Payment Services Directive 2
PUI	Process Unique Identifier
R&D	Research & Development
RaaS	RegTech-as-a-Service
RPA	Robotic Process Automation
SaaS	Software-as-a-Service
SCA	Strong Customer Authentication
SLA	Service Level Agreement
SME	Subject Matter Expert
VC	Venture Capital

Executive Summary

The EBA is focused on monitoring financial innovation, promoting knowledge-sharing and fostering technological neutrality in regulatory and supervisory approaches.

Article 31 of the European Banking Authority (EBA) Founding Regulation (EU) No 1093/2010 mandates the Authority to promote supervisory convergence and facilitate entry into the market of actors or products relying on technological innovation, in particular through the exchange of information and best practices. The aim of this mandate is to contribute to the establishment of a common European approach towards technological innovation.

The use of innovative technology in the financial sector continues at fast pace. RegTech, defined as *any range of applications of technology-enabled innovation for regulatory, compliance and reporting requirements implemented by a regulated institution (with or without the assistance of RegTech provider*), has the potential to make compliance more effective in the European financial sector.

Financial institutions using RegTech solutions highlight enhanced risk management, better monitoring and sampling capabilities, and reduced human error as the main benefits of use of RegTech solutions. Meanwhile the RegTech providers emphasise the ability to increase efficiency, quell the impact of ongoing regulatory change and improve effectiveness as key benefits associated with the use of their RegTech solutions.

However, RegTech solutions, if not properly implemented, may give rise of risks for FIs that would need to be identified, monitored, and managed. These risks may relate to, for example, compliance, concentration, business continuity, ICT and security, reputational, internal governance, conduct and consumer protection, or technology. At the same time RegTech may give rise to new risks for competent authorities supervising FIs that use RegTech solutions. In particular, potential risks may arise when trying to assess the effectiveness and reliability of the technological solutions used by FIs, and there may be a potential lack of the skills and tools needed to supervise the use of technology-enabled RegTech solutions, for example, when trying to audit the underlying algorithms.

As a result, a balanced approach is needed to acknowledge RegTech benefits and create an innovate-supportive environment, but at the same time to closely monitor and be prepared to manage any associated risks.

Against this backdrop, RegTech implementation is not without its own challenges. The table below provides a summary of the main challenges from the perspective of FIs and RegTech providers.

Main challenges for RegTech adoption **encountered by FIs**	Main challenges for RegTech adoption **encountered by RegTech providers**
1. Data-related challenges and cybersecurity threats	1. Lack of technological capabilities on FIs' side
2. Interoperability and integration with the existing legacy systems	2. Security, data privacy and protection issues
3. Changes to regulation	3. Changes of national and international regulation
4. Costs and procurement process	4. Cost of user acquisition
5. Lack of necessary skills and training	5. Lack of FIs' understanding of RegTech solutions
6. Perceived immaturity of RegTech providers' solutions	6. Lack of harmonised legal and regulatory requirements
	7. Clarity of regulatory / supervisory guidance
	8. Competition with other solutions

*Note: Highlighted in orange – challenges considered to be **INTERNAL** to FIs and RegTech providers.*

As the majority of challenges that hold back RegTech market development seem to be **internal factors** related to FIs and RegTech providers, it would be primarily for these companies to take further actions aimed at removing barriers related to data (data quality, security, and privacy, etc.), interoperability and integration with the existing legacy systems, a lack of FIs' API capabilities, costly and often lengthy and complex due diligence processes, and limited awareness of RegTech solutions.

Whilst the current legal and regulatory framework has not been identified as the most material obstacle for RegTech adoption under this study, a lack of **regulatory standards for technical requirements and data-related standards** or a lack of **harmonisation of legal and regulatory requirements** across the Member States could pose certain barriers for wider market adoption of RegTech solutions across the Single Market. Limited clarity and guidance from supervisors on the potential acceptance of certain innovative RegTech solutions has been also identified as an issue.

Building on the existing EBA's, ESAs' and CAs' ongoing initiatives, the EBA proposes the following further steps to be taken to support sound adoption and scale-up of RegTech solutions:

- further **deepen knowledge** and address any skill gaps among regulators and supervisors on RegTech, and **support convergence of supervisory practices across the EU** in the treatment of RegTech and in providing clarity on supervisory expectations;
- take further steps to **harmonise the legal and regulatory requirements**, where appropriate;
- further leverage the role and expertise of the **European Forum for Innovation Facilitators (EFIF)** and the national **regulatory sandboxes** and **innovation hubs.**

Background

Regulatory Technology (RegTech) means any range of applications of technology-enabled innovation for regulatory, compliance and reporting requirements implemented by a regulated institution (with or without the assistance of RegTech provider).

Article 31 of the European Banking Authority (EBA) Founding Regulation[1] mandates the Authority to promote supervisory convergence and facilitate entry into the market of actors or products relying on technological innovation, in particular through the exchange of information and best practices. The aim of this mandate is to contribute to the establishment of a common European approach towards technological innovation.

In practice it means that the EBA and competent authorities need to monitor RegTech developments to be aware of the benefits that RegTech solutions can bring, develop good understanding of any emerging risks, and make sure that the regulatory and supervisory frameworks can capture and mitigate those risks. Last but not least, accumulated experience can be used to apply innovation in supervisory processes when developing SupTech tools.

This report, based on several sources of information elaborated in the methodology section, provides insights into the following:

- the current RegTech landscape in the EU, providing a mapping and understanding of the existing RegTech solutions, identifying the status of adoption, financial institutions' spending, the impact of COVID-19 as well as trends and drivers.

- the overall benefits of the use of RegTech, either developed by financial institutions or provided by RegTech providers, as well as its perceived advantages of RegTech solutions over 'traditional' methods.

- the overall challenges faced by financial institutions when using RegTech solutions and RegTech providers, when offering their service, identifying the main barriers and risks related to the adoption and use of RegTech solutions. This is followed by a section on risks that FIs could face if RegTech solutions are not properly implemented, and main supervisory risks that may arise for competent authorities when supervising FIs that use RegTech solutions.

- Report continues with deep dives into five RegTech segments: Anti Money-Laundering/Countering the Financing of Terrorism (AML/CFT), fraud prevention, prudential reporting, ICT security, and creditworthiness assessment (CWA). These deep dives provide an insight into RegTech segment-specific current uses, benefits, challenges and supervisory risks.

[1] Regulation (EU) No 1093/2010

- The report concludes with a summary of findings and proposals suggesting the way forward to facilitate the scale-up of innovation for RegTech in the EU to support the digital transformation of the EU financial sector.

The analysis of the RegTech market in the EU financial sector and proposals included in this report will form part of future policy discussions within the wider objectives of facilitation of innovation and aim to assist the European Commission's objectives included in the Digital Finance Strategy.

The proposals are all technology neutral, meaning that the use of a specific technology is neither preferred nor prejudiced and the use of new technologies is not inadvertently prevented because of the regulatory or supervisory approaches.

EBA approach to technological neutrality

The EBA is focused on monitoring financial innovation, promoting knowledge-sharing and fostering technological neutrality in regulatory and supervisory approaches.

The EBA keeps a close eye on the emerging market developments to understand, on a timely basis, opportunities and risks arising from innovative technologies and, where appropriate, to respond with changes to regulatory and supervisory approaches to i) remove inadvertent barriers to applications of these technologies in the financial sector and ii) to mitigate effectively any risks arising.

The EBA seeks to promote a common approach across the EU to the acceptance, regulation and supervision of applications of innovative technologies, regardless of whether incumbents seek to use RegTech solutions across a group, or RegTech providers seek to scale up their products or services cross-border.

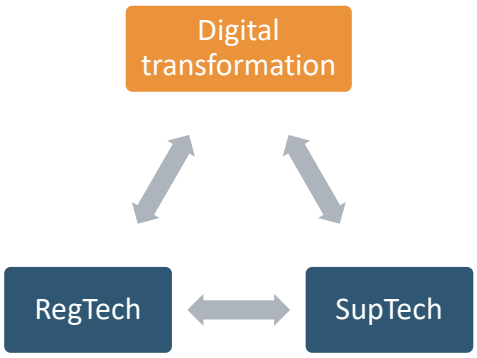
Technological neutrality is about achieving the right balance between facilitating innovation, scalability and competition across the EU Single Market whilst continuing to achieve the central regulatory objectives of consumer protection, prudential resilience, market integrity and ultimately financial stability. Technological neutrality principle means that (i) the use of a specific technology should neither be preferred nor prejudiced and (ii) the use of new technologies should not be inadvertently prevented because of the regulatory or supervisory approach.

EBA technology-related work and RegTech

As part of the EBA's current and future FinTech priorities, which include a range of actions to support the scaling of innovative technology cross-border, the EBA has produced this report on the use of RegTech with the aim of providing an overview over the RegTech market activity in the EU, raising awareness on RegTech within the regulatory and supervisory community, and of informing any relevant future policy discussion as to how best to ensure that regulatory and supervisory initiatives facilitate scaling of innovation. RegTech is one of the priority topics for the EBA in its

2020 – 2021 work programme. This work is consistent with the European Commission's Digital Finance Strategy[2], where RegTech falls among one of the main topics.

Technologies are changing the world with a possibility of challenging legacy systems with more effective and advanced systems. This technological change puts digital transformation on top of the agenda of most of the institutions around the world. These days when data is becoming 'the new gold', effective data gathering, governance, and analytics become an essential attribute of successful institutions.



The financial sector differs from others by its large amount of data and because it is highly regulated. As a result, RegTech and SupTech solutions stand ready to become key for financial market participants and regulators to ensure an effective, safe, and sustainable market. RegTech is only one part of the digital transformation of the regulatory compliance processes. The RegTech part covers interaction with financial institutions, data gathering and initial steps of data governance. Another very important part linked to the transformation of regulatory activities is related to the use of technologies for supervisory purposes (SupTech), covering the data analytics and second part of data governance at the supervisory and regulatory side. The use of SupTech will be in the focus of the EBA analysis in the near future.

[2] Digital Finance Strategy for the EU (24 September 2020). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591

Methodology

The RegTech report has benefited from many information sources to ensure comprehensive coverage of both the current landscape and to identify the potential way forward:

- desk-based research carried out regarding the overall RegTech developments and activities within and across Member States,
- competent authorities' survey on RegTech (2019),
- EBA industry survey (August – September 2020),
- EBA virtual RegTech workshop (December 2020),
- in-depth external RegTech market study (January – February 2021),
- European Forum for Innovation Facilitators (EFIF) survey on RegTech (January 2021),
- bilateral industry interviews,
- cost of compliance study and the Discussion Paper on Feasibility study for integrated reporting system (2020 – 2021),
- EBA Risk Assessment Questionnaire (Spring 2021),
- discussions with competent authorities.

From the desk-based research, the EBA identified five areas with an increasing use of technology-enabled innovation to assist financial institutions in meeting their regulatory, compliance and reporting requirements. These five areas are the five deep dive areas included in this report.

In mid-2020 and early 2021, the EBA conducted a general RegTech industry survey and a further deep-dive market study, where all relevant stakeholders (financial institutions[3] and RegTech providers) were invited to share their views and experience on the use of RegTech solutions. A total of 115 financial institutions (from 26 Member States) and 147 RegTech providers (both based in the EEA and outside EEA) responded to the survey[4]. The non-EEA RegTech providers were included in the survey sample since they are working with financial institutions based in the EU.

In December 2020, the EBA organised a virtual workshop on RegTech, attended by RegTech providers, financial institutions and competent authorities, which provided insights into the main challenges faced by RegTech market participants, governance-related aspects from both financial

[3] Credit institutions, payment institutions, electronic money institutions, investment firms and other types of financial institution

[4] Some of the respondents contributed to both a general RegTech industry survey and a deep dive market study.

institutions and RegTech providers' perspective, and further examples of AML/CFT and ICT use cases.

The aforementioned sources ensured broad feedback from a wide range of stakeholders, i.e. competent authorities, financial institutions and RegTech providers, which has been essential to better understand the extent of, and the impact on the use of RegTech solutions.

Across the various channels used, as described above, the respondent sample is broad enough to provide valuable insights into RegTech market developments. In terms of the geographic distribution of financial institution respondents, the sample covers all regions within the EEA and represents a mix of credit institutions, payment institutions, electronic money institutions and investment firms. However, the interpretation of findings needs to take into account the sample size described above, acknowledging that not all findings (especially in the deep dive findings) may be representative of the whole population of financial institutions and RegTech providers.

The sources above have provided the necessary insights to build and share knowledge on RegTech and identify ways to facilitate the adoption and scale-up of RegTech solutions across the EU.

1. Current RegTech landscape in the EU

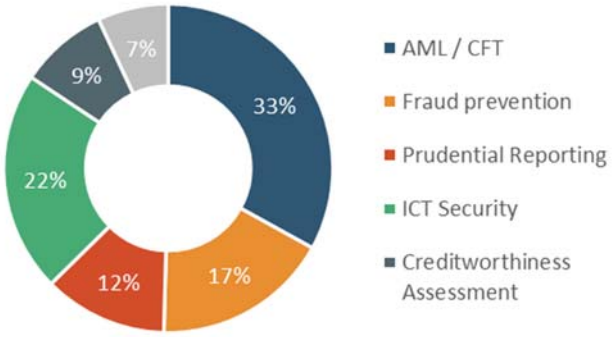
This chapter provides an overview of the current RegTech landscape in the EU. It illustrates the main RegTech solutions used by financial institutions and indicates areas in which RegTech providers are the most active. It also provides information on the status of adoption, key trends and drivers on RegTech development in the EU, main technology solutions behind the RegTech solutions and governance processes for RegTech adoption.

1.1 Overview of the RegTech market in the EU

Based on the sample of surveyed financial institutions (FIs) and RegTech providers, the most frequently used RegTech solutions are related to AML/CFT, but there is a broad range of RegTech solutions available in the market.

The survey responses provided by FIs demonstrate a balanced coverage of RegTech solutions in terms of areas covered. RegTech solutions in the field of AML/CFT are followed by RegTech for ICT security, fraud prevention, prudential reporting, and creditworthiness assessment. This may indicate the relative priorities on areas where technology-based innovations may bring the most significant value, also taking into account the risk-based focus.

Figure 1.: RegTech market segments – proportion RegTech solutions used by FIs



However, the large share of FIs' reported ICT security-related RegTech solutions may include 'usual' ICT security tools and compliance solutions, which could explain a high percentage of use cases here, since the use of technology in this field is very common. This issue is further explored in deep dive section 4.4 on ICT security. Data from the recent EBA Risk Assessment Questionnaire[5] also suggests that the distribution of RegTech solutions used by FIs is closer to the one indicated by

[5] EBA conducts semi-annual Risk Assessment Questionnaires (RAQs) among banks and market analysts. RAQs carried out in spring 2021 have received responses from 59 banks. 75% of surveyed banks have RegTech solutions in use; out of them, 80% have RegTech solutions in the AML/CFT segment, 55% in fraud prevention, 36% in prudential reporting, 25% in creditworthiness assessment, 23% in ICT security, and 16% in 'other' category.

RegTech providers below, with ICT security-related RegTech solutions among the least frequently used ones.

Figure 2.: RegTech solutions that financial institutions have experience with and areas where RegTech providers offer their services

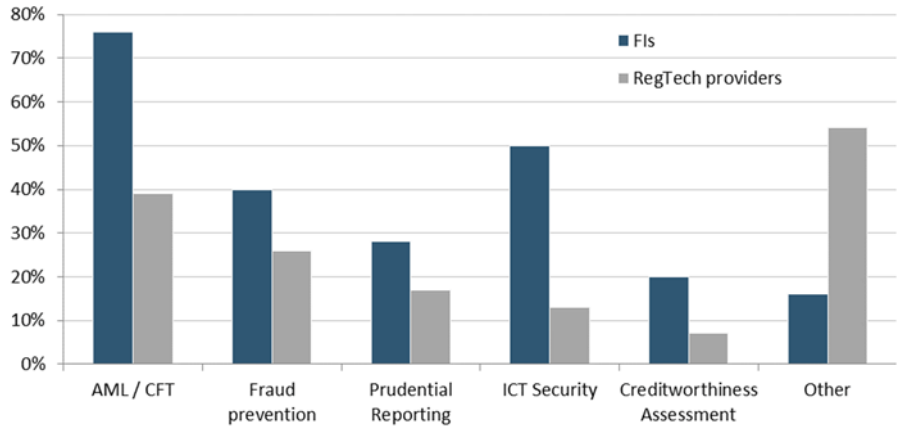
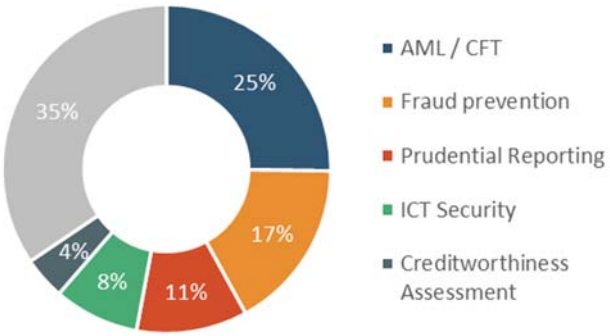


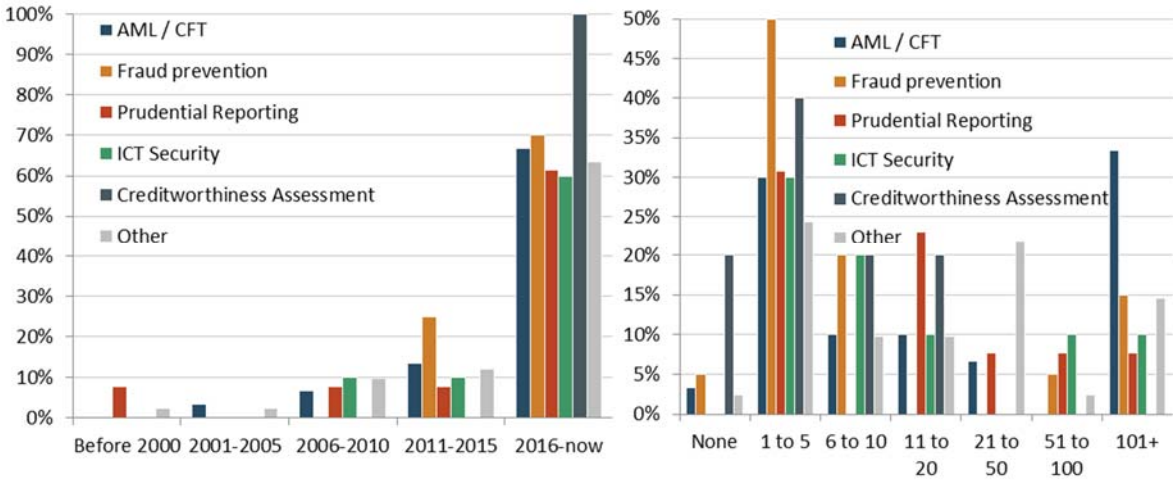
Figure 3.: RegTech market segments – proportion RegTech solutions offered by RegTech providers



One third of all solutions offered by RegTech providers were self-categorised as 'other' solutions. This indicates a broad range of fields that RegTech solutions available in the market can cover. The set of 'other' RegTech solutions includes various RegTech use cases ranging, for example, from regulatory horizon screening and third-party due diligence solutions to self-sovereign identities or 'know your employee' solutions which were not deemed to fall under the five selected categories. The full list of 'other' RegTech solutions offered by RegTech providers is included in the Annex to this Report.

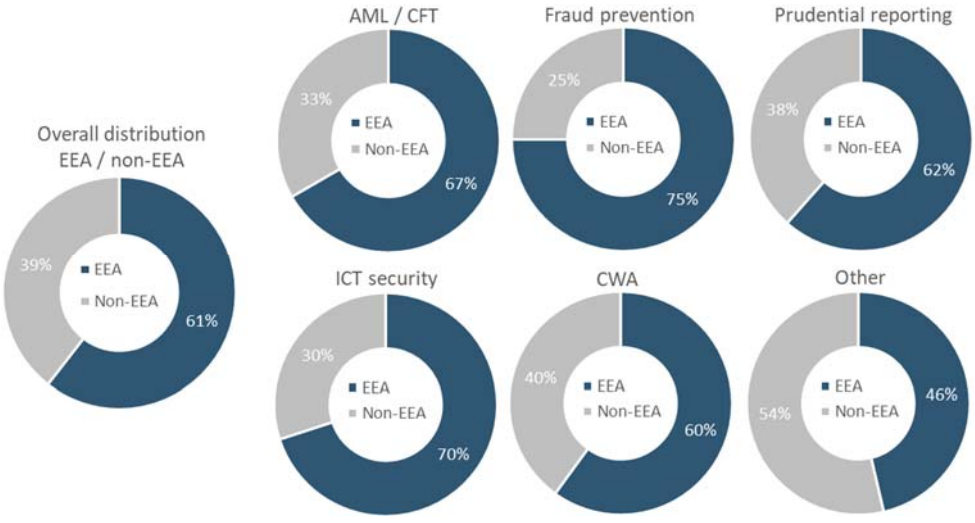
The survey results exhibit that there is a sizeable RegTech market accessible to FIs, although the majority of surveyed RegTech providers went live with their solutions only within the last six years. More noticeable origins of RegTech market development seem to have started after 2006, but the RegTech development pace rapidly picked up after 2016. The large fraction of relatively new RegTech solutions in the sample data is also reflected in the big share of RegTech providers with a small number of clients – about 39% of the RegTech providers in the sample have less than six financial institutions as their clients.

Figure 4.: Year of RegTech solution going live first (left) and number of financial institution clients (in production) (right)



From a geographical perspective, the RegTech market share covered by EEA RegTech providers (blue) is larger than the non-EEA RegTech providers (light grey). Approximately 60% of all respondent RegTech providers are EEA-based, with a strong presence across all of the identified areas of focus, primarily fraud prevention, ICT security, AML/CFT and prudential reporting, indicating an active market of solutions in the key RegTech areas. The exception is the 'other' category of RegTech solutions, where more than half of surveyed RegTech providers are non-EEA-based. This suggests that they are broadening the scope of available RegTech solutions for FIs in the EEA**.**

Figure 5.: RegTech providers distribution – EEA vs non-EEA



The research findings indicate that currently non-EEA-based RegTech providers covered by the study seem to be larger and somewhat more successful than their EEA peers[6]. Surveyed non-EEA RegTech providers currently have in the pipeline more ongoing implementation projects (on

[6] This is based on 2/3 of non-EEA country RegTech providers represented in the sample located in UK.

average 14 versus 7 projects by EEA RegTech providers). The survey data captures the trend that, on average, non-EEA-based RegTech providers included in the sample appear to have 2.3 times more customers than the average EEA-based competitor, and, on average, have more employees. The share of RegTech providers with more than 50 employees is twice as high in non-EEA countries (38%) compared to RegTech providers in the EEA (18%). In addition, non-EEA RegTech providers have five times more RegTech solutions falling into the 'other' category which went live in 2019/2020. This may signal potentially innovative solutions, meeting emerging market needs**.** However, all the above findings need to be interpreted taking into account that the majority of surveyed non-EEA-based RegTech providers were headquartered in the United Kingdom and until recently benefited from the Single Market. This finding may also be due to the fact that smaller, or compared to EEA RegTech providers, equally-sized non-EEA RegTech providers did not take part in the survey, possibly because of limited focus on the EEA market, and the rather significant effort generated by taking part in the survey.

Survey results also indicate some signs of RegTech market saturation beginning in certain RegTech segments in terms of solutions offered. A large proportion (40%) of RegTech providers are already in the growth phase (with advanced rounds of venture capital funding), moving away from the early stage (e.g. seed, crowdfunding, etc.) and build-up stage (e.g. angels, venture capital). There are noticeable differences in the higher proportion of non-EEA-based RegTech providers (50%) in the growth phase than EEA-based RegTech providers (34%). A number of the latter is in ideation (self-funded) and early-stage phase of development.

Status of adoption

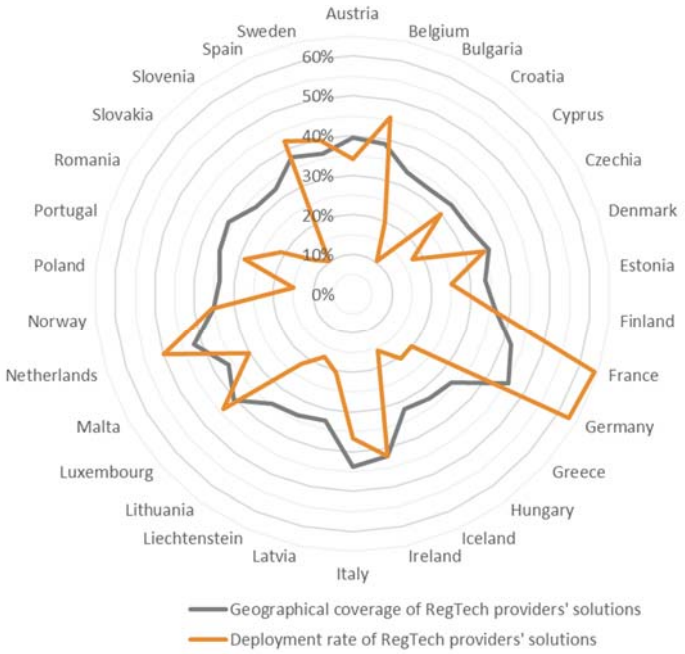
This section provides a glance into the actual and potential RegTech adoption rates across the various segments and countries, an overview of national developments related to facilitate RegTech, RegTech spending trends and level of FI satisfaction with the adopted RegTech solutions.

RegTech solution adoption rates

FIs' responses indicate that there are a number of FIs with rather advanced experience of RegTech solutions and services. From a maturity perspective, on average, more than a half of RegTech projects are already in the production stage. In the fields of AML/CFT, fraud prevention and ICT in production share are even higher – above 60% of RegTech solutions. The remaining FI engagement on RegTech cases is almost equally split between a proof-of-concept pilot and introductory vendor presentations.

Analysis of geographical coverage of RegTech providers' solutions across the EEA countries suggests a rather similar distribution. The differences in coverage seem to depend on a particular RegTech market segment. On average, the highest coverage is in the case of the prudential reporting RegTech solutions (51%). The theoretical coverage, and potential for adoption, is closely followed by CWA solutions (42%), AML/CFT (36%), ICT security (33%) related solutions, and fraud prevention (27%) RegTech solutions. From the RegTech providers' perspective, fraud prevention-related solutions have, on average, the lowest coverage level, which indicates that such solutions are targeting FIs in fewer countries.

Figure 6.: The geographical coverage of RegTech providers' RegTech solutions and deployment rate



However, the observed scale of RegTech solutions adoption is not homogenous across the different RegTech segments and among the EU Member States. The current environment, with COVID-19-facilitated digitalisation trends and the shift to remote and online solutions, was in particular beneficial for AML/CFT and onboarding solutions. Considerable opportunities emerged for AML/CFT-related providers because of the growing needs of FIs, for instance, for remote onboarding solutions, or sanctions and Politically Exposed Persons (PEP) screening tools. The COVID-19 pandemic effect was less pronounced for other RegTech use cases, such as reporting.

While the results on RegTech solutions offered and deployed may be affected by the respondents' sample size and its distribution, collected data suggests that the market adoption rates may be high in some countries, whilst lower in others. Among the possible reasons to explain this difference may be the smaller size of the latter jurisdictions' financial markets and/or complexity in terms of international linkages.

Overview of national developments related to RegTech

Public authorities across the EU undertake several RegTech-related activities to address inadvertent barriers to the application of these technologies and to the scaling up of innovation in this field. Although the majority of national competent authorities are by law neutral towards competition and do not have specific mandates to support or promote particular business fields, including the RegTech sector, they have an interest in finding ways to engage with the industry on RegTech-related topics from a supervisory perspective. This helps them to keep up-to-date with the market developments, increases understanding of RegTech solutions which facilitate supervision of risks, and, at the same time, allows the opportunity to provide guidance (to the degree possible) for FIs and RegTech providers.

Public authorities are seen to hold regular innovation facilitators initiatives (regulatory sandboxes and innovation hubs, brought together at the EU level by the European Forum for Innovation Facilitators) and thematic meetings with the FIs, RegTech and industry associations. Some CAs regularly discuss with the industry the obstacles to innovation they face in the regulatory framework when developing RegTech solutions and try to better understand the potential use cases of innovation in the field of RegTech. Other CAs use innovation facilitators to consult RegTech providers on regulated market matters or relevant legislation requirements.

When particular obstacles are identified, some CAs organise *ad hoc* taskforces to discuss potential solutions. In some instances, CAs issue guidance notes. In others, they establish specific requirements and quality standards for RegTech providers. For example, RegTech providers offering online identification solutions to financial institutions (i.e. automated video analysis for client onboarding) have to meet certain requirements and must be certified by the national agency for the safety of the information systems[7].

CAs also are seen to establish working groups and hold workshops with industry to conduct in-depth thematic studies into specific issues related to the use of regulatory technology (e.g. on the use of AI in the financial sector, use of AI and ML in credit scoring, etc.). Some CAs also intend to host TechSprints to gain further practical experience in RegTech use cases (e.g. use of AI for credit assessment).

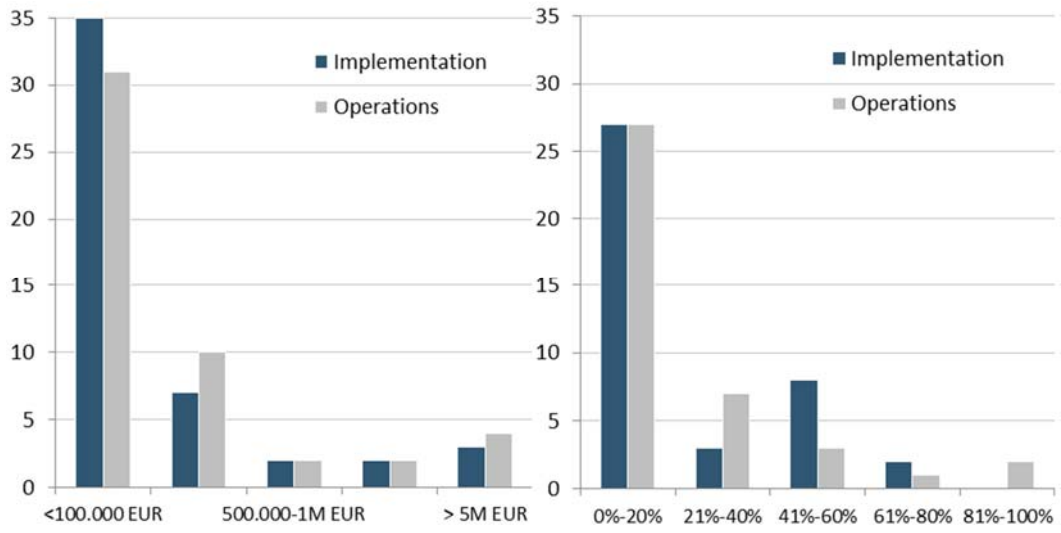
Spending on RegTech

In half of the surveyed FIs, investment and spending on RegTech solutions, in terms of the overall IT budget, is below 20%. However, the survey results indicate that there is a handful of FIs that seem to have significant reliance on RegTech, with up to 40%-60% of the total IT budget going into the operations of RegTech solutions. Only in a few cases were RegTech budgets indicated to exceed 60% of total IT spend.

In nominal terms, most of the respondent FIs (70%) spend less than EUR 100,000 on the implementation and operations of their RegTech solutions. There is another group of FIs that allocate more significant budgets (up to EUR 500,000) for RegTech solutions, and a few of those with an IT spend on RegTech solutions above EUR 5 million. However, it remains to be seen if rather small RegTech budgets of some FIs become a challenge in the future to fully leverage digitalisation and use of technology trends.

[7] Since 1 April 2021, in one Member State RegTech providers providing online identification solutions to FIs (automated video analysis for client onboarding) have to meet certain requirements and must be certified by the national agency for the safety of the information systems.

Figure 7.: 2020 IT spend on RegTech solutions



Looking into the future, despite the ongoing pressure to reduce costs, the spending forecast on RegTech technology for 2020 and 2021 compared to 2019 was rather positive. The majority of FIs were planning a slight or moderate increase of investments into RegTech. 10% of FIs predicted a significant increase of more than 50% of the current investment, 19% assumed an increase of 25% – 50%, and 29% of FIs – a slight increase of less than 25%. 19% did not see the need to change the current spending on RegTech, whereas a total of 6% of FIs stated their intention to decrease their spending. However, this forecast may be impacted by the developments of the COVID-19 pandemic in both positive and negative ways, therefore it will be important to continue closely monitoring the emerging trends.

COVID-19 impact on RegTech

For the majority of FIs, the COVID-19 pandemic did not have any impact on their RegTech projects. More than half of FIs indicated that COVID-19 had no impact on their RegTech project implementation. Almost one fifth indicated either slight positive or slight negative impact, with only a minor share reporting strong impacts on either side. Among the FIs' RegTech solutions that experienced negative impact were creditworthiness assessment (40%), prudential reporting (31%) and, interestingly, AML/CFT (31%) use cases.

The impact of COVID-19 on RegTech adoption has a strong dependency on the type of FIs. A third of electronic money institutions and payment institutions reported a negative impact of the pandemic on their RegTech projects.

From the RegTech providers' perspective, the COVID-19 situation was more binary, with some RegTech providers benefiting a great deal (15%) and others feeling a strong negative impact (9%). Overall, a slightly higher share of RegTech providers experienced slight positive impact (29% versus 26% of slight negative impact). The biggest winners on the RegTech providers' side seem to be those that offer ICT security and AML/CFT services. Half of the RegTech respondents in those two

segments stated that the impact was 'strongly positive' or 'slightly positive', with 17% of AML/CFT segment and 10 % of ICT segment RegTech providers indicating 'strongly positive' results. This suggests that while some RegTech providers have experienced difficulties, others managed to reap the benefits of increased demand for their services.

The RegTech projects of both the smallest (less than 10 employees) and very large RegTech providers and small FIs (less than 100 employees) seem to be the most negatively impacted with slower adoption and budget decreases being reported.

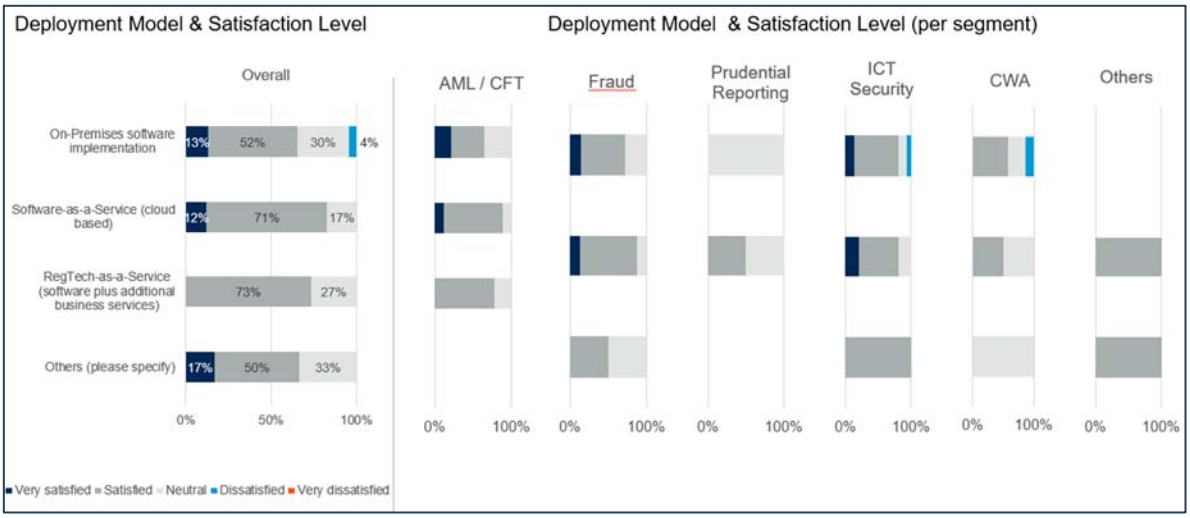
Level of FIs' satisfaction with RegTech solutions

The overall level of satisfaction with RegTech solutions in terms of their value added is high. Approximately 10% of FIs are very satisfied and 60% are satisfied with realised benefits of adopted RegTech solutions. The highest level of positive feedback is seen across the ICT security, fraud prevention and creditworthiness-related RegTech solutions. On the other side of the spectrum, some FIs had a negative experience with the RegTech solutions in the areas of prudential reporting (33%) and AML/CFT (22%). Interestingly, the sample of prudential reporting RegTech solutions received no 'satisfied' responses from FIs. However, this finding may have been influenced by a rather small FI sample size with reporting solutions in place.

The comparison of external RegTech solutions with internal solutions shows that differences between external and internal solutions tend to be limited, with **the overall satisfaction level with external solutions slightly higher.** In 75% of all cases, the FIs were very satisfied (11%) and satisfied (64%) with external RegTech projects. Only in 25% of all mentioned RegTech use cases were the FIs neutral (22%) or dissatisfied (3%). In the case of in-house RegTech initiatives, the same share of FIs expressed the highest level of satisfaction (11%), but a somewhat smaller part was satisfied (52%) with their RegTech solutions in place. One third of FIs indicated a 'neutral' attitude towards the project success, while 4% of FIs respondents suggested being very dissatisfied with the in-house RegTech project.

Further split of RegTech solutions by the deployment model reveals limited differences between Software-as-a-Service (SaaS), RegTech-as-a-Service (RaaS) and on-premises solutions. The **highest degree of satisfaction is reached in case of SaaS solutions**, with 12% of them delivering 'very satisfying' results and 71% 'satisfying' results. RaaS solutions follow the positive ranking by 73% of the solutions delivering satisfying results. On-premises implementation module has the lowest share of 'satisfactory' level (52%). In 13% of the cases, on-premises RegTech solutions deliver very satisfying results, however there are instances where results are dissatisfactory (this was, in particular, the case for a few CWA and ICT security solutions).

Figure 8.: Satisfaction level with RegTech solutions (deployment model and RegTech segment)

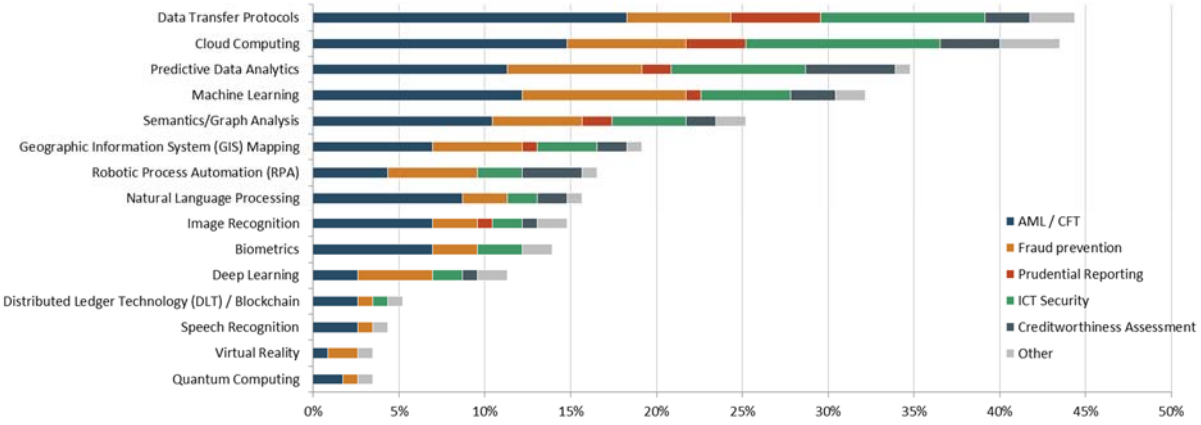


1.2 The underlying technologies behind the RegTech solutions

This section provides an overview of the main technologies applied by FIs and offered by RegTech providers to develop their RegTech solutions. It illustrates that the evolution of the existing and emergence of new technologies are the key factors that drive the development of innovative RegTech solutions.

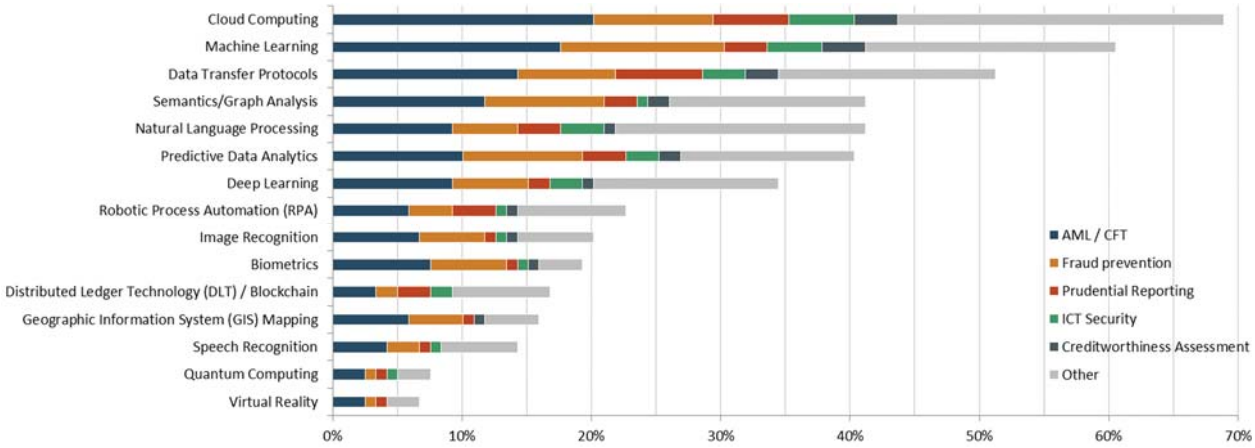
From the FIs' perspective, the top five most commonly used technologies are **Data Transfer Protocols** (44% of all RegTech use cases), closely followed by **Cloud Computing** (43%), **Predictive Analytics** (34%), **Machine Learning** (32%), and **Semantic/Graph Analysis** (25%).

Figure 9.: FIs – use of technology (by RegTech segment)



The top five technologies behind the RegTech providers' solutions are Cloud Computing, enabling 69% of RegTech solutions, **Machine Learning** (61%), **Data Transfer Protocols** (51%), **Semantics/Graph Analysis** (41%), and **Natural Language Processing** (NLP) (41%). The use of APIs (although not featured in these figures) plays a key role in the performance of RegTech solutions. Use of APIs is found in the majority of RegTech solutions, and a combination of AI and ML, Big Data, Cloud computing or APIs are present in about two-thirds of RegTech solutions.

Figure 10.: RegTech providers – use of technology (by RegTech segment)



The top technologies used by FIs and RegTech providers to develop their RegTech solutions are more or less the same, but in a slightly different order. However, the level of technology adoption seems to be somewhat lower on the FIs' side compared to RegTech providers. It can be the case that RegTech providers have more experience with the use of innovative technologies, but it can also be true that RegTech providers associate their solutions with a number of forward-looking technologies, even if some of these still may be in the process of development.

Looking into specific technologies, for example, **the use of cloud computing across all RegTech segments on the FIs' side is lower than on RegTech providers' side.** RegTech providers use cloud computing the most in the area of CWA (100%), AML/CFT (83%), ICT (80%) and 'other' solutions (93%). The FIs use cloud technology in the area of ICT (64%), fraud prevention (50%) and 'other solutions' (50%).

A similar trend is observed in case of Machine Learning (ML), which is also much more frequently used by RegTech providers than by FIs. RegTech providers leverage ML in the area of CWA (80%), AML/CFT (77%), Other Solutions (76%), fraud prevention (75%), and ICT (70%). FIs mostly find the use of machine learning in the area of fraud prevention (65%), CWA (60%), and AML/CFT (45%).

RegTech providers and FIs share the view that, at the moment, the least important technologies for RegTech are virtual reality and quantum computing. Also, very limited use of speech recognition and distributed ledger technology is observed among FIs.

The prevalence of the number of underlying technologies means that competent authorities also need to continuously educate themselves about how these technologies operate and monitor any emerging issues related, for instance, to consent, linking multiple data sources, data transfers or critical infrastructure providers. In the longer term, it would also be useful to consider where these underlying technologies could add value in a supervisory technologies (SupTech) context.

1.3 Governance processes for RegTech adoption

This section discusses the governance process components that are necessary for FIs to adopt RegTech solutions. It involves undertaking risk assessment and due diligence, obtaining senior-level sponsor for the RegTech project with an FI, reaching agreement on ICT spending, ensuring interoperability of RegTech solutions with any legacy systems, ensuring that the RegTech solution is always up-to-date with the latest regulatory requirements, and planning an exit strategy in case a RegTech solution is no longer needed.

1.3.1 Key components involved in governance processes for RegTech adoption

There are many tasks to be taken by FIs before a RegTech solution can be rolled out and also to ensure that it performs as expected. This section highlights some of them and includes both observed and recommended practices. In order to ensure successful adoption of RegTech solution, FIs:

1. **Undertake due diligence and risk assessment**. FIs are open to explore innovative ideas via collaboration with other providers, which can be a useful way to scout new solutions, test innovations and understand their added value. The EBA Guidelines on outsourcing arrangements[8] provide the necessary steps to undertake the due diligence and risk assessment process to be followed in cases where a RegTech solution is recognised as an outsourcing arrangement. Getting RegTech solutions accepted into an FI's value chain requires a thorough due diligence assessment, making sure an FI understands how the external RegTech solutions works. FIs often request prospective RegTech partners to have an established track record and provide detailed evidence about their solution in practice. The due diligence process can be costly and complex, because FIs have to be sure that their performance and stability will not be weakened via outsourcing or reliance on the third-party provider.

   From the RegTech providers' perspective, since in every case the RegTech provider (which usually has a well-working solution in other FIs already) is requested to make a new assessment about its soon-to-be-adopted solution, they would welcome initiatives that could help to share knowledge of RegTech solutions among FIs and facilitate compliance and due diligence processes. However, this could only facilitate RegTech adoption, as each FI is responsible for its own compliance and may have different needs based on their business models, so a one-size-fits-all approach would not be possible.

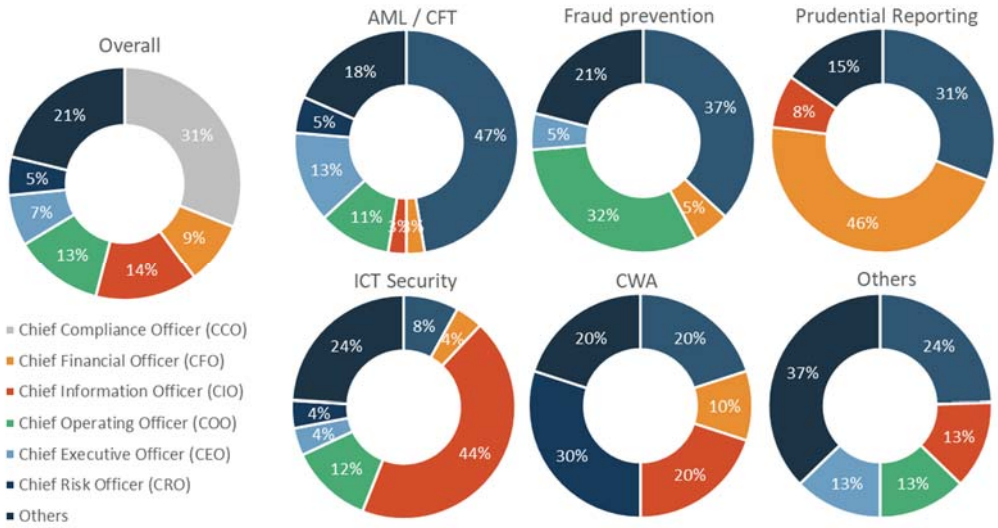
2. **Assess technological readiness.** The differences in technological readiness between the RegTech provider and the FI can hinder fast implementation. Despite willingness from both parties, RegTech provider and FI, implementation processes in the majority of the cases can reach up to 12-18 months to prepare thorough business and IT blueprinting, develop and customise solutions, and conduct necessary tests, etc. Ensuring that RegTech providers can

[8] EBA/GL/2019/02

connect to FIs' core systems (e.g. via APIs) and coordination with all units involved (e.g. business, IT, etc.) is also a time-intense process.

3. **Establish the RegTech sponsor.** The sponsor's role is to oversee the project, to enable an FI to have a structured approach to test innovations, understand value-added by RegTech and operationalise RegTech solutions. In practice, a range of sponsors identified for RegTech solutions are distributed heterogeneously throughout the FIs' C-level officers – usually senior officers sponsor the RegTech solutions in their respective areas of responsibility. For example, CCOs sponsor 47% of all AML/CFT projects, CFOs sponsor 46% of prudential reporting solutions, 44% of ICT security projects are sponsored by CIOs, 32% of fraud prevention projects by COOs. Moreover, 30% of CWA projects are sponsored by CROs, since this appears to be part of the core business of financial institutions.

Figure 11.: Sponsors of RegTech Projects



The above-mentioned officers took the sponsorship of 79% of all analysed RegTech projects. The remaining 21% of the RegTech projects have different sponsors, e.g. the Audit Committee, the AML Compliance Officer, the Chief Technology Officer (CTO) or the heads responsible for the different RegTech domains, e.g. Head of AML/CFT, Head of Credit, Risk Reporting Manager.

Observed differences across FIs and among various RegTech segments in terms of the governance and sponsorship models suggest that the ongoing digital transformation process may not have yet impacted existing governance structures, with transformation, in a number of cases, happening horizontally (across business areas) and not being vertically coordinated and integrated to ensure clear value added to the whole organisation. RegTech project governance process on the FIs' side still remains rather complex, with challenges related to the involvement and management of complex teams, including business, operations, risk, compliance, technology and other teams within a FI, with sometimes different priorities and technical expertise.

4. **Determine the most appropriate deployment model, including 'build' versus 'buy' decision. Among FIs, on-premises implementation of the RegTech solutions approach is the most prevalent.** 55% of FIs have their RegTech solutions on-premises, 41% are deployed in an SaaS model, and 15% in an RaaS. On-premises implementation is the dominating deployment model in the area of prudential reporting (83%) and CWA (70%). Fraud preventions and AML/CFT RegTech solutions are predominantly deployed as SaaS or RaaS solutions – respectively 53% and 50% of such solutions are deployed as SaaS models. 24% of the AML/CTF solutions are deployed as RaaS models by FIs.

   Among the RegTech providers, the dominant deployment model is as Software-as-a-Service (SaaS) solutions. Responding to the question of how their solutions are deployed (with multiple methods available), **in 85% of cases RegTech providers are able to deploy their solution in a cloud-based SaaS model**, in 42% they offer on-premises software implementation, and 40% of RegTech providers can offer a RegTech-as-a-service (RaaS) model (software and additional business process services). Looking across the different RegTech segments, all ICT security and CWA solutions are offered as an SaaS model by RegTech providers, while the highest percentage of RaaS solution as deployment model is provided in the prudential reporting segment.

   In terms of the 'build' versus 'buy' trade-off decisions for FIs, the first approach to developing their own RegTech solutions could give FIs more flexibility and control. In particular, this can help FIs meet very specific business needs, but it may also be slower due to available in-house expertise. However, building and maintaining all RegTech solutions that are needed may not be sustainable or the most effective approach. Some of the main advantages of the 'buy' approach for FIs include the ability to choose from a broad range of external RegTech solutions available to address the most common regulatory compliance requirements and to work with the most advanced solutions in the market (in terms of technology used and the approach taken). However, when relying on an external solution, FIs need to assess the ability to customise that solution to meet individual FI needs and to keep it updated by RegTech provider.

5. **Undertake rigorous regulatory screening and monitoring upcoming changes processes.** Ability of a RegTech solution to cope with ongoing changes in regulation is a key part of the decision-making process for both FIs and RegTech providers. As regulation is evolving and adapting to technological developments, changes in both national and international regulation sets the path and the frameworks in which RegTech solutions operate. As it is essential to ensure that RegTech solutions comply with the latest regulatory requirements, RegTech providers and FIs take various approaches to keep up with the dynamic regulatory environment.

   A key to maintaining the capacity to accommodate any updates on a regular basis is the openness of the system to new regulations. FIs avail themselves of internal and external education offers, annual reviews and audits, in addition to internal compliance and ongoing checks. The second line of defence also takes responsibility to make sure that the solutions are in line with the current regulation. FIs also state that they have in place dedicated regulatory change management processes to keep up with changes.

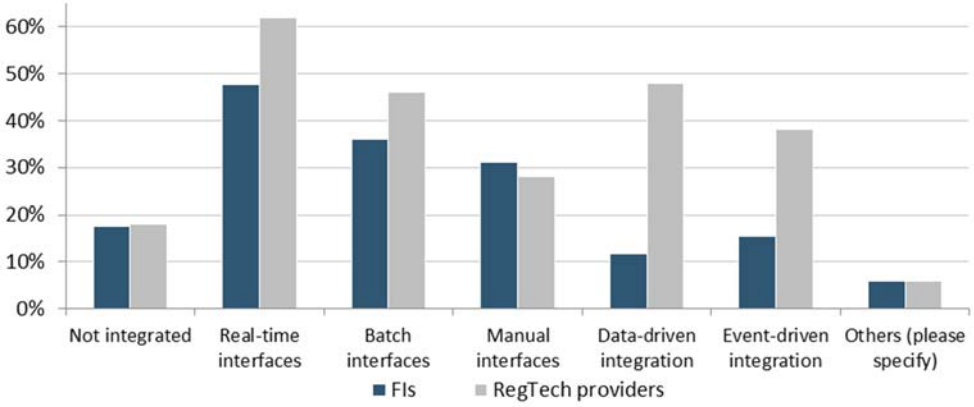
RegTech providers conduct a continuous screening of laws and regulations, subscribe to regulatory newsletters and foster contact and exchanges with regulatory bodies, partners and customers. To keep their systems up-to-date, some RegTech providers have established dedicated teams continuously monitoring regulatory landscape and developments in the financial markets. To increase efficiency, bots and other automated tools are used to scan regulations and spot any changes as soon as they are released. RegTech providers also rely on profound regulatory expertise. To be assured of this expertise, some RegTech providers cooperate substantially with their clients and jointly implement changes. Others consult with external specialists (e.g. law firms, credit bureaux, consultancies) or hire former regulators who possess expertise in legal requirements and regulatory processes. Furthermore, hosting webinars/meetings, participating in industry forums and client conferences on upcoming regulations and changes helps to anticipate upcoming adaptions at an early stage.

6. **Maintain adequate information and data-sharing processes.** In a model where several stakeholders cooperate, the information and data sharing processes should always be satisfactory. It is important to monitor data security, privacy and protection processes and effectively handle any emerging issues. Data quality itself is also a very important aspect, as a number of resources are needed for checking and resolving data quality issues to make sure data can contribute to a reliable operation of RegTech solutions. From the FIs' perspective, the data-related obstacles, including data availability, data quality, data standards, and data privacy and protection play a prominent role in the RegTech adoption process.

7. **Ensure that the RegTech solutions are properly embedded in the organisation's systems and processes, and all associated risks are managed.** To ensure interoperability of RegTech solutions with existing systems, FIs should ensure that RegTech solutions are properly integrated into their internal infrastructure and systems.

   Technical integration may be based on a few (not mutually exclusive) approaches. On the FIs' side, RegTech solutions are mainly integrated via real-time interfaces (48%). Batch interfaces (36%) and manual interfaces (31%) are also frequently used. The RegTech solutions provided by RegTech providers are also primarily integrated via real-time interfaces (62%). The second most common approach is data-driven integration (48%), followed by batch interfaces (46%).

Figure 12.: Technical integration of RegTech solutions into the existing legacy systems



Although FIs might use RegTech solutions from external vendors to reap benefits of not facing extensive in-house capabilities and development costs, FIs remains accountable for fulfilling all regulatory obligations. As a result, they need to manage risks that may occur when using externally provided solutions, such as reliance on a single vendor, business continuity risks or vendor capabilities to cope with regulatory change. For this purpose, FIs use several measures, e.g. for cloud-based solutions, key performance indicators are set up and monitored via maintenance contracts or service level agreements. In addition, regular meetings with the cloud providers ensure transparency regarding the functionality and current developments. Moreover, RegTech solutions are assessed through a risk assessment process and evaluated during the implementation; after the implementation, processes are continuously monitored. Another control measure is the integration of RegTech solutions into the existing corporate governance or internal control system. Finally, quality of an integration can be confirmed via internal and external audits and having sound three lines of defence functions in place.

1.3.2 Cooperation/partnership

Willing to stay ahead of the learning curve, RegTech providers establish a variety of partnerships with FIs, organisations or other RegTech providers. Apart from the competition in pricing, to convince FIs to implement their products, RegTech providers need to deliver a high-quality product. From the RegTech providers' point of view, they face a high degree of rivalry in the market. To stand out, they need to continually expand their expertise and the functionality of their systems. As a result, 75% of RegTech providers claim to have started to run a partnership with advisory companies, core-banking system providers, Software-as-a-Service (SaaS) companies, cloud service providers, BigTech firms, data vendors, compliance-related organisations or other institutions.

However, FIs seem to be underutilising the potential benefits of cooperation, with only 11% of FIs developing or exploring the possibility of developing RegTech solution(s) in collaboration with other market participants. This may be due to associated costs and project management complexities involved when working with external parties, which often are new to a complex regulatory framework that applies to FIs.

1.3.3 Time to production

The time between the decision to implement a new RegTech solution and bringing it into production can be another criterion for the selection of a particular RegTech provider. The average time in months, as indicated by RegTech providers, from the start of a proof-of-concept until going live into production for two-thirds of all solutions is less than three months. It takes less than six months for almost 90% of solutions.

Figure 13.: Time to bring the system into production

However, the time varies between the different RegTech areas. Based on the sample data, prudential reporting solutions seem to take the shortest implementation time, with 82% of the solutions able to be used in less than three months. In contrast, fraud prevention RegTech solutions have on average the longest implementation time (24% of the cases takes longer than six months).

In practice, the overall time from the FI initial contact with the RegTech provider to the solution being implemented can be substantially longer, as it involves completion of numerous tasks related to the vendor selection process. Complex governance process on the FIs' side may also contribute to the situation where moving from the proof-of-concept to production and scale-up of solution across an entire FI can take substantial time.

2. Benefits of RegTech use

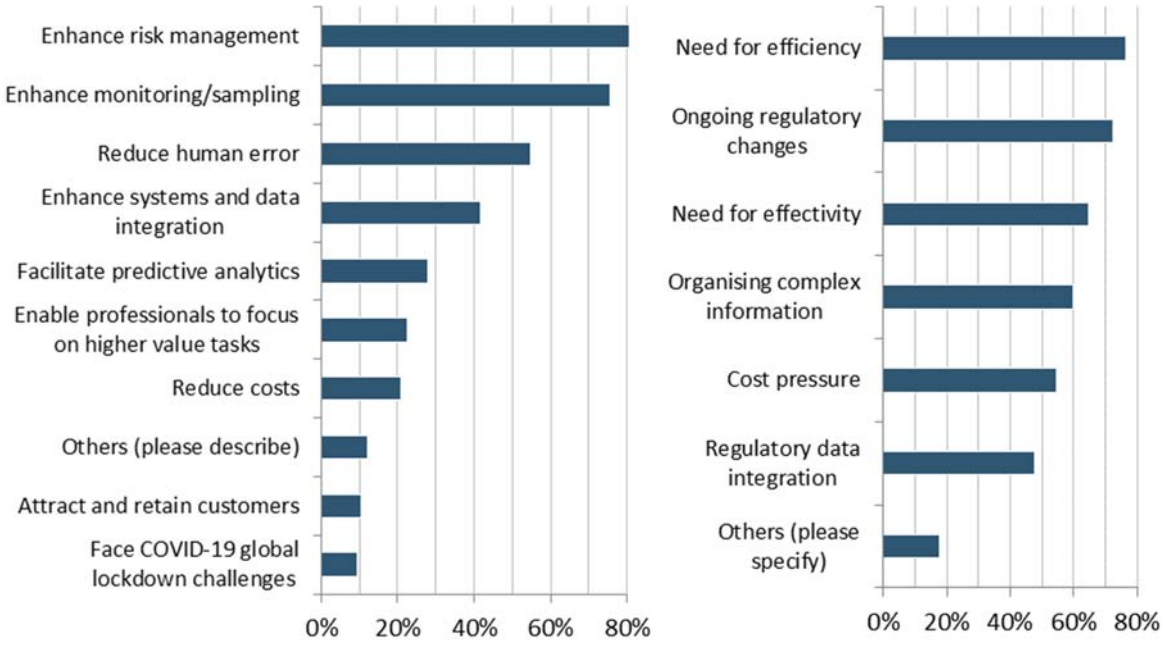
This section provides an overview of the main benefits of use of RegTech solutions by FIs as well as the perceived advantages of using RegTech solutions over traditional solutions based on both FIs' and RegTech providers' perspective.

2.1 Main benefits

The table below illustrates the main benefits of using RegTech from FIs' and RegTech providers' perspective in order of priority. **FIs primarily highlight enhanced risk management, enhanced monitoring and sampling capabilities, and reduction in human errors** as their key benefits to implementing RegTech solutions. Meanwhile, **the RegTech providers emphasise increased efficiency and ability to quell the impact of ongoing regulatory change** as key benefits associated with the use of their RegTech solutions. As some of the main benefits of RegTech solutions are perceived quite differently by FIs and RegTech providers, this may sometimes be a hurdle in the discussions about RegTech solution adoption. In some cases, RegTech providers may be presenting their solutions and emphasising benefits that may not be prioritised by FIs. As a result, closer cooperation between FIs and RegTech providers may be mutually beneficial. RegTech providers need to better identify the FIs' actual pain points and needs, while FIs could benefit from better awareness of offered (and in an ideal case substantiated and quantified) advantages of RegTech providers' solutions.

Main benefits of using RegTech solutions

Figure 14.: The key reasons for FIs to implement RegTech solutions (**FIs' perspective – left side)** and the key reasons for using RegTech solutions (**RegTech providers' perspective – right side)**

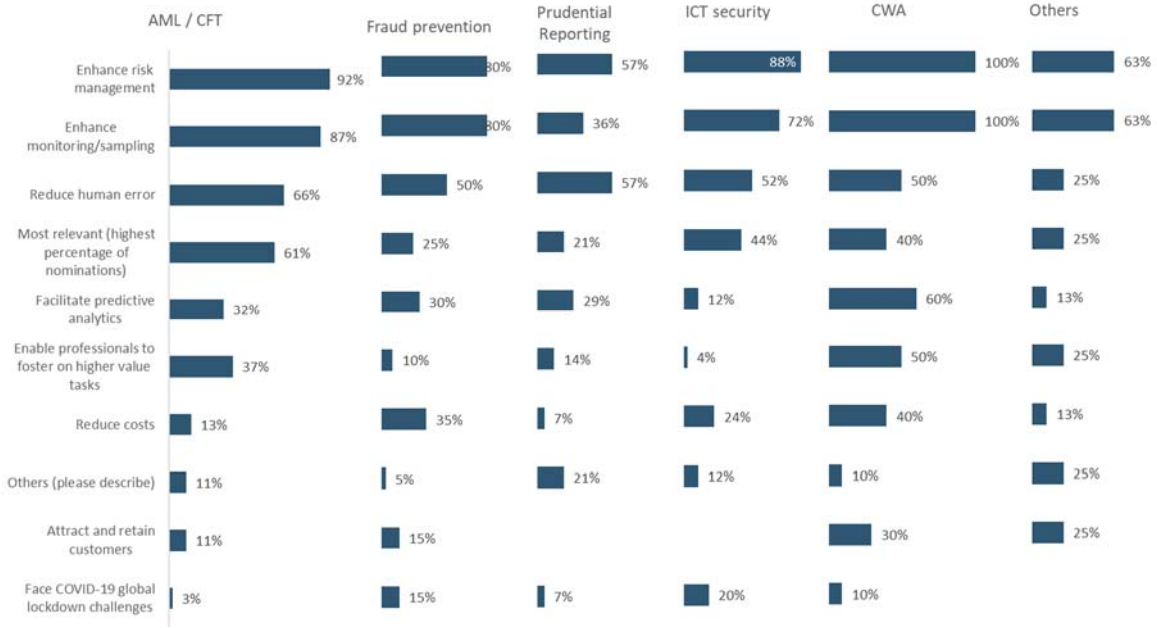


For both FIs and RegTech providers, cost pressure and cost reduction are seen lower down on their list of key benefits. However, there are quite significant differences in the perceived cost pressure as a driver for RegTech adoption. RegTech providers consider cost as a significant factor for FIs using their prudential reporting and AML/CFT solutions. However, from the FIs' perspective, the RegTech segments where the cost factor is seen as a driver are primarily CWA, fraud prevention and ICT security. On the side of FIs, the cost factor may be of some lower importance because of the initial costs associated with onboarding a new RegTech solution, the unclear extent of potential cost savings, and cost efficiencies that tend to come only later in the lifecycle of a RegTech solution, even if in practice FIs try to consider the total cost of ownership of software investments.

FIs are also keen to leverage on RegTech solutions to enhance systems and data integration and facilitate predictive analytics, enabling experts to focus on higher value-added tasks and processes. However, this may not always be easy to achieve in practice, as interoperability and integration are still reported as one of the main challenges faced by FIs in adopting RegTech solutions (as further explained in Chapter 3).

Further insights from FIs' perspective suggest that the different RegTech segments show a very similar pattern in terms of the key reasons to adopt RegTech solutions compared to the general trends explained above. Some slight deviations can be observed in the area of CWA, where more focus is placed on the need to 'facilitate predictive analytics' and to 'enable professional to focus on higher value tasks'. The latter factor is also seen as more relevant in AML/CFT-related RegTech solutions.

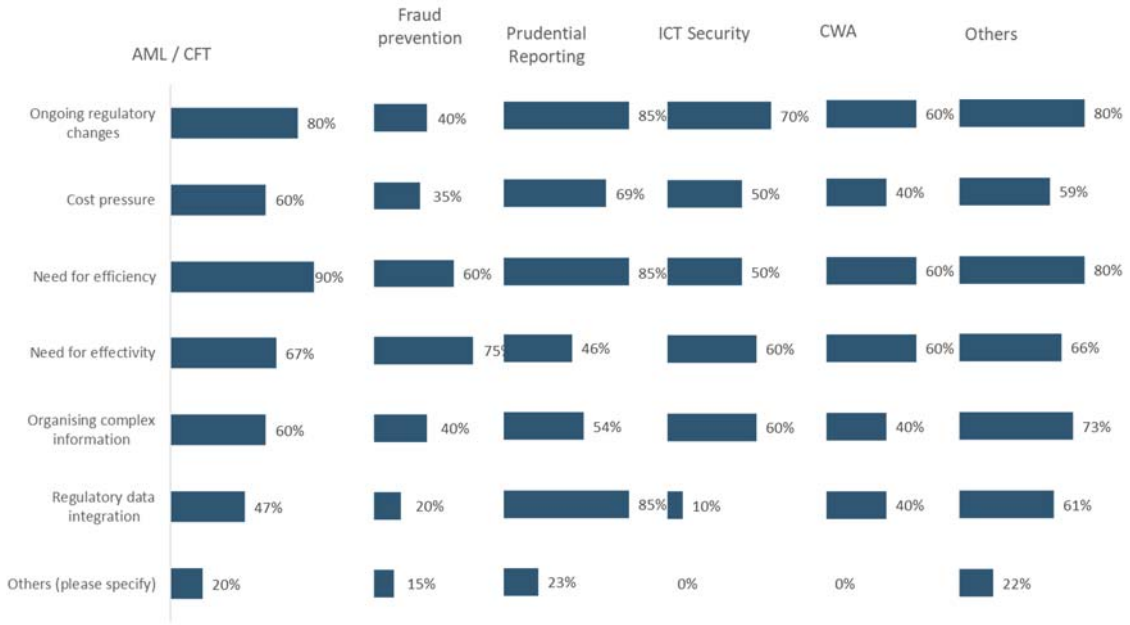
Figure 15.: The key reasons for FIs to implement RegTech (FIs' view, **per RegTech segment**)



A closer analysis of the main drivers across different RegTech segments from the RegTech providers' perspective identifies the following key factors. The major perceived reason to use AML/CFT solutions, according to RegTech providers, is the 'need for efficiency', the key driver for fraud prevention in the use of RegTech solutions is the 'need for effectivity', while prudential

reporting RegTech solutions are mostly used because of 'ongoing regulatory change', 'need for efficiency', and 'regulatory data integration'. ICT solutions implemented are mostly driven by 'ongoing regulatory change', and the main drivers behind CWA solutions are 'ongoing regulatory change', 'need for effectivity' and 'need for efficiency'.

Figure 16.: the key reasons for using RegTech (RegTech providers' view, **per RegTech segment**)

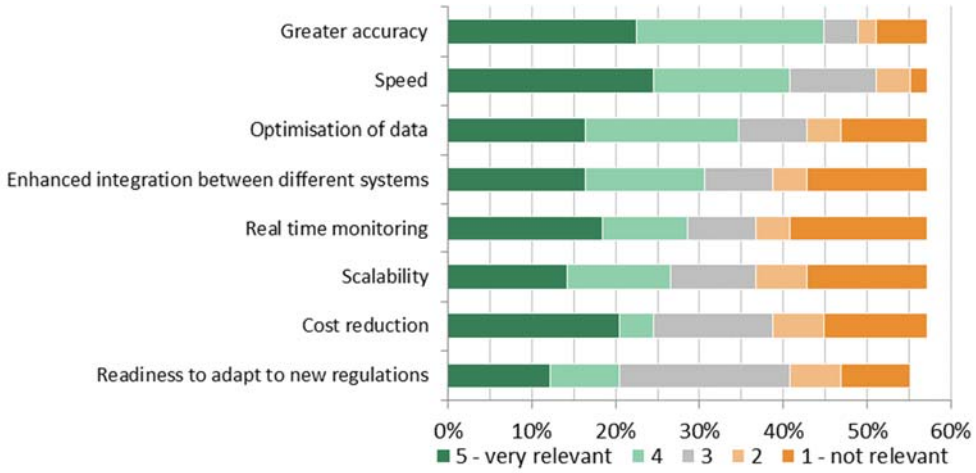


Overall, RegTech solutions can assist FIs comply with regulatory standards, support risk management and counter financial crime. For example, AML/CFT solutions can at the same time identify instances of bribery, corruption or insider trading, making the financial system safer. Technology usually helps to speed up the processing of regulatory compliance checks and reduce the scale of routine tasks, leaving more time and capacity for FI staff to focus on priority tasks. However, all these benefits can materialise only if RegTech solutions work properly as expected at all times and do not face any ICT/cyber issues (e.g. are not being compromised, which could potentially take time to notice).

2.2 Perceived RegTech advantages versus traditional solutions

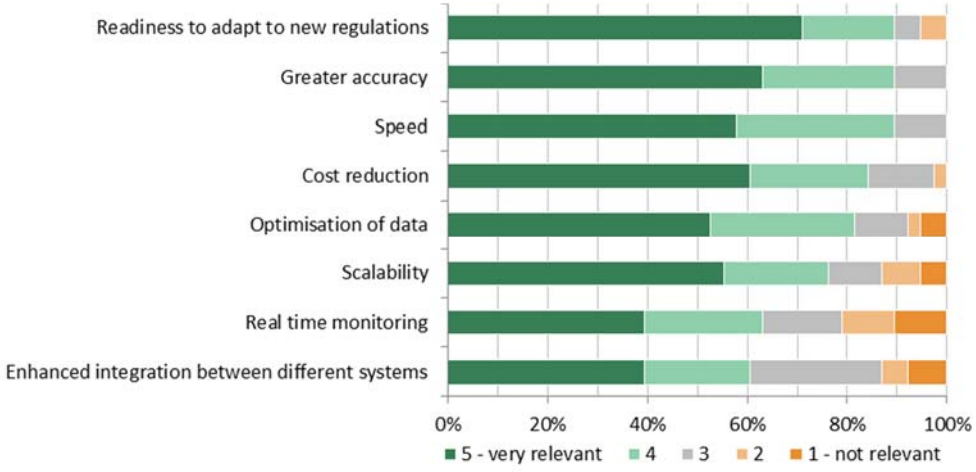
From the FIs' perspective, the most relevant perceived advantages in adopting RegTech solutions compared to traditional solutions are **greater accuracy, speed and data optimisation**. Less relevant are the potential advantages related to easier scalability, cost reduction opportunities and readiness to adapt to new regulations.

Figure 17.: Perceived advantages of the RegTech solutions **adopted by FIs** versus traditional solutions (FIs' perspective)



RegTech providers consider many of the advantages over traditional solutions nearly equally relevant, with the **readiness to adapt to new regulations** cited as a key advantage, followed by **greater accuracy, speed, cost reduction,** optimisation of data and scalability.

Figure 18.: Perceived advantages of the RegTech solutions **offered by RegTech providers** versus traditional solutions (RegTech providers' perspective)



Some of the emerging differences between FIs and RegTech providers views, e.g. on the perceived ability of RegTech solutions to adapt to new regulations or the enhancement of the integration between different FIs' legacy systems, indicate that there is room for closer investigation and better understanding in the market on the advantages that RegTech solutions can actually deliver.

3. Challenges of RegTech use

Based on the feedback received from FIs and RegTech providers, this section provides an overview of the challenges faced by FIs in adopting and RegTech providers in developing RegTech solutions. The findings suggest that RegTech market participants still need to overcome obstacles in order for RegTech solutions to reach their full potential and to become one of the main drivers of the digitalisation of the financial sector.

The analysis highlights that in terms of general obstacles and operational challenges, FIs and RegTech providers have a somewhat different perception of what the major obstacles for market adoption are. However, they share the views on challenges related to FIs' technological capabilities, integration with legacy systems, and changes of national or international regulation and laws.

3.1 Challenges from the FI perspective

Implementation of RegTech solutions to assist FIs in meeting their regulatory requirements in effective and efficient manner does not come without challenges. The main challenges FIs face revolve around these six main areas:

1. **Data-related challenges and cybersecurity threats** – data-related obstacles tend to be the most important ones. FIs often indicate data quality, data privacy and protection, lack of data integration, data availability, and lack of data standardisation and harmonisation as issues. These challenges became relevant to different degrees in a number of use cases, e.g. when FIs attempt to leverage internal or external data, financial or non-financial data. Data-related obstacles also include the cybersecurity threats which are increased by the interconnectedness of various RegTech solutions and legacy systems used. Not surprisingly, data-related challenges and cybersecurity threats may be crucial barriers that may discourage certain FIs from adopting RegTech solutions. Overall, FIs perceive the requirements for processing personal data and domain-specific requirements as the most important legal and regulatory obstacles.

2. **Interoperability and integration with the existing legacy systems** – there are too many silos within FI legacy systems and processes that make RegTech adoption difficult and this is compounded by a 'lack of confidence in the ability of FIs' ICT infrastructure to be able to support FinTech, RegTech and InsurTech solutions'[9]. In addition, RegTech providers are seen to be specialised (providing in-depth expertise in a narrow field), but FIs in general prefer to adopt broad end-to-end RegTech solutions that could cover as many compliance aspects as possible. As a result, integration issues with legacy infrastructures (mainframes) are seen by FIs as a relevant obstacle across all RegTech segments.

[9] Thomson Reuters Regulatory Intelligence. Fintech, RegTech and the role of compliance in 2021

3. **Changes to regulation** – changes with national or international regulations and other regulatory challenges can be another key barrier to RegTech adoption. It is apparent that for some FIs, the lack of clear rules and regulations, and lack of common positions of regulators and supervisors could be a setback for the adoption of RegTech. In addition, the complex and continuously evolving regulatory landscape of national and international regulation and laws is also perceived by some as a challenge. For example, although there are some available RegTech regulatory horizon scanning tools, in many cases FIs leverage a manual regulatory tracking process to identify and assess relevant changes and their impact on RegTech solutions. RegTech solutions already in use have to be checked to determine whether they have to be adapted in the light of any new regulation, whereas any new RegTech solutions or functionalities might support FIs and reduce the burden of the legal changes.

4. **Costs and procurement process** – RegTech solutions seen as part of compliance and usually treated as a back-office function may be at risk of underinvestment[10]. The procurement processes can also be lengthy and complicated, leaving larger and more complex RegTech solutions out of sight of a large share of FIs with limited RegTech spending budgets. However, smaller scale RegTech projects under established procurement thresholds are more likely to be taken onboard.

5. **Lack of necessary skills and training** – when working with either in-house or external RegTech solutions, FIs need specialists, e.g. data scientists and engineers, to be able, where relevant, to scout, assess, operate, and maintain updated RegTech solutions. In case resources are not available internally, recruitment of such specialists may pose a challenge for the FIs, as currently there is high competition in both private and public sectors for talent. Furthermore, further training in regulatory and supervisory disciplines for FI staff (for the new joiners and existing staff) may be required.

6. **Perceived immaturity of RegTech providers' solutions** – FIs that see RegTech as a potential competitive advantage often cite the lack of available and mature RegTech solutions as a challenge. In cases where RegTech providers' solutions are generic and not tailor-made to individual FIs' needs, the value generated and the cost savings by the RegTech solution may remain unclear for the FIs, thus relevant stakeholders and RegTech sponsors may not consider RegTech a driver of competitive advantage. FIs need to monitor the RegTech market and as RegTech solutions become more mature, it would be important for FIs to reassess the value those solutions could provide.

It is interesting to note that the majority of challenges faced by FIs are internal ones, i.e. related to data, interoperability and integration with legacy systems, lengthy procurement processes, lack of necessary skills and training, and limited awareness about external RegTech solutions. Evolving regulatory change and different regulatory requirements or supervisory expectations can also be important in some cases, but they are not the major factor affecting implementation of RegTech solutions.

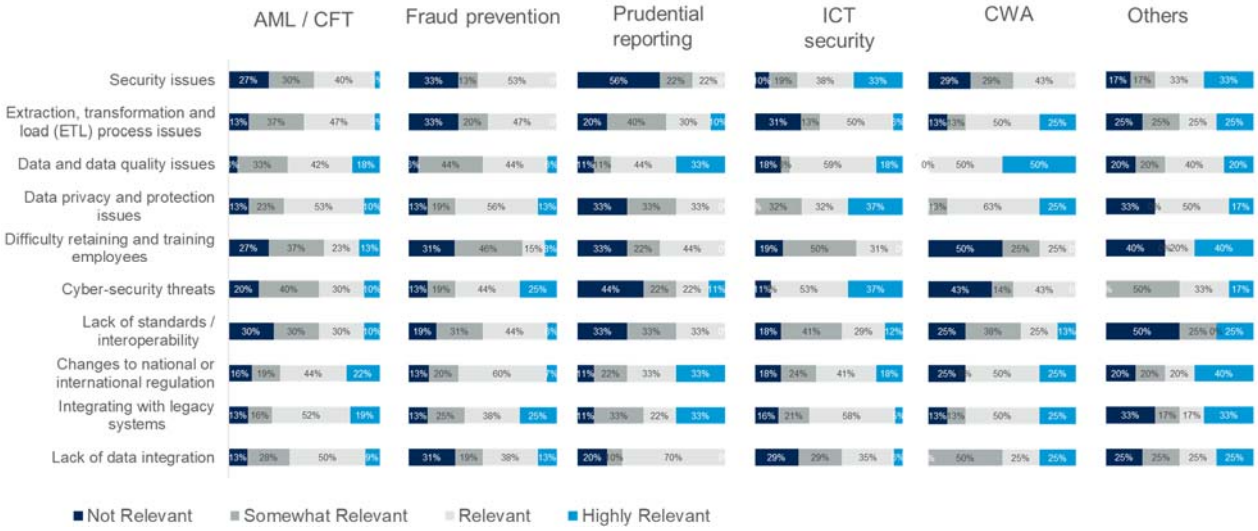
[10] Cambridge Centre for Alternative Finance. The Global RegTech Industry Benchmark Report 2019

Overview of FIs' RegTech segment-specific challenges

Regardless of the main challenges identified above, specific RegTech-related challenges that FIs experience differ across various RegTech segments and they are further explored in more detail in Chapter 4 under the deep dive sections on specific RegTech segments.

The chart below illustrates and summarises some of the differences in obstacles and operational challenges encountered by FIs in each RegTech segment. However, the granular analysis of challenges faced by FIs may be somewhat limited as, in general, FIs are somewhat reluctant to share detailed information about their RegTech initiatives and the challenges experienced during the adopting process.

Figure 19.: Obstacles and operational challenges per RegTech segment: FI perspective



For AML/CFT RegTech segment, the survey results exhibit that 'Data and data quality Issues' (94%), 'Integrating with legacy systems' (87%) and 'Lack of data integration' (87%) are the most relevant obstacles, these being representative of the general obstacles perceived by FIs across all RegTech segments.

For fraud prevention, FIs observe 'Data and data quality Issues' (94%), 'Cybersecurity threats' (87%) and 'Integrating with legacy systems' (87%) as the most relevant issues, which illustrate that fraud prevention solutions contain cybersecurity threats aspects that need to be addressed.

For prudential reporting, the survey responses appear to be aligned with the findings related to the general obstacles. FIs observe 'Data and data quality issues' (89%), 'Changes of national and international regulation' (89%) and 'Integrating with legacy systems' (89%) as the most relevant issues for wider market adoption.

For ICT security RegTech solutions, the most relevant obstacles perceived by the FIs are 'Data privacy and protection' (100%), 'Security issues' (90%) and 'Cybersecurity threats' (89%) which is in line with the general expectation that ICT security RegTech providers need to very carefully manage

and address any (cyber)security-related issues before the deployment of their solution within FIs' systems.

For CWA, the most widely considered obstacles are related to 'Data and data quality issues' (100%), 'Data privacy and protection' (100%) and 'Lack of data integration' (100%) which suggests that RegTech providers need to address the issues related to processing of personally identifiable information.

3.2 Challenges from the RegTech provider perspective

RegTech providers consider the following eight factors as the main challenges to wider market adoption of RegTech solutions in the EU:

1. **Lack of technological capabilities on FIs' side –** the lack of some FI client API capabilities and lack of standardisation are perceived as obstacles for technical integration of RegTech providers' solutions. The majority of RegTech solutions require FIs to aggregate data from different source systems into relevant datasets, e.g. in the public cloud. Given the fact that currently the majority of RegTech solutions are narrow in scope and cover rather targeted RegTech segments, they cannot replace overall legacy core banking systems. As a result, FIs are seen to have focused on optimising current workflows by using RegTech solutions instead of transforming their overall processes and modernising their legacy systems. This has resulted in a situation where the RegTech solutions (or even any new internal functionalities and systems) are difficult to integrate into the legacy system landscape without the adoption of a central data layer and the standardisation of APIs.

2. **Security**, **data privacy and protection issues** – privacy regulation may be one of the key inhibitors for FIs from sharing datasets with RegTech providers. As most FIs are intrinsically risk-averse and bound by strict GDPR regulation, they consider carefully what data they are willing and able to share with RegTech providers. In terms of perceived data privacy and protection obstacles, no workaround solutions may be possible, as necessary safeguards need to be implemented by RegTech providers, which by their very nature currently act as hurdles for some providers. However, at the same time, GDPR and data protection aspects become differentiating factors between sustainable and successful RegTech solutions that may successfully find their way within the regulatory framework, and those RegTech providers that tend to treat legal aspects somewhat lightly.

3. **Changes of national and international regulation** – complex and continuously evolving regulatory landscape of national and international regulation and laws is perceived as a challenge, in particular in the area of prudential reporting, fraud prevention, AML/CFT.

4. **Cost of user acquisition** – it is also a challenge, especially for recently established and smaller RegTech providers. The bargaining power of FIs is likely to be high (e.g. due to high customer switching costs, demand-side benefits of scale, etc.), which creates high barriers for RegTech providers to enter the market and increases the user acquisition costs.

5. **Lack of FI understanding of RegTech solutions** – from the perspective of RegTech providers, the perceived lack of buyer awareness of RegTech potential is observed across all RegTech segments, with percentages ranging from 71% in the ICT security field to 96% in fraud prevention. Reflecting on findings related to the perceived advantages of RegTech solutions over traditional methods, it appears to RegTech providers that FIs may not be fully aware of all advantages that RegTech solutions may bring. The disparity between the identified advantages by RegTech providers (for example, on readiness to adapt to new regulations) and the low perceived benefit on the same issue by FIs potentially signal a lack of understanding of RegTech capabilities. However, this can also indicate an overestimation to certain degree by the RegTech providers of the actual capabilities their solutions can offer.

6. **Lack of harmonised legal and regulatory requirements** – some RegTech providers perceive the lack of harmonisation of regulatory requirements across the EU and the lack of regulatory data standards to be the obstacles for wider market adoption of RegTech solutions, which can be addressed by the regulatory authorities and governments. The existence of multiple standards at a global level and across the EU in a number of fields, e.g. AML/CFT and fraud prevention, is perceived by RegTech providers as obstacles to scale up across different countries within the EU. Nevertheless, some RegTech providers have built their business models and value proposition around the ability to address the challenges faced by FIs to navigate and comply with complex regulatory and legal frameworks.

   Looking more granularly into RegTech segment-specific obstacles, RegTech providers perceive the requirement for processing personal data as fraud prevention and an AML/CFT segment-specific regulatory obstacle. For prudential reporting solutions, the segment-specific regulatory requirements are also perceived as relevant legal/regulatory obstacles. For the CWA, RegTech providers primarily experience issues with requirements for data sources, which relates to the database connectivity, data format and data extraction mechanisms. In cases where FIs do business in several jurisdictions, the lack of common regulation and divergent regulatory requirements fragment the RegTech market and may require FIs to adopt multiple solutions from different vendors, which increases operational risk and reduces the attractiveness for RegTech solutions.

   In general, 66% of surveyed RegTech providers perceive a 'lack of regulatory standards' as a general obstacle for market scalability within the European Union. Recent initiatives include the European Commission's proposal for harmonised rules on Artificial Intelligence (Artificial Intelligence Act)[11] which is an example of an emerging harmonised requirement on, for example, transparency to consumers, human oversight, data accuracy, robustness and security, documentation and record-keeping requirements, etc. that should ensure legal certainty and, in turn, facilitate adoption of innovation in the EU.

[11] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS (COM/2021/206 final)

7. **Clarity of regulatory/supervisory guidance** – from the perspective of RegTech providers, the regulators are overall perceived positively, with 40% of the RegTech providers considering the regulator as 'supportive' and further 48% as 'neutral'. This neutral perception towards the regulator/supervisor can be explained by the fact that in many cases, CAs do not have the mandate to promote or facilitate specific business models. However, the perception varies across the different RegTech segments, with RegTech providers in prudential reporting, AML/CFT and fraud prevention areas indicating that more support and guidance would be appreciated to support the roll-out of RegTech solutions across different countries. Initiatives on building and sharing knowledge about technologies and applicable regulation (e.g. via TechSprints which facilitate conversations between RegTech providers, FIs and regulators about the use of technology to deal with areas of challenge) could be helpful. However, fundamental principles like the principle of equal treatment or the principle of technological neutrality have to be respected to avoid support for any specific private endeavours.

8. **Competition with other solutions** – a high level of industry competition with other solutions is observed, in particular in segments where RegTech providers offer comparable solutions.

   Similarly, as indicated by FIs, the majority of challenges faced by RegTech providers seem to be related to FIs (e.g. lack of technological capabilities and awareness on the FIs' side), but RegTech-providers' internal factors (e.g. high user acquisition costs), data privacy and protection issues and lack of harmonised regulatory standards also play a role.

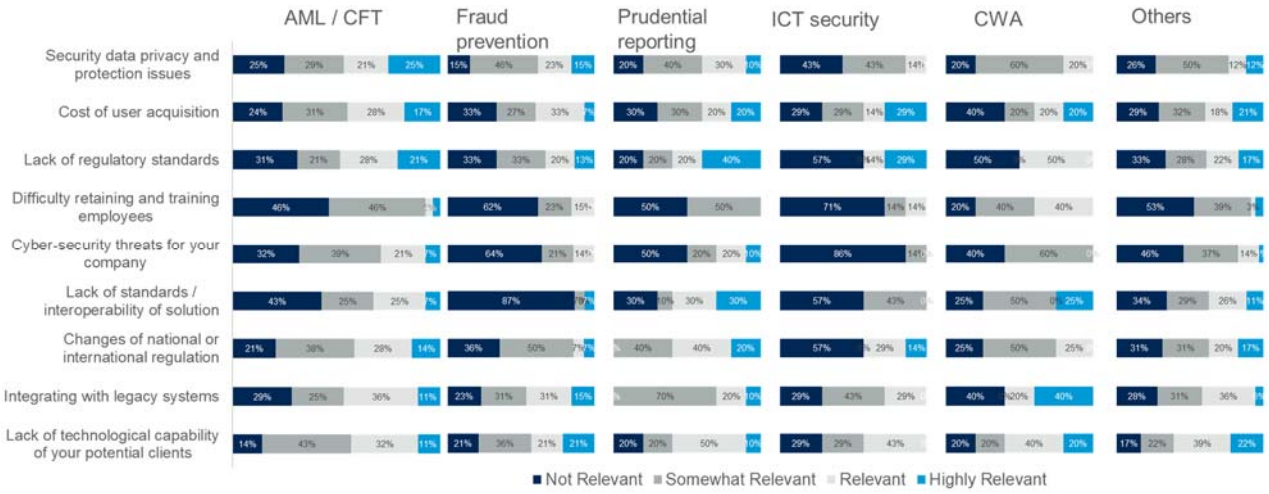
   More than 90% of RegTech providers consider that the lack of regulatory/supervisory guidance and support can be an obstacle preventing the roll-out of their solutions across different countries. However, the majority of FIs hold completely the opposite view, and do not see guidance factor as a potential obstacle for the cross-border scale-up of their RegTech solutions.

Overview of RegTech providers' RegTech segment-specific challenges

Challenges for RegTech providers differ across various RegTech segments and they are further explored in the deep dive in Chapter 4 into specific RegTech areas. The chart below summarises and demonstrates the main obstacles and operational challenges as encountered by RegTech providers in each identified RegTech segment.

From a RegTech provider's perspective, the different RegTech segments exhibit different obstacles, depending on the RegTech segment-specific data availability, system integration needs and applicable regulatory requirements.

Figure 20.: Obstacles and operational challenges per RegTech segment: RegTech providers' perspective



In AML/CFT segment, the RegTech providers quote primarily the 'Lack of technological capabilities on client side' (86%), 'Changes of national and international regulation' (79%) and 'Cost of user acquisition' (71%) as the major obstacles.

The survey results for fraud prevention indicate that 'Security, data privacy and protection issues' (85%), 'Lack of technological capabilities on client side' (79%) and 'Integration with legacy systems' (77%) appear to be the most relevant issues.

For prudential reporting, 'Changes of national and international regulation' (100%), 'Integration with legacy systems' (100%) and 'Lack of regulatory standards' (80%) are widely seen as the primary obstacles.

ICT security RegTech providers see 'Cost of user acquisition' (81%), 'Lack of technological capabilities on client side' (79%) and 'Integration with legacy systems' (77%) as the key challenges.

Lastly, for CWA RegTech solutions, 'Lack of technological capabilities on client side (80%)', 'Difficulty in retaining and training employees' (80%) and 'Security, data privacy and protection issues' (80%) are perceived as the most relevant obstacles.

3.3 Main risks

The deployment of RegTech solutions can help make FIs more effective and efficient in managing risks and meeting their compliance obligations. However, if not properly implemented, RegTech solutions may give rise to risks for FIs that would need to be identified, monitored, and managed. At the same time, RegTech solutions may give rise to new supervisory internal risks for competent authorities, i.e. risks that supervisors face when supervising FIs who use RegTech solutions.

Taking into account that the use of RegTech solutions may involve the outsourcing of FIs' critical or important functions, FIs and RegTech providers need to ensure their RegTech solutions comply

with the relevant provisions of the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02). In particular, it is worth reiterating that each FI's management body remains responsible for that institution and all of its activities, at all times, and to this end should ensure that sufficient resources are available to appropriately support and ensure the performance of those responsibilities, including overseeing all risks and managing the outsourcing arrangements. With regard to outsourcing to service providers located in third countries, FIs are expected to take particular care that compliance with EU legislation and regulatory requirements (e.g. professional secrecy, access to information and data, protection of personal data) is ensured. In addition, competent authorities should be able to effectively supervise FIs, in particular regarding critical or important functions outsourced to service providers. It is important to emphasise that FIs remain fully responsible and accountable for complying with all of their regulatory obligations.

Some of the risks for FIs mentioned below may be addressed by the forthcoming new **regulation on digital operational resilience in the financial sector (Digital Operational Resilience Act)**, proposed by the European Commission in September 2020. The Act will define requirements for the ICT risk management, ICT third-party management, and will include the concept of regulation and supervision of critical third-party providers that some RegTech providers may fall under in the future. In the meantime, FIs need to mitigate and manage their information and communication technology (ICT) and security risks by following EBA Guidelines on ICT and security risk management (EBA/GL/2019/04).

RegTech segment-specific risks are highlighted and analysed in more detail in Chapter 4 (Deep dives into RegTech segments). Below is the summary of the potential main risks that FIs may face when using RegTech solutions, regardless of a particular area of application. Some competent authorities are already asking FIs to demonstrate how some of the potential risks could be managed, and even questioning the suitability of deploying certain RegTech solutions to meet legal or regulatory requirements if some of the risks below are known prior to implementation.

Some examples of potential risks that may emerge for FIs when using RegTech solutions include:

- **compliance risk** – understood as the risk that reliance on RegTech solutions may cause FIs to fail to comply with the applicable legal and regulatory framework (for a number of possible reasons, e.g. if RegTech solution fails to deliver as expected, if AML/CFT risk-based approach is replaced by a tick-box approach, etc.);

- **concentration risk** – FI reliance on a certain RegTech provider may lead to the emergence of a systemically important (unregulated) RegTech provider, whose failure may have system-wide implications;

- **business continuity risk** – potentially caused by RegTech solution's outages or disruptions, posing risks for the continuity of services and/or affecting confidentiality, integrity or availability of data;

- **technology-related risk (e.g. in use of cloud computing) and personal data protection risk** – regarding cloud-based RegTech solutions, there is a risk that the FIs may not actually know

where the provider's servers and data storage are located which, in light of the recent developments in GDPR requirements (i.e. invalidation of the EU-US Privacy Shield[12]), might represent an issue when no adequate level of data controls is in place.

- **Operational risk** including:
  - **ICT and security risk** – risk of loss due to breach of confidentiality, failure of integrity of systems and data, inappropriateness or unavailability of systems and data or inability to change information technology (IT) within a reasonable time and with reasonable costs when the environment or business requirements change (i.e. agility). This includes security risks resulting from inadequate or failed internal processes or external events including cyberattacks or inadequate physical security;
  - **reputational risk** – risk due to strong links between the FI and RegTech provider and potential loss of confidence in the FI or dissatisfaction with FI by its main stakeholders (investors, depositors, etc.) in case RegTech solution does not perform as expected;
  - **internal governance/legal risk** – failure to comply with applicable legislation or with internal regulations. Some FIs that lack understanding of what controls RegTech providers have in place to tackle certain requirements (e.g. data protection requirements, data localisation, etc.) and whose responsibility it is to monitor them, may find it difficult to explain to supervisors how risk control mechanisms are put in place;
  - **conduct and consumer protection risks** (e.g. in case of Machine Learning algorithms used for RegTech solutions). Taking CWA as an example, even if the use of new technologies in credit scoring tools may facilitate the access of consumers to loans, it may also lead to financial exclusion from access to financial services. If the algorithm was based on factors not directly related to creditworthiness, this could negatively affect conduct risk. In addition, if it is accepted that models using such algorithms tend to provide very accurate predictions, some issues may arise regarding the explainability and interpretability of technologies associated to the use of CWA solutions. The subjects of such decisions (consumers and businesses alike) may face situations in which they have no real possibility to assess the correctness or appropriateness of the relevant decision. As stated in the EBA report on Big Data and Advanced Analytics (EBA/REP/2020/01), the effectiveness of human involvement depends on the level of understanding of the outputs of the models, making explainability a key feature for model accuracy and representativeness. Ongoing research and development of tools and techniques may assist in addressing current issues with explainability and interpretability, as well as bias detection and prevention, which could possibly facilitate the responsible use of more sophisticated advanced analytics solutions.

12 Judgment of the Court (Grand Chamber) of 16 July 2020. EUR-Lex - 62018CJ0311 - EN - EUR-Lex (europa.eu)

From the competent authorities' perspective, the main risks that may derive from the supervision of FIs that use RegTech solutions relate to:

- potential difficulties in the **assessment of the effectiveness and reliability of the technological solutions** used by FIs, and

- potential **lack of the skill set and tool set needed to supervise the use of technology-enabled RegTech solutions** and, for example, to audit the underlying algorithms. Furthermore, due to the continuous evolution that the use of new technologies imposes on FIs and RegTech providers, it might be challenging for supervisory authorities to assess, challenge, validate, and supervise the models, or the algorithms used to calibrate them. For example, it could be unclear which model is currently in use, how it was calibrated, how it may change over time when new data is added, or how certain variables are used by the model, increasing operational and model risk. These issues have already been flagged in the EBA report on Big Data and Advanced Analytics[13] and are being partially addressed by guidance set out in the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02).

[13] According to the EBA Report on Big Data and Advanced Analytics, 'transparency' consists of making data, features, algorithms and training methods available for external inspection and constitutes a basis for building trustworthy models. Explainability and interpretability are two of the transparency's elements: a model is explainable when its internal behaviour can be directly understood by humans (interpretability) or when explanations (justifications) can be provided for the main factors that led to its output (e.g., to enable effective supervision and audits).

4. Deep dives into RegTech segments

This chapter provides an in-depth analysis into five RegTech segments: i) Anti Money-Laundering / Countering the Financing of Terrorism (AML/CFT); ii) Fraud prevention; iii) Prudential reporting; iv) ICT security; and v) Creditworthiness assessment (CWA). These areas were identified as the most common focus areas for RegTech solutions and therefore merit further analysis.

The sub-chapters below highlight the activities of FIs and RegTech providers in each of these RegTech focus areas, specifying the technologies used and discussing specific benefits and challenges associated with each RegTech use area. Where identified, they also provide examples of innovative use cases.

4.1 AML/CFT

AML/CFT RegTech solutions are put in place by FIs to comply with their obligations under Directive (EU) 2015/849[14] (AMLD), with a particular focus on the customer due diligence (CDD) requirements set out in Article 13(1) AMLD[15].

The EBA's work on RegTech in the area of AML/CFT started in 2018, with the European Supervisory Authorities (ESAs) publishing their **Opinion on the use of innovative solutions by credit and financial institutions[16] when complying with their CDD obligations**. This opinion identified the factors that CAs should consider when: a) assessing the adequacy of firms' CDD measures where innovative solutions are used and the application of such measures by firms, and b) assessing controls in place at firms that enable them to mitigate any risks associated with innovative solutions. This instrument has since become part of the ESAs' wider work on creating a common understanding of the responsible and effective use of innovation by credit and financial institutions for AML/CFT compliance purposes, which now includes a dedicated section in the **EBA's ML/TF Risk Factors Guidelines**[17] and forthcoming guidelines on remote customer onboarding. In Guidelines 4.32 to 4.37 of its revised ML/TF Risk Factors Guidelines, the EBA sets out criteria that firms should

[14] Amended by Directive (EU) 2018/843.

[15] AMLD follows the principle of technology neutrality and firms should assess the technologies that best address Article 13(1). Article 13(1) of the AMLD requires obliged entities to: a) identify the customer and verify the customer´s identity on the basis of documents, data or information obtained from a reliable and independent source, whether this source be paper-based or electronic; b) identify the customer's beneficial owner and take reasonable measures to verify the beneficial owner's identity so that the obliged entity is satisfied that it knows who the beneficial owner is; c) assess and, as appropriate, obtain information on the purpose and intended nature of the business relationship; and d) conduct ongoing monitoring of the business relationship, which includes transaction monitoring and keeping the underlying information up to date.

[16] ESAs' Opinion on the use of innovative solutions by credit and financial institutions, addressed to competent authorities and published on 23 January 2018.

[17] EBA Guidelines *on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions* ('The ML/TF Risk Factors Guidelines') published on 1 March 2021. These guidelines are addressed to credit and financial institutions and competent authorities responsible for supervising these firms' compliance with their anti-money laundering and counter-terrorist financing (AML/CFT) obligations.

consider when using innovative technological means to verify identity to promote convergence among the firms. These Guidelines were issued in March 2021.

Also, the EBA is currently working to respond to the EU Commission request, articulated in the Commission's Supranational Risk Assessments 2017 and 2019, to develop **Guidelines on Remote On-Boarding and Digital Identities**, which are due to be published for consultation by Q3 2021.

Looking ahead, the **EBA's response to the EC consultation on the digital finance strategy/action plan**[18] set out the EBA's views on FinTech and RegTech-related topics in the area of AML/CFT and the extent to which the current legal framework is sufficient to ensure the responsible and effective uptake by FIs of those tools. For example, the EBA recommended measures that should be taken into EU law to facilitate interoperable cross-border solutions for digital on-boarding, the reliance by FIs on digital identities provided by third parties (including by other FIs) and data re-use/portability. Furthermore, the EBA's response expressed views on the mandatory use of identifiers such as Legal Entity Identifier (LEI), Unique Transaction Identifier (UTI), and Unique Product Identifier (UPI) to facilitate digital and/or automated processes in financial services.

Furthermore, in the **EBA report on the future AML/CFT framework in the EU**[19], the EBA considered that greater harmonisation of CDD measures should not result in a prescriptive approach. Instead, the EBA recommended that the Commission should ensure that any future CDD requirements are technologically neutral while facilitating innovation and the development of a common CDD infrastructure.

4.1.1 General overview

AML/CFT is the area where RegTech is most active in the market from both a supply and demand perspective. Indeed, the RegTech deep dive study shows that 76% of participating FIs have had some experience with RegTech solutions in the AML/CFT area, and 39% of responding RegTech providers offer solutions for AML/CFT.

Based on the sample data, the first RegTech providers in the AML/CFT space were established in 2001, two-thirds of which are EU-based companies. The expansion of the segment was greatest in the period between 2016 and 2020, with RegTech solutions provided by EU-based firms being particularly noteworthy. These developments and in particular the growth of new solutions to tackle specific AML/CFT compliance challenges led to the adoption in 2018 of the ESAs' Opinion on the use of innovative solutions by credit and financial institutions.

4.1.2 Activities of FIs and RegTech providers

There are **five major areas of activity within the AML/CFT segment in which RegTech tools are being offered by RegTech providers and implemented by FIs**: (1) sanctions/PEP screening tools;

[18] EBA response to EC consultation on the digital finance strategy/action plan published on 26 June 2020.

[19] EBA report on the future AML/CFT framework in the EU is the EBA response to the European Commission's Call for Advice on defining the scope of application and the enacting terms of a regulation to be adopted in the field of preventing ML/TF, published on 10 September 2020.

(2) identification and verification of natural and legal persons (ID&V); (3) adverse media screening solutions; (4) tools for assessment of the risk associated with the business relationship; and (5) behaviour and transaction monitoring.

The results of the survey demonstrate that the current solutions mostly cover sanctions/PEP screening tools, both developed by RegTech providers or FIs. **More specifically, in what concerns the end-to-end technical steps in the AML/CFT processes, the AML/CFT solutions support data governance, the ETL process, detection engine, case management, investigation and analysis, and reporting.**

Half of the FIs rely on external standard solutions, with half of that volume having developed in-house solutions, and even fewer in-house solutions with external support. Only a small percentage of FIs have external solutions tailored to their needs. On the RegTech providers' side, they source on average 41% of their technologies in-house, around half of which are sourced through external technologies to complement their products or developed in-house with external support.

On the FIs' side, the main triggers for the implementation of RegTech solutions are the need to enhance risk management followed by the need to enhance monitoring/sampling, reduce human error, enhance systems and data integration, enable professionals to focus on higher value tasks and facilitate predictive analytics.

The need for efficiency is the key perceived reason for FIs using RegTech providers' solutions (as reported by 90% of RegTech providers), followed by ongoing regulatory changes, need for effectivity, cost pressure, organising complex information, and regulatory data integration.

4.1.3 Use of technology-based innovations

The top three technologies used in AML/CFT RegTech solutions are Cloud Computing, Data Transfers Protocols and Machine Learning. In the ranking of the most used technologies, these are followed by Semantics/Graph Analysis, Predictive Data Analytics, Natural Language Processing. Despite not being included in the top three, there is one additional technology that stands out in the sample, in that **Deep Learning has much higher usage by RegTech providers compared to FIs.**

In addition, and although being less used in AML/CFT, the respondents also indicated having contact with Biometrics, Image Recognition, Geographic Information System (GIS) Mapping, Robotic Process Automation (RPA), Distributed Ledger Technology (DLT)/Blockchain, Virtual Reality and Quantum Computing. Despite being less prevalent in this Report, their innovation and out-of-box features might actually be the real emergent technologies and have potential in the future to be well spread across the financial sector.

As far as deployment models are concerned, RegTech providers and FIs mostly offer and use Software-as-a-Service (cloud-based), followed by on-premises software implementation and RegTech-as-a-Service[20].

[20] Software plus additional business process services.

In terms of technical integration, the offer on the RegTech providers' side is led by real-time interfaces. Nevertheless, RegTech providers also offer data-driven integration, batch interfaces, event-driven integration or even manual interfaces. **On the FIs' side, both real-time and batch interfaces are the main technical integration models in use**, followed by manual interfaces, data-driven integration and event-driven integration. There do not seem to be significant differences in the preferred integration models between new and established RegTech providers.

4.1.4 Benefits, challenges and risks associated with use of AML/CFT RegTech solutions

Benefits associated with use of AML/CFT RegTech solutions

The deployment of AML/CFT RegTech solutions can add value to more traditional AML/CFT compliance solutions, regardless of the firm's sector, size or maturity. **The added value of RegTech solutions for AML/CFT compliance activities described in the 'Activities of FIs and RegTech providers' section is driven mainly by a) the increasing process efficiency, b) process effectiveness, and c) increased data quality.**

In addition, **for FIs, real-time monitoring seems to be a relevant value added** in sanction/PEP screening, ID&V, and behaviour and transaction monitoring. **RegTech providers**, on the other hand, identify **cost-saving benefits** in the behaviour and transaction monitoring tools and in the assessment of the risk associated with the business relationship.

Challenges associated with use of AML/CFT RegTech solutions

Significant obstacles and challenges with a wide impact were reported in the: 1) roll-out across different countries; 2) integration into clients' (FIs) legacy applications; 3) general obstacles and operational challenges; and 4) legal and regulatory obstacles.

According to RegTech providers, the rolling out of their RegTech solutions across different EU countries is hampered by the lack of buyer education/awareness and competition from other solutions that are already well established in other jurisdictions where the respondents have no market presence yet. Most FIs do not see issues on the roll-out to other jurisdictions; however, when barriers are identified, these relate to the different legal and regulatory requirements.

The obstacles related to the integration of RegTech solutions into clients' legacy applications are linked to the lack of clients' API capabilities. RegTech providers also refer to the lack of technical standardisation (e.g. data, interfaces, etc.), lack of data or data quality issues, legal and/or data privacy issues, lack of client documentation. Other obstacles identified relate to the existing and complex client processes and multiple APIs, and the lack of management understanding of the extraction, transformation and loading (ETL) processes, which is frequently a barrier to any data handling endeavours (including simple format conversions). According to RegTech providers, because legacy applications contain critical functions and data, if the integration challenges are not well understood and addressed by both sides, it can lead to overall reliability issues which will impact the outputs delivered by the new RegTech solutions.

The top three 'highly relevant' general obstacles and operational challenges that RegTech providers see for RegTech solutions to be successful in the AML/CFT market are the security, data privacy and protection issues, the lack of regulatory standards and the cost of user acquisition. On the other side, difficulties retaining and training employees, lack of standards and interoperability of solution and cyber security threats for the RegTech provider, despite still being material for most of the respondents, are considered to be the least relevant obstacles. **On the FIs' side, changes to national or international regulations, integration with legacy systems and data quality issues are the top three 'highly relevant' general obstacles and operational challenges**.

In what concerns, specifically, possible legal and regulatory obstacles to the adoption of solutions, in the view of RegTech providers, requirements for processing personal data are of major relevance, followed by the evolving AML/CFT regulatory requirements, and requirements for outsourcing. **From the FIs' perspective, the areas where legal and regulatory obstacles are most relevant are evolving AML/CFT regulatory requirements, requirements for outsourcing, and requirements in data processing**. Deeper analysis reveals that FIs perceive that supervisors should be aware that these innovative solutions have a different logic and may not all provide the same outputs, which depends on their architecture and quality of the data. Also, FIs state that the benefits of new technologies are amplified by the necessity to collect and share information across borders from/to different counterparties. However, survey respondents consider that personal data protection legislations may contain provisions that pose difficulties for information sharing or for data retention that do not allow a smooth usage of RegTech technologies. This finding is corroborated by all the sources used for the purpose of this Report.

Risks associated with use of AML/CFT RegTech solutions[21]

RegTech solutions can help make FIs' AML/CFT efforts more effective but, if poorly designed or applied unthinkingly, may carry risks. **Most FIs agree that the main risks relate to legal, concentration, and reputational risk**. Regarding concentration risks, FIs state that because many firms use the same tools, the same operational risks affect a large number of FIs that become vulnerable to the same points of failure. The legal and reputational risks can be linked to an array of root causes. Mention is also made to the risk of increased fraud or processing of illicit funds due to faulty solutions which are not in compliance with AML/CFT obligations. In addition, FIs also refer to the lack of understanding of what controls RegTech providers have in place to tackle data protection concerns (including data storage in third countries) and whose responsibility it is to monitor them. A perceived lack of transparency[22] of some RegTech applications is seen in some cases to impose difficulties in explaining to supervisors how certain controls are put in place.

An in-depth analysis also indicates that there are concerns about the software and data not being up-to-date, and this is valid for both internal and external solutions. Despite automation being

[21] AML/CFT and Fraud identified risks were considered interchangeable.

22 According to the EBA Report on Big Data and Advanced Analytics, published in January 2020, 'transparency' consists in making data, features, algorithms and training methods available for external inspection and constitutes a basis for building trustworthy models. Explainability and interpretability are two of the transparency's element: a model is explainable when its internal behaviour can be directly understood by humans (interpretability) or when explanations (justifications) can be provided for the main factors that led to its output (e.g., to enable effective supervision and audits).

considered one of the prime advantages of the new technologies incorporated in RegTech solutions, if not properly monitored over time, it can represent a risk for its unidentified software and data-related gaps.

Other operational risks mentioned by FIs include potential software outages and disruptions which may negatively impact not only the immediate flow of operations but also might leave space for remediation gaps (e.g. manual correction of data). **Security concerns** are also very relevant for FIs that highlight the possibility of data breaches (also linked to the concentration of risk). Finally, risk of impersonation is particularly highlighted by FIs using remote on-boarding solutions.

Overall, RegTech providers and FIs should be mindful that innovative RegTech solutions bring not only benefits but also contain risks and challenges. The key to assessing the value of new technologies is to understand the limitations and implement the necessary safeguards for the consistent oversight. It is important that firms can demonstrate to their competent authorities that they have identified, assessed and mitigated all relevant risks before introducing the innovative solution in their CDD process.

4.1.5 Case studies

Enhancing cryptocurrency trust and transparency using blockchain technology in AML/CFT

Targeted problem(s):

- Emergence of cryptocurrencies in the financial market with specific patterns of activity strange to FIs,
- Need for greater trust and transparency,
- New sophisticated Fraud trends using cryptocurrencies.

Proposed solution(s): RegTech A assists in the understanding of FI exposure to cryptocurrencies, monitoring of ongoing customer activity, and complying with regulatory requirements. The company uses blockchain technology in its solutions to visualise the flow of funds, enrich cryptocurrency investigations with contextual information, and assess risks at any stage of the customer relationship.

Reducing the false positive rate in AML/CFT name screening with Machine Learning

Targeted problem(s):

- Noise volume and false positives hits.

Proposed solution(s): Financial Institution A has deployed a Machine Learning-based solution able to learn from the context and operator feedback to cut down false positive hits concerning sanctions screening of an implemented third-party tool. Although this tool cannot eliminate false positives, it has proven to significantly reduce the false positive rate.

4.2 Fraud prevention

Another segment with an active RegTech market is fraud prevention which is the third segment where the RegTech market is the most active from an FI perspective, and the second one for RegTech providers. 40% of participating FIs in the survey have experience with RegTech solutions in the fraud prevention area, whereas 26% of responding RegTech providers provide fraud prevention solutions.

Bearing in mind that fraud is a crime and a predicate offence for ML/TF, the EBA's work linked to innovative solutions and emerging technologies in the AML/CFT area also applies here. In addition, specifically in the area of payments, the EBA had an active role under the Directive (EU) 2015/2366 on payment services in the internal market (Payment Services Directive 2 – PSD2)[23] by developing, in close cooperation with the ECB, the Regulatory Technical Standards on strong customer authentication and common and secure communication (RTS on SCA & CSC), the Guidelines on Fraud reporting under PSD2[24] and the Guidelines on major incident reporting under PSD2. The RTS on SCA & CSC set, inter alia, the requirements for strong customer authentication and other security measures, which aim to increase the security of electronic payments in the EU by reducing to the maximum extent possible the risk of fraud and ensuring the protection of customer funds and data. The Guidelines on fraud reporting specify the data to be collected and reported on payment transactions and fraudulent payment transactions by using a consistent methodology, definitions and data breakdowns. They also specify that the aggregated data is to be shared by CAs with the EBA and the ECB.

4.2.1 General overview

The constant advances in the digitally enabled financial sector gave rise to the adaptation of 'traditional' fraud schemes and emergence of new and complex ones. Fraud prevention underpins the need for cutting-edge technology to face such developments. The main RegTech providers' purpose in this area is to help FIs to introduce adequate controls to mitigate the risk of fraud and to fulfil their regulatory expectations.

Most fraud prevention RegTech solutions implemented by FIs are external solutions rather than developed in-house. An in-depth analysis shows that regarding the primary sourcing model for the use and development of such technologies, there is an expected difference between RegTech providers and FIs. On the RegTech providers' side, the solutions are mainly developed in-house and in-house with external support for specific tasks, whereas for FIs, these are primarily external, either standard or tailored to FIs' needs. Only one FI in the sample mentioned developing a fraud prevention RegTech solution in joint cooperation with an academic institution, specifically using machine learning.

[23] Entered into force in the European Union (EU) on 12 January 2016 and has applied since 13 January 2018.

[24] Final Report Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2), addressed to payment service providers and competent authorities, and published on 18 July 2018.

In terms of key drivers, on the FIs' side the top six triggers for the implementation of RegTech solutions are the need to enhance monitoring, enhance risk management, reduce human error, reduce costs, facilitate predictive analytics, enhance systems and data integration. A few FIs also reported COVID-19 global lockdown challenges as another important factor.

RegTech providers state that their solutions respond to the industry's call for effectiveness and efficiency, followed by the need to stay up-to-date with ongoing regulatory changes, organise complex information, cost pressure, and regulatory data integration. Adequate risk management is also mentioned as one of the main reasons for using fraud prevention RegTech tools.

4.2.2 Activities of FIs and RegTech providers

In the fraud prevention environment, innovative solutions for both RegTech providers and FIs are mainly addressed to a specific part of the process chain – behaviour and transaction monitoring. Recent developments in the area show that other types of fraud checks are available in the market, too. The examples include fraud checks at the on-boarding phase (mainly identity fraud and risk scoring) and fraud reporting.

4.2.3 Use of technology-based innovations

Technological breakthroughs in fraud prevention are being led by Machine Learning by both FIs and RegTech providers. Machine Learning is identified as of most use in behaviour and transaction monitoring solutions and fraud reporting and is being used in diverse products and services (e.g. payment transactions, client application usage, etc.) to uncover trends and patterns in real time. Additional data reveals that this can be specifically used to tackle an array of fraud schemes, e.g. from phishing and smishing, identity fraud (e.g. account takeover attacks, ID document fraud, and fake account identification), to plastic card fraud, loans, and customer on-boarding, etc. It is highlighted by the respondents that higher data quantity and better data quality lead to enhanced classifications, predictions and insights, which result in better decision-making capabilities. In a dynamic world where data has become big and datasets complex and diverse, Machine Learning has come to process it and help to increase efficiency and effectivity. This is pointed as an alternative or complement to rules-based solutions conceived to be too manual and static in time, with enhanced limitation as regards the volume of rules that can be implemented.

In addition, cloud computing and predictive data are reported to be the most used technologies leverage in fraud prevention, followed by semantics/graph analysis and data transfers protocols. Advancements in cloud computing technologies are perceived to be especially a measure for cost savings and usage flexibility in fraud prevention, and in many other segments. The cloud environment can be available on demand, thus greatly reducing the time for fraud data acquisition and analysis.

RegTech providers are offering biometrics solutions (followed by robotic process automation (RPA). Biometrics refers to the use of certain measurements directly linked to human biology. In fraud prevention, the most common ones are fingerprint scanning, facial geometry/patterns and retinal scanning. The roll-out of these technologies is highly dependent on availability of adequate

equipment. Interviews held with market participants indicate that, as expected, the PSD2 requirements have fostered the use of innovative behavioural biometric solutions, especially in the application of strong customer authentication (SCA). Additional research shows that solutions available in this segment also offer alternative biometrics (such as keystroke dynamics and mobile phone movements' measurements), but no evidence has been collected to assess the extent of its prevalence in the market.

Despite being less used by both FIs and RegTech providers, no less relevant are natural language processing (NLP), deep learning, geographic information system (GIS) mapping, image recognition, speech recognition, distribution ledger technology (DLT)/blockchain, virtual reality and quantum computing technologies. The use of speech recognition – a ramification of biometrics – deserves special mention. It is applied in fraud prevention to verify legitimate customers over the phone via voice-printing capabilities. The respondents identified this as one of the main wish-list investments to tackle social engineering attacks against FIs' fraud call centres.

In what concerns deployment models, the FIs and RegTech providers indicate that their solutions can and are mainly delivered as Software-as-a-Service (cloud based) models, followed by on-premises software implementations, and RegTech-as-a-Service.

The most common technical integration model into the existing legacy applications is, on both sides, real-time interfaces. RegTech providers also offer data-driven integrations, batch interfaces, event-driven integrations, manual interfaces, or no integration. The FIs usually opt for manual interfaces, batch interfaces, even-driven integration, data-driven integration or no integration at all.

4.2.4 Benefits, challenges and risks associated with use of fraud prevention RegTech solutions

Benefits associated with use of fraud prevention RegTech solutions

In the fraud space, innovative technologies and available RegTech solutions (for both RegTech providers and FIs) are greatly beneficial in **behaviour and transaction monitoring**. In this respect, **RegTech providers and FIs concur in the ranking of the value added generated by the developed fraud prevention solutions, with the following cited as the main benefits in order of priority: increased process effectiveness,** increased process efficiency, real-time monitoring, cost savings, improved data quality, ease of integration with existing systems, and information sharing.

Challenges associated with use of fraud prevention RegTech solutions

The use of fraud prevention RegTech solutions also presents major obstacles and challenges related to 1) roll-out across different countries; 2) integration into clients' legacy applications; 3) general obstacles and its operational challenges; 4) legal and regulatory obstacles.

In terms of roll-out, what prevents RegTech providers from scaling across the EU is the lack of buyer education and awareness, competition from other solutions already deployed in other

countries, lack of regulators/supervisor support, different legal/regulatory requirements, and different technical standards. On the FIs' side, not much relevance is given to these obstacles; however, when barriers in the roll-out are identified, these relate to the different legal and regulatory requirements.

With regard to challenges in *the integration into clients' legacy applications*, the top three obstacles reported by RegTech providers are the lack of client API capabilities, followed by legal and data privacy issues and the lack of data quality issues.

With regards to *general obstacles and operational challenges*, RegTech providers, on the one hand, find the lack of technological capabilities of the potential clients, the integration with legacy systems and the security data privacy and protection issues to be the top three 'highly relevant' obstacles. The FIs face challenges in integrating with legacy systems as well, but for FIs cybersecurity threats and data privacy and protection issues complement the top three.

In what concerns specifically *legal and regulatory obstacles to the adoption of solutions*, RegTech providers state that requirements for processing personal data are of major relevance. From an FI's perspective, the areas where legal and regulatory obstacles are most relevant are requirements in data processing, and requirements for outsourcing.

Risks associated with use of fraud prevention RegTech solutions[25]

One of the risks identified relates to **automation without an effective oversight**. Risks associated with the complexity of processes might lead to waterfall errors and inaccuracies when incitements or events of diverse natures occur. This is particularly relevant in the behaviour and transaction monitoring where the false positives and false negatives are of utmost concern. This can lead to the obsolescence of existing controls. A particular FI mentioned this has happened in the abrupt beginning of the COVID-19 pandemic marked by a spike in false positives, which adversely impacted business performances and customer services. It has highlighted the need for regular monitoring of solutions and the performance of the underlying technology in order to assess gaps and required calibrations of the automation process over time.

Unclear liability of business relationships between FIs and RegTech providers is also identified as a risk for effective oversight. The highly desired **golden source of data** in centralisation of processes is also seen as a risk in case of cyberattack **vulnerabilities**. For the same reason, RegTech providers are also perceived to be prone to cyberattacks due to the availability of their valuable data. On the FIs' side, respondents indicate that RegTech solutions are often not fully customisable, which gives rise to an incomplete business process with added complexity. The RegTech providers and FIs also commonly identify a possibility where the RegTech solutions can be employed correctly and be performing as expected, but the risks may arise given their interactions with **existent legacy infrastructures** (that may not perform as expected), and create a damaging impact in the outcomes.

[25] AML/CFT and Fraud identified risks were considered interchangeable.

Specific technologies' risks can also be identified. For example, in case of Machine Learning, there is the identified risk that an adequate maintenance of algorithms and inspection of the risk scores' accuracy does not always exist. Regarding cloud-based solutions, there is a risk that the FIs do not actually know where the provider's servers and data storage are located, which, in light of the recent developments in GDPR requirements, might represent an issue when no adequate data controls are in place. Last but not least, FIs using biometrics also identify that as biometric authentication becomes more popular, fraudsters are likely to increase their attacks vectors on both customers' devices and FIs' systems.

4.2.5 Case studies

Enhancing data protection and data privacy using blockchain technology in fraud prevention

Case study 1

Targeted problem(s):

- Data protection and data privacy issues in the process of online customer authentication and verification;
- New sophisticated fraud trends (e.g. phishing, identity theft, fraud impersonation, malware attacks or data breaches).

Proposed solution(s):

RegTech A uses *Zero Knowledge Proof protocol* in its authentication software. This is a component of blockchain technology which allows two end entities to prove to each other they have the same data without the effective sharing of any data in a secure and anonymous way. Consequently, it eliminates the transmission, storage and exposure of any personally identifiable information during authentication and identity verification (e.g. passport details, birth date, gender, nationality, card numbers, passwords, address details). Once the verification is established, the outputs are stored using abstract patterns. It can be used in a different array of tasks, e.g. anti-SIM swap fraud prevention, authentication, card authorisation.

Case study 2

Targeted problem(s):

- Data protection and data privacy issues in the detection and investigation processes;
- Challenges in data sharing between two or more organisations;
- False positives in transaction monitoring;
- New sophisticated fraud trends (e.g., authorised push payment fraud).

Proposed solution(s):

RegTech A has developed a solution using *secure multi-party computation cryptographic protocol* to perform privacy-preserving computations on data in the context of fraud prevention and AML/CFT, enabling private collaborative processing. This allows the involved parties (FIs and other organisations) to jointly compute a risk score without having to actually disclose it. Parties agree on the underlying rules, data taxonomy and attributes pertaining to accounts (e.g., KYC data, login activity, transactional activity). This helps FIs to identify potentially suspicious transactions and detect criminal activity more clearly and accurately by combining the information they have. In addition, because of their audit tracking features, FIUs and CAs can still access the data, as the FIs can share the keys to decrypt it on their side. It can be used in a different array of tasks, e.g. risk assessment, transaction monitoring processes.

4.3 Prudential reporting

This chapter provides an in-depth analysis of the state of play of solutions and technologies RegTech providers put in place to assist FIs with their reporting functions and obligations. This section also takes into consideration the evidence on the use of technology by FIs collected through the *Cost of compliance study*[26] and provided in the *Discussion Paper on Feasibility study for integrated reporting system*[27].

4.3.1 General overview

Prudential reporting is one of the main areas of interest in the RegTech universe, with 11% of RegTech solutions specialised in reporting services.

The Implementing Technical Standards (ITS) contained in the EBA reporting framework are provided in the form of templates and instructions which are then further developed in a technical package containing Data Point Model (DPM), validation rules and XBRL taxonomy. Apart from the reporting data provided through the EBA reporting framework, the FIs need to provide further data to the EBA through ad hoc data collections and to national data collections to comply with specific national legislation.

The FI reporting landscape is broad and entails certain investments to reporting institutions legacy systems to comply with the reporting needs for supervisory purposes.

Existing RegTech reporting solutions already cover a variety of reporting requirements and support users in their tasks and processes.

4.3.2 Activities of FIs and RegTech providers

The RegTech solutions for prudential reporting have a wide scope of applicability which covers different steps along the reporting process chain[28]. Many solutions combine reporting processes with automation by using supporting technological approaches. **The degree of automation varies heavily throughout the different parts of the reporting process chain.** The figure below shows different parts of the reporting process chain and which steps of the process are covered by technology and hence have an increased level of automation.

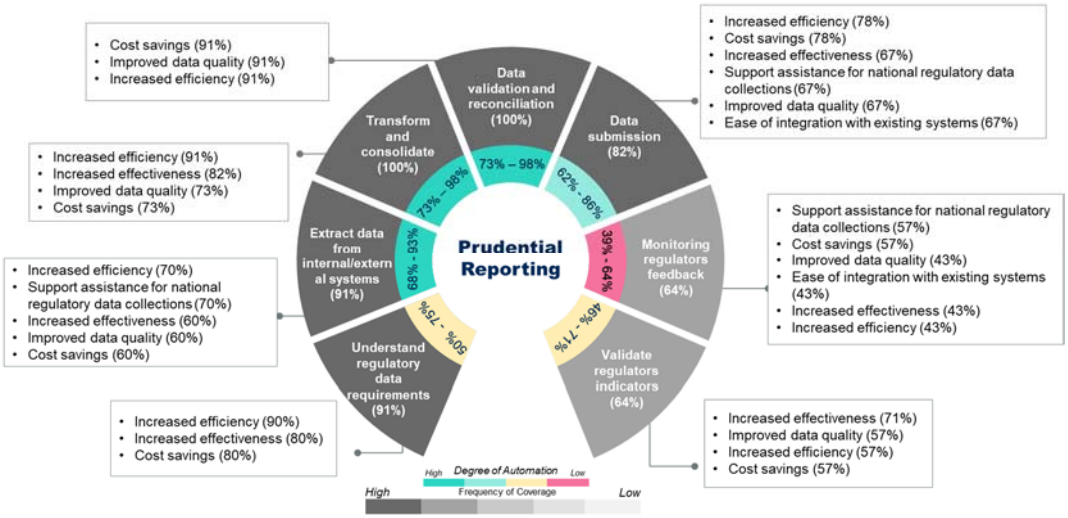
The evidence collected from RegTech providers shows that most of the RegTech services provided are focused on the first steps of the reporting process, mainly on understanding the regulatory data requirements, data validation and data reconciliation.

[26] REPORT EBA/REP/2021/15

[27] Discussion Paper on a Feasibility Study of an Integrated Reporting System under Article 430c CRR (EBA/DP/2021/01)

[28] Following the definition provided in the Discussion paper on Feasibility study of the Integrated reporting system, the reporting process chain consists of different steps: data definition, data collection, data transformation and data exploration.

Figure 21.: Reporting process areas covered by RegTech solution



Similarly, those steps of the reporting process present a higher level of automation:

- **understanding regulatory data requirements** – a commonly used functionality of the RegTech services is the possibility of having in a single platform an overview of all the different reporting requirements which enables the reporting institutions to better navigate through the different reporting requirements and simplify the management of the reporting process. Additionally, apart from the software, the RegTech providers offer in some cases consultancy services on providing further clarifications on the understanding of the regulatory products.

- **data quality and the effective management of the data** through the reporting process is the central focus within the systems for RegTech. Some RegTech providers offer the possibility to produce different reporting requirements by integrating them into the same platform. This includes a set of data checks to test the reconciliation of data within different reports. Additionally, some platforms offer the possibility to trace all the reports from aggregated data to granular data.

- **extract data from internal/external systems** – the RegTech providers get data from the legacy systems of the reporting institutions; in some cases they need to be connected to different databases to prepare the report. This facilitates the aggregation of some data from different databases which, in some cases, is manually done by reporting institutions. RegTech solutions can automate manual processes, reduce errors, and provide quicker access to accurate consolidated data and, thus, new insights.

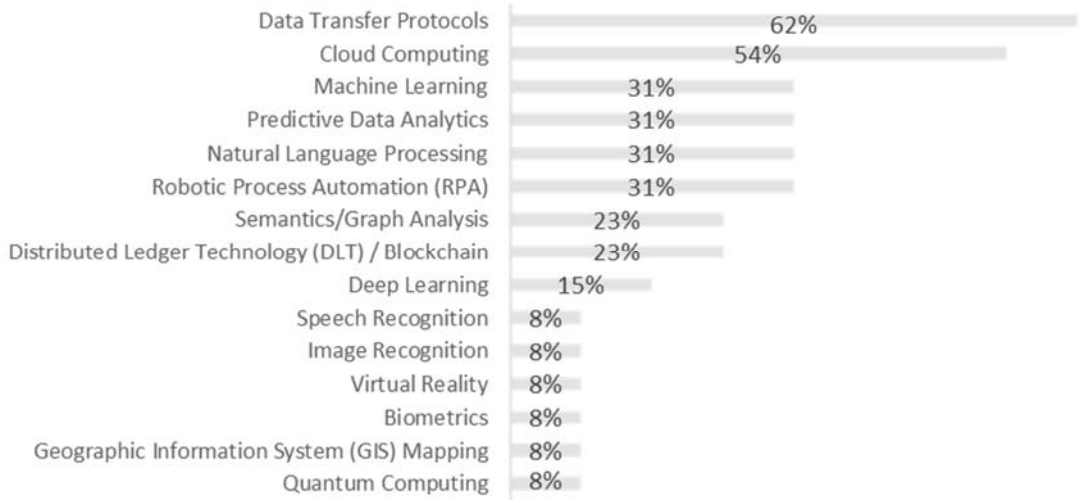
Additionally, data exploration and tools that assist this task also play a relevant role, as the data can also be used for further analytics and calculations in other areas of application. According to RegTech providers, their technology for reporting purposes supports FIs to regain control and oversight on their different reporting requirements without the necessity to compromise on data quality and reporting deadlines.

Use of technology-based innovations

With 57% of all solutions not being in the production stage (36% reported in a vendor presentation stage and 21% in a proof of concept/pilot stage), prudential reporting is the least mature of the major RegTech segments analysed in this report in terms of implementation stages. In addition, compared to other RegTech segments, reporting solutions are often developed in-house by FIs.

The technologies used by RegTech providers in the area of reporting are broadly distributed. Data Transfer Protocols are the most commonly utilised technology included in 62% of RegTech providers' solutions. Also, cloud computing claimed to be used by 54% of RegTech solutions providers. Other technologies seem to play a minor role for reporting solutions.

Figure 22.: RegTech providers - use of technology for prudential reporting



Not only the technologies deployed are of interest. The interoperability is also an issue that RegTech providers have to tackle. Half of the solutions offered by RegTech providers are claimed to be interoperable with both main core banking systems and ICT software, and some other RegTech solutions. However, 23% of solutions do not enable interoperability with other systems or applications.

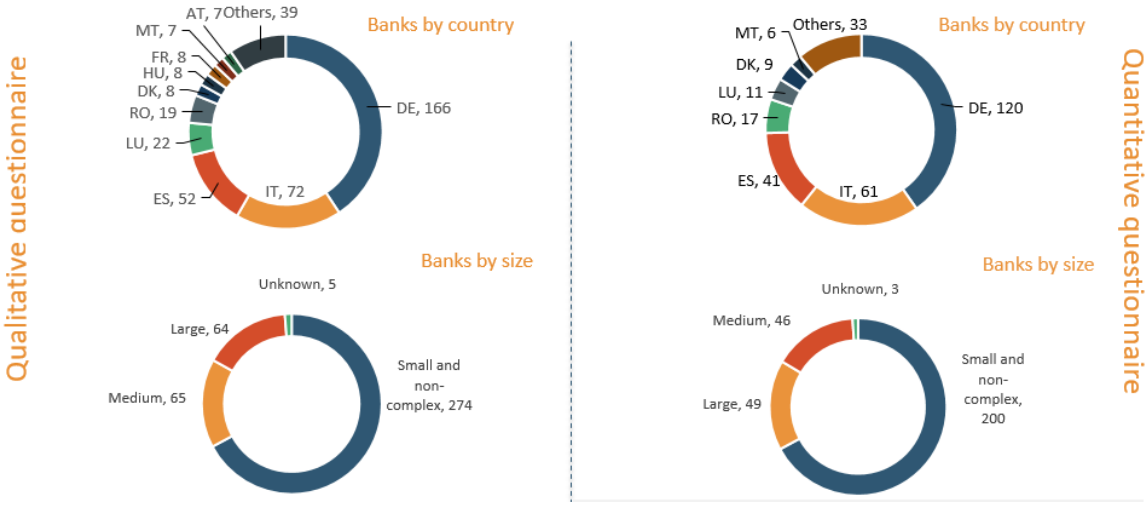
4.3.3 Use of technology by FIs - evidence from the Cost of compliance study

The analysis provided below is an extract of the Discussion Paper on Feasibility study on Integrated Reporting which includes evidence from the Cost of Compliance study.

The EBA Cost of Compliance study (CoC) gathered evidence on the nature and complexity of the IT solutions used for regulatory compliance and associated reporting obligations. The objective of this study was to identify how FIs perform regulatory reporting on top of their regulatory compliance, and to understand the general setup of the IT solutions used along the four different phases of the regulatory data chain.

The industry responses received from the qualitative and quantitative questionnaires were 408 and 298 respectively. The responses covered 8.5% of all banks (27.6% of large banks, 3.3% of medium ones and 10.5% of small and non-complex banks). The following graph shows the distribution of institutions by country and size.

Figure 23.: Industry responses to the EBA Cost of Compliance study



For the purpose of the CoC study, the FIs were asked to answer how they use technology and organise their data through the four principal phases of their processes of regulatory and reporting compliance: i) understanding regulation; ii) extracting data from sources; iii) calculating and reconciling data; and iv) reporting and monitoring data for compliance.

There were no significant differences in the type of IT solutions supporting both the overall regulatory compliance and the reporting processes. For all types of institutions (small and non-complex, medium, large) and in each of the different phases, both compliance processes used similar types of technical solutions. This can be a sign of possible integration of reporting processes within the internal processes of compliance.

Setup of the IT solutions in the distinct phases of regulatory compliance

The general setup of the IT solutions is very different along the distinct phases in all types of institutions.

In the initial phase of understanding regulation, small and medium-size institutions mostly rely on service providers' solutions and, in second place, on internal solutions, while being less dependent on COTS[29] software. Large institutions have an equal usage of service providers, internal solutions and COTS software. Other possible technologies are not relevant to any types of institutions.

In the phase of extracting data from the sources, small institutions almost exclusively rely on service providers' solutions, few have internal solutions and the usage of COTS is insignificant.

[29] Commercial-off-the-shelf (COTS) software is a term for software products that are ready-made and available for purchase in the commercial market.

Medium institutions rely equally on service providers and internal solutions and the COTS software is less relevant. Large institutions use fewer service providers and have a strong implementation of internal IT solutions with some COTS software usage.

In data calculation and reconciliation, small institutions almost exclusively rely on service providers' solutions, few have internal solutions and the usage of COTS is insignificant. Medium institutions rely more on service providers, but they still have a relevant number of internal solutions and also an increased use in COTS software in comparison with data extraction processes. Large institutions use fewer service providers and have strong preferences for implementing internal IT solutions and using COTS software. However, when comparing with the data extraction phase, they are increasing all the three types of IT solutions, which can be a signal of a more intense use of IT solutions in this phase of regulatory and reporting preparation.

In reporting and monitoring processes, small and medium-sized institutions almost exclusively rely on service providers' solutions, few have internal solutions, and the usage of COTS is insignificant. Large institutions use some service providers, but rely more strongly on internal IT solutions. The usage of COTS software is more significant in reporting and monitoring than in the other processes.

4.3.4 Benefits, challenges and risks associated with use of prudential reporting RegTech solutions

Benefits associated with use of prudential reporting RegTech solutions

When asked about the reasons for using RegTech solutions for prudential reporting, respondents list numerous expected benefits. These include state-of-the-art technology, rapid implementation, the correctness of analytics, ease of use (intuitive), customised report designs, data and benchmark handling integrated, near-real-time production, high productivity and high quality with consistency (enter data once).

'Ongoing regulatory change' and the need for 'regulatory data integration' seem to be the most important drivers in the scope of prudential reporting. When comparing this to the overall RegTech market, 'need for efficiency' and 'ongoing regulatory change' are the most significant factors indicated by FIs across all RegTech segments. On the other hand, RegTech providers consider that 'cost pressure' is the most important factor determining the FIs' decision on implementing RegTech solutions for prudential reporting.

Challenges associated with use of prudential reporting RegTech solutions

RegTech providers point to some inconveniences restraining their clients from implementing reporting RegTech solutions. Prudential reporting seems to be 'neither-in-house nor BigTech solution', as it requires deeper integration, testing and detailed planning to comply on time with the reporting requirements.

Legacy systems and data quality – FIs are reliant on operational systems that are built on older technology, which carries its own operational and integration challenges. The data required to

populate RegTech tools is extracted or processed by these systems. New reporting solutions need far-reaching overall concepts instead of solving fragmented problems. Often legacy solutions provide breadth (coverage) but do not provide the necessary depth, while RegTech providers usually offer deep solutions to narrow problem spaces, i.e. they do not provide the same coverage as legacy solutions.

The main challenge for the successful application of RegTech for prudential reporting is data quality. This problem manifests itself in various aspects. Even though reported data is generated within the FIs, it is often difficult to collect it. Errors made at this stage often can be detected over time, but it gets harder to amend them.

Ongoing regulatory changes – changes of national and international regulation entail barriers to integration with legacy systems and interoperability when different types of non-standardised reports are requested by different competent authorities.

Lack of data standardisation – FIs and RegTech providers agree that solving the problem of data standardisation and data integration is crucial for the efficient development of prudential reporting RegTech solutions. The differences in standard definitions, procedures, or technical requirements from the different authorities can add difficulties to the efficient definition and operation of data systems.

Standardisation of data would help also with the problem of insufficient data and data quality issues. The more data is standardised, the easier it will be to automate the processes and improve data quality along the reporting process. The use of common data standards could also facilitate the implementation of digital reporting instructions, which would facilitate the implementation of machine executable regulation.

Some of the challenges mentioned above are currently being analysed through different initiatives around data standardisation and the creation of common data definitions.

On prudential and resolution reporting, the EBA implemented the DPM data dictionary, which integrates all the data definitions included in the reporting regulations produced by the EBA and the reporting requirements defined by the SRB. The EBA is currently working on a Feasibility Study on Integrated Reporting, following the mandate contained in Article 430c CRR, according to which the EBA will need to analyse if it is possible to integrate different types of data (supervisory, resolution, statistical data) for reporting purposes with a view to further enhance efficiency and reduce the reporting burden for institutions. One key aspect to take into account in this regard is how the use of new technology such as RegTech could help to streamline the reporting process.

In addition, there are other initiatives in the EU on data standardisation and the creation of common definitions. The ECB initiative on 'Banks Integrated Reporting Dictionary' (BIRD)[6] aims to help banks organise information stored in their internal systems by providing a data model that describes the data to be extracted from the banks' internal IT systems to derive reports required by authorities.

Similarly, other countries have set up reporting platforms such as the AuRep platform in Austria and Puma 2 in Italy.

Risks associated with use of prudential reporting RegTech solutions

There is a risk that RegTech solutions could be used to avoid the responsibility of FIs to set up accurate controls on the quality of data reported to authorities. The supervised entities using RegTech solutions should remain responsible for the quality of the data reported to competent authorities in compliance with BCBS 239 principles on data aggregation and reporting[30].

When considering risk related to the implementation of the prudential reporting solutions, concentration risk and operational risk (ICT/cyber risk) should be carefully assessed and managed.

As cloud computing becomes the industry standard, related security and data privacy issues become more important also in the context of prudential reporting.

[30] See: https://www.bis.org/publ/bcbs239.htm

4.4 ICT security

The use of RegTech solutions implemented by FIs for ICT security was reported as another prevalent RegTech segment. According to the survey, the use of RegTech services for ICT-related matters seems quite common; however, most of these services related to general ICT services which aim to facilitate compliance with ICT-related regulatory requirements, therefore it is quite challenging to crystallise 'pure' RegTech solutions in the area of ICT security.

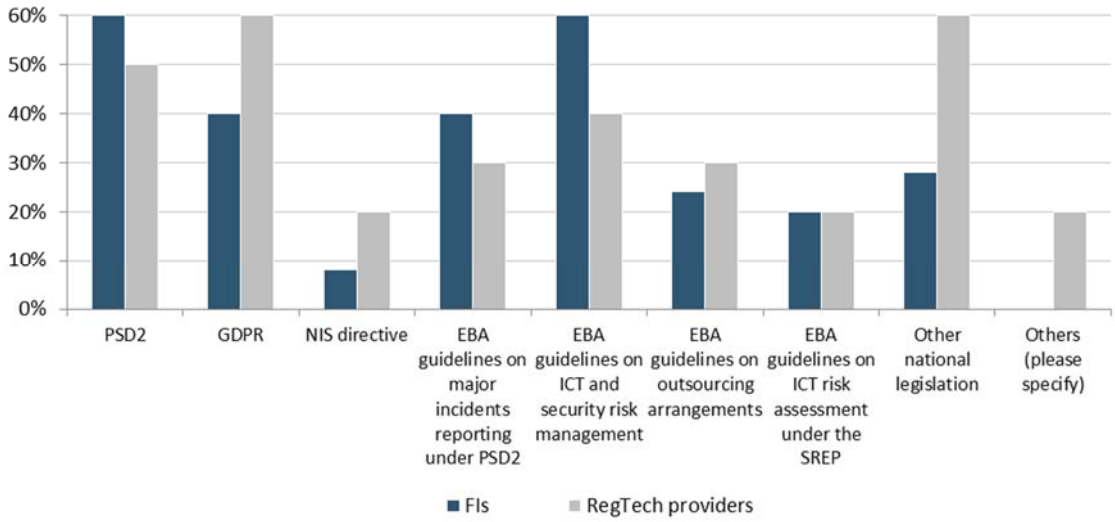
4.4.1 General overview

The EBA has defined several ICT-related guidelines and recommendations over the last few years for the financial sector. First of all, in 2017 the EBA issued Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP) that aims to define and promote common procedures and methodologies for the assessment of ICT risk. Having identified that the usage of the cloud services was becoming of utmost importance within the financial sector, the EBA issued the recommendations on outsourcing to cloud service providers (EBA/REC/2017/03). These recommendations intended to clarify the EU-wide supervisory expectations for FIs to allow them to leverage the benefits of using cloud services, while ensuring that any related risks are adequately identified and managed. In 2019, EBA revised its Guidelines on outsourcing arrangements (EBA/GL/2019/02) that established a more harmonised framework for outsourcing arrangements.

Furthermore, in 2019 the EBA issued Guidelines on ICT and security risk management (EBA/GL/2019/04) that established requirements for FIs on the mitigation and management of their information and communication technology (ICT) and security risks and aim to ensure a consistent and robust approach across the Single Market. Finally, in September 2020 the European Commission published a proposal for a new regulation of digital operational resilience in the financial sector (Digital Operational Resilience Act). The Act will define requirements for the ICT risk management and ICT third-party management as well.

Against this backdrop, most ICT security-related RegTech solutions aim to facilitate compliance with regulatory requirements (e.g. incident reporting requirements defined by PSD2 or NIS directive, different ICT-related requirements of the EBA Guidelines on ICT and security risk management, and national or international standards, e.g. ISO 27001 or Cobit 5). A significant number of ICT security RegTech solutions went live between 2016 and 2020. However, ICT-related RegTech tools can also be used, applying mathematical models, to ensure the necessary anonymity, such as through the usage of synthetic data, when using machine learning and advanced analytics in combination with cloud-based delivery models to comply with GDPR and personal data protection requirements.

Figure 24.: ICT Security-related regulatory requirements targeted by RegTech solutions

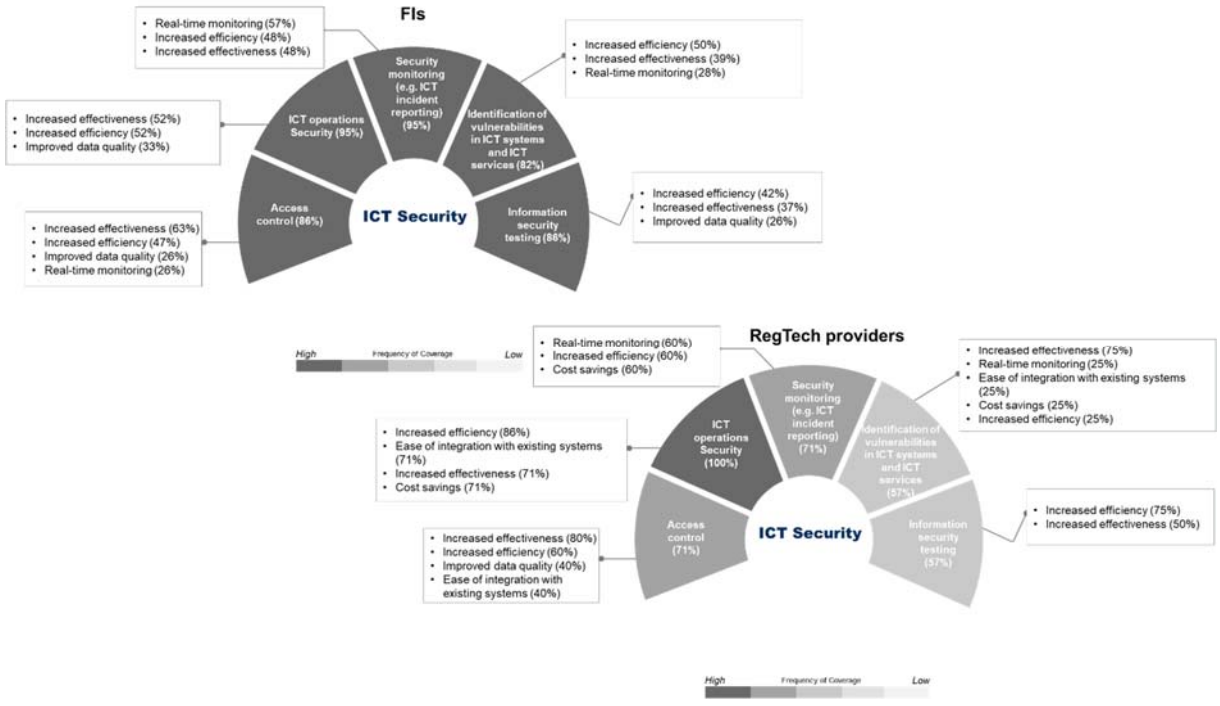


4.4.2 Activities of FIs and RegTech providers

74% of FIs consider that RegTech solutions can be of value within the ICT security area. A further 22% of the FIs see only limited potential for RegTech solutions within ICT security, while 4% of the FIs do not see any value of RegTech services within the ICT security area.

ICT security-related RegTech services offer inter alia solutions for access control, ICT operations security, security monitoring (including ICT incident reporting) and identification of vulnerabilities in ICT systems and services, and information security testing. However, the survey data analysis shows that the majority of ICT RegTech solutions are still under development.

Figure 25.: FIs and RegTech – ICT RegTech solutions' process chain and value added



Several ICT-related RegTech services support **ICT operations security** and, for example, can restrict access and actions permitted for authorised users, limit data circulation, classify incidents, provide threat intelligence or security dashboard. In addition, RegTech solutions provide the ability to aggregate a secure audit trail, flexible reporting on various ICT operations security aspects, provide Advanced Persistent Threat preventive technologies or security scorecard for third parties.

The services in connection with the security monitoring can provide automatic monitoring tools (even real-time monitoring of all elements of the ICT systems), provide warnings in case of breaches, different incident reporting services or applications (classification, reporting, response, identification and logging of incidents or information sharing), or they could even correlate data from multiple sources to provide monitoring and response functionality.

Services that help in the **identification of vulnerabilities in ICT systems and services** provide some kind of threat intelligence solution or perform regular vulnerability scans, manage detection and vulnerability response.

On **information security testing**, FIs indicate solutions to conduct regular penetration and software performance testing[31], often conducted by skilled third parties to test that the security controls are in place to ensure issues are discovered and corrected on time.

Furthermore, other ICT-related RegTech services help undertakings to **identify and apply the new ICT-related requirements** by monitoring and identifying recently issued laws and legislation and support the assessment of new elements or solutions that digitalise, automate and foster the ICT risk assessment processes.

FIs choose to use ICT-related RegTech services mainly to enhance risk management, monitoring/sampling and to reduce human error. Based on the RegTech providers' view, their FIs customers use RegTech mainly because of the ongoing regulatory challenges, need for efficiency and to organise complex information.

However, in terms of level of automation achieved, nearly half of FIs indicated that RegTech services provide limited automation (i.e. 0%-29% automation level) where human intervention is still needed to record information manually, collect qualitative information, evaluate the results or conduct data consistency checks.

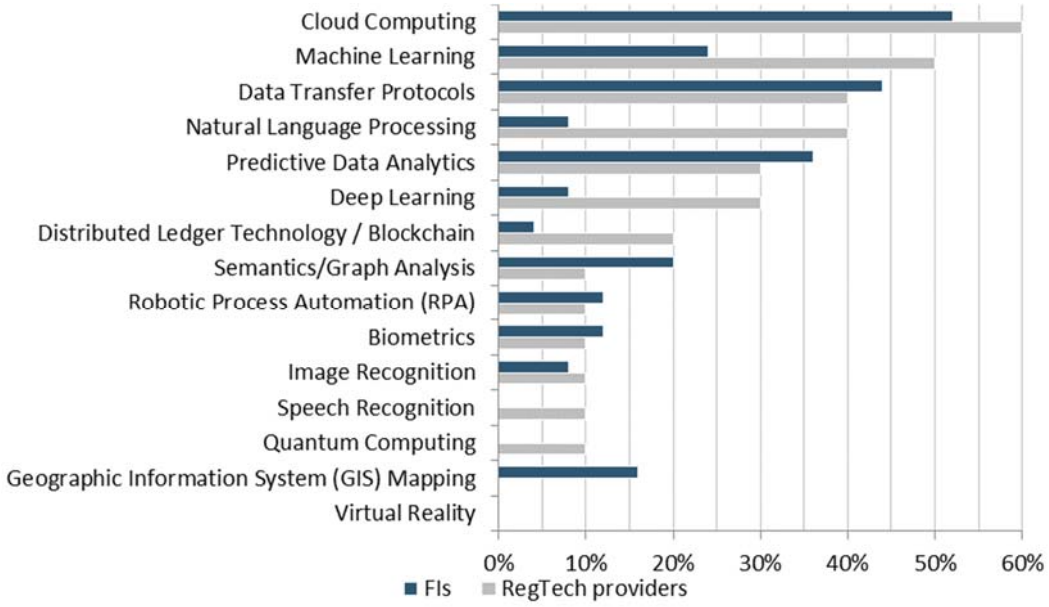
4.4.3 Use of technology-based innovations

The most used technologies for ICT-related RegTech solutions are cloud computing and machine learning. More than 50% of the ICT-related RegTech services use cloud computing (both FIs and RegTech providers). AI-related technologies (ML and NLP) and the Data Transfer Protocols are the most common technologies after cloud computing used by RegTech providers.

[31] Software performance testing means a software testing process that is used for testing the speed, response time, stability, reliability, scalability and resource usage of a software application.

In the case of FIs, Data Transfer Protocols (44%) and Predictive Data Analytics (36%) are the most commonly used technologies after cloud computing. It is important to highlight that usually different combination of technologies are used within one service. For example, usually AI-related technologies are enabled by cloud computing and used together with Big Data Analytics.

Figure 26.: Degree of use of technologies in ICT security RegTech solutions



In terms of underlying technologies, most FIs use external technology solutions, in particular in the case of cloud computing and Data Transfer Protocols. **The RegTech providers' solutions are mainly developed in-house,** with the exception of standard external solutions, e.g. in case of the cloud computing technology, and only a few cases of in-house development of RegTech solutions with external support.

4.4.4 Benefits, challenges and risks associated with use of ICT security RegTech solutions

Benefits associated with use of ICT security RegTech solutions

Potential effectiveness and efficiency increase are the main drivers for RegTech providers and for FIs to develop RegTech solutions.

From the FIs' perspective**, enhanced risk management**, **real-time monitoring** and the **increased effectiveness** are the biggest value added that ICT-related RegTech services can generate. Improved data quality also seems to be an important benefit for FIs.

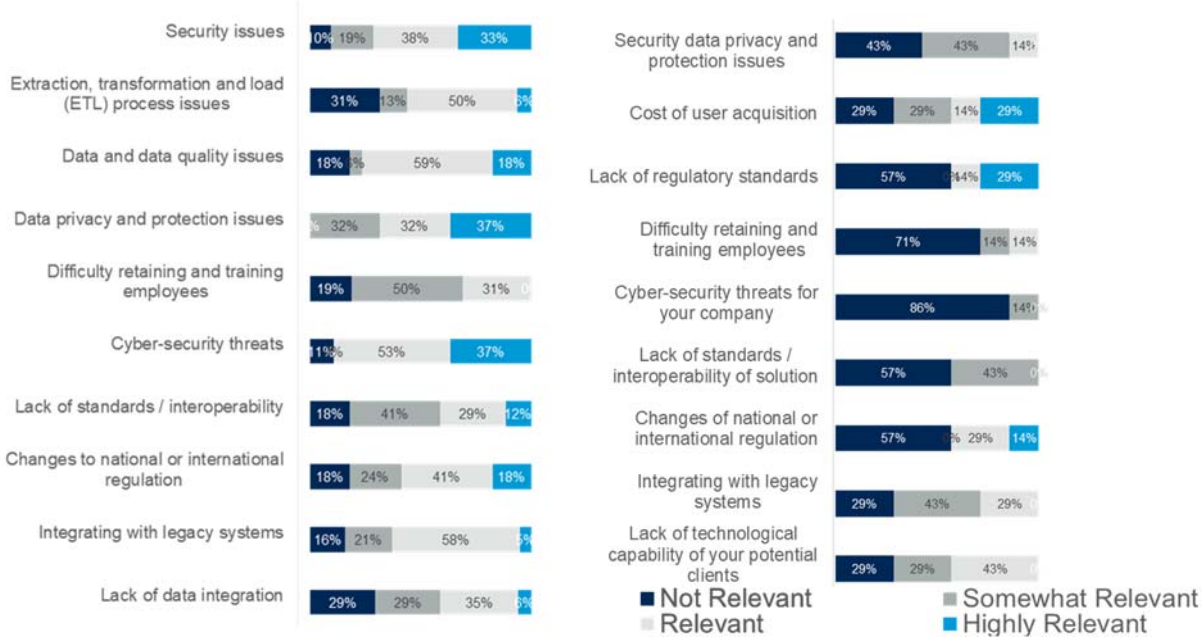
From the RegTech providers' perspective, the key reasons for using their ICT security-related RegTech solutions are **support in addressing ongoing regulatory changes**, **organising complex information** and **increasing effectiveness**.

Challenges associated with use of ICT security RegTech solutions

For the FIs, **Data Privacy and Protection issues, Cyber Security Threats and other Security Issues** cause the biggest challenges and obstacles. Data quality issues, the training of the employees and the lack of interoperability/standards also seem to be relevant challenges.

According to the RegTech providers, the main general obstacles and challenges of their RegTech services are the **cost of user acquisition, the lack of regulatory standards and the changes in national and international regulation**. The data privacy and protection issues, the integration with legacy systems and the lack of technological capabilities of the clients are also mentioned as a relevant operational challenge for RegTech providers. According to the RegTech providers, it would be beneficial to ease integration with FIs' legacy systems.

Figure 27.: Challenges faced by FIs (left-hand side) and RegTech providers (right-hand side)



In line with the above-mentioned challenges, the most relevant regulatory obstacles for the RegTech providers are the requirements for processing personal data. The FIs refer to outsourcing and RegTech solution-related requirements as regulatory obstacles as well.

Risks associated with use of ICT security RegTech solutions

The ICT/cyber risk in general is identified by most of the FIs as the most relevant risk, but the legal/conduct risk and reputational risks are also flagged by several FIs as somewhat relevant. Only a minority of FIs find the step-in risk, money laundering/terrorist financing risk, concentration risk and sub-outsourcing risks as relevant for their ICT-related RegTech service. At this time, it was not possible to investigate in detail the exact ICT-related risks identified as the biggest concern for the FIs, but it is clearly seen that ICT risks are among the most important ones.

To mitigate the ICT/cyber risk, some FIs use monitoring solutions, human intervention or they rely on backup processes. In situations where FIs use RegTech services delivered by RegTech providers, FIs create exit strategies (with data migration) to be executed in case of termination of the contract agreement with a RegTech provider, in line with the respective EU outsourcing framework.

4.4.5 Case study

ICT case study

A RegTech provider focuses on the vision to build technology that is easy to use and simplifies ICT risk management for all organisations. It provides an ICT-related RegTech service that helps customers to check their maturity level and compliance with specific regulatory requirements and standards (for example EBA GL on ICT and security risk management).

This RegTech solution is an SaaS solution built on the cloud infrastructure. This model makes the implementation of the solution for the clients simpler, as there is no need to develop or install anything in their systems, and there is no need to get access to client ICT systems.

The ICT-related RegTech solution is a platform with a number of tailored control sets to assist the implementation of an information security management system and assess the current maturity of the security management function. It also provides a quick way to obtain transparency of another organisation's IT security management capability.

The solution is automated from a certain point of view, as the regulatory requirements are translated into control sets, so the customer can create the assessment easily by answering the connecting questions, according to any chosen requested control set. Currently, the regulations are translated into control sets and questions by a dedicated team, but in the future, the company is planning to support this task with AI solutions.

The platform provides more reliable and meaningful information as well as a holistic overview, hinting at specific areas for further evidence-based inspection, where needed. This enables experts to focus their attention on the key issues.

From the customer's point of view, this service simplifies, digitalises, automates and reduces the necessary effort for the compliance assessment, and it creates useful and meaningful charts to support the management in launching smart workflows and making informed decisions.

4.5 Creditworthiness assessment

Robust and accurate creditworthiness assessment (CWA) when originating loans is crucial to credit risk management and to prevent over-indebtedness of consumers. It also contributes to preserving financial stability while ensuring solid protection of the interest of borrowers. The obligation to assess the creditworthiness of individuals is one of the regulatory tools usually considered a duty of 'responsible lending' and is included in the Consumer Credit Directive (CCD)[32] and the Mortgage Credit Directive (MCD)[33] and is further specified in the EBA Guidelines on loan origination and monitoring[34].

4.5.1 General overview

CWA is a main element of the EBA's comprehensive Guidelines on loan origination and monitoring, which bring together prudential, governance, AML/CFT and consumer protection requirements. The objective of these EBA Guidelines, which were developed and consulted on in 2019/20 and have applied since June 2021, is to ensure that the CWA of the borrower is robust, accurate and relies on adequate information, while ensuring that the institutions' practices are compliant with consumer protection requirements. In this context, the EBA Guidelines further set out principle-based criteria for the use of technology-enabled innovation for credit-granting purposes and the use of automated statistical models for collateral valuation.

The EBA Guidelines cover not only criteria for banks and non-bank creditors to follow in loan origination and monitoring, but also pay specific attention to the use of automated models for credit decision-making and credit-granting. There are a number of points in the EBA Guidelines which are closely related to the content of this report. These are, for example, Section 4 of the Guidelines on internal governance for credit granting and monitoring, Section 5 on 'Loan origination procedure' and Section 8 on 'Monitoring framework'. In particular, the EBA Guidelines set out supervisory expectations for the design and use of models varying from conventional scoring models to more advanced models based, for example, on artificial intelligence or other emerging technologies[35].

It should be acknowledged that prudential risk management (IRB/STA) is excluded from the scope of this report which focuses on CWA at the point of loan origination only.

[32] Article 8 of Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC, OJ L 133, 22.5.2008

[33] Article 18 and 20 of Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 Text with EEA relevance, OJ L 60, 28.2.2014, p. 34–85

[34] EBA Guidelines on loan origination and monitoring 1 EBA/GL/2020/06 published on 29 May 2020

[35] See EBA loan origination and monitoring guidelines: Guideline 4.3 Credit risk policies and procedures in particular 4.3.3 Technology-enabled innovation for credit and granting and 4.3.4 Models for creditworthiness assessment and credit decision-making, as well as Guideline 4.4 Credit decision-making

4.5.2 Activities of FIs and RegTech providers

The majority of FIs reported having only limited activities regarding CWA RegTech solutions based on new technologies. According to FIs, CWA is mainly part of the traditional 'risk assessment system'. FIs have been using traditional data analytics solutions for many years to evaluate credit risks, relying mostly on automated credit-scoring mechanisms to determine whether and on what conditions a person or SME can be granted credit.

According to FIs, the growing importance of new technologies such as big data, cloud computing, ML and increased computational power have prompted the emergence of alternative credit-scoring models to assess creditworthiness, and CWA RegTech solutions might be more used in the future. Some FIs are currently testing solutions, for instance, based on the use of AI, including ML and NLP, as well as image recognition and RPA, to assess customer data and behaviour, analyse financial reports, mitigate human error and facilitate predictive analytics (e.g. to collect data or to mitigate fraud). The solutions presently tested concern mainly lending to micro, and small and medium-size enterprises (SMEs), lending to consumers to acquire residential immovable property, unsecured lending to consumer and credit cards.

FIs' development of CWA RegTech solutions remains still at an early stage and most FIs consider developing CWA solutions in-house, without necessarily involving external partners. According to most surveyed FIs, introducing scoring models based on new technologies would imply developing a new core banking system with a redesign of the CWA process and would require a higher number of persons involved. This system should be able to integrate all customer information to provide a more comprehensive picture, make a customer risk analysis and assign to the analysis a respective credit score.

RegTech providers on their side seem to be willing to seize the opportunities of Open Banking in an effort to extend the range of their products and services and leverage their existing customer base to create or enlarge their digital ecosystems, including on credit products. The RegTech providers are also partnering with universities to gather external data. When compared to the other RegTech segments, CWA has a lower number of RegTech providers located inside the EEA. The development of CWA RegTech solutions appears to be a growing trend, mostly stimulated by the business opportunities offered by Open Banking, even if, currently, only a limited number of RegTech providers appear to have developed CWA solutions at EU level over the last five years.

FIs and RegTech providers reported using a wide range of data sources on CWA RegTech solutions. The basic categories of data for CWA are identity/demographic data and credit data. In the context of the growing importance of new technologies, credit-scoring models to assess CWA might rely on a variety of data sources: i) financial data requested from the borrower, banks' data accessed via APIs or from public resources; ii) behavioural data which includes financial and non-financial data to help understand consumers' habits and which could be, for example, obtained from credit reporting companies; iii) alternative data, for example social media, data geo-location data, web data which could include also non-behavioural data. According to FIs and RegTech providers, accessing alternative data would be an effective way to expand the range of data

available internally or distributed by credit registries. All respondents clarified that, at this stage, they do not use or do not intend to use social media data mainly due to reputational risks and the lack of acceptance by customers. Some mentioned however that they might explore the possibility to use it in the future as long as the model complies with the regulatory framework. Others explained that the use of social media data is not allowed in certain countries.

Based on the feedback collected by FIs and RegTech providers, exploring how new financial technologies could be used to develop an alternative credit-scoring framework for FIs appears of paramount importance for lending money without being exposed to excessive risk, keeping in mind both prudential and consumer protection objectives.

4.5.3 Use of technology-based innovations

FIs and RegTech providers reported using technological innovation to add features to FIs' main systems and, in the vast majority of cases, those features are related to data collection and data analytics. According to FIs and RegTech providers, different technologies are used, but **the most used to support CWA are AI, including ML and NLP, APIs and cloud computing**.

The use of AI is seen to enable more accurate scoring and to allow for improved access to credit by reducing the risks and the number of false negatives. According to the respondents, this can help to determine the most suitable debt plan for the customers. It can also support FIs to ensure they properly manage credit risk, which is essential for financial stability.

Surveyed FIs explained that ML methods are already being planned to be used in both customer-facing and back-office operations, in particular for credit scoring, monitoring customer behaviour for customer segmentation, identification and automated remittance of specific payments or documentation analysis.

In addition, some FIs and RegTech providers indicated using NLP. This technology can analyse both text and audible speech and is commonly used in applications such as chatbots and tools that automate the process of gathering customer information from a different source (see case study 2).

The majority of RegTech providers reported positive outcomes from the use of APIs, mentioning that through APIs, they can improve their product development process, including the speed of launching new products and services into the market. RegTech providers have however indicated a certain reluctance from FIs to share data.

Most of the RegTech and FIs respondents reported that they use cloud computing in particular to support innovative scoring models (e.g. to provide the storage and computing power needed for resources such as a repository of data stored in its natural/raw format and real-time analytics). The large majority of RegTech providers indicated that they operate entirely in the cloud with no in-house servers, while FIs are seen to use cloud services for ICT infrastructure, data storage, hosting systems and processes, and communication services.

4.5.4 Benefits and challenges associated with use of CWA RegTech solutions

Benefits associated with use of CWA RegTech solutions

FIs stated that technology, in particular data-driven intelligence, is intended to contri**bute to greater accuracy and speed of CWA, better performance, increased efficiency with fewer human errors** (which could be linked to manual validations) and **shorter time to market**.

Both FIs' and RegTech providers' respondents reported that CWA RegTech solutions would enhance access to credit, thus, according to them, reduce the risks of false negatives and help improve predictive analysis by FIs' staff. Nevertheless, at the same time, biased data may feed into the scoring model. When setting up a CWA RegTech solution, FIs and RegTech providers should, however, pay particular attention to avoid biased assessments by FIs' staff.

Some FIs also reported that CWA RegTech solutions would reduce operational costs (fewer staff), reduce financial losses, enhance risk management and monitoring and attract/retain customers by providing a better customer experience to consumers who could potentially obtain a loan faster. As reported by FIs, the use of technology might also play an important role to mitigate the risk of fraud by increasing the reliability of the documents to reduce the stress of staff and to facilitate predictive analytics.

Challenges associated with use of CWA RegTech solutions

Several challenges have been identified by FIs and RegTech providers to the deployment of CWA RegTech solutions. It should be noted that the list of risks and challenges identified by FIs and RegTech providers does not include any risks and challenges that might arise for consumers, such as financial exclusion.

The risks and challenges, which are listed below, have been identified mainly by FIs and tend to be the same for all of them:

- **data protection and privacy issues** – complying with data protection requirements is a priority for FIs, as any issues could lead to important reputational risks for FIs (e.g. data breaches, lack of consumer consent). Some FIs explained that certain data protection and privacy requirements limiting the use of data mining techniques for commercial purposes may restrict the development and the use of CWA RegTech solutions.

- **security issues** – cybersecurity threats also represent important challenges for the FIs. The collection of data and the use of (cloud-based) analytical systems require robust safety measures against hacking and unauthorised access to such data (cybersecurity).

- **regulatory/supervisory requirements** – one major issue that FIs reported is the lack of written standards or guidance by regulators and supervisors regarding the use of new technologies (e.g.

clearly identifying what FIs are able to do or not and if supervisory authorities would allow the use of alternative data sources). According to FIs, the validation of CWA systems (risk system) by supervisors takes also a lot of time and has an impact on the time to market.

- **lack of harmonised regulatory framework across the EU** – **FIs** and RegTech providers reported that it is difficult to develop a solution that can be applied consistently across the different countries. According to FIs, this situation brings more costs and time expenditure to CWA RegTech solutions projects.

- **integration with legacy systems and lack of full technological capability** – the majority of RegTech solutions require FIs to aggregate data from different source systems into the relevant datasets, e.g. in the public cloud. Given the complex internal systems of FIs, FIs explained that it is still difficult to integrate new technology in the existing systems without any core changes to the banking process (e.g. transforming their overall processes and modernising their legacy systems), in particular regarding credit risk modelling.

- **data availability** – RegTech providers consider the lack of access to data as an important challenge to the development of their activity. They stressed however that the implementation of PSD 2 and the increasing use of Open Banking solutions relying on APIs will facilitate access to FIs' data.

It should be recalled that the EBA Guidelines on loan origination and monitoring intend to be future proof and technology neutral. The EBA Guidelines therefore set out criteria on the input data for CWA that are applicable for all approaches, also covering methodologies based on automated models. They stress[36] that the data to be used for the borrower's CWA should be financial data (e.g. income and regular expenses of the borrower, value of the collateral) and any other relevant information that may directly be related to the assessment of the repayment capacity of the borrower (e.g. household composition in the case of consumer lending).

The EBA Guidelines further clarify the internal governance and control framework for credit decision-making and credit-granting processes, and account for the growing importance of automated models and technology-based innovation. In the near future, the EBA intends to issue a discussion paper on the use of ML in credit risk modelling for regulatory capital and to build up a common understanding of the technical aspects of ML and related regulatory requirements.

Furthermore, the fact that the European Commission's recent proposal for a regulation *laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts* identified the use of AI for creditworthiness as high-risk should be also taken into account.

[36] See Guideline 5 on loan origination procedures

4.5.5 Case studies

Increasing consumer satisfaction through automation of lending/faster CWA process

Targeted problem/objective(s):

- Comply with MCD and CCD requirements and the EBA GL on loan origination and monitoring, while at the same time ensuring a successful customer experience.
- Automate the process of CWA for faster loan approval.
- Reduce complexity and time.
- Secure competitive advantage due to advanced offering.
- Ensure reliability of the solutions to ensure that potential human errors are avoided.

Proposed solution(s):

Case study 1

Financial institution A developed a fully digital lending solution with the possibility for a consumer to be granted a loan in only few minutes from his/her mobile phone as soon as he/she complies with all the necessary due diligence and KYC requirements. This new digital lending solution allows the FI to move from a traditional lending process which was mixing semi-automated processes (internal and external data collection and controls) and manual processes (examination of the application, decision-making process, offer, signing, disbursement and archiving) to a fully automated process. The consumers can submit their application for a loan in only five minutes. Due to the use of automated solutions, the assessment of the consumer's CWA is reduced as well as the time to provide the answer to the consumer, as the credit decision takes only few minutes.

When applying for a loan, the customer is categorised in three categories:

- green (loan can be granted if all criteria are met – machine decides based on criteria defined by the bank);
- yellow (uncertainty – machine is unable to make a decision based on the criteria set by the bank) – loan officer needs to assess to take the final decision;
- red (denial without intervention of a loan officer – consumer did not meet the criteria at all).

Consumer's information is checked in a public register so the consumer does not have to provide much information. Information is also checked based on a scoring system, consumer internal payment behaviour data (e.g. payment behaviour such as reminders, forbearance) and external data and payment behaviour data (e.g. official income) as well as calculation of consumer repayment ability which rely on both internal and external data. The process, however, does not allow any differentiation between profiles. The processing time is shortened from 24 hours to 10 minutes.

Technologies involved/used include a combination of robotics, biometrics (via cell phones) and advanced statistical models. The FI intended to use ML and Deep Learning, but it was too early because it is still seen as a black box by certain supervisors/consumers - opaque systems for which the internal behaviour cannot be easily understood, and for which therefore it is not easy to understand (and verify) how a model has reached a certain conclusion or prediction.

Some challenges remain however - real time process remains a challenge to ensure information is up-to-date and to ensure fraud prevention is preserved, in particular in a context where criminals are adapting rapidly to digital environment. Different core IT systems/legacy system used across subsidiaries remain also a challenge for group level roll-out.

Case study 2

RegTech A is using an SaaS decision-assisting tool, known as Credit Decisioning, which operates at the intersection of Open Banking and credit analysis. This solution has been developed on top of PSD2 via APIs (open-banking) and encompasses three pillars:

1. credit insights: screening of a client's income, relevant expenses and credit events through Open Banking data to help lenders assess budget metrics and draw an enriched risk profile. It produces a precise transaction categorisation, as well as risk indicators dedicated to credit analysis, including detection of regular bank charges and income and of relevant credit events (default, recent financing, notice to third-party holder, gambling, etc.).
2. dashboards - single view of the applicants (e.g. revenues, incomes, outcomes, loans, etc.): it provides an instant overview and detailed analysis of the financial situation, for all credit operators, e.g. for issues related to granting new loans, refinancing, or for debt collection. Data is categorised and classified in the dashboard and anonymised to be compliant with GDPR.
3. credit score - development of algorithms that allow for a better scoring based on the information they received: it converts three months of bank statements into a one-year default probability, which reflects the financial behaviour of the loan applicant and is exploitable by anyone who wishes to know his/her credit risk.

This solution leverages on Open Banking data to take adequate credit decisions and guarantee the smoothest and most transparent customer journey possible.
The application for the loan is done via a chatbot (company says hello to the consumer, asks for further information about the reasons of such application/purpose of the loan, the amount needed, consumers provide their consent to share the data or allow access to the bank account data to facilitate credit scoring). This RegTech provider works with other partners at different stages of the process (e.g. face recognition – KYC verifications, signature of the contract). The lender can decide to add cross-selling products (e.g. insurance) if it so wishes.
However, the ownership of the decision remains in the hands of the FIs, which can decide to grant or not to grant the loan to the consumer.

Collection of data is done in five minutes instead of one week and risk management has improved by 70%, the time-to-market is reduced and the solution facilitates the financial inclusion of millennials.

Some challenges remain however: lack of trust of FIs in Open Banking opportunities is an important challenge, as it leads to reluctance from FIs to give access to data. However, the implementation of PSD 2 and the increasing use of Open Banking solutions relying on APIs will facilitate the access to FIs' data.

5. Conclusions and way forward

5.1 Conclusions

This report provides an overview of the current RegTech landscape in the EU and it has been developed with the aim of increasing understanding and sharing knowledge of RegTech among the involved stakeholders, primarily competent authorities, FIs and RegTech providers.

The EU RegTech sector has undergone a vast transformation in recent years, and therefore benefits, challenges and associated risks need to be well understood to pave the way for the use of technology for compliance purposes in a technologically neutral way, without favouring any particular solutions, but also avoiding inadvertently hindering implementation and scaling up of innovation across the EU.

The RegTech report captures that 60% of surveyed RegTech providers are based in the EEA, providing a range of solutions, covering AML/CFT, fraud prevention, prudential reporting, ICT security, and creditworthiness assessment segments, among others. With access to both EEA and non-EEA providers that offer a broad range of RegTech solutions, FIs in the EU benefit from a wide supply of RegTech providers and their solutions.

The deployment rate of RegTech solution adoption across the EU is not homogenous, with noticeable differences in the use of RegTech solutions by FIs across the different Member States and among the various RegTech market segments. FIs are seen to have highest RegTech adoption rates in AML/CFT and fraud prevention, and lower in prudential reporting, creditworthiness assessment and ICT security.

AML/CFT is the primary RegTech segment where benefits are being realised. The use of innovative technologies has created a number of benefits for FIs, including enhancing their monitoring and sampling abilities, and reducing human errors. There may also be longer term benefits for the FIs, such as a reduction in the risk that the FIs' business may be exposed to money laundering or terrorist financing.

Besides the AML/CFT market segment, there are a number of RegTech solutions on fraud prevention, prudential reporting, ICT security and CWA which demonstrate the broad capabilities of such innovations. These currently lesser-used RegTech solutions have recently been on the rise.

In terms of the most prevalent innovative technologies used in RegTech solutions, these include Cloud Computing, Predictive Analytics, Machine Learning, Semantics/Graph Analysis, and Natural Language Processing.

The emergence of new technologies and potential of (near) real-time data collection can benefit FIs and in turn may, in the future, enable supervisors to proactively make data-based and evidence supported decisions.

The ongoing impact of COVID-19 which has, in many respects, sped up the process of digitalisation in the financial sector does not seem to have had any major effect on FIs' RegTech projects. However, COVID-19 was a real test for the RegTech providers – for some, especially smaller ones, it brought real operational challenges, while others stood to gain from the increase in the digitalisation trend. The current environment, with COVID-19-facilitated digitalisation trends and the shift to remote and online solutions, has been in particular favourable for certain RegTech market segments, in particular AML/CFT and on-boarding solutions, and ICT security. However, for some FIs, currently rather small budgets for RegTech solutions might be a challenge to leverage digitalisation going forward.

The report identified that the main benefits for FIs using RegTech solutions are **enhanced risk management**, **enhanced monitoring** and reduction of human error. In comparison, the major drivers from the RegTech providers' perspective for offering their services are the potential to bring **efficiency and effectiveness**, assist FIs in addressing **ongoing regulatory change** requirements, and the ability to organise complex information. FIs and RegTech providers appear to have a similar perspective on the RegTech benefits and, therefore, mutual interests in the adoption of RegTech solutions, but some existing differences in the indicated priority areas for RegTech adoption may hinder cooperation. As a result, closer industry coordination between FIs and RegTech providers could help to address this information asymmetry gap and foster collaboration.

As RegTech solutions have the potential to foster a more efficient and effective financial sector and be a factor in the successful implementation of the regulatory framework, a number of competent authorities have already taken steps on RegTech-related initiatives in order to address inadvertent barriers to the application of these technologies and to scale up innovation in this field. They include innovation facilitator initiatives (regulatory sandboxes and innovation hubs, brought together at the EU level by the European Forum for Innovation Facilitators), regular thematic discussions with the industry, and specific requirements and quality standards for RegTech providers, e.g. certification for the safety of their ICT systems.

As analysed in detail in Chapter 3, there are still a number of significant challenges faced by FIs and RegTech providers in adopting and developing RegTech solutions. These challenges can hinder the use and scale-up of innovation in RegTech. The main challenges indicated by FIs and RegTech providers are summarised below.

Main challenges for RegTech adoption **encountered by FIs**	Main challenges for RegTech adoption **encountered by RegTech providers**
1. Data-related challenges and cybersecurity threats	1. Lack of technological capabilities on FIs' side
2. Interoperability and integration with the existing legacy systems	2. Security, data privacy and protection issues
3. Changes to regulation	3. Changes of national and international regulation
4. Costs and procurement process	4. Cost of user acquisition
5. Lack of necessary skills and training	5. Lack of FIs' understanding of RegTech solutions
5. Perceived immaturity of RegTech providers' solutions	6. Lack of harmonised legal and regulatory requirements
	7. Clarity of regulatory / supervisory guidance
	8. Competition with other solutions

*Note: Highlighted in orange – challenges considered to be **INTERNAL** to FIs and RegTech providers.*

RegTech market study results suggest that the **majority of challenges that hold back RegTech market development seem to be internal to FIs and RegTech providers.** The most prevailing challenges relate to data (data quality, security, and privacy, etc.), interoperability and integration with the existing legacy systems, a lack of FIs' API capabilities, costly and often lengthy and complex due diligence processes, and limited in-depth awareness of RegTech solutions. Lack of some FIs' technological capabilities, internal skills and trust in RegTech solutions may lead to situations where FIs do not trust and invest enough in innovative technologies for RegTech.

Indeed, with regard to the data and technology obstacles for wider market adoption, 91% of surveyed FIs perceive 'data and data quality issues' as primary obstacles, whilst 91% of the FIs and 74% of the RegTech providers perceive 'integration with legacy systems' as one of the major obstacles.

External factors to FIs and RegTech providers, **i.e. legal and regulatory framework or supervisory treatment-related challenges, may pose some challenges for the RegTech market development** and there is some room for improvement, **but regulation is not perceived as a major barrier to scaling up RegTech solutions in the Single Market**. Despite the EBA's key role in building up the Single Rulebook that aims to provide a single set of harmonised rules which institutions throughout the EU must respect, there are instances, e.g. in the case of minimum harmonisation where directives set minimum standards that have to be transposed into national laws, where a lack of harmonised regulatory standards and differences still exists across the EU Member States.

The complex and continuously evolving nature of national and international regulations, necessary to keep regulation relevant and able to address any emerging risks, may also be a barrier to RegTech adoption. Acquiring and implementing RegTech solutions in the existing infrastructure is typically costly, therefore FIs need to have certainty that investment will serve the purpose for the longer term. Existing RegTech tools are not currently able to substitute a manual horizontal legislation tracking process and a lot of expert-based work will continue to be required to properly scan the regulatory horizon. Investigated areas and potential for **machine-readable and machine-executable** regulation could be the way forward to facilitate regulatory compliance automation.

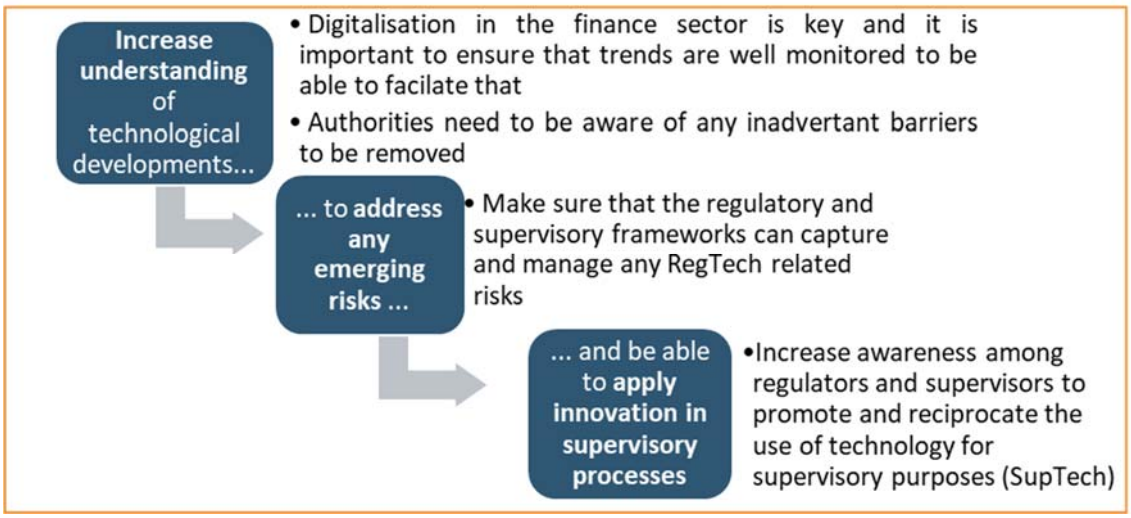
Finally, it seems that **in some cases, limited clarity and guidance from supervisors on the potential acceptance of certain innovative RegTech solutions and approaches** may hold back some FIs using RegTech solutions and limit the scale-up of opportunities for some RegTech providers. In view of some FIs and RegTech providers, regulatory and supervisory bodies have somewhat different perceptions regarding the use of RegTech solutions. RegTech providers, in particular, consider that regulatory and supervisory bodies may sometimes be too neutral and not provide necessary support. In practice, the majority of national competent authorities are open to innovations, but are by law neutral towards competition and, to maintain technological neutrality principle, cannot promote specific RegTech providers and their services.

In order for the EU financial sector to remain robust and effective in an increasingly digitalised world, efforts to overcome challenges mentioned above should be made. The next section explores possible ways for public authorities to take to overcome some of the listed challenges.

5.2 Way forward

There are a number of challenges that could be considered a hindrance to scaling innovation across the EU in the field of RegTech. In line with the European Commission's ongoing and foreseen initiatives, in particular on the Digital Finance Strategy, this section sets out the way forward to facilitate the uptake and scale-up of innovation for RegTech use in the financial sector in a technologically neutral way across the EU to address some of the identified challenges.

The graph below explains how a better understanding of technological developments can facilitate the scale-up of innovation.



As the majority of identified challenges that hold back the RegTech market development are linked to internal factors of FIs and RegTech providers, it would be primarily for these companies to take further actions to address the challenges, such as data quality, technological readiness, internal governance processes, ICT systems capabilities and FIs' skills and knowledge of RegTech solutions.

For regulators and supervisors, there are three main issues to be addressed to support scaling up RegTech innovation. Firstly, the lack of skills and understanding of RegTech solutions among regulators and supervisors needs to be addressed. Secondly, whilst the applicable law and regulatory framework has not been identified as the most material obstacle for RegTech adoption under this study, a lack of regulatory standards for technical requirements and data-related standards or a lack of harmonisation of regulatory requirements across the Member States could pose certain barriers for wider market adoption of RegTech solutions across the Single Market. Finally, limited clarity and guidance from supervisors on the potential acceptance of certain innovative RegTech solutions has been also identified as an issue.

Building and leveraging on the ongoing initiatives, **the EBA identified the following actions to be taken to support sound adoption and scale-up of RegTech solutions:**

Building knowledge and raising awareness about RegTech

Continue building knowledge and raising awareness about RegTech among the regulatory and supervisory community and build convergent supervisory practices, primarily through workshops, forums, and targeted events. There is a need to have an efficient knowledge exchange and to continue to improve the knowledge and skills of regulators and supervisors on RegTech.

The existing platforms for cooperation, e.g. the **EBA FinTech Knowledge Hub** and the **European Forum for Innovation Facilitators (EFIF)** (within the strategic priorities and taking established workplans into account), can be leveraged to bring together FIs, RegTech providers, academia and public authorities to discuss thematic RegTech implementation cases, recurrent obstacles and gaps impeding the scale-up of financial innovation that may warrant attention by the ESAs and/or European Commission, and recurrent risks with reference to the use of RegTech solutions.

As part of its mandate on convergence of supervisory practices, the EBA will monitor existing supervisory practices in the areas where innovative technologies are widely used and respond with the tools at its disposal to contribute to supervisory practices sharing and convergence in the approach to RegTech.

Supporting Single Market by contributing to the **harmonisation of legal and regulatory framework**

Continue the effort to identify where there is a need to harmonise the legal and regulatory framework across the EU on identified priority issues by issuing guidance on RegTech-related matters or flagging any issues for the attention of the European Commission. In practice this could involve the following steps:

(1) MONITOR: ongoing **monitoring** of the existing and emerging RegTech use cases and applicable laws and regulation via engagement with industry and competent authorities;

(2) ASSESS: **identification of differences** across the applicable laws and national or EU-level regulation and **evaluation if harmonisation may be needed** (e.g. as is currently done in the area of remote onboarding and digital IDs[37] and data standardisation[38]);

(3) ADAPT: **where relevant, propose measures to harmonise** relevant requirements to ensure level playing field.

[37] The EBA is currently working to respond to the EU Commission request[37] to develop Guidelines on Remote On-Boarding and Digital Identities, which are due to be published for consultation by Q3 2021

[38] The EBA implemented the DPM data dictionary, which integrates all the data definitions included in the reporting regulations (produced by the EBA) and the reporting requirements (defined by the SRB). The EBA is currently working on a Feasibility study on Integrated Reporting to analyse the possibility to integrate different types of data (supervisory, resolution, statistical data) for reporting purposes with a view to further enhance efficiency and reduce the reporting burden for FIs. One key aspect of this analysis is how RegTech could help to streamline the reporting process.

Leverage role and expertise of the European Forum for Innovation Facilitators (EFIF) and the national Regulatory Sandboxes and Innovation Hubs to facilitate innovation by fostering collaboration and dialogue between financial institutions, RegTech providers and competent authorities.

The EBA and the CAs have already taken initiatives to understand the latest technological developments and to create and foster an innovation-friendly environment, in particular via activities of sandboxes, innovation hubs and EFIF. Additionally, the EBA notes that in 2021, a framework to support cross-border sandbox testing will be published following work of the EFIF. This will support firms that seek to engage multiple competent authorities in the testing process (for instance through joint sandbox testing or through structured test observation and discussion of findings).

In general, further leveraging innovation facilitators should both help to improve understanding of RegTech and to identify supervisory and regulatory issues arising. This engagement will also provide supervisors with first-hand experience and knowledge that can be leveraged when supervising FIs' activities or developing own SupTech solutions.

Longer-term perspective

In the longer term, additional actions, such as the creation of a centralised EU database of **RegTech solutions** or a **potential certification of RegTech** (as suggested and preferred in particular by RegTech providers and some FIs) could be further explored and considered at the EU, together with an evaluation of who would be the best placed to implement such solutions. Having a RegTech database may serve as a tool to share information about available RegTech solutions (e.g. description, status of adoption by FIs, RegTech providers offering service, etc.).

In addition, building on accumulated experience, potential certification of RegTech to showcase compliance with the regulatory requirements within specific market segments could be assessed. An in-depth study would need to be conducted to identify: i) priority areas in which RegTech providers or solutions could be certified, ii) clear legal basis or reference standards that RegTech solutions could be assessed against, iii) potential stakeholders to be involved in the certification process, and to address any other operational aspects.

Currently neither of those two options are within the current mandate and focus of the EBA.

6. Annex

List of 'other' RegTech solutions observed beyond five areas of focus assessed in-depth in the EBA RegTech report:

- Management of New Regulations
- Horizon Screening
- Regulatory Change Screening / Management
- Automated derivation of requirements
- KYE (Know Your Employee)
- Screening of conversations, chats, voice platforms (risks, fraud, abuse, etc.)
- Regulatory Filing Support
- Transaction/Trade Data Screening
- Market Abuse Surveillance
- Due Diligence of Third Parties (e.g. vendors)
- Network Analysis (non-financial risks)
- Human Centric Personal Data Management (GDPR)
- Process Management (e.g. compliant document management)
- Policy Management
- Tax Report (Crypto Assets)
- SSI (Self Sovereign ID)
- PSD2/SCA solutions
- Electronic Signature
- Open RegTech Initiatives
- Open Banking Related Risks and Fraud
- Account Servicing Payment Service Provider (ASPSP)
- Policy Management
- Client Onboarding Services
- Consumer Complaints
- EU Taxonomy Regulation
- Management of Compliance Processes
- Regulatory Risk Management
- MiFID 2 / SFTR Reporting
- PSD2

EUROPEAN BANKING AUTHORITY

Tour Europlaza, 20 avenue André Prothin CS 30154
92927 Paris La Défense CEDEX, FRANCE

Tel. +33 1 86 52 70 00

E-mail: info@eba.europa.eu

https://eba.europa.eu