BRIEFING

Initial Appraisal of a European Commission Impact Assessment

European Parliament

Strengthening digital operational resilience in the financial sector

Impact assessment (SWD(2020) 198/SWD(2020) 203), SWD(2020) 199 (summary)/SWD(2020) 04 (summary)) accompanying a Commission proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (COM(2020) 595), and a Commission proposal for a directive of the European Parliament and of the Council amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU)2015/2366 and EU/2016/2341 (COM(2020) 596).

This briefing provides an initial analysis of the strengths and weaknesses of the European Commission's impact assessment (IA) (staff working documents SWD(2020) 198/SWD(2020) 203 refer to the same IA), accompanying Commission proposals to strengthen digital operational resilience in the European Union (EU) financial sector (COM(2020) 595 and COM(2020) 596), adopted on 24 September 2020 and referred to the European Parliament's Economic and Monetary Affairs Committee (ECON). The proposal for a regulation – included in the Commission's 2020 work programme – aims at setting up an EU-wide comprehensive framework on digital operational resilience for EU financial entities, which would improve the risk management dimension of the Single Rulebook. As the proposal for a regulation would have an impact on several directives, a proposal for a directive would amend or clarify several provisions in the existing EU legislation concerning financial services. This initiative is part of the digital finance package and in line with the Commission's priorities to make Europe 'fit for the digital age and to build a future-ready economy that works for people'.[1]

Problem definition

At first, the IA discusses the digitalisation of the financial sector – which has become the 'largest ICT sector of the economy' – and the ensuing risks and challenges (IA, p. 5). The IA notes that, while on the one hand, the financial sector – financial institutions, markets, infrastructures and IT systems is highly interconnected – on the other hand the level of information and communications technology (ICT) risk management is uneven. This can constitute a vulnerability in the system, as for example a local ICT incident can spread fast across markets and jurisdictions (IA, pp. 8, 12). The IA points out therefore that the ICT risks can constitute systemic risks, as they can trigger liquidity crisis, impact on the stability of the financial system, and cause a loss of trust in financial markets (IA, pp. 8-9). In the EU legislation on financial services, ICT risk management has mostly focused on a quantitative approach (e.g. a capital requirement to cover risks), rather than providing qualitative requirements in relation to 'protection, detection, containment, recovery and repair capabilities from operational incidents and failure' (IA, pp. 7, 10). The IA finds that digital operational resilience would complement ICT risk management in the financial sector, and defines it as 'the qualitative processes that a financial institution undergoes to build, maintain and review, on a continuous basis, the full operational integrity of its ICT systems, for a safe and compliant running of its operations and deployment of services' (IA, p. 7). The IA also refers to the technical advice of the European Supervisory Authorities (ESAs), which have stressed the need to strengthen the digital operational resilience of the financial services through an EU sector-specific initiative (IA, p. 5).[2]

Author: Mari Tuominen
Ex-Ante Impact Assessment Unit

PE 654.210 – December 2020

EN

The IA identifies **eight problems**: i) 'insufficient regulatory response to increased levels of ICT risks'; ii) 'incomplete view over the frequency and significance of incidents'; iii) 'complex, inconsistent and overlapping reporting obligations'; iv) 'insufficient information sharing and cooperation on threat intelligence' (between financial institutions); v) 'fragmentation due to multiple testing and no cross-border recognition of results'; vi) 'insufficient assessment of preventive and resilience capabilities'; vii) 'challenges for financial institutions to assure compliance with the regulatory framework'; and viii) 'unmonitored ICT third-party providers' (TPP) risks'. (IA, p. 22) The **problem drivers** are explained for each problem. The first problem, i) relates to the fragmentation in managing ICT risks, such as a lack of specific requirements on ICT risks and disparity of ICT risk requirements across financial sectors. Problems ii-iv) result from ineffective reporting of and limited awareness about threats and incidents, in particular a lack of, or multiple, incident reporting requirements for some financial institutions, insufficient trust in sharing threat intelligence and uncertainty over legal compliance when sharing. Limited and uncoordinated testing, namely a lack of and overlapping testing for some financial institutions, leads to problems v-vi). The drivers for problems vii-viii) concern risks linked to ICT third-party providers (e.g. data providers, cloud service providers), on which the financial sector increasingly relies, mentioning contractual limitations or gaps in written agreements with ICT third-party providers for example (e.g. outsourcing, sub-outsourcing), and a lack of coherent oversight for ICT TPPs (IA, pp. 8, 10-22).

The IA finds that the defined problems cause risks to financial sector stability and integrity; excessive administrative burden due to multiple reporting and testing; and limited supervisory effectiveness, which reduces public authorities' capability to assess and monitor risks and to impose necessary preventive measures against ICT risks. The IA does not provide quantified estimates of the administrative burden and compliance costs concerning multiple reporting and testing in the problem definition section, but illustrates the scale by giving estimates in the banking sector on potential savings in these fields when discussing the benefits of the preferred option (IA, pp. 14, 17, 42-43). As an indirect consequence, the IA mentions insufficient and unequal protection of consumers and investors, which is not discussed. The IA also raises the aspect of competitiveness (level playing field), due to the different requirements of market participants, but does not illustrate this in a more detailed way (IA, pp. 11-22, 27). The IA discusses the scale of the risks of cyber-attacks in financial services and the costs of operational incidents, and provides further discussion on various risk scenarios in a separate Annex (IA, pp. 95-98). On the basis of the International Monetary Fund (IMF) modelling in 2018, the 'base-case average aggregated annual loss due to cyber-attacks' was estimated at around US$100 billion to financial institutions. The IA also notes that between 2013 and 2018, the annual costs to financial institutions of cyber-attacks increased by 72 %. (IA, p. 8). In relation to the risks of the ICT TPPs, the IA mentions that around 60 % of 'surveyed companies experienced a data breach caused by a third party' (IA, p. 18). The IA notes the difficulties of estimating the costs of cyber incidents, as such incidents are not always reported and it is often not known if they concern direct or indirect losses (IA, p. 40).

In the baseline, without any change to the EU legislative framework, the IA expects requirements on ICT risk management to remain fragmented. The financial institutions would remain subject to multiple reporting obligations and information sharing would remain limited. Member States would continue to develop their national testing frameworks, which would create a multiplication of testing requirements in a cross-border context, due to lack of mutual acceptance of testing results. The IA also discusses how such problems might evolve, and concludes that improvements are not expected through individual legislation reviews or without action taken at the EU level. The IA refers to the forthcoming revision of the Security of Network and Information Systems Directive (NIS Directive), which may expand the ICT risk requirements, but would not solve the fragmentation, as the requirements have been established by sectoral legislation. Furthermore, the Commission seeks to standardise contractual clauses for financial institutions outsourcing to cloud resources – and the NIS Directive covers ex-post supervision of security requirements and incident reporting of cloud service providers – but as these concern only cloud service providers, it would not solve the supervision of and outsourcing to all critical ICT TPPs (IA, pp. 29-31).

Subsidiarity/proportionality

The proposal for a regulation is based on Article 114 and the proposal for a directive on Articles 53(1) and 114 of the Treaty on the Functioning of the European Union (TFEU). Due to interdependencies and the cross-border dimension of the financial sector, the uncoordinated national level measures or initiatives by individual financial institutions would not be adequate to manage the ICT risks. According to the IA, EU action would enhance coherent ICT risk management, mutual recognition of testing in a cross-border context, and an oversight framework, and would also reduce the burden and costs of incident reporting. Proportionality has been discussed in the context of options, but has not been a key criterion to consider in the comparison of the options, which would be required in the Better Regulation Toolbox (Tool#5) (IA, pp. 23-25). The deadline for national parliaments' subsidiarity check is not yet set. At the time of writing, no reasoned opinions had been submitted.

Objectives of the initiative

The overall objective is to 'strengthen the digital operational resilience of the EU financial sector entities by streamlining and upgrading existing rules and bringing in new requirements where there are gaps' (IA, p. 25). The IA notes that this would also 'contribute to the overall resiliency of the EU economy', 'enhance the Single Rulebook on its digital dimension' and 'maximise the benefits associated with the horizontal framework' (IA, p. 25). The IA identifies **three general objectives**: i) 'to reduce the risk of financial disruption and instability'; ii) 'to reduce the administrative burden and increase supervisory effectiveness'; and iii) 'to increase consumer and investor protection' (IA, p. 26). **Under the first objective, six specific objectives** have been defined: i) 'to address ICT and security risks more comprehensively and strengthen the overall level of digital resilience of the financial sector'; ii) 'to enable financial supervisors' access to information on ICT-related incidents'; iii) 'to ensure that financial institutions assess the effectiveness of their preventive and resilience capabilities and identify ICT vulnerabilities'; iv) 'to strengthen the outsourcing rules governing the indirect oversight of ICT TPPs'; v) 'to enable a direct oversight of the activities of ICT TPPs'; and vi) 'to incentivise the exchange of threat intelligence in the financial sector' (IA, pp. 26-27). **Two specific objectives are linked to the second general objective**: i) 'to streamline ICT-related incident reporting and address overlapping requirements' and ii) 'to reduce costs (and single market fragmentation) and enable cross-border acceptance of testing results' (IA, p. 27). It should be noted that **for the third general objective, no specific objectives** have been indicated, and there are no monitoring plans for it either. The IA only explains that the problems negatively affect consumer and investor protection, and that strengthening the digital operational resilience indirectly increases both consumer and investor protection. (IA, pp. 22, 26-27, 53-54) According to the Better Regulation Guidelines, the IA is due to present operational objectives, which are 'defined in terms of the deliverables of specific policy actions', after having selected the preferred option (Tool#16). However, it appears that no operational objectives have been defined, as in the monitoring and evaluation section the monitoring indicators are linked to the specific objectives (IA, pp. 53-54). According to the Better Regulation Toolbox (Tool#16), the objectives should be specific, measurable, achievable, relevant and time-bound (S.M.A.R.T.). The objectives are not time-bound, but other criteria appear to be met, except that the specific objectives are not defined for the third general objective, and the operational objectives are not presented.

Range of options considered

In view of addressing the defined problems and achieving the set objectives, the IA presents three policy options in addition to the baseline.

Baseline: No change in the EU financial services regulatory framework.

Option 1 ('Strengthening financial institutions' ability to absorb losses stemming from lack of digital operational resilience') would follow a quantitative approach by increasing the capital charges and loss absorption capacity for operational risks. The current operational risk framework would be amended by a specific loss event type on ICT risk, and a new capital buffer for ICT risk

would be created. Capital charges would incentivise financial institutions to reduce exposure to the risks. Digital operational resilience would be assessed through stress testing. The existing EU-wide stress tests would be used for banks, and a similar test would be developed by the ESAs for other financial institutions, and carried out with the national competent authorities. Option 1 would set a dedicated capital buffer for exposure to ICT TPPs, which would increase the loss absorption capacity from operational incidents. Option 1 would not improve and streamline the incident reporting, and would not change information sharing, remaining voluntary (IA, pp. 33-34).

Option 2 ('A digital operational resilience act for the financial sector') (preferred option) would provide a comprehensive framework addressing the digital operational resilience needs of all regulated financial institutions. An ICT risk management framework would be in line with the joint ESAs' technical advice, and would be based on the core requirements of which the IA provides explanation in a dedicated annex (IA, pp. 86-88). The proportionality principle would be applied across subsectors and within each subsector, and aspects such as systematic relevance of financial institutions, size and specific needs for various categories and business models, would be taken into account. The reporting of ICT related incidents to the competent authorities would be extended to cover the subsectors which currently do not apply such reporting rules. Incident reporting would be streamlined to ensure a single reporting scheme, preventing divergences and multiple reporting. This option would also comprise a complementary voluntary scheme on ex-ante information sharing on threats (awareness). Comprehensive EU rules would apply for digital operational resilience testing, and testing results would be mutually recognised by national authorities. Testing of preventive and responsive capabilities of financial institutions would be required, and would be more demanding for significant financial institutions. As regards the ICT third party risk, this option provides outsourcing rules to ICT TPPs and oversight tools for supervisors, for example enhanced inspection right, pooled audits (IA, pp. 38-40).

Option 3 ('A financial services digital operational resilience act together with centralised supervision of activities of critical ICT TPPs') would replace all existing relevant provisions on ICT risk management in all EU financial services legislation by a regulatory framework. This option would propose to dis-apply the NIS Directive in the financial sector (three financial subsectors are currently under its scope), to 'ensure full legal clarity'. Option 3 differs from Option 2 regarding testing requirements, as the ESAs would coordinate a European testing exercise, whereas Option 2 is based on mutual recognition of testing among national authorities. As regards information sharing, Option 3 introduces mandatory rules, contrary to the voluntary approach of Option 2. A new authority for cybersecurity in the financial services sector would be created to supervise activities of critical ICT TTPs providing services to financial institutions (IA, pp. 46-47).

The options appear to address the defined problems and objectives. Impacts on stakeholders are assessed in the options, but stakeholders' views are not clearly presented for each option. The range of options seems – in principle – to be sufficiently broad, as required by the Better Regulation Guidelines. However, it is not entirely clear why Option 1 was retained as a policy option, given that the aim of the initiative is rather to focus on strengthening the operational resilience (qualitative measures) – as it provides quantitative measures, which are costly and which are not sufficient to increase digital operational resilience. Moreover, its effectiveness would be very limited as it would help achieve (partially) only two of the eight specific objectives (IA, p. 37). It should also be pointed out that, referring to the economic situation and the Covid-19 context, the IA finds that Option 1 'is not considered feasible to implement', given that it would increase capital requirements for financial institutions (IA, p. 51). Likewise, the IA considers that Option 3 is not viable as it would entail substantial costs in setting up a new oversight authority. Besides the cost implications, the IA also finds that the new supervisory authority 'would be questionable and legally challenging' and 'dis-applying the NIS Directive to the financial sector would create a gap in the national cyber security strategy of each Member State' (IA, p. 49).

Assessment of impacts

The IA assesses the costs and benefits of each option against the three general objectives, and presents the main advantages and disadvantages of the options. In **Option 1** the benefits are assessed only qualitatively. Regarding the costs for the financial institutions, the IA gives indications of the potential additional levels of capitalisation, based on past incidents. Other costs are expected for reporting, stress testing and adapting the IT systems, but these are not quantified. For supervisors, significant costs, in the range of 25-50 full-time employees (FTEs), are predicted in relation to stress testing (IA, pp. 35-36) **Option 2** is expected to reduce the risk to financial sector stability and to mitigate the negative impacts of ICT incidents, which are estimated in the EU financial sector to be in the range of US$2 billion to US$27 billion. The IA notes that a risk reduction of 10 % would bring benefits between US$200 million and US$2.7 billion. This option would reduce administrative burden for all financial institutions, in particular as a result of eliminating double incident reporting. The IA illustrates this by estimating potential savings in the banking sector at between €29 million and €68 million, calculated with reference to the IT budget of six top EU banks (IA, p. 42). Potential savings are also expected from mutual acceptance of testing results in cross-border activities (savings estimated at between €250 000 and €2 million per cross-border financial institution). Option 2 would entail administrative and compliance costs for financial institutions and supervisors, for example: the testing costs to 100 financial institutions not currently participating in threat-led penetration testing (TLPT) are estimated at between €25 million and €50 million; in incident reporting one-off costs for financial institutions at between €9 million and €18 million); and recurring costs for managing incidents and reporting at between €18 million and €36 million). The staffing costs for an ICT TPP (subject to direct oversight), would relate to 2-6 FTEs. For supervisors, the estimated increase would be 1-5 FTEs for the leading authority and participating authorities around 0.25 FTEs (IA, pp. 40-45, 89-94). In **Option 3**, given the partial similarities with Option 2, the benefits and costs would be similar to a certain extent, but there are also differences. In benefits, the IA estimates that, in relation to ICT and testing, 'administrative burden and uncertainty around incident notification would be reduced even more' than in Option 2, although the IA does not provide a quantified estimate. On the other hand, higher costs for financial institutions would result from the obligation to share threat intelligence (estimated in the range of €1 000 to €50 000, and 1-3 FTEs), and the costs entailing of a new supervisory authority would be estimated at €16.5 million (one-off costs) and around 66 FTEs for all three ESAs covered (IA, pp. 47-48).

The options are compared against the Better Regulation criteria of effectiveness, efficiency and coherence, but, however, not against proportionality. The preferred option is Option 2, as the IA finds it as effective but more efficient than Option 3, which would entail higher costs for setting up a new supervisory authority and mandatory participation in information sharing platforms. Furthermore, Option 3 is considered the least coherent option with the existing horizontal EU framework, due to the extraction from the NIS directive. One might have expected that other issues mentioned in relation to Option 3 would also have been discussed in this comparison, such as 'questionable and legally challenging' aspects of the new authority for example (IA, p. 49). The IA says that the stakeholders' support for Option 2 is higher than for other options, but it would have been useful to have more information, as this is not clearly explained (IA, pp. 50-51). The IA finds that Option 2 would provide the best balance across the above mentioned criteria, and it would offer an effective comprehensive framework in improving the digital operational resilience of the financial sector at reasonable costs, while ensuring 'full clarity and coherence with the Single Rulebook' (IA, p. 45). The IA openly notes that the preferred option may not entirely solve the problems (e.g. concentration of risks) arising from ICT TPPs, as four large players dominating the ICT TPP market are non-European. In addition, Option 2 would only include a complementary voluntary scheme for ex-ante information sharing of threats, and due to the link with the NIS Directive, some uncertainty in the interaction between the horizontal and sectoral framework might remain (IA, pp. 46-47).

The IA only addresses social and environmental impacts and impacts on small and medium-sized enterprises (SMEs) for the preferred Option 2. The IA considers that the main social impacts would

concern consumers and investors, but does not really discuss these impacts (e.g. data protection aspects, fundamental rights) and notes only that 'the whole eco-system will be perceived as safer and more resilient, especially by end-users, once the retained policy option will be applicable' (IA, p. 52). The consumer and investor aspect is actually embedded in the discussion of the consequences of the problems and of the third objective, although the discussion is limited. Regarding environmental impacts, the IA finds that Option 2 would favour using the latest, more sustainable smart technologies, ICT services and infrastructure, which are more environment-friendly and facilitate recycling and reduction of harmful emissions and consumption of electricity (IA, p. 53). However, as the references are largely missing, the IA does not detail on what information the assessment is based.

SMEs/Competitiveness

It is not apparent from the IA to what extent SMEs are affected by the problems defined. However, in the preferred option, the size of financial institutions has been taken into account, and, according to the IA, Option 2 would have positive impacts on SMEs in the financial sector, as the single set of rules would, for example, reduce administrative burden – of which no quantified estimate concerning SMEs is provided – and enhance their capacity to operate in a cross-border context. The IA also finds that the new regulatory framework, which would provide clarity on various rules, would be particularly beneficial for SMEs as they have fewer resources for hiring legal advice (IA, p. 52). As this assessment is not referenced, it is not clear on which data it is based. Regarding competitiveness, the problem definition mentions that, due to the fragmented ICT risk requirements, financial institutions are in a different situation in terms of level playing field, but this competitiveness aspect is not specifically further discussed when assessing the impacts (IA, pp. 11-12, 17, 27-53).

Simplification and other regulatory implications

The proposal for a regulation would establish an EU-wide framework on digital operational resilience for EU financial entities, it would therefore comprise the measures of the preferred option. As the regulation would affect several directives concerning financial services, the proposal for a directive would introduce cross-references to the provisions concerning operational risk or risk management requirements, to attain legal clarity. In addition, legal certainty for crypto-assets and a temporary exemption for multilateral facilities would be provided. The IA explains how this initiative relates to the existing EU legislation, in particular, the NIS Directive, as well as, for example, the MiFID Directive on markets in financial instruments, the EMIR Directive on market infrastructure, the PSD2 Directive on payment services, and the ECI Directive on critical infrastructure (IA, pp. 10-11, 14, 57-66). As regards data protection and fundamental rights, the explanatory memoranda of the legislative proposals state that the measures of the initiative respect the EU data protection rules, in particular the General Data Protection Regulation (GDPR, (EU) 2016/679). The IA explains that the GDPR notifications would be outside the scope of this initiative (IA, p. 24). According to the IA, the preferred option would streamline the ICT related incident reporting requirements, which would reduce administrative burden and associated costs. Furthermore, mutual recognition of testing results in the cross-border context would decrease costs for the companies operating across Member States (IA, pp. 40-46).

Monitoring and evaluation

The IA presents a monitoring and evaluation plan with defined monitoring indicators and sources of data (the ESAs, financial institutions and industry). Progress would be monitored in relation to the specific objectives, as no operational objectives are indicated. The monitoring and evaluation section is silent on the third general objective. The IA does not explain why it is not monitored (e.g. an indicator, a survey). The data would be collected annually and the ESAs are due to set targets in relation to the indicators for comparison purposes. The first review would be made three years after the entry into force of the legislation (IA, pp. 53-54).

Stakeholder consultation

As required in the Better Regulation Guidelines, the IA provides a separate annex to describe the stakeholder consultation concerning the 'digital operational resilience framework for financial services' initiative (IA, pp. 67-85). In the Inception Impact Assessment (on a regulation) two responses were received between 19 December 2019 and 16 January 2020. In the meeting of the expert group on banking, payments and insurance (EGBPI) on 18 May 2020, a majority of the Member States supported actions 'along four elements outlined by the Commission', which the IA did not specify further (IA, p. 67). A workshop (webinar) was organised on 19 May 2020, gathering around 240 participants, who supported a framework on the digital operational resilience for the financial sector 'with actions focused on the four areas outlined in the public consultation document' (IA, p. 67). An open public consultation conducted between 19 December 2019 and 19 March 2020, in line with the 12-week requirement in the Better Regulation Guidelines, received 101 responses, of which 10 were confidential and anonymised. The stated aim was to gather stakeholders' views especially in relation to ICT and security risks; the main features of a legal framework (e.g. incident reporting, testing, oversight); and the impacts of the 'potential policy options'. However, regarding the last aspect it is noteworthy that questions were asked about potential impacts of the possible EU initiative and not on specific policy options (IA, pp. 67-68). The IA does not provide a link to the consultation document. Although it appears from the consultation feedback that a large number of respondents had stressed the aspects which are also relevant to SMEs (proportionate rules, consideration of factors such as a size, systemic relevance), the extent to which the defined problems concern them is not made specifically clear in the IA. Finally, the references to stakeholders are at times quite vague, such as 'many', 'some' or 'fewer' respondents, which is not informative in terms of the representativeness of the views.

Supporting data and analytical methods used

The IA has been elaborated by the Commission services and no externally commissioned supporting study is mentioned. The analysis is based on various sources, such as two pieces of joint technical advice by the European supervisory authorities (ESAs), reports and industry research, and is supported by extensive stakeholder consultations (IA, p. 56). The data is recent and mostly referenced, although some useful links are missing, for example the public consultation document. The assessment is mostly qualitative, but also provides quantified estimates. The Commission openly notes some limitations to the data on incident reporting, as this data is only reported to supervisors in a limited number of subsectors, and disclosures on expenses to cyber security by financial institutions and ICT TPPs. According to the IA, the reasons for the latter is reluctance on the part of financial institutions and TPPs to share that kind of information (IA, pp. 56, 89-94).

Follow-up to the opinion of the Commission Regulatory Scrutiny Board

The Regulatory Scrutiny Board (RSB) adopted a positive opinion with reservations on a draft version of the IA report on 29 May 2020 (Two documents, referenced SEC(2020)307 and SEC(2020)309, refer to the same RSB opinion). The RSB found that the IA does not sufficiently focus on the political decisions to take; it does not provide enough information on proportionality; it does not adequately account for the 2019 joint advice from the European Supervisory Agencies. It also considered that the report should discuss the choice between revisions of sectoral legislations and a new cross-sectoral initiative; that the report does not demonstrate that the preferred option is the optimal option (should include stakeholders' views on the options); does not sufficiently explain how this initiative would work together with parallel EU legislation under revision, in particular the NIS and ECI Directives. The RSB also called for neutral presentation of options. The IA provides explanation as to how the RSB's comments have been addressed in the revised IA (pp. 55-56). It seems that the IA has taken these points into account only partially. Impacts of options on stakeholders are assessed, but stakeholders' views are not clearly presented for each option. The IA explains how the initiative relates to the existing NIS and ECI Directives, but could have given more information on

how the forthcoming revisions of these directives would relate to this initiative. In addition, a more balanced set of options would have benefited the IA.

Coherence between the Commission's legislative proposals and IA

The legislative proposals appear to follow the IA's preferred option except that, whereas in Option 2 the review would be made three years after the entry into force of the legislation, the review clause (Article 51) of the proposed regulation refers to five years.

The analysis is based on various sources and extensive stakeholder consultation. In addition to the qualitative assessment, the IA also provides quantitative estimates, openly recognising some data limitations. The IA would have benefited from a more balanced set of options, as it appears that among the three policy options, the IA considers two of them not viable. Furthermore, in the comparison of options, it should be noted that the options have not been considered against proportionality, and it would have been useful to further clarify the arguments supporting the choice between options 2 and 3. The assessment of social impacts is very limited and the competitiveness aspect raised could have been discussed at greater length. The extent to which SMEs are specifically affected by the defined problems is not apparent from the IA. However, the IA estimates that a single set of rules would have positive impacts on SMEs in the financial sector, such as a reduced administrative burden – of which no quantified estimate is provided – and improved capacity to operate in a cross-border context.

ENDNOTES

1 See also L. Zandersone, Crypto-assets and pilot regime for distributed ledger, Initial appraisal, EPRS, European Parliament, forthcoming; European Parliament resolution 2020/2034 (INL) on digital finance: emerging risks in crypto-assets – regulatory and supervisory challenges in the area of financial services, institutions and markets.

2 European Commission, FinTech action plan, COM(2018) 109; European Parliament resolution 2016/2243 (INI) on FinTech: the influence of technology in the future of the financial sector.

This briefing, prepared for the Economic and Monetary Affairs Committee (ECON), analyses whether the principal criteria laid down in the Commission's own Better Regulation Guidelines, as well as additional factors identified by the Parliament in its Impact Assessment Handbook, appear to be met by the IA. It does not attempt to deal with the substance of the proposal.

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)