COMMISSION
EUROPÉENNE

Bruxelles, le 24.9.2020
SWD(2020) 204 final

La présente version linguistique tient compte des corrections apportées à la version originale EN transmise à nouveau sous le numéro SWD(2020) 204 final/2 du 16.10.2020

DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION

RÉSUMÉ DU RAPPORT D'ANALYSE D'IMPACT

accompagnant le document:

Proposition de directive du Parlement européen et du Conseil

modifiant les directives 2006/43/CE, 2009/65/CE, 2009/138/UE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341

{COM(2020) 596 final} - {SEC(2020) 309 final} - {SWD(2020) 203 final}

Résumé de l'analyse d'impact

Analyse d'impact concernant la proposition de règlement sur la résilience opérationnelle numérique du secteur financier

A. Nécessité d'une action

Pourquoi? Quel est le problème abordé?

Le secteur financier fait appel dans une large mesure aux technologies de l'information et de la communication (TIC). La pandémie de COVID-19 actuelle contribuera probablement à accélérer ce phénomène, compte tenu des avantages d'un accès continu à distance aux services financiers. La dépendance à l'égard des technologies numériques suscite cependant des inquiétudes. Les entreprises doivent être capables de résister à d'éventuelles perturbations informatiques afin que les incidents et les menaces numériques soient traités et les services maintenus. Dans un secteur financier fortement interconnecté qui déploie des services transfrontières essentiels dont dépend l'économie réelle, les vulnérabilités qui découlent de la dépendance aux TIC, bien qu'elles concernent tous les secteurs économiques, sont particulièrement prononcées en raison 1) de l'utilisation intensive et étendue des TIC, et 2) de la possibilité que les effets d'un incident opérationnel dans une entreprise financière ou un sous-secteur financier se propagent rapidement à d'autres entreprises ou parties du secteur financier et, en fin de compte, au reste de l'économie.

Bien que le secteur financier soit très avancé dans son intégration des marchés et des réglementations et qu'il prospère grâce à un ensemble unique de règles harmonisées – le corpus réglementaire unique de l'Union –, la réponse apportée par l'Union européenne aux besoins accrus de résilience opérationnelle au niveau tant horizontal que sectoriel:

- soit a été fondée sur une harmonisation minimale, laissant ainsi le champ libre à l'interprétation nationale et à la fragmentation du marché unique,
- soit s'est révélée trop générale et d'une applicabilité limitée, traitant le risque opérationnel global dans une mesure variable, en réglementant partiellement certaines composantes de la *résilience* opérationnelle numérique (par exemple, la gestion des risques informatiques, la notification des incidents et le risque lié aux tiers prestataires de services informatiques) tout en laissant d'autres de côté (tests).

Jusqu'à présent, l'intervention de l'Union n'a pas abordé le risque opérationnel d'une manière qui corresponde aux besoins des entreprises financières de résister et de réagir aux vulnérabilités informatiques et de s'en rétablir, et elle ne fournit pas non plus aux autorités de surveillance financière les outils dont elles ont besoin pour s'acquitter de leur mandat consistant à maîtriser l'instabilité financière découlant de ces vulnérabilités informatiques.

Les lacunes et les incohérences actuelles ont favorisé la prolifération d'initiatives nationales (par exemple en matière de tests) et d'approches de surveillance (par exemple en ce qui concerne les relations de dépendance à l'égard de tiers prestataires de services informatiques) non coordonnées, ce qui se traduit soit par des chevauchements, des doubles emplois dans les exigences ainsi que des coûts administratifs et de mise en conformité élevés pour les entreprises financières transfrontières, soit par des risques informatiques qui ne sont ni détectés ni traités. Dans l'ensemble, la stabilité et l'intégrité du secteur financier ne sont pas garanties et le marché unique des services financiers demeure fragmenté, ce qui a pour conséquence d'affaiblir la protection des consommateurs et des investisseurs.

Quels objectifs cette initiative devrait-elle atteindre?

L'objectif global est de renforcer la résilience opérationnelle numérique du secteur financier de l'Union européenne en rationalisant et en améliorant la législation financière européenne en vigueur et en introduisant de nouvelles exigences sur les points où il existe des lacunes, dans le but:

- d'améliorer la gestion des risques informatiques par les entreprises financières;
- d'accroître les connaissances des autorités de surveillance en ce qui concerne les menaces et les incidents;
- de faire en sorte que les entreprises financières testent mieux leurs systèmes informatiques; et
- d'assurer une meilleure supervision des risques découlant des relations de dépendance des entreprises financières à l'égard de tiers prestataires de services informatiques.

Plus précisément, la proposition établirait des mécanismes de notification des incidents plus cohérents et plus homogènes, ce qui réduirait les charges administratives imposées aux établissements financiers et renforcerait l'efficacité de la surveillance.

Quelle est la valeur ajoutée d'une action à l'échelle de l'Union?

Le marché unique européen des services financiers est régi par un vaste ensemble de règles établies au niveau de l'Union qui permettent aux entreprises financières agréées dans un État membre de fournir des services

dans l'ensemble du marché unique grâce à un passeport européen. Par conséquent, l'adoption de règles au niveau national ne constituerait pas un moyen efficace de renforcer la résilience opérationnelle des entreprises financières qui font usage du passeport. En outre, le corpus réglementaire unique de l'Union comporte, en conséquence de la crise financière, des règles très détaillées et normatives qui traitent des risques plus «traditionnels» tels que les risques de crédit, de marché, de contrepartie et de liquidité. Les dispositions actuellement applicables en matière de risque opérationnel sont d'ordre général. Le renforcement de la résilience opérationnelle numérique exige d'ajuster les dispositions relatives aux risques opérationnels qui sont déjà définies au niveau de l'Union – et qui ne peuvent donc être mises à jour et complétées qu'à ce même niveau.

B. Les solutions

Quelles sont les options législatives et non législatives envisagées? Y a-t-il une option privilégiée? Pourquoi?

L'analyse d'impact a examiné trois options, en plus d'un scénario de base de statu quo en ce qui concerne la législation de l'Union européenne relative aux services financiers. Plus précisément:

- **«Ne rien changer»**: les règles relatives à la résilience opérationnelle continueraient à être fixées par l'ensemble des dispositions actuelles et divergentes de l'Union en matière de services financiers, en partie par la directive SRI, et par les régimes nationaux actuels ou futurs;
- **Option 1 – le renforcement des coussins de fonds propres**: des coussins de fonds propres supplémentaires seraient constitués afin d'accroître la capacité des entités financières à absorber les pertes qui pourraient survenir en raison d'un manque de résilience opérationnelle;
- **Option 2 – un acte législatif sur la résilience opérationnelle numérique des services financiers**: cette option favoriserait la mise en place, au niveau de l'Union, d'un cadre global comportant des règles sur la résilience opérationnelle numérique pour tous les établissements financiers réglementés, lequel:
  - aborderait les risques informatiques de manière plus globale,
  - permettrait aux autorités de surveillance financière d'avoir accès aux informations sur les incidents informatiques,
  - ferait en sorte que les entreprises financières évaluent l'efficacité de leurs mesures de prévention et de résilience et recensent les vulnérabilités liées aux TIC;
  - renforcerait les règles d'externalisation régissant la supervision indirecte des tiers prestataires de services informatiques;
  - permettrait de mener une supervision directe des activités des tiers prestataires de services informatiques lorsque ceux-ci fournissent leurs services à des entreprises financières et
  - contribuerait à encourager l'échange de renseignements sur les menaces dans le secteur financier.
- **Option 3 – un acte législatif sur la résilience combiné à une surveillance centralisée des tiers prestataires critiques de services informatiques**: outre un acte législatif sur la résilience opérationnelle (option 2), une nouvelle autorité serait créée pour surveiller les tiers prestataires de services informatiques critiques qui desservent des entreprises financières. Cette option permettrait également de délimiter plus clairement le secteur financier par rapport au champ d'application de la directive SRI.

L'option nº 2 est privilégiée. Par rapport aux autres options, c'est celle qui permet d'atteindre la plupart des objectifs de l'initiative, tout en tenant compte des critères d'efficience et de cohérence. Cette option bénéficie également du soutien le plus marqué de la part des parties prenantes.

Qui soutient quelle option?

La plupart des parties prenantes (privées, publiques) conviennent qu'une action au niveau de l'Union européenne est nécessaire pour mieux préserver la résilience opérationnelle des entreprises financières. Nombreuses sont celles qui estiment également qu'une action de l'Union est nécessaire pour alléger les charges réglementaires engendrées par l'existence de règles redondantes et incohérentes imposées aux entreprises financières, énoncées dans la directive SRI, dans la législation européenne relative aux services financiers et dans les régimes nationaux (par exemple en ce qui concerne les notifications d'incidents). En conséquence, peu de parties prenantes sont favorables à l'inaction. Rares sont les parties prenantes qui voient l'intérêt de garantir la résilience opérationnelle au moyen de coussins de fonds propres supplémentaires (option 1). Il s'agit néanmoins de l'approche traditionnelle du risque opérationnel, notamment dans le secteur bancaire, et, à ce titre, elle est envisagée par les organismes internationaux de normalisation, entre autres. Le type de mesures qualitatives énoncées dans l'option 2, qui permettrait de rationaliser et d'améliorer la législation financière de l'Union et d'introduire de nouvelles exigences en cas de lacunes tout en maintenant les liens avec la directive NIS horizontale, recueille un large soutien de la part des parties prenantes qui ont répondu à la

consultation publique. Si certaines parties prenantes (notamment publiques) voient l'intérêt de renforcer la surveillance des tiers prestataires de services informatiques, comme proposé dans l'option 3, la création d'une nouvelle autorité européenne à cette fin ne recueille qu'un soutien limité de la part des parties prenantes, tout comme la rupture plus marquée avec le cadre SRI.

C. Incidence des options privilégiées

Quels sont les avantages de l'option privilégiée (ou, à défaut, des options principales)?

L'option 2 permettrait de traiter les **risques informatiques** dans l'ensemble du secteur financier en renforçant les capacités des établissements financiers à résister aux incidents informatiques. Cela permettrait de réduire le risque qu'un cyberincident se propage rapidement sur les marchés financiers. Bien qu'il soit difficile d'estimer les coûts induits par les incidents opérationnels dans le secteur financier (tous les incidents ne sont pas notifiés; l'ampleur des coûts est incertaine), les évaluations sectorielles indiquent que les coûts pour le secteur financier de l'Union pourraient se situer entre 2 et 27 milliards d'EUR par an. L'option privilégiée permettrait d'atténuer ces coûts directs et toute incidence plus importante que les cyberincidents majeurs sont susceptibles d'avoir sur la stabilité financière. L'élimination des chevauchements dans les **exigences de notification** réduirait les charges administratives. Par exemple, pour certaines des banques les plus importantes, les économies associées pourraient atteindre entre 40 et 100 millions d'EUR par an. La notification directe permettrait également d'améliorer la connaissance qu'ont les autorités de surveillance des incidents informatiques. **L'harmonisation des pratiques de test** contribuerait à accroître la détection des vulnérabilités et des risques inconnus. Cela permettrait également de réduire les coûts, en particulier pour les entreprises transfrontières. Par exemple, pour les 44 plus grandes banques transfrontières, les bénéfices totaux escomptés d'une approche commune en matière de tests pourraient être compris entre 11 et 88 millions d'EUR. Si l'on introduit un ensemble cohérent de règles sur la gestion des risques liés aux **tiers prestataires de services informatiques**, les entreprises financières auraient davantage de contrôle sur la mesure dans laquelle les tiers prestataires se conforment au cadre réglementaire, ce qui pourrait apporter une certaine assurance aux autorités de surveillance. Des avantages prudentiels découleraient également de la supervision des tiers prestataires de services informatiques. Dans l'ensemble, l'option privilégiée est porteuse d'avantages sociétaux plus larges, qui découlent d'un environnement opérationnel plus résilient pour tous les acteurs des marchés financiers et d'une protection renforcée des consommateurs et des investisseurs.

Quels sont les coûts de l'option privilégiée (ou, à défaut, des options principales)?

L'option retenue entraînerait des coûts de nature tant ponctuelle que récurrente. En ce qui concerne les premiers, ils sont dus aux investissements à consentir dans les systèmes informatiques et sont difficiles à quantifier étant donné l'état variable des systèmes informatiques antérieurs des entreprises. En l'absence d'intervention réglementaire, certaines entreprises financières ont déjà réalisé des investissements importants dans les systèmes informatiques. Cela signifie que pour les grandes entreprises financières, la mise en œuvre des mesures de cette proposition sera probablement peu importante. Pour les petites entreprises, les coûts devraient également être moins élevés, car celles-ci seraient soumises à des mesures moins strictes du fait du risque plus faible qu'elles présentent. En ce qui concerne les tests, les autorités européennes de surveillance ont estimé que les coûts liés aux tests de pénétration fondés sur la menace représentent entre 0,1 % et 0,3 % du budget TIC total des entreprises concernées. Les coûts associés à la notification des incidents seraient considérablement réduits, car il n'y aurait pas de chevauchement avec les notifications au titre de la directive SRI. Les autorités de surveillance devront également engager certains coûts, en raison des tâches supplémentaires qu'elles assumeront. Par exemple, pour les autorités de surveillance participant à la supervision directe de tiers prestataires de services informatiques, l'augmentation estimée des ETP pourrait être de l'ordre de 1 à 5 ETP pour l'autorité principale, et d'environ 0,25 ETP pour les autorités participantes.

Quelle sera l'incidence sur les entreprises, les PME et les microentreprises?

L'option privilégiée couvrirait toutes les entreprises financières afin d'accroître la résilience opérationnelle du secteur dans son ensemble. Cette portée étendue est importante compte tenu de la nature interconnectée du secteur financier et de la nécessité connexe de garantir un niveau adéquat de résilience opérationnelle globale. Toutefois, lorsqu'il s'agira de définir les exigences de base dans les principaux domaines d'intervention, le principe de proportionnalité s'appliquerait à la fois à l'ensemble des sous-secteurs et au sein de chaque sous-secteur. Cette approche tiendrait compte, entre autres, des différences en matière de modèles d'entreprise, de taille, de profil de risque, d'importance systémique, etc. Par exemple, les mesures relatives à la notification des incidents et aux tests seraient moins strictes pour les petites entreprises financières.

Y aura-t-il une incidence notable sur les budgets nationaux et les administrations nationales?

Non. La supervision supplémentaire peut, comme démontré ci-dessus, nécessiter un niveau limité de

ressources supplémentaires en matière de surveillance, qui peuvent en tout ou en partie (en cas de redevances de surveillance) être prises en charge par les budgets publics.

Y aura-t-il d'autres incidences notables?

Les conséquences socio-économiques de la pandémie de COVID-19 mettent en évidence la nature critique des marchés financiers numériques et de leur résilience opérationnelle. L'option privilégiée constituerait une base solide pour exploiter la transformation numérique en veillant à ce que le marché unique des services financiers, y compris au sein de l'union bancaire et de l'union des marchés des capitaux, soit résilient sur le plan opérationnel, sur la base d'un ensemble commun de règles et d'exigences visant à garantir la sécurité, la performance, la stabilité et des conditions de concurrence équitables. Cela permettra également de renforcer la position de l'Europe en tant que chef de file mondial dans le domaine financier et numérique, un objectif fixé par la Commission dans sa communication «Façonner l'avenir numérique de l'Europe».

D. Suivi

Quand la législation sera-t-elle réexaminée?

Le premier réexamen aurait lieu trois ans après l'entrée en vigueur de l'instrument juridique. La Commission présenterait un rapport au Parlement européen et au Conseil sur son réexamen. Le réexamen pourrait être accompagné d'une consultation publique, d'études, de discussions d'experts, d'enquêtes, d'ateliers, le cas échéant.