COM(2020) 829 final

ASSEMBLÉE NATIONALE

QUINZIÈME LÉGISLATURE

SÉNAT

SESSION ORDINAIRE DE 2020-2021

Reçu à la Présidence de l'Assemblée nationale
le 9 février 2021

Enregistré à la Présidence du Sénat
le 9 février 2021

TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT.

Proposition de directive du Parlement européen et du Conseil sur la résilience des entités critiques

E 15496

Conseil de
l'Union européenne

Bruxelles, le 18 décembre 2020
(OR. en)

14262/20

Dossier interinstitutionnel:
2020/0365 (COD)

PROCIV 105	**ECOFIN 1182**
JAI 1132	**ENV 832**
COSI 258	**SAN 490**
ENFOPOL 354	**CHIMIE 69**
CT 121	**RECH 539**
COTER 120	**DENLEG 90**
ENER 512	**RELEX 1037**
TRANS 621	**HYBRID 49**
TELECOM 277	**CYBER 283**
ATO 91	**ESPACE 85**

NOTE DE TRANSMISSION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	16 décembre 2020
Destinataire:	Monsieur Jeppe TRANHOLM-MIKKELSEN, secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	COM(2020) 829 final
Objet:	Proposition de DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL sur la résilience des entités critiques

Les délégations trouveront ci-joint le document COM(2020) 829 final.

p.j.: COM(2020) 829 final

COMMISSION
EUROPÉENNE

Bruxelles, le 16.12.2020
COM(2020) 829 final

2020/0365 (COD)

Proposition de

DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL

sur la résilience des entités critiques

{SEC(2020) 433 final} - {SWD(2020) 358 final} - {SWD(2020) 359 final}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

Pour protéger efficacement les Européens, l'Union européenne doit continuer à réduire les vulnérabilités, notamment à l'égard des infrastructures critiques qui sont essentielles au fonctionnement de nos sociétés et de notre économie. Les moyens de subsistance des citoyens européens et le bon fonctionnement du marché intérieur dépendent de différentes infrastructures pour la fourniture fiable des services nécessaires au maintien d'activités sociétales et économiques critiques. Ces services, essentiels dans des circonstances normales, sont d'autant plus importants alors que l'Europe gère les effets de la pandémie de COVID-19 et aspire à s'en relever. Il s'ensuit que les entités fournissant des services essentiels doivent être résilientes, c'est-à-dire capables de résister aux incidents susceptibles d'entraîner des perturbations graves, potentiellement transsectorielles et transfrontières, de les absorber, de s'y adapter et de s'en remettre.

La présente proposition vise à améliorer la fourniture, dans le marché intérieur, de services essentiels au maintien de fonctions sociétales ou d'activités économiques vitales en renforçant la résilience des entités critiques qui fournissent de tels services. Elle reflète les récents appels du Conseil[1] et du Parlement européen[2], qui ont tous deux encouragé la Commission à revoir l'approche actuelle afin de mieux tenir compte des défis croissants auxquels sont confrontées les entités critiques et d'assurer un alignement plus étroit sur la directive sur les réseaux et les systèmes d'information (la «directive SRI»)[3]. La présente proposition est cohérente avec la proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (la «directive SRI 2»), qui remplacera la directive SRI, avec laquelle elle établit des synergies étroites, afin de tenir compte de l'interconnexion accrue entre le monde physique et le monde numérique, en mettant en place un cadre législatif prévoyant des mesures solides à la fois en faveur de la cyber-résilience et de la résilience physique, comme prévu dans la stratégie pour l'union de la sécurité[4].

En outre, la proposition reflète les approches nationales adoptées dans un nombre croissant d'États membres, qui tendent à mettre l'accent sur les interdépendances transsectorielles et transfrontières et sont de plus en plus guidées par la réflexion sur la résilience, dont la protection ne constitue que l'un des piliers, aux côtés de la prévention et de l'atténuation des risques, ainsi que de la continuité et de la reprise des activités. Étant donné que les infrastructures critiques risquent également d'être des cibles potentielles des terroristes, les mesures visant à garantir la résilience des entités critiques contenues dans la présente

---

1 Conclusions du Conseil du 10 décembre 2019 sur les efforts complémentaires pour renforcer la résilience et lutter contre les menaces hybrides (14972/19).

2 Rapport sur les observations et les recommandations de la commission spéciale sur le terrorisme du Parlement européen [2018/2044(INI)].

3 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

4 COM(2020) 605.

proposition contribuent à la réalisation des objectifs du programme de lutte antiterroriste pour l'UE adopté récemment[5].

L'Union européenne (UE) reconnaît depuis longtemps l'importance paneuropéenne des infrastructures critiques. Ainsi, l'UE a établi le programme européen de protection des infrastructures critiques (EPCIP) en 2006[6] et a adopté la directive sur les infrastructures critiques européennes (la «directive sur les ICE») en 2008[7]. La directive sur les ICE, qui ne s'applique qu'aux secteurs de l'énergie et des transports, prévoit une procédure de recensement et de désignation des ICE dont l'arrêt ou la destruction aurait un impact considérable sur deux États membres au moins. Elle définit également des exigences de protection spécifiques pour les opérateurs d'ICE et les autorités compétentes des États membres. À ce jour, 94 ICE ont été désignées, dont les deux tiers sont situées dans trois États membres d'Europe centrale et orientale. Toutefois, la portée de l'action de l'UE en matière de résilience des infrastructures critiques va au-delà de ces mesures et comprend des mesures sectorielles et transsectorielles portant, entre autres, sur la résilience au changement climatique, la protection civile, les investissements directs étrangers et la cybersécurité[8]. Parallèlement, les États membres ont adopté leurs propres mesures dans ce domaine, chacun à leur manière.

Il apparaît donc que le cadre actuel en matière de protection des infrastructures critiques n'est pas suffisant pour relever les défis auxquels sont actuellement confrontées les infrastructures critiques et les entités qui les exploitent. Compte tenu de l'interconnexion croissante entre les infrastructures, les réseaux et les opérateurs fournissant des services essentiels dans le marché intérieur, il est nécessaire de modifier fondamentalement l'approche actuelle et de passer de la protection de biens spécifiques au renforcement de la résilience des entités critiques qui les exploitent.

L'environnement opérationnel dans lequel s'inscrivent les entités critiques a considérablement évolué ces dernières années. Premièrement, le paysage des risques est plus complexe qu'en 2008 et inclut aujourd'hui des risques naturels[9] (souvent exacerbés par le changement climatique), des actions hybrides soutenues par l'État, le terrorisme, des menaces internes, des pandémies et des accidents (tels que les accidents industriels). Deuxièmement, les opérateurs sont confrontés à des difficultés lorsqu'ils doivent intégrer dans leurs activités de nouvelles technologies telles que la 5G et les véhicules autonomes, tout en tenant compte des vulnérabilités que ces technologies pourraient créer. Troisièmement, ces technologies et d'autres tendances accroissent l'interdépendance des opérateurs. Les conséquences sont

---

5 COM(2020) 795.

6 Communication de la Commission sur un programme européen de protection des infrastructures critiques [COM(2006) 786].

7 Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.

8 Communication de la Commission sur la stratégie de l'UE relative à l'adaptation au changement climatique [COM(2013) 216]; décision nº 1313/2013/UE du Parlement européen et du Conseil du 17 décembre 2013 relative au mécanisme de protection civile de l'Union; règlement (UE) 2019/452 du 19 mars 2019 établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union; directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

9 «Overview of Natural and Man-made Disaster Risks the European Union may face» (Inventaire des risques de catastrophes naturelles ou d'origine humaine auxquels l'Union européenne peut être exposée). [SWD(2020) 330].

évidentes: une perturbation affectant la fourniture d'un service par un opérateur d'un secteur est susceptible de produire des effets en cascade sur la fourniture de services dans d'autres secteurs, ainsi que, potentiellement, dans d'autres États membres ou dans l'ensemble de l'Union.

Comme l'a montré l'évaluation de la directive sur les ICE[10] réalisée en 2019, les mesures européennes et nationales existantes se heurtent à des limitations lorsqu'il s'agit d'aider les opérateurs à faire face aux défis opérationnels auxquels ils sont confrontés aujourd'hui et aux vulnérabilités liées à leur nature interdépendante.

Plusieurs raisons expliquent cette situation, comme indiqué dans l'analyse d'impact qui a étayé l'élaboration de cette proposition. Premièrement, les opérateurs ne connaissent pas pleinement ou ne comprennent pas parfaitement les implications du paysage dynamique des risques dans lequel ils évoluent. Deuxièmement, les efforts en matière de résilience varient considérablement d'un État membre à l'autre et d'un secteur à l'autre. Troisièmement, des types d'entités similaires sont considérés comme critiques par certains États membres mais pas par d'autres, ce qui signifie que des entités comparables bénéficient de degrés divers d'aide publique au renforcement des capacités (sous la forme, par exemple, d'orientations, de formations et d'organisation d'exercices) en fonction de l'endroit où elles exercent leurs activités dans l'Union, et sont soumises à des exigences différentes. Le fait que les exigences et le soutien public aux opérateurs varient d'un État membre à l'autre crée des obstacles pour les opérateurs dont les activités sont transfrontières, notamment pour les entités critiques actives dans des États membres appliquant des cadres plus stricts. Compte tenu du caractère de plus en plus interconnecté de la fourniture de services et des secteurs dans les États membres et dans l'UE, un niveau de résilience insuffisant de la part d'un opérateur constitue un risque grave pour des entités situées ailleurs dans le marché intérieur.

Outre le fait qu'elles compromettent le bon fonctionnement du marché intérieur, les perturbations, en particulier celles qui ont des implications transfrontières et potentiellement paneuropéennes, peuvent avoir de graves répercussions négatives pour les citoyens, les entreprises, les pouvoirs publics et l'environnement. En effet, au niveau individuel, des perturbations peuvent affecter la capacité des Européens à voyager librement, à travailler et à bénéficier de services publics essentiels tels que les soins de santé. Dans de nombreux cas, ces services, ainsi que d'autres services essentiels qui sous-tendent la vie quotidienne, sont fournis par des réseaux étroitement interconnectés d'entreprises européennes; une perturbation dans une entreprise dans un secteur peut entraîner des effets en cascade dans de nombreux autres secteurs économiques. Enfin, des perturbations, telles que des coupures d'électricité à grande échelle et de graves accidents de transport, peuvent nuire à la sécurité et à la sûreté publique, faisant ainsi naître l'incertitude et sapant la confiance dans les entités critiques, ainsi que dans les autorités chargées de les surveiller et d'assurer la sécurité et la protection de la population.

- **Cohérence avec les dispositions existantes dans le domaine d'action**

La présente proposition reflète les priorités exposées dans la stratégie de l'Union européenne pour l'union de la sécurité[11], qui préconise une nouvelle approche à l'égard de la résilience

[10] SWD(2019) 308.

[11] Communication de la Commission relative à la stratégie de l'UE pour l'union de la sécurité COM(2020) 605.

des infrastructures critiques qui reflète mieux le paysage actuel et anticipé des risques, les interdépendances de plus en plus étroites entre les différents secteurs, ainsi que les relations de plus en plus interdépendantes entre les infrastructures physiques et numériques.

La directive proposée remplace la directive sur les ICE et tient compte d'autres instruments existants et envisagés et les développe. La directive proposée constitue un changement considérable par rapport à la directive sur les ICE, qui ne s'applique qu'aux secteurs de l'énergie et des transports, se concentre uniquement sur les mesures de protection et prévoit une procédure de recensement et de désignation des ICE dans le cadre du dialogue transfrontière. Premièrement, la directive proposée aurait un champ d'application sectoriel beaucoup plus vaste, étant donné qu'elle couvrirait dix secteurs, à savoir l'énergie, les transports, le secteur bancaire, les infrastructures des marchés financiers, la santé, l'eau potable, les eaux usées, les infrastructures numériques, l'administration publique et l'espace. Deuxièmement, la directive prévoit une procédure qui permettra aux États membres de recenser les entités critiques en appliquant des critères communs sur la base d'une évaluation nationale des risques. Troisièmement, la proposition impose des obligations aux États membres et aux entités critiques qu'ils recensent, y compris celles qui revêtent une importance européenne particulière, c'est-à-dire les entités critiques qui fournissent des services essentiels à ou dans plus d'un tiers des États membres, qui feraient l'objet d'une surveillance spécifique.

Selon les besoins, la Commission apporterait aux autorités compétentes et aux entités critiques un soutien pour les aider à se conformer aux obligations qui leur incombent en vertu de la directive. En outre, le groupe sur la résilience des entités critiques, qui est un groupe d'experts de la Commission soumis au cadre horizontal applicable à ces groupes, conseillerait la Commission et encouragerait la coopération stratégique et l'échange d'informations. Enfin, étant donné que les interdépendances ne s'arrêtent pas aux frontières extérieures de l'UE, un dialogue avec les pays partenaires est également nécessaire. La directive proposée prévoit la possibilité d'une telle coopération, par exemple dans le domaine de l'évaluation des risques.

Cohérence avec les autres politiques de l'Union

La directive proposée présente des liens évidents et est cohérente avec d'autres initiatives sectorielles et transsectorielles de l'UE concernant, entre autres, la résilience au changement climatique, la protection civile, les investissements directs étrangers (IDE), la cybersécurité et l'acquis en matière de services financiers. En particulier, la proposition concorde étroitement et crée des synergies étroites avec la proposition de directive SRI 2, qui vise à renforcer la résilience des technologies de l'information et de la communication (TIC) à l'égard de tous les risques dans les «entités essentielles» et les «entités importantes» qui atteignent des seuils spécifiques dans un grand nombre de secteurs. La présente proposition de directive sur la résilience des entités critiques vise à faire en sorte que les autorités compétentes désignées en vertu de cette directive et celles désignées en vertu de la proposition de directive SRI 2 prennent des mesures complémentaires et échangent si nécessaire des informations concernant la cyber-résilience et la résilience en dehors du cyberespace, et que les entités particulièrement critiques des secteurs considérés comme «essentiels» par la directive SRI 2 proposée soient également soumises à des obligations plus générales visant à renforcer la résilience afin de faire face aux risques non liés au cyberespace. La sécurité physique des réseaux et des systèmes d'information des entités du secteur des infrastructures numériques est abordée de manière exhaustive dans la proposition de directive SRI 2 dans le cadre des obligations en matière de gestion des risques

pour la cybersécurité et de rapports auxquelles ces entités sont soumises. En outre, la proposition s'appuie sur l'acquis existant dans le domaine des services financiers, qui établit des exigences complètes à l'intention des entités financières, en ce qui concerne la gestion des risques opérationnels et la continuité des activités. Par conséquent, les entités relevant du secteur des infrastructures numériques, du secteur bancaire et du secteur des infrastructures financières devraient être traitées comme des entités équivalentes à des entités critiques au sens de la présente directive aux fins des obligations et des activités des États membres, bien que la directive proposée n'impose pas d'obligations supplémentaires à ces entités.

La proposition tient également compte d'autres initiatives sectorielles et transsectorielles concernant, par exemple, la protection civile, la réduction des risques de catastrophe et l'adaptation au changement climatique. En outre, la proposition reconnaît que, dans certains cas, la législation existante de l'UE impose aux entités l'obligation de remédier à certains risques par des mesures de protection. Dans de tels cas, par exemple en matière de sûreté aérienne ou maritime, les entités critiques devraient décrire ces mesures dans leurs plans de résilience. En outre, la directive proposée est sans préjudice de l'application des règles de concurrence prévues par le traité sur le fonctionnement de l'Union européenne (TFUE).

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

- **Base juridique**

Contrairement à la directive 2008/114/CE, qui était fondée sur l'article 308 du traité instituant la Communauté européenne (correspondant à l'actuel article 352 du traité sur le fonctionnement de l'Union européenne), la présente proposition de directive est fondée sur l'article 114 du TFUE, qui concerne le rapprochement des législations qui ont pour objet l'amélioration du marché intérieur. Cette optique est justifiée par la modification de l'objectif, du champ d'application et du contenu de la directive, par les interdépendances croissantes et par la nécessité d'établir des conditions de concurrence plus équitables pour les entités critiques. Au lieu de protéger un ensemble limité d'infrastructures physiques dont la perturbation des activités ou la destruction entraînerait des incidences transfrontières importantes, l'objectif est de renforcer la résilience des entités des États membres qui sont critiques pour la fourniture de services essentiels au maintien de fonctions sociétales ou d'activités économiques vitales dans le marché intérieur, dans un certain nombre de secteurs qui sous-tendent le fonctionnement de nombreux autres secteurs de l'économie de l'Union. En raison des interdépendances transfrontières croissantes entre les services fournis au moyen d'infrastructures critiques dans ces secteurs, une perturbation dans un État membre peut avoir des conséquences dans d'autres États membres ou dans toute l'Union.

Le cadre juridique actuel, tel qu'il a été mis en place au niveau des États membres pour réglementer les services en question, impose des obligations très divergentes, susceptibles de prendre de l'ampleur. Les divergences entre les règles nationales auxquelles les entités critiques sont soumises compromettent non seulement la fiabilité de la fourniture des services dans le marché intérieur, mais risquent également d'avoir une incidence négative sur la concurrence. En effet, des types similaires d'entités fournissant des types similaires de services sont considérés comme critiques dans certains États membres, mais pas dans d'autres. Dès lors, les entités qui sont ou souhaitent être actives dans plus d'un État membre sont soumises à des obligations divergentes lorsqu'elles opèrent dans l'ensemble du marché intérieur et les entités actives dans des États membres qui imposent des exigences plus strictes

peuvent être confrontées à des obstacles auxquels ne sont pas soumises celles qui opèrent dans des États membres appliquant des cadres plus souples. Ces divergences sont telles qu'elles ont un effet négatif direct sur le fonctionnement du marché intérieur.

- **Subsidiarité**

Un cadre législatif commun au niveau européen dans ce domaine se justifie compte tenu de la nature interdépendante et transfrontière des relations entre les activités des infrastructures critiques et leurs prestations, c'est-à-dire les services essentiels. En effet, un opérateur situé dans un État membre peut fournir des services dans plusieurs autres États membres ou dans l'ensemble de l'UE dans le cadre de réseaux étroitement liés. Il s'ensuit qu'une perturbation touchant cet opérateur pourrait avoir des effets considérables dans d'autres secteurs et au-delà des frontières nationales. Les éventuelles implications paneuropéennes des perturbations requièrent une action au niveau de l'UE. En outre, les règles nationales divergentes ont un effet négatif direct sur le fonctionnement du marché intérieur. Ainsi que l'analyse d'impact l'a démontré, de nombreux États membres et parties prenantes du secteur considèrent qu'il est nécessaire d'adopter une approche européenne plus commune et mieux coordonnée visant à garantir que les entités sont suffisamment résilientes face à différents risques qui, bien qu'ils diffèrent quelque peu d'un État membre à l'autre, créent de nombreux défis communs qui ne peuvent être relevés par des mesures nationales ou par des opérateurs individuels.

- **Proportionnalité**

La proposition est proportionnée par rapport à l'objectif global déclaré de l'initiative. Si les obligations imposées aux États membres et aux entités critiques peuvent, dans certains cas, entraîner une charge administrative supplémentaire, par exemple lorsque les États membres doivent élaborer une stratégie nationale ou lorsque les entités critiques doivent mettre en œuvre certaines mesures techniques et organisationnelles, elles devraient être généralement limitées par nature. À cet égard, il convient de noter que de nombreuses entités ont déjà adopté certaines mesures de sécurité pour protéger leurs infrastructures et assurer la continuité des activités.

Dans certains cas, toutefois, le respect de la directive peut nécessiter des investissements plus importants. Même dans de tels cas, ces investissements sont justifiés dans la mesure où ils contribuent à renforcer la résilience au niveau des opérateurs et la résilience systémique, ainsi qu'à développer une approche plus cohérente et une capacité accrue à fournir des services fiables dans l'Union. En outre, toute charge supplémentaire résultant de la directive devrait être largement inférieure aux coûts découlant de la gestion et de la résolution des perturbations majeures qui compromettent la fourniture ininterrompue de services liés à des fonctions sociétales vitales et au bien-être économique des opérateurs, des États membres, de l'Union et, plus généralement, de ses citoyens.

- **Choix de l'instrument**

La proposition prend la forme d'une directive visant à garantir une approche plus commune de la résilience des entités critiques dans un certain nombre de secteurs dans l'Union. La proposition impose aux autorités compétentes des obligations spécifiques afin qu'elles recensent les entités critiques sur la base de critères communs et des résultats de l'évaluation des risques. Au moyen d'une directive, il est possible de garantir que les États membres appliquent une approche uniforme pour le recensement des entités critiques, tout en tenant

compte des spécificités nationales, y compris des divers niveaux d'exposition aux risques et d'interdépendances entre les secteurs et au-delà des frontières.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

- **Évaluations ex post/bilans de qualité de la législation existante**

En 2019, la directive sur les infrastructures critiques européennes (ICE) a fait l'objet d'une évaluation visant à apprécier sa mise en œuvre du point de vue de sa pertinence, de sa cohérence, de son efficacité, de son efficience, de sa valeur ajoutée européenne et de sa durabilité[12].

Cette évaluation a fait apparaître que le contexte a considérablement changé depuis l'entrée en vigueur de la directive. Eu égard à ces changements, il a été constaté que la directive n'avait qu'une pertinence partielle. Si l'évaluation a montré que la directive était globalement cohérente avec la législation sectorielle européenne pertinente et la politique correspondante au niveau international, il est apparu qu'elle n'était que partiellement efficace en raison du caractère général de certaines de ses dispositions. L'évaluation a révélé que la directive a généré une valeur ajoutée européenne dans la mesure où elle a produit des résultats (c'est-à-dire un cadre commun de protection des ICE) qu'aucune initiative nationale ou qu'aucune autre initiative européenne n'aurait pu atteindre autrement sans engager des processus beaucoup plus longs, plus coûteux et moins bien définis. Cela étant dit, il a été constaté que certaines dispositions n'avaient produit qu'une valeur ajoutée limitée dans de nombreux États membres.

En ce qui concerne la durabilité, certains effets générés par la directive (par exemple, les discussions transfrontières, les obligations de rapport) prendraient fin si la directive devait être abrogée sans être remplacée. L'évaluation a montré que les États membres restaient favorables à la participation de l'UE aux efforts visant à renforcer la résilience des infrastructures critiques et craignaient que l'abrogation pure et simple de la directive puisse avoir des effets négatifs dans ce domaine, en particulier sur le plan de la protection des ICE désignées. Les États membres aspiraient à ce que l'engagement de l'Union dans ce domaine continue à respecter le principe de subsidiarité, soutienne les mesures prises au niveau national et facilite la coopération transfrontière, y compris avec les pays tiers.

- **Consultation des parties intéressées**

Lors de l'élaboration de la présente proposition, la Commission a consulté un large éventail de parties prenantes, notamment: les institutions et agences de l'Union européenne, des organisations internationales, les autorités des États membres, des entités privées dont des opérateurs individuels et des associations sectorielles nationales et européennes représentant les opérateurs de nombreux secteurs différents, des experts et réseaux d'experts dont le réseau européen de référence pour la protection des infrastructures critiques (ERNCIP), des membres du monde universitaire, des organisations non gouvernementales, ainsi que le grand public.

[12] SWD(2019) 310.

Les parties prenantes ont été consultées par divers moyens, notamment: un retour d'information du public sur l'analyse d'impact initiale de la présente proposition, des séminaires de consultation, des questionnaires ciblés, des échanges bilatéraux et une consultation publique (à l'appui de l'évaluation de 2019 de la directive sur les ICE). En outre, le contractant externe chargé de l'étude de faisabilité ayant servi à l'élaboration de l'analyse d'impact a consulté de nombreuses parties prenantes au moyen, par exemple, d'une enquête en ligne, d'un questionnaire écrit, d'entretiens individuels et de visites virtuelles sur place dans 10 États membres.

Ces consultations ont permis à la Commission d'examiner l'efficacité, l'efficience, la pertinence, la cohérence et la valeur ajoutée européenne du cadre existant en matière de résilience des infrastructures critiques (c'est-à-dire la situation de départ), les problèmes qu'il a engendrés, les différents choix de mesures qui pourraient être envisagées pour résoudre ces problèmes et les incidences spécifiques que ces choix pourraient avoir. D'une manière générale, les consultations ont mis en évidence un certain nombre de domaines faisant l'objet d'un consensus général parmi les parties prenantes, notamment le fait que le cadre existant de l'UE sur la résilience des infrastructures critiques devrait être revu à la lumière des interdépendances transsectorielles croissantes et de l'évolution du paysage des menaces.

En particulier, les parties prenantes estimaient généralement que toute nouvelle approche devrait consister en une combinaison de mesures contraignantes et non contraignantes, mettre l'accent sur la résilience plutôt que sur la protection centrée sur les biens, et établir un lien plus évident entre les mesures visant à renforcer la cyber-résilience et la résilience en dehors du cyberespace. En outre, elles étaient favorables à une approche qui tienne compte des dispositions de la législation sectorielle existante, qui inclue au moins les secteurs couverts par l'actuelle directive SRI et qui définisse des obligations plus uniformes applicables aux entités critiques au niveau national, qui, à leur tour, devraient pouvoir exercer un contrôle de sécurité suffisant du personnel ayant accès à des installations/informations sensibles. En outre, les parties prenantes ont suggéré que toute nouvelle approche devrait permettre aux États membres d'exercer une surveillance renforcée des activités des entités critiques, mais elle devrait aussi garantir que les entités critiques d'importance paneuropéenne soient recensées et soient suffisamment résilientes. Enfin, elles ont plaidé en faveur d'un financement et d'un soutien accrus de l'UE, par exemple pour la mise en œuvre de tout nouvel instrument, le renforcement des capacités au niveau national, la coordination/coopération public-privé et le partage de bonnes pratiques, de connaissances et d'expertise à différents niveaux. La proposition à l'examen contient des dispositions qui reflètent généralement les points de vue et préférences exprimés par les parties prenantes.

- **Obtention et utilisation d'expertise**

Comme indiqué dans la section précédente, la Commission a fait appel à des experts externes, dans le cadre de consultations menées entre autres avec des experts indépendants, des réseaux d'experts et des membres du monde universitaire, pour élaborer la proposition à l'examen.

- **Analyse d'impact**

L'analyse d'impact qui a étayé l'élaboration de la présente initiative a examiné différents choix de mesures, afin de remédier aux problèmes généraux et spécifiques décrits

précédemment. Outre la situation de départ, qui n'entraînerait aucun changement par rapport à la situation actuelle, les options sont les suivantes:

– option 1: maintien de la directive sur les ICE existante, accompagnée de mesures volontaires dans le cadre du programme EPCIP existant;

– option 2: révision de la directive sur les ICE existante afin qu'elle englobe les mêmes secteurs que la directive SRI et qu'elle mette davantage l'accent sur la résilience. La nouvelle directive sur les ICE apporterait des modifications au processus actuel de désignation des ICE transfrontières, notamment en définissant de nouveaux critères de désignation et en imposant de nouvelles exigences aux États membres et aux opérateurs;

– option 3: remplacement de la directive sur les ICE existante par un nouvel instrument visant à renforcer la résilience des entités critiques dans les secteurs considérés comme essentiels par la directive SRI 2 proposée. Cette option se traduirait par la définition d'exigences minimales pour les États membres et les entités critiques recensées en vertu du nouveau cadre. Une procédure d'identification des entités critiques offrant des services à ou dans plusieurs États membres de l'UE, sinon tous, serait mise en place. La mise en œuvre de la législation serait soutenue par un pôle de connaissances spécifique au sein de la Commission;

– option 4: remplacement de la directive sur les ICE existante par un nouvel instrument visant à renforcer la résilience des entités critiques dans les secteurs considérés comme essentiels par la directive SRI 2 proposée, attribution d'un rôle plus important à la Commission dans l'identification des entités critiques et création d'une agence de l'UE spécifiquement chargée de la résilience des infrastructures critiques (qui assumerait les rôles et responsabilités du pôle de connaissances proposé dans l'option précédente).

À la lumière des différentes incidences économiques, sociales et environnementales associées à chacune des options, mais aussi de leur valeur en termes d'efficacité, d'efficience et de proportionnalité, l'analyse d'impact a conclu que l'option 3 constituait l'option privilégiée. Alors que les options 1 et 2 n'apporteraient pas les changements nécessaires pour résoudre le problème, l'option 3 permettrait de mettre en place un cadre de résilience harmonisé et plus complet qui serait également aligné sur le droit de l'Union existant dans des domaines connexes et qui tiendrait compte de celui-ci. L'option 3 a également été jugée proportionnée et semble politiquement réalisable étant donné qu'elle reflète les déclarations du Conseil et du Parlement concernant la nécessité d'une action de l'Union dans ce domaine. En outre, cette option a été jugée susceptible de garantir une flexibilité et d'offrir un cadre à l'épreuve du temps qui permettrait aux entités critiques de réagir à différents risques au fil du temps. Enfin, l'analyse d'impact a montré que cette option serait complémentaire des cadres et instruments sectoriels et transsectoriels existants. Par exemple, cette option tient compte de la situation dans laquelle des entités désignées satisferaient à certaines obligations contenues dans le nouvel instrument par le biais d'obligations découlant d'autres instruments existants, auquel cas elles ne seraient pas tenues de prendre d'autres mesures. Par contre, elles seraient tenues de prendre des mesures lorsque les instruments existants ne couvrent pas le domaine ou se limitent à certains types de risques ou mesures.

L'analyse d'impact a été examinée par le comité d'examen de la réglementation, qui a émis un avis favorable assorti de réserves le 20 novembre 2020. Le comité a mis en évidence un certain nombre d'éléments de l'analyse d'impact qui devront être examinés. Plus précisément, le comité a demandé des précisions concernant les risques liés aux infrastructures critiques et à la dimension transfrontière, le lien entre l'initiative et la révision en cours de la directive SRI, ainsi que la relation entre l'option privilégiée et d'autres actes législatifs sectoriels. En outre, le comité a estimé que l'élargissement du champ d'application sectoriel de l'instrument devait être davantage justifié et a demandé des informations supplémentaires concernant les critères de sélection des entités critiques. Enfin, en ce qui concerne la proportionnalité, le comité a demandé des éclaircissements supplémentaires sur la manière dont l'option privilégiée permettrait de mieux répondre sur le plan national aux risques transfrontières. Ces observations ainsi que d'autres commentaires plus détaillés formulés par le comité ont été abordés dans la version finale de l'analyse d'impact, qui décrit ainsi plus en détail les risques transfrontières affectant les infrastructures critiques et le lien entre la présente proposition et la proposition de directive SRI 2. Les observations du comité ont également été prises en compte dans la proposition de directive qui suit.

- **Réglementation affûtée et simplification**

Conformément au programme pour une réglementation affûtée et performante (REFIT) de la Commission, toutes les initiatives visant à modifier la législation existante de l'UE devraient tendre à simplifier et à réaliser plus efficacement les objectifs déclarés de l'action. Les conclusions de l'analyse d'impact indiquent que la proposition devrait réduire la charge globale pesant sur les États membres. Un alignement plus étroit sur l'approche axée sur les services, adoptée dans la directive SRI actuelle, devrait entraîner une réduction des coûts de mise en conformité au fil du temps. Par exemple, la lourde procédure de recensement et de désignation transfrontière prévue par la directive sur les ICE existante serait remplacée par une procédure reposant sur les risques au niveau national, visant uniquement à identifier les entités critiques soumises à diverses obligations. Sur la base de l'évaluation des risques, les États membres recenseraient les entités critiques, dont la plupart sont déjà désignées comme des opérateurs de services essentiels en vertu de la directive SRI en vigueur.

En outre, en prenant des mesures pour renforcer leur résilience, les entités critiques seront moins susceptibles de subir des perturbations. Dès lors, la probabilité que des incidents perturbateurs affectent négativement la fourniture de services essentiels dans les différents États membres et dans toute l'Europe serait réduite. Cela, conjugué aux effets positifs résultant de l'harmonisation au niveau de l'Union des règles nationales divergentes, aurait une incidence positive sur les entreprises, y compris les microentreprises et les petites et moyennes entreprises, sur la santé globale de l'économie de l'Union et sur le fonctionnement fiable du marché intérieur.

- **Droits fondamentaux**

La législation proposée vise à renforcer la résilience des entités critiques qui fournissent différentes formes de services essentiels, tout en éliminant les obstacles réglementaires entravant leur capacité à fournir leurs services dans l'Union. Ce faisant, le risque global de perturbations tant au niveau de la société qu'au niveau individuel serait réduit et, de même, les charges seraient moindres. La législation proposée contribuerait à accroître le niveau de sécurité publique, influencerait positivement la liberté d'entreprise et serait bénéfique à de nombreux autres opérateurs économiques tributaires de la fourniture de services essentiels, ce

qui profiterait en fin de compte aux consommateurs. Les dispositions de la proposition visant à garantir une gestion efficace de la sécurité des employés toucheront normalement au traitement de données à caractère personnel. Cette mesure se justifie par la nécessité de procéder à une vérification des antécédents de certaines catégories de personnel. En outre, tout traitement de ce type de données à caractère personnel sera toujours soumis au respect des règles de l'Union relatives à la protection des données à caractère personnel, y compris le règlement général sur la protection des données[13].

4. INCIDENCE BUDGÉTAIRE

La directive proposée a des incidences sur le budget de l'Union. Les ressources financières totales nécessaires pour soutenir la mise en œuvre de la présente proposition sont estimées à 42,9 millions d'EUR pour la période 2021-2027, dont 5,1 millions d'EUR en dépenses administratives. Ces coûts peuvent être ventilés comme suit:

– activités de soutien de la Commission, y compris la mise à disposition de personnel, les projets, les études et les activités de soutien;

– missions de conseil organisées par la Commission;

– réunions régulières du groupe sur la résilience des entités critiques et du comité de comitologie et autres réunions.

Des informations plus détaillées sont disponibles dans la fiche financière législative qui accompagne la présente proposition.

5. AUTRES ÉLÉMENTS

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

La mise en œuvre de la directive proposée sera réexaminée quatre ans et demi après son entrée en vigueur et, à l'issue de ce réexamen, la Commission présentera un rapport au Parlement européen et au Conseil. Ce rapport vise à déterminer dans quelle mesure les États membres ont pris les dispositions nécessaires pour se conformer à la directive. La Commission présentera un rapport évaluant l'impact et la valeur ajoutée de la directive au Parlement européen et au Conseil au plus tard six ans après l'entrée en vigueur de la directive.

- **Explication détaillée des différentes dispositions de la proposition**

Objet, champ d'application et définitions (articles 1er et 2)

L'article 1er définit l'objet et le champ d'application de la directive, qui impose aux États membres l'obligation d'adopter certaines mesures afin d'assurer la fourniture dans le marché intérieur de services essentiels au maintien de fonctions sociétales ou d'activités économiques

[13] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

vitales, en particulier l'obligation de recenser les entités critiques et de leur permettre de satisfaire aux obligations spécifiques visant à renforcer leur résilience et à améliorer leur capacité à fournir ces services dans le marché intérieur. La directive établit également des règles de surveillance et de coercition des entités critiques et prévoit une surveillance spécifique des entités critiques considérées comme revêtant une importance européenne particulière. L'article 1er explique également la relation entre la directive et d'autres actes pertinents du droit de l'Union, ainsi que les conditions dans lesquelles les informations confidentielles en vertu des règles nationales et de l'Union sont échangées avec la Commission et les autres autorités compétentes. L'article 2 comprend une liste de définitions applicables.

Cadres nationaux pour la résilience des entités critiques (articles 3 à 9)

L'article 3 prévoit que les États membres adoptent une stratégie visant à renforcer la résilience des entités critiques, décrit les éléments qu'elle devrait contenir, explique qu'elle devrait être mise à jour régulièrement et si nécessaire, et dispose que les États membres communiquent leurs stratégies et toute mise à jour de leurs stratégies à la Commission. L'article 4 prévoit que les autorités compétentes établissent une liste des services essentiels et procèdent régulièrement à une évaluation de tous les risques pertinents susceptibles d'affecter la fourniture de ces services essentiels en vue de recenser les entités critiques. Cette évaluation rend compte des évaluations des risques effectuées conformément à d'autres actes pertinents du droit de l'Union, des risques découlant des dépendances existant entre des secteurs spécifiques et des informations disponibles sur les incidents. Les États membres veillent à ce que les éléments pertinents de l'évaluation des risques soient mis à la disposition des entités critiques et à ce que les données relatives aux types de risques recensés et les résultats de leurs évaluations des risques soient régulièrement communiqués à la Commission.

L'article 5 prévoit que les États membres recensent les entités critiques dans des secteurs et sous-secteurs spécifiques. Le processus de recensement devrait tenir compte des résultats de l'évaluation des risques et appliquer des critères spécifiques. Les États membres établissent une liste des entités critiques, qui est mise à jour régulièrement et si nécessaire. Les entités critiques sont dûment informées de leur recensement et des obligations qui en découlent. Les autorités compétentes responsables de la mise en œuvre de la directive notifient le recensement des entités critiques aux autorités compétentes responsables de l'application de la directive SRI 2. Lorsqu'une entité a été recensée en tant qu'entité critique par deux États membres ou plus, les États membres se consultent en vue de réduire la charge pesant sur cette entité critique. Lorsque des entités critiques fournissent des services à ou dans plus d'un tiers des États membres, l'État membre concerné notifie à la Commission l'identité de ces entités critiques.

L'article 6 définit la notion d'«effet perturbateur important» figurant à l'article 5, paragraphe 2, et impose aux États membres de communiquer à la Commission certaines formes d'informations concernant les entités critiques qu'ils recensent et la manière dont elles ont été identifiées. L'article 6 habilite également la Commission, après consultation du groupe sur la résilience des entités critiques, à adopter des lignes directrices pertinentes.

L'article 7 prévoit que les États membres devraient recenser les entités relevant des secteurs des banques, des infrastructures du marché financier et des infrastructures numériques, qui

doivent être considérées comme équivalentes aux entités critiques uniquement aux fins du chapitre II. Ces entités devraient être informées de leur recensement.

L'article 8 prévoit que chaque État membre désigne une ou plusieurs autorités compétentes responsables de la bonne application de la directive au niveau national, ainsi qu'un point de contact unique chargé d'assurer la coopération transfrontière, et veille à ce que des ressources adéquates leur soient allouées. Le point de contact unique fournit régulièrement à la Commission un rapport de synthèse sur les notifications d'incidents. L'article 8 exige que les autorités compétentes chargées de l'application de la directive coopèrent avec les autres autorités nationales concernées, y compris les autorités compétentes désignées en vertu de la directive SRI 2. L'article 9 prévoit que les États membres aident les entités critiques à assurer leur résilience et facilitent la coopération et l'échange volontaire d'informations et de bonnes pratiques entre les autorités compétentes et les entités critiques.

Résilience des entités critiques (articles 10 à 13)

L'article 10 prévoit que les entités critiques évaluent régulièrement tous les risques pertinents sur la base d'évaluations nationales des risques et d'autres sources d'information pertinentes. L'article 11 prévoit que les entités critiques adoptent des mesures techniques et organisationnelles appropriées et proportionnées pour assurer leur résilience et veillent à ce que ces mesures soient décrites dans un plan de résilience ou dans un ou plusieurs documents équivalents. Les États membres peuvent demander à la Commission d'organiser des missions de conseil afin de conseiller les entités critiques en vue du respect de leurs obligations. L'article 11 habilite également, le cas échéant, la Commission à adopter des actes délégués et des actes d'exécution.

L'article 12 prévoit que les États membres veillent à ce que les entités critiques puissent soumettre des demandes de vérification des antécédents de personnes qui relèvent ou pourraient relever de certaines catégories spécifiques de personnel, et à ce que ces demandes soient évaluées rapidement par les autorités chargées d'effectuer ces vérifications. L'article décrit la finalité, la portée et le contenu des vérifications des antécédents, qui doivent être conformes au règlement général sur la protection des données.

L'article 13 prévoit que les États membres veillent à ce que les entités critiques notifient à l'autorité compétente les incidents qui perturbent ou sont susceptibles de perturber de manière significative leurs activités. Les autorités compétentes fournissent à leur tour les informations de suivi pertinentes à l'entité critique notifiante. Par l'intermédiaire du point de contact unique, les autorités compétentes informent également les points de contact uniques des autres États membres concernés lorsque l'incident a ou risque d'avoir des incidences transfrontières dans un ou plusieurs autres États membres.

Surveillance spécifique des entités critiques revêtant une importance européenne particulière (articles 14 et 15)

L'article 14 définit les entités critiques revêtant une importance européenne particulière comme étant des entités qui ont été recensées comme des entités critiques et qui fournissent des services essentiels à ou dans plus d'un tiers des États membres. Dès réception de la notification visée à l'article 5, paragraphe 6, la Commission informe l'entité concernée de son

recensement en tant qu'entité critique revêtant une importance européenne particulière, des obligations qui en découlent et de la date à partir de laquelle ces obligations commencent à s'appliquer. L'article 15 décrit les modalités spécifiques de surveillance applicables aux entités critiques revêtant une importance européenne particulière, qui prévoient notamment que, sur demande, les États membres d'accueil communiquent à la Commission et au groupe sur la résilience des entités critiques des informations concernant l'évaluation des risques conformément à l'article 10 et les mesures prises conformément à l'article 11, ainsi que toute mesure de surveillance ou de coercition. L'article 15 prévoit également que la Commission peut organiser des missions de conseil pour évaluer les mesures mises en place par des entités critiques spécifiques revêtant une importance européenne particulière. Sur la base de l'analyse des conclusions de la mission de conseil réalisée par le groupe sur la résilience des entités critiques, la Commission communique à l'État membre dans lequel se situe l'infrastructure de l'entité son avis concernant le respect par cette entité des obligations qui lui incombent et, le cas échéant, concernant les mesures qui pourraient être prises pour améliorer la résilience de l'entité. L'article décrit la composition, l'organisation et le financement des missions de conseil. Il prévoit également que la Commission adopte un acte d'exécution établissant les règles relatives aux modalités de procédure pour la conduite et les rapports des missions de conseil.

Coopération et rapports (articles 16 et 17)

L'article 16 décrit le rôle et les missions du groupe sur la résilience des entités critiques, qui est composé de représentants des États membres et de la Commission. Il assiste la Commission et facilite la coopération stratégique et l'échange d'informations. L'article explique que la Commission peut adopter des actes d'exécution établissant les modalités de procédure nécessaires au fonctionnement du groupe sur la résilience des entités critiques. L'article 17 prévoit que la Commission aide, s'il y a lieu, les États membres et les entités critiques à se conformer aux obligations qui leur incombent en vertu de la directive et complète l'action des États membres visée à l'article 9.

Surveillance et coercition (articles 18 et 19)

L'article 18 prévoit que les États membres ont certains pouvoirs, moyens et responsabilités pour assurer la mise en œuvre de la directive et faire respecter celle-ci. Les États membres veillent, lorsqu'une autorité compétente évalue si une entité critique respecte ses obligations, à ce que ladite autorité en informe les autorités compétentes de l'État membre concerné désignées en vertu de la directive SRI 2 et à ce qu'elle puisse demander à ces autorités d'évaluer la cybersécurité de cette entité, et elles devraient coopérer et échanger des informations à cette fin. L'article 19 prévoit que, conformément à la pratique constante, les États membres déterminent le régime des sanctions applicables aux violations des dispositions et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions.

Dispositions finales (articles 20 à 26)

L'article 20 prévoit que la Commission est assistée par un comité au sens du règlement (UE) nº 182/2011. Il s'agit d'un article standard. L'article 21 confère à la Commission le pouvoir d'adopter des actes délégués sous réserve des conditions fixées dans cet article. Il s'agit là aussi d'un article standard. L'article 22 prévoit que la Commission présente au Parlement européen et au Conseil un rapport évaluant dans quelle mesure les États membres ont pris les

dispositions nécessaires pour se conformer à la directive. Un rapport évaluant l'incidence et la valeur ajoutée de la directive ainsi que l'opportunité d'étendre son champ d'application à d'autres secteurs ou sous-secteurs, y compris le secteur de la production, de la transformation et de la distribution des denrées alimentaires, doit être présenté régulièrement au Parlement européen et au Conseil.

L'article 23 prévoit que la directive 2008/114/CE est abrogée avec effet à la date d'entrée en vigueur de la directive. L'article 24 prévoit que les États membres adoptent et publient, dans le délai fixé, les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la directive, et en informent la Commission. Les États membres doivent communiquer à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine couvert par la présente directive. L'article 25 prévoit que la directive entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*. L'article 26 indique que les États membres sont destinataires de la directive.

2020/0365 (COD)

Proposition de

DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL

sur la résilience des entités critiques

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen[14],

vu l'avis du Comité des régions[15],

statuant conformément à la procédure législative ordinaire[16],

considérant ce qui suit:

(1) La directive 2008/114/CE[17] du Conseil établit une procédure de désignation des infrastructures critiques européennes dans les secteurs de l'énergie et des transports, dont la perturbation des activités ou la destruction aurait un impact transfrontière significatif sur deux États membres au moins. Cette directive vise exclusivement la protection de ces infrastructures. Toutefois, l'évaluation de la directive 2008/114/CE réalisée en 2019[18] a montré qu'en raison de la nature de plus en plus interconnectée et transfrontière des activités faisant appel à des infrastructures critiques, les mesures de protection portant sur des biens individuels ne suffisent pas à elles seules pour empêcher toute perturbation. Par conséquent, il est nécessaire de réorienter l'approche en vue de garantir la résilience des entités critiques, c'est-à-dire leur capacité à atténuer les conséquences d' incidents susceptibles de perturber leur fonctionnement, à les absorber, à s'y adapter et à s'en remettre.

(2) Malgré les mesures existantes au niveau de l'Union[19] et au niveau national visant à soutenir la protection des infrastructures critiques dans l'Union, les entités qui exploitent ces infrastructures ne sont pas équipées de manière adéquate pour faire face

14 JO C du , p. .
15 JO C […] du […], p. […].
16 Position du Parlement européen […] et du Conseil […].
17 Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (JO L 345 du 23.12.2008, p. 75).
18 SDW(2019) 308.
19 Programme européen de protection des infrastructures critiques (EPCIP).

aux risques actuels et anticipés pesant sur leurs activités, qui pourraient entraîner des perturbations dans la fourniture de services essentiels à l'exercice de fonctions sociétales ou d'activités économiques vitales. Cette situation est la conséquence du paysage dynamique des menaces, caractérisé par l'évolution de la menace terroriste et par les interdépendances croissantes entre les infrastructures et les secteurs, ainsi que par l'accroissement du risque physique lié aux catastrophes naturelles et au changement climatique, qui augmente la fréquence et l'ampleur des phénomènes météorologiques extrêmes et entraîne des changements à long terme des conditions climatiques moyennes, susceptibles de réduire la capacité et l'efficacité de certains types d'infrastructures si des mesures de résilience ou d'adaptation au changement climatique ne sont pas mises en place. En outre, les secteurs et types d'entités concernés critiques ne sont pas systématiquement reconnus comme critiques dans tous les États membres.

(3) Ces interdépendances croissantes découlent d'un réseau de fourniture de services de plus en plus transfrontière et interdépendant, qui utilise des infrastructures essentielles dans toute l'Union dans les secteurs de l'énergie, des transports, des banques, des infrastructures du marché financier, des infrastructures numériques, de l'eau potable, des eaux usées, de la santé, de certains aspects de l'administration publique et de l'espace, dans la mesure où la fourniture de certains services dépendant de structures terrestres détenues, gérées et exploitées par des États membres ou par des parties privées est concernée, ce qui ne couvre donc pas les infrastructures détenues, gérées ou exploitées par ou au nom de l'Union dans le cadre de ses programmes spatiaux. Ces interdépendances signifient que toute perturbation, même initialement limitée à une entité ou un secteur, peut produire des effets en cascade plus larges, entraînant éventuellement des incidences négatives durables et de grande ampleur pour la fourniture de services dans l'ensemble du marché intérieur. La pandémie de COVID-19 a mis en évidence la vulnérabilité de nos sociétés de plus en plus interdépendantes face à des risques peu probables.

(4) Les entités participant à la fourniture de services essentiels sont de plus en plus soumises à des exigences divergentes imposées par les législations des États membres. Le fait que certains États membres imposent des exigences de sécurité moins strictes à ces entités risque non seulement d'avoir une incidence négative sur le maintien de fonctions sociétales ou d'activités économiques vitales dans l'ensemble de l'Union, mais entrave aussi le bon fonctionnement du marché intérieur. Des types d'entités similaires sont considérés comme critiques dans certains États membres mais pas dans d'autres, et ceux qui sont considérés comme critiques sont soumis à des exigences différentes selon les États membres. Il en résulte des charges administratives supplémentaires et inutiles pour les entreprises exerçant des activités transfrontières, notamment pour les entreprises actives dans des États membres imposant des exigences plus strictes.

(5) Il est donc nécessaire d'établir des règles minimales harmonisées afin de garantir la fourniture de services essentiels dans le marché intérieur et de renforcer la résilience des entités critiques.

(6) Afin d'atteindre cet objectif, les États membres devraient recenser les entités critiques qui devraient être soumises à des exigences et à une surveillance spécifiques, mais qui devraient aussi bénéficier d'un soutien et de conseils particuliers visant à atteindre un niveau élevé de résilience face à tous les risques pertinents.

(7) Certains secteurs de l'économie, tels que l'énergie et les transports, sont déjà réglementés ou pourraient l'être à l'avenir par des actes sectoriels du droit de l'Union qui contiennent des règles relatives à certains aspects de la résilience des entités actives dans ces secteurs. Afin de régir de manière globale la résilience des entités qui sont essentielles au bon fonctionnement du marché intérieur, ces mesures sectorielles devraient être complétées par celles prévues dans la présente directive, qui crée un cadre général applicable à la résilience des entités critiques face à tous les risques, à savoir naturels et d'origine humaine, accidentels et intentionnels.

(8) Compte tenu de l'importance de la cybersécurité pour la résilience des entités critiques et dans un souci d'uniformité, une approche cohérente entre la présente directive et la directive (UE) XX/YY du Parlement européen et du Conseil[20] [proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 (ci-après la «directive SRI 2»)] est indispensable, chaque fois que c'est possible. Compte tenu de la fréquence plus élevée et des caractéristiques particulières des risques en matière de cybersécurité, la directive SRI 2 impose des exigences complètes à un grand nombre d'entités afin de garantir leur cybersécurité. Étant donné que la cybersécurité est dûment traitée dans la directive SRI 2, les questions qu'elle englobe devraient être exclues du champ d'application de la présente directive, sans préjudice du régime particulier applicable aux entités du secteur des infrastructures numériques.

(9) Lorsque des dispositions d'autres actes du droit de l'Union exigent des entités critiques qu'elles évaluent les risques pertinents, prennent des mesures pour assurer leur résilience ou notifient les incidents, et lorsque ces exigences sont au moins équivalentes aux obligations correspondantes énoncées dans la présente directive, les dispositions pertinentes de la présente directive ne devraient pas s'appliquer, de manière à éviter toute redondance et les charges inutiles. Dans un tel cas, les dispositions pertinentes de ces autres actes devraient s'appliquer. Lorsque les dispositions pertinentes de la présente directive ne s'appliquent pas, ses dispositions relatives à la surveillance et à la coercition ne devraient pas non plus s'appliquer. Les États membres devraient néanmoins inclure tous les secteurs énumérés à l'annexe dans leur stratégie visant à renforcer la résilience des entités critiques, dans l'évaluation des risques et dans les mesures de soutien prévues au chapitre II, et être en mesure de recenser les entités critiques dans les secteurs dans lesquels les conditions applicables sont remplies, en tenant compte du régime particulier applicable aux entités des secteurs des banques, des infrastructures des marchés financiers et des infrastructures numériques.

(10) Afin de garantir une approche globale de la résilience des entités critiques, chaque État membre devrait disposer d'une stratégie définissant les objectifs et les mesures à mettre en œuvre. À cet effet, les États membres devraient veiller à ce que leurs stratégies de cybersécurité prévoient un cadre d'action pour une coordination renforcée entre l'autorité compétente en vertu de la présente directive et l'autorité compétente en vertu de la directive SRI 2 dans le contexte du partage d'informations relatives aux incidents et aux cybermenaces ainsi que de l'exercice des tâches de surveillance.

---

[20] [Référence à la directive SRI 2, après adoption.]

(11) Les mesures prises par les États membres pour recenser les entités critiques et contribuer à garantir leur résilience devraient adopter une approche fondée sur les risques orientant les efforts vers les entités les plus utiles à l'exercice de fonctions sociétales ou d'activités économiques vitales. Afin de garantir une telle approche ciblée, chaque État membre devrait procéder, dans un cadre harmonisé, à une évaluation de tous les risques naturels et d'origine humaine susceptibles d'affecter la fourniture de services essentiels, y compris les accidents, les catastrophes naturelles, les urgences de santé publique telles que les pandémies, et les menaces antagonistes, dont les infractions terroristes. Lorsqu'ils procèdent à ces évaluations des risques, les États membres devraient tenir compte d'autres évaluations générales ou sectorielles des risques effectuées en vertu d'autres actes du droit de l'Union et prendre en considération les dépendances entre les secteurs, y compris à l'égard des autres États membres et des pays tiers. Les résultats de l'évaluation des risques devraient être utilisés dans le processus de recensement des entités critiques et pour aider ces entités à satisfaire aux exigences en matière de résilience énoncées par la présente directive.

(12) Afin de garantir que toutes les entités concernées sont soumises à ces exigences et de réduire les divergences à cet égard, il importe d'établir des règles harmonisées permettant un recensement cohérent des entités critiques dans l'ensemble de l'Union, tout en permettant aux États membres de tenir compte des spécificités nationales. Par conséquent, il convient de définir des critères de recensement des entités critiques. Dans un souci d'efficacité, d'efficience, de cohérence et de sécurité juridique, il convient également d'établir des règles appropriées applicables à la notification et à la coopération relatives à ce recensement, ainsi qu'aux conséquences juridiques de celui-ci. Afin de permettre à la Commission d'évaluer la bonne application de la présente directive, les États membres devraient lui communiquer, d'une manière aussi détaillée et spécifique que possible, les informations pertinentes et, en tout état de cause, la liste des services essentiels, le nombre d'entités critiques recensées dans chaque secteur et sous-secteur mentionné à l'annexe et le ou les services essentiels fournis par chaque entité, ainsi que les seuils éventuellement appliqués.

(13) Des critères devraient également être fixés afin de déterminer l'importance de l'effet perturbateur causé par les incidents susmentionnés. Ces critères devraient se fonder sur les critères prévus dans la directive (UE) 2016/1148 du Parlement européen et du Conseil[21] afin de tirer parti des efforts déployés par les États membres pour recenser les opérateurs concernés et de l'expérience acquise à cet égard.

(14) Les entités relevant du secteur des infrastructures numériques sont essentiellement fondées sur les réseaux et les systèmes d'information et relèvent du champ d'application de la directive SRI 2, qui traite de la sécurité physique de ces systèmes dans le cadre de leurs obligations en matière de gestion des risques pour la cybersécurité et de rapports. Étant donné que ces questions sont couvertes par la directive SRI 2, les obligations de la présente directive ne s'appliquent pas à ces entités. Toutefois, compte tenu de l'importance des services fournis par les entités du secteur des infrastructures numériques pour la fourniture d'autres services essentiels, les États membres devraient recenser, sur la base des critères et selon la procédure

[21] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

prévus dans la présente directive mutatis mutandis, les entités relevant du secteur des infrastructures numériques qui devraient être considérées comme équivalentes aux entités critiques aux seules fins du chapitre II, y compris sur le plan de la fourniture d'un soutien par les États membres pour renforcer la résilience de ces entités. Par conséquent, ces entités ne devraient pas être soumises aux obligations énoncées aux chapitres III à VI. Étant donné que les obligations qui incombent aux entités critiques en vertu du chapitre II de fournir certaines informations aux autorités compétentes sont liées l'application des chapitres III et IV, ces entités ne devraient pas non plus être soumises à ces obligations.

(15) L'acquis de l'UE en matière de services financiers impose aux entités financières l'obligation de gérer de manière exhaustive tous les risques auxquels elles sont confrontées, y compris les risques opérationnels, et d'assurer la continuité des activités. Les obligations découlent notamment du règlement (CE) nº 648/2012 du Parlement européen et du Conseil[22], de la directive 2014/65/UE du Parlement européen et du Conseil[23] et du règlement (UE) nº 600/2014 du Parlement européen et du Conseil[24], ainsi que du règlement (UE) nº 575/2013 du Parlement européen et du Conseil[25] et de la directive 2013/36/UE du Parlement européen et du Conseil[26]. La Commission a récemment proposé de compléter ce cadre par le règlement XX/YYYY du Parlement européen et du Conseil [proposition de règlement sur la résilience opérationnelle numérique du secteur financier[27]], qui impose aux entreprises financières des obligations en matière de gestion des risques liés aux technologies de l'information et de la communication, y compris la protection des infrastructures physiques correspondantes. Étant donné que la résilience des entités énumérées aux points 3 et 4 de l'annexe est couverte de manière exhaustive par l'acquis de l'UE en matière de services financiers, ces entités devraient également être considérées comme des entités critiques aux seules fins du chapitre II de la présente directive. Afin de garantir une application cohérente des règles relatives aux risques opérationnels et à la résilience numérique dans le secteur financier, le soutien des États membres au renforcement de la résilience globale des entités financières considérées comme équivalentes aux entités critiques devrait être assuré par les autorités désignées en vertu de l'article 41 du [règlement sur la résilience opérationnelle numérique du

---

22 Règlement (UE) nº 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux (JO L 201 du 27.7.2012, p. 1).

23 Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE (JO L 173 du 12.6.2014, p. 349).

24 Règlement (UE) nº 600/2014 du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant le règlement (UE) nº 648/2012 (JO L 173 du 12.6.2014, p. 84).

25 Règlement (UE) nº 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) nº 648/2012 (JO L 176 du 27.6.2013, p. 1).

26 Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE (JO L 176 du 27.6.2013, p. 338).

27 Proposition de règlement du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014, COM(2020) 595.

secteur financier], et soumis aux procédures établies dans cet acte législatif d'une manière pleinement harmonisée.

(16) Les États membres devraient désigner les autorités chargées de superviser l'application des règles de la présente directive et, s'il y a lieu, de les faire respecter, et veiller à ce que ces autorités disposent des pouvoirs et des ressources adéquats. Compte tenu des différences entre les structures de gouvernance nationales et afin de préserver les dispositifs sectoriels existants ou les organismes de surveillance et de réglementation de l'Union, et afin d'éviter la duplication des efforts, les États membres devraient pouvoir désigner plus d'une autorité compétente. Dans ce cas, ils devraient toutefois définir clairement les tâches respectives des autorités concernées et veiller à ce qu'elles coopèrent de manière harmonieuse et efficace. Toutes les autorités compétentes devraient également coopérer plus généralement avec d'autres autorités concernées, tant au niveau national qu'au niveau de l'Union.

(17) Afin de faciliter la coopération et la communication transfrontières et de permettre la mise en œuvre effective de la présente directive, et sans préjudice des exigences juridiques sectorielles de l'Union, chaque État membre devrait désigner, au sein de l'une des autorités qu'il a désignées comme autorité compétente en vertu de la présente directive, un point de contact unique chargé de coordonner les questions liées à la résilience des entités critiques et à la coopération transfrontière à cet égard au niveau de l'Union.

(18) Étant donné qu'en vertu de la directive SRI 2, les entités recensées en tant qu'entités critiques, ainsi que les entités identifiées dans le secteur des infrastructures numériques qui doivent être considérées comme équivalentes aux entités critiques en vertu de la présente directive sont soumises aux exigences en matière de cybersécurité imposées par la directive SRI 2, les autorités compétentes désignées en vertu des deux directives devraient coopérer, notamment en ce qui concerne les risques et incidents de cybersécurité touchant ces entités.

(19) Les États membres devraient aider les entités critiques à renforcer leur résilience, conformément à leurs obligations en vertu de la présente directive, sans préjudice de la responsabilité juridique qui incombe aux entités de garantir le respect de ces obligations. En particulier, les États membres pourraient élaborer des documents d'orientation et des méthodologies, apporter leur soutien à l'organisation d'exercices visant à tester la résilience et dispenser des formations au personnel des entités critiques. En outre, compte tenu des interdépendances entre les entités et les secteurs, les États membres devraient mettre en place des outils de partage d'informations pour favoriser le partage volontaire d'informations entre les entités critiques, sans préjudice de l'application des règles de concurrence énoncées dans le traité sur le fonctionnement de l'Union européenne.

(20) Pour être en mesure de garantir leur résilience, les entités critiques devraient avoir une connaissance approfondie de tous les risques pertinents auxquels elles sont exposées et les analyser. À cette fin, elles devraient procéder à des évaluations des risques, chaque fois que cela s'avère nécessaire compte tenu de leur situation particulière et de l'évolution de ces risques, et, en tout cas, tous les quatre ans. Les évaluations des risques effectuées par les entités critiques devraient se fonder sur l'évaluation des risques effectuée par les États membres.

(21) Les entités critiques devraient adopter des mesures organisationnelles et techniques appropriées et proportionnées aux risques auxquels elles sont confrontées, de manière à prévenir tout incident, à y résister, à l'atténuer, à l'absorber, à s'y adapter et à s'en remettre. Bien que les entités critiques soient tenues de prendre des mesures sur tous les points précisés dans la présente directive, les détails et la portée de ces mesures devraient refléter de manière appropriée et proportionnée les différents risques que chaque entité a recensés dans le cadre de son évaluation des risques et en fonction de ses spécificités.

(22) Dans un souci d'efficacité et de responsabilité, les entités critiques devraient décrire ces mesures avec un niveau de détail suffisant pour atteindre ces objectifs, eu égard aux risques identifiés, dans un plan de résilience ou dans un ou plusieurs documents équivalents, et appliquer ce plan dans la pratique. Ce ou ces documents équivalents peuvent être établis conformément aux exigences et normes élaborées dans le contexte des accords internationaux sur la protection physique auxquels les États membres sont parties, y compris, le cas échéant, la convention sur la protection physique des matières nucléaires et des installations nucléaires.

(23) Le règlement (CE) nº 300/2008 du Parlement européen et du Conseil[28], le règlement (CE) nº 725/2004 du Parlement européen et du Conseil[29] et la directive nº 2005/65/CE du Parlement européen et du Conseil[30] définissent des exigences applicables aux entités des secteurs de l'aviation et du transport maritime afin de prévenir les incidents causés par des actes illicites, d'y résister et d'en atténuer les conséquences. Bien que les mesures requises par la présente directive soient plus vastes en termes de risques pris en compte et de types de mesures devant être adoptées, les entités critiques de ces secteurs devraient refléter dans leur plan de résilience ou dans les documents équivalents les mesures prises en application de ces autres actes de l'Union. En outre, lorsqu'elles mettent en œuvre des mesures de résilience au titre de la présente directive, les entités critiques peuvent envisager de se référer à des lignes directrices non contraignantes et à des documents de bonnes pratiques élaborés dans le cadre de groupes de travail sectoriels, tels que la plateforme de l'UE en matière de sûreté des voyageurs ferroviaires[31].

(24) Le risque que des membres du personnel des entités critiques utilisent de manière abusive, par exemple, leurs droits d'accès au sein de l'organisation de l'entité pour nuire et causer un préjudice est de plus en plus préoccupant. Ce risque est aggravé par le phénomène croissant de radicalisation conduisant à l'extrémisme violent et au terrorisme. Il est donc nécessaire de permettre aux entités critiques de demander une vérification des antécédents de personnes relevant de catégories spécifiques de leur personnel et de veiller à ce que ces demandes soient évaluées rapidement par les

---

28 Règlement (CE) nº 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) nº 2320/2002 (JO L 97 du 9.4.2008, p. 72).

29 Règlement (CE) nº 725/2004 du Parlement européen et du Conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires (JO L 129 du 29.4.2004, p. 6).

30 Directive 2005/65/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à l'amélioration de la sûreté des ports (JO L 310 du 25.11.2005, p. 28).

31 Décision de la Commission du 29 juin 2018 portant création de la plateforme de l'Union européenne en matière de sûreté des voyageurs ferroviaires (C/2018/4014).

autorités compétentes, conformément aux règles applicables du droit de l'Union et du droit national, y compris en matière de protection des données à caractère personnel.

(25) Les entités critiques devraient notifier aux autorités compétentes des États membres, dès qu'elles sont raisonnablement en mesure de le faire compte tenu des circonstances, les incidents qui perturbent ou sont susceptibles de perturber de manière significative leurs activités. La notification devrait permettre aux autorités compétentes de réagir rapidement et de manière adéquate aux incidents et de disposer d'une vue d'ensemble complète des risques globaux auxquels sont confrontées les entités critiques. À cette fin, il convient d'établir une procédure de notification de certains incidents et de définir des paramètres permettant de déterminer quand la perturbation réelle ou potentielle est importante et requiert une notification des incidents. Compte tenu des incidences transfrontières potentielles de telles perturbations, il convient de mettre en place une procédure permettant aux États membres d'informer les autres États membres concernés par l'intermédiaire de points de contact uniques.

(26) Si les entités critiques exercent généralement leurs activités dans le cadre d'un réseau de fourniture de services et d'infrastructures de plus en plus interconnecté et fournissent souvent des services essentiels dans plus d'un État membre, certaines de ces entités revêtent une importance particulière pour l'Union car elles fournissent des services essentiels à un grand nombre d'États membres et nécessitent donc une surveillance spécifique au niveau de l'Union. Il y a donc lieu d'établir des règles relatives à la surveillance spécifique de ces entités critiques revêtant une importance européenne particulière. Ces règles sont sans préjudice des règles de surveillance et de coercition énoncées dans la présente directive.

(27) Lorsqu'un État membre estime que des informations supplémentaires sont nécessaires pour conseiller une entité critique en vue du respect de ses obligations au titre du chapitre III ou pour évaluer le respect de ces obligations par une entité critique revêtant une importance européenne particulière, la Commission devrait organiser une mission de conseil, afin d'évaluer les mesures mises en place par cette entité, en accord avec l'État membre dans lequel l'infrastructure de cette entité est située. Afin de garantir la bonne exécution de ces missions de conseil, il convient d'établir des règles complémentaires, notamment en ce qui concerne leur organisation et leur déroulement, les suites à leur donner et les obligations incombant aux entités critiques revêtant une importance européenne particulière concernées. Sans préjudice de la nécessité pour l'État membre dans lequel la mission de conseil est organisée et pour l'entité concernée de se conformer aux règles de la présente directive, les missions de conseil devraient être menées dans le respect des règles détaillées du droit de cet État membre, par exemple en ce qui concerne les conditions précises à remplir pour obtenir l'accès aux locaux ou aux documents pertinents et les voies de recours juridictionnel. L'expertise spécifique requise pour de telles missions pourrait, selon les besoins, être demandée par l'intermédiaire du Centre de coordination de la réaction d'urgence.

(28) Afin de soutenir la Commission et de faciliter la coopération stratégique et l'échange d'informations, y compris des bonnes pratiques, sur les questions liées à la présente directive, il convient de créer un groupe sur la résilience des entités critiques, c'est-à-dire un groupe d'experts de la Commission. Les États membres devraient s'efforcer d'assurer une coopération effective et efficace des représentants désignés de leurs autorités compétentes au sein du groupe sur la résilience des entités critiques. Le groupe devrait commencer à s'acquitter de ses tâches six mois après l'entrée en

vigueur de la présente directive, de manière à mettre à disposition des moyens supplémentaires pour une coopération appropriée pendant la période de transposition de la présente directive.

(29) Afin d'atteindre les objectifs de la présente directive, et sans préjudice de la responsabilité juridique qui incombe aux États membres et aux entités critiques de veiller au respect de leurs obligations respectives qui y sont énoncées, la Commission devrait, lorsqu'elle le juge opportun, entreprendre certaines activités de soutien visant à faciliter le respect de ces obligations. Lorsqu'elle apporte un soutien aux États membres et aux entités critiques dans la mise en œuvre des obligations découlant de la présente directive, la Commission devrait s'appuyer sur les structures et outils existants, tels que ceux relevant du mécanisme de protection civile de l'Union et du réseau européen de référence pour la protection des infrastructures critiques.

(30) Les États membres devraient veiller à ce que leurs autorités compétentes disposent de certains pouvoirs spécifiques pour assurer la bonne application et le contrôle du respect de la présente directive à l'égard des entités critiques, lorsque ces entités relèvent de leur compétence conformément à la présente directive. Ces pouvoirs devraient notamment comprendre le pouvoir d'effectuer des inspections, une surveillance et des audits, d'exiger des entités critiques qu'elles fournissent des informations et des éléments de preuve concernant les mesures qu'elles ont prises pour se conformer à leurs obligations et, s'il y a lieu, d'adresser des injonctions afin qu'il soit remédié aux violations constatées. Lorsqu'ils adressent de telles injonctions, les États membres ne devraient pas exiger de mesures allant au-delà de ce qui est nécessaire et proportionné pour garantir le respect par l'entité critique concernée de ses obligations, compte tenu notamment de la gravité de la violation et de la capacité économique de l'entité critique. Plus généralement, ces pouvoirs devraient s'accompagner de garanties appropriées et effectives, devant être précisées dans le droit national, conformément aux exigences découlant de la charte des droits fondamentaux de l'Union européenne. Lorsqu'elles évaluent le respect par les entités critiques des obligations qui leur incombent en vertu de la présente directive, les autorités compétentes désignées au titre de la présente directive devraient pouvoir demander aux autorités compétentes désignées en vertu de la directive SRI 2 d'évaluer la cybersécurité de ces entités. Les autorités compétentes devraient coopérer et échanger des informations à cette fin.

(31) Afin de tenir compte des nouveaux risques, des évolutions technologiques ou des spécificités d'un ou de plusieurs des secteurs, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne pour compléter les mesures de résilience que les entités critiques doivent prendre, en précisant davantage certaines ou l'ensemble de ces mesures. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer»[32]. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États

[32] JO L 123 du 12.5.2016, p. 1.

membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

(32) Afin d'assurer des conditions uniformes d'exécution de la présente directive, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées conformément au règlement (UE) nº 182/2011 du Parlement européen et du Conseil[33].

(33) Étant donné que les objectifs de la présente directive, à savoir garantir la fourniture de services essentiels en vue du maintien de fonctions sociétales ou d'activités économiques vitales dans le marché intérieur et améliorer la résilience des entités critiques qui fournissent ces services, ne peuvent pas être atteints de manière suffisante par les États membres mais peuvent, en raison des effets de l'action, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé à l'article 5, la présente directive n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(34) Il convient donc d'abroger la directive 2008/114/CE,

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

CHAPITRE I

OBJET, CHAMP D'APPLICATION ET DEFINITIONS

Article premier

Objet et champ d'application

1. La présente directive:

(a) impose aux États membres l'obligation d'adopter certaines mesures visant à assurer la fourniture dans le marché intérieur de services essentiels au maintien de fonctions sociétales ou d'activités économiques vitales, en particulier de recenser les entités critiques et les entités devant être traitées comme équivalentes à certains égards, et de leur permettre de s'acquitter de leurs obligations;

(b) impose aux entités critiques des obligations visant à renforcer leur résilience et à améliorer leur capacité à fournir ces services dans le marché intérieur;

[33] Règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

(c) établit des règles concernant la surveillance et la coercition des entités critiques, ainsi que la surveillance spécifique des entités critiques considérées comme revêtant une importance européenne particulière.

2. La présente directive ne s'applique pas aux questions couvertes par la directive (UE) XX/YY [proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 (la «directive SRI 2»)], sans préjudice de l'article 7.

3. Lorsque des dispositions d'actes sectoriels du droit de l'Union exigent des entités critiques qu'elles adoptent des mesures prévues au chapitre III, et lorsque ces exigences sont au moins équivalentes aux obligations prévues par la présente directive, les dispositions pertinentes de la présente directive ne s'appliquent pas , y compris les dispositions relatives à la surveillance et à la coercition prévues au chapitre VI.

4. Sans préjudice de l'article 346 du traité sur le fonctionnement de l'Union européenne, les informations considérées comme confidentielles en application de la réglementation nationale ou de l'Union, telle que les règles applicables au secret des affaires, ne peuvent faire l'objet d'un échange avec la Commission et d'autres autorités concernées que si cet échange est nécessaire à l'application de la présente directive. Les informations échangées se limitent au minimum nécessaire et sont proportionnées à l'objectif de cet échange. Cet échange d'informations préserve la confidentialité des informations concernées et protège la sécurité et les intérêts commerciaux des entités critiques.

Article 2

Définitions

Aux fins de la présente directive, on entend par:

(1) «entité critique»: une entité publique ou privée d'un type visé à l'annexe, qui a été recensée comme telle par un État membre conformément à l'article 5;

(2) «résilience»: la capacité de prévenir tout incident qui perturbe ou est susceptible de perturber les activités d'une entité critique, d'y résister, de l'atténuer, de l'absorber, de s'y adapter et de s'en remettre;

(3) «incident»: tout événement susceptible de perturber ou perturbant les activités de l'entité critique;

(4) «infrastructure»: un bien, un système ou une partie de celui-ci, qui est nécessaire à la fourniture d'un service essentiel;

(5) «service essentiel»: un service qui est essentiel au maintien de fonctions sociétales ou d'activités économiques vitales;

(6) «risque»: toute circonstance ou tout événement ayant une incidence négative potentielle sur la résilience des entités critiques;

(7) «évaluation des risques»: une méthode visant à déterminer la nature et l'ampleur d'un risque en analysant les menaces et dangers potentiels et en évaluant les conditions de vulnérabilité existantes qui pourraient perturber les activités de l'entité critique.

CHAPITRE II

CADRES NATIONAUX POUR LA RESILIENCE DES ENTITES CRITIQUES

Article 3

Stratégie en faveur de la résilience des entités critiques

1. Chaque État membre adopte, au plus tard le [trois ans après l'entrée en vigueur de la présente directive], une stratégie visant à renforcer la résilience des entités critiques. Cette stratégie définit des objectifs stratégiques et des mesures en vue d'atteindre et de maintenir un niveau élevé de résilience de ces entités critiques et couvrant au moins les secteurs mentionnés dans l'annexe.

2. La stratégie contient au minimum les éléments suivants:

   (a) les objectifs et priorités stratégiques aux fins de renforcer la résilience globale des entités critiques, compte tenu des interdépendances transfrontières et transsectorielles;

   (b) un cadre de gouvernance permettant d'atteindre les objectifs et priorités stratégiques, y compris une description des rôles et des responsabilités des différentes autorités, entités critiques et autres parties participant à la mise en œuvre de la stratégie;

   (c) une description des mesures nécessaires pour renforcer la résilience globale des entités critiques, y compris une évaluation nationale des risques, le recensement des entités critiques et des entités équivalentes, et les mesures de soutien aux entités critiques prises conformément au présent chapitre;

   (d) un cadre d'action visant une coordination renforcée entre les autorités compétentes désignées en vertu de l'article 8 de la présente directive et en vertu de [la directive SIR 2] aux fins du partage d'informations sur les incidents et les cybermenaces et de l'exercice des tâches de surveillance.

   La stratégie est mise à jour selon les besoins et au moins tous les quatre ans.

3. Les États membres communiquent leurs stratégies et leurs éventuelles mises à jour à la Commission dans un délai de trois mois suivant leur adoption.

Article 4

Évaluation des risques par les États membres

1. Les autorités compétentes désignées en vertu de l'article 8 établissent une liste des services essentiels dans les secteurs mentionnés à l'annexe. Elles effectuent, au plus tard le [trois ans après l'entrée en vigueur de la présente directive], puis selon les besoins, et au moins tous les quatre ans, une évaluation de tous les risques pertinents susceptibles d'affecter la fourniture de ces services essentiels, en vue de recenser les entités critiques conformément à l'article 5, paragraphe 1, et d'aider celles-ci à prendre des mesures au titre de l'article 11.

   L'évaluation des risques tient compte de tous les risques naturels et d'origine humaine, y compris les accidents, les catastrophes naturelles, les urgences de santé publique et les menaces antagonistes, dont les infractions terroristes au sens de la directive (UE) 2017/541 du Parlement européen et du Conseil[34].

2. Lorsqu'ils procèdent à l'évaluation des risques, les États membres tiennent compte au minimum des éléments suivants:

   (a) l'évaluation générale des risques effectuée conformément à l'article 6, paragraphe 1, de la décision nº 1313/2013/UE du Parlement européen et du Conseil[35];

   (b) d'autres évaluations pertinentes des risques effectuées conformément aux exigences des actes sectoriels pertinents du droit de l'Union, y compris le règlement (UE) 2019/941 du Parlement européen et du Conseil[36] et le règlement (UE) 2017/1938 du Parlement européen et du Conseil[37];

   (c) les risques découlant des dépendances entre les secteurs mentionnés à l'annexe, y compris à l'égard des autres États membres et des pays tiers, et l'incidence qu'une perturbation dans un secteur peut avoir sur d'autres secteurs;

   (d) toute information sur les incidents notifiés conformément à l'article 13.

   Aux fins du premier alinéa, point c), les États membres coopèrent, s'il y a lieu, avec les autorités compétentes d'autres États membres et de pays tiers.

3. Les États membres mettent les éléments pertinents de l'évaluation des risques visée au paragraphe 1 à la disposition des entités critiques qu'ils ont recensées conformément à l'article 5 afin de les aider à réaliser leur évaluation des risques,

---

34 Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil (JO L 88 du 31.3.2017, p. 6).

35 Décision nº 1313/2013/UE du Parlement européen et du Conseil du 17 décembre 2013 relative au mécanisme de protection civile de l'Union (JO L 347 du 20.12.2013, p. 924).

36 Règlement (UE) 2019/941 du Parlement européen et du Conseil du 5 juin 2019 sur la préparation aux risques dans le secteur de l'électricité et abrogeant la directive 2005/89/CE (JO L 158 du 14.6.2019, p. 1).

37 Règlement (UE) 2017/1938 du Parlement européen et du Conseil du 25 octobre 2017 concernant des mesures visant à garantir la sécurité de l'approvisionnement en gaz naturel et abrogeant le règlement (UE) nº 994/2010 (JO L 280 du 28.10.2017, p. 1).

conformément à l'article 10, et à prendre des mesures pour assurer leur résilience conformément à l'article 11.

4. Chaque État membre fournit à la Commission des données sur les types de risques recensés et les résultats des évaluations des risques, par secteur et sous-secteur mentionné à l'annexe, au plus tard le [trois ans après l'entrée en vigueur de la présente directive], puis selon les besoins et au moins tous les quatre ans.

5. La Commission peut, en coopération avec les États membres, élaborer un modèle commun de rapport facultatif aux fins du paragraphe 4.

Article 5

Recensement des entités critiques

1. Au plus tard le [trois ans et trois mois après l'entrée en vigueur de la présente directive], les États membres recensent les entités critiques, pour chacun des secteurs et sous-secteurs mentionnés à l'annexe, autres que ceux mentionnés aux points 3, 4 et 8.

2. Lorsqu'ils recensent les entités critiques conformément au paragraphe 1, les États membres tiennent compte des résultats de l'évaluation des risques effectuée au titre de l'article 4 et appliquent les critères suivants:

   (a) l'entité fournit un ou plusieurs services essentiels;

   (b) la fourniture de ce service dépend de l'infrastructure située dans l'État membre; et

   (c) un incident aurait des effets perturbateurs importants sur la fourniture dudit service ou d'autres services essentiels dans les secteurs mentionnés à l'annexe qui dépendent dudit service.

3. Chaque État membre dresse une liste des entités critiques recensées et veille à ce que ces entités critiques reçoivent la notification de leur recensement en tant qu'entités critiques dans un délai d'un mois à compter de ce recensement et soient informées des obligations qui leur incombent en vertu des chapitres II et III et de la date à partir de laquelle les dispositions de ces chapitres s'appliquent à elles.

   Les dispositions du présent chapitre s'appliquent aux entités critiques concernées à compter de la date de la notification et les dispositions du chapitre III s'appliquent six mois après cette date.

4. Les États membres veillent à ce que leurs autorités compétentes désignées en vertu de l'article 8 de la présente directive notifient aux autorités compétentes désignées conformément à l'article 8 de la [directive SRI 2] l'identité des entités critiques qu'ils ont recensées au titre du présent article dans un délai d'un mois à compter de ce recensement.

5. À la suite de la notification visée au paragraphe 3, les États membres veillent à ce que les entités critiques communiquent à leurs autorités compétentes désignées

conformément à l'article 8 de la présente directive des informations spécifiant si elles ont été recensées en tant qu'entités critiques dans un ou plusieurs autres États membres. Lorsqu'une entité a été recensée en tant qu'entité critique par deux États membres ou plus, ces États membres se consultent en vue de réduire la charge pesant sur l'entité critique en ce qui concerne les obligations prévues au chapitre III.

6. Aux fins du chapitre IV, les États membres veillent à ce qu'à la suite de la notification visée au paragraphe 3, les entités critiques communiquent à leurs autorités compétentes désignées conformément à l'article 8 de la présente directive des informations précisant si elles fournissent des services essentiels à ou dans plus d'un tiers des États membres. Lorsque tel est le cas, l'État membre concerné notifie dans les meilleurs délais à la Commission l'identité de ces entités critiques.

7. Si nécessaire et en tout cas au moins tous les quatre ans, les États membres réexaminent et, s'il y a lieu, mettent à jour la liste des entités critiques recensées.

Lorsque ces mises à jour entraînent le recensement d'entités critiques supplémentaires, les paragraphes 3, 4, 5 et 6 s'appliquent. En outre, les États membres veillent à ce que les entités qui ne sont plus recensées en tant qu'entités critiques en vertu d'une telle mise à jour en reçoivent la notification et soient informées qu'elles ne sont plus soumises aux obligations prévues au chapitre III dès la réception de la notification.

Article 6

Effet perturbateur important

1. Lorsque les États membres déterminent l'importance d'un effet perturbateur visé à l'article 5, paragraphe 2, point c), ils prennent en compte les critères suivants:

(a) le nombre d'utilisateurs tributaires du service fourni par l'entité;

(b) la dépendance d'autres secteurs mentionnés à l'annexe à l'égard dudit service;

(c) les conséquences que des incidents pourraient avoir, en termes de degré et de durée, sur les fonctions économiques et sociétales, sur l'environnement et sur la sûreté publique;

(d) la part de marché de l'entité sur le marché de ce service;

(e) la zone géographique susceptible d'être touchée par un incident, y compris eu égard à toute incidence transfrontière;

(f) l'importance que revêt l'entité pour garantir un niveau de service suffisant, compte tenu de la disponibilité de solutions de rechange pour la fourniture de ce service.

2. Les États membres communiquent à la Commission, au plus tard le [trois ans et trois mois après l'entrée en vigueur de la présente directive], les informations suivantes:

(a) la liste des services visée à l'article 4, paragraphe 1;

(b) le nombre d'entités critiques recensées dans chacun des secteurs et sous-secteurs mentionnés à l'annexe et le ou les services visés à l'article 4, paragraphe 1, que chaque entité fournit;

(c) tout seuil appliqué en vue de préciser un ou plusieurs des critères énoncés au paragraphe 1.

Par la suite, ils communiquent ces informations selon les besoins et au moins tous les quatre ans.

3. Après consultation du groupe sur la résilience des entités critiques, la Commission peut adopter des lignes directrices afin de faciliter l'application des critères visés au paragraphe 1, en tenant compte des informations visées au paragraphe 2.

Article 7

Entités équivalentes aux entités critiques dans le cadre du présent chapitre

1. En ce qui concerne les secteurs mentionnés aux points 3, 4 et 8 de l'annexe, les États membres recensent, au plus tard le [trois ans et trois mois après l'entrée en vigueur de la présente directive], les entités qui sont considérées comme équivalentes aux entités critiques aux fins du présent chapitre. Ils appliquent, à l'égard de ces entités, les dispositions de l'article 3, de l'article 4, de l'article 5, paragraphes 1 à 4 et paragraphe 7, et de l'article 9.

2. En ce qui concerne les entités des secteurs mentionnés aux points 3 et 4 de l'annexe recensées conformément au paragraphe 1, les États membres veillent à ce qu'aux fins de l'application de l'article 8, paragraphe 1, les autorités compétentes désignées soient les autorités compétentes désignées conformément à l'article 41 du [règlement sur la résilience opérationnelle numérique du secteur financier].

3. Les États membres veillent à ce que les entités visées au paragraphe 1 soient informées dans les meilleurs délais de leur recensement en tant qu'entités visées au présent article.

Article 8

Autorités compétentes et point de contact unique

1. Chaque État membre désigne une ou plusieurs autorités compétentes chargées de veiller à l'application correcte des règles énoncées dans la présente directive au niveau national et, s'il y a lieu, de faire respecter ces règles (l'«autorité compétente»). Les États membres peuvent désigner une ou des autorités existantes.

Lorsqu'ils désignent plus d'une autorité, ils définissent clairement les tâches respectives des autorités concernées et veillent à ce qu'elles coopèrent efficacement pour accomplir les tâches qui leur incombent en vertu de la présente directive, y compris en ce qui concerne la désignation et les activités du point de contact unique visé au paragraphe 2.

2. Chaque État membre désigne, au sein de l'autorité compétente, un point de contact unique chargé d'exercer une fonction de liaison afin d'assurer la coopération

transfrontière avec les autorités compétentes des autres États membres et avec le groupe sur la résilience des entités critiques visé à l'article 16 (le «point de contact unique»).

3. Au plus tard le [trois ans et six mois après l'entrée en vigueur de la présente directive], et tous les ans par la suite, les points de contact uniques présentent à la Commission et au groupe sur la résilience des entités critiques un rapport de synthèse sur les notifications reçues, mentionnant le nombre de notifications, la nature des incidents signalés et les mesures prises conformément à l'article 13, paragraphe 3.

4. Chaque État membre veille à ce que l'autorité compétente, y compris le point de contact unique désigné, dispose des pouvoirs et des ressources financières, humaines et techniques nécessaires pour accomplir, de manière efficace et efficiente, les tâches qui lui sont assignées.

5. Les États membres font en sorte que leurs autorités compétentes, s'il y a lieu, et conformément au droit de l'Union et au droit national, consultent les autres autorités nationales concernées, en particulier celles chargées de la protection civile, de la répression et de la protection des données à caractère personnel, ainsi que les parties intéressées concernées, y compris les entités critiques, et coopèrent avec elles.

6. Les États membres veillent à ce que leurs autorités compétentes désignées en vertu du présent article coopèrent avec les autorités compétentes désignées en vertu de [la directive SRI 2] sur les risques et incidents de cybersécurité concernant les entités critiques, ainsi que sur les mesures adoptées par les autorités compétentes désignées en vertu de [la directive SRI 2] qui sont pertinentes pour les entités critiques.

7. Chaque État membre notifie à la Commission la désignation de l'autorité compétente et du point de contact unique dans un délai de trois mois à compter de cette désignation, y compris les tâches et responsabilités précises qui leur incombent en vertu de la présente directive, leurs coordonnées, ainsi que toute modification ultérieure dans ce cadre. Chaque État membre rend publique la désignation de l'autorité compétente et du point de contact unique.

8. La Commission publie la liste des points de contact uniques des États membres.

Article 9

Soutien des États membres aux entités critiques

1. Les États membres aident les entités critiques à renforcer leur résilience. Dans ce cadre, ils peuvent élaborer des documents d'orientation et des méthodologies, apporter leur soutien à l'organisation d'exercices visant à tester la résilience et dispenser des formations au personnel des entités critiques.

2. Les États membres veillent à ce que les autorités compétentes coopèrent et échangent des informations et des bonnes pratiques avec les entités critiques des secteurs mentionnés à l'annexe.

3. Les États membres mettent en place des outils de partage d'informations pour faciliter le partage volontaire d'informations entre les entités critiques sur les

questions couvertes par la présente directive, conformément au droit de l'Union et au droit national en matière, en particulier, de concurrence et de protection des données à caractère personnel.

CHAPITRE III

RESILIENCE DES ENTITES CRITIQUES

Article 10

Évaluation des risques par les entités critiques

Les États membres veillent à ce que les entités critiques évaluent tous les risques pertinents susceptibles de perturber leurs activités, dans un délai de six mois à compter de la réception de la notification visée à l'article 5, paragraphe 3, puis selon les besoins et au moins tous les quatre ans, sur la base des évaluations des risques des États membres et d'autres sources d'information pertinentes.

L'évaluation des risques tient compte de tous les risques pertinents visés à l'article 4, paragraphe 1, susceptibles d'entraîner une perturbation de la fourniture de services essentiels. Elle tient compte de toute dépendance d'autres secteurs mentionnés à l'annexe à l'égard du service essentiel fourni par l'entité critique, y compris dans les États membres voisins et les pays tiers, le cas échéant, et de l'incidence qu'une perturbation de la fourniture de services essentiels dans un ou plusieurs de ces secteurs peut avoir sur le service essentiel fourni par l'entité critique.

Article 11

Mesures de résilience des entités critiques

1. Les États membres veillent à ce que les entités critiques prennent des mesures techniques et organisationnelles appropriées et proportionnées pour assurer leur résilience, y compris des mesures nécessaires pour:

   (a) prévenir les incidents, y compris au moyen de mesures de réduction des risques de catastrophe et d'adaptation au changement climatique;

   (b) assurer une protection physique adéquate des zones, installations et autres infrastructures sensibles, notamment par des clôtures, des barrières, des outils et procédures de surveillance des enceintes, ainsi que par des équipements de détection et de contrôle des accès;

   (c) résister aux conséquences des incidents et les atténuer, y compris par la mise en œuvre de procédures et protocoles de gestion des risques et des crises et de procédures d'alerte;

(d) se remettre des incidents, y compris grâce à des mesures assurant la continuité des activités et à l'identification d'autres chaînes d'approvisionnement;

(e) assurer une gestion adéquate de la sécurité du personnel, notamment en définissant des catégories de personnel exerçant des fonctions critiques, en établissant des droits d'accès aux zones, installations et autres infrastructures sensibles, de même qu'aux informations sensibles, ainsi qu'en identifiant des catégories spécifiques de personnel eu égard à l'article 12;

(f) sensibiliser le personnel concerné aux mesures visées aux points a) à e).

2. Les États membres veillent à ce que les entités critiques aient mis en place et appliquent un plan de résilience ou un ou des documents équivalents, décrivant en détail les mesures visées au paragraphe 1. Lorsque des entités critiques ont pris des mesures en vertu d'obligations figurant dans d'autres actes du droit de l'Union qui sont également pertinentes pour les mesures visées au paragraphe 1, elles décrivent également ces mesures dans le plan de résilience ou dans le ou les documents équivalents.

3. À la demande de l'État membre qui a recensé l'entité critique et avec l'accord de celle-ci, la Commission organise des missions de conseil, conformément aux dispositions de l'article 15, paragraphes 4, 5, 7 et 8, afin de conseiller l'entité critique concernée en vue du respect des obligations qui lui incombent en vertu du chapitre III. La mission de conseil communique ses conclusions à la Commission, à l'État membre et à l'entité critique concernée.

4. La Commission est habilitée à adopter des actes délégués conformément à l'article 21 qui complètent le paragraphe 1 en établissant des règles détaillées précisant certaines ou l'ensemble des mesures à prendre en vertu dudit paragraphe. Elle adopte ces actes délégués dans la mesure nécessaire à l'application effective et cohérente dudit paragraphe conformément aux objectifs de la présente directive, compte tenu de toute évolution pertinente des risques, de la technologie ou de la fourniture des services concernés, ainsi que de toute spécificité relative à des secteurs et types d'entités particuliers.

5. La Commission adopte des actes d'exécution afin d'établir les spécifications techniques et méthodologiques nécessaires relatives à l'application des mesures visées au paragraphe 1. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 20, paragraphe 2.

Article 12

Vérification des antécédents

1. Les États membres veillent à ce que les entités critiques puissent soumettre des demandes de vérification des antécédents des personnes qui font partie de certaines catégories spécifiques de leur personnel, y compris les personnes dont le recrutement est envisagé à des postes relevant de ces catégories, et à ce que ces demandes soient évaluées rapidement par les autorités chargées de procéder à cette vérification.

2. Conformément au droit de l'Union et au droit national applicables, y compris le règlement (UE) 2016/679 du Parlement européen et du Conseil [38], la vérification des antécédents visée au paragraphe 1:

(a) établit l'identité de la personne sur la base de documents;

(b) prend en considération les éventuels antécédents judiciaires des cinq dernières années au minimum et des dix dernières années au maximum, relatifs aux infractions à prendre en compte pour le recrutement à un poste donné, dans l'État membre ou les États membres dont la personne a la nationalité, ainsi que dans tout État membre ou pays tiers de résidence au cours de cette période;

(c) prend en considération les emplois antérieurs, les études et les hiatus éventuels dans le parcours de formation ou d'emploi figurant dans le curriculum vitae de la personne, au cours des cinq dernières années au moins et des dix dernières années au plus.

En ce qui concerne le point b) du premier alinéa, les États membres veillent à ce que leurs autorités chargées de la vérification des antécédents obtiennent les informations relatives au casier judiciaire auprès d'autres États membres par l'intermédiaire de l'ECRIS, conformément aux procédures prévues dans la décision-cadre 2009/315/JAI du Conseil et, s'il y a lieu, dans le règlement (UE) 2019/816 du Parlement européen et du Conseil[39]. Les autorités centrales visées à l'article 3 de ladite décision-cadre et à l'article 3, paragraphe 5, dudit règlement répondent aux demandes d'informations dans un délai de dix jours ouvrables à compter de la date de réception de la demande.

3. Conformément au droit de l'Union et au droit national applicables, y compris le règlement (UE) 2016/679, chaque État membre veille à ce que la vérification des antécédents visée au paragraphe 1 puisse également être élargie, sur la base d'une demande dûment justifiée de l'entité critique, pour inclure des éléments de renseignement et d'autres informations objectives disponibles qui pourraient être nécessaires pour déterminer si la personne concernée convient pour le poste pour lequel l'entité critique a demandé une vérification élargie des antécédents.

Article 13

Notification d'incident

1. Les États membres veillent à ce que les entités critiques notifient dans les meilleurs délais à l'autorité compétente les incidents qui perturbent ou sont susceptibles de perturber de manière significative leurs activités. Les notifications comprennent toutes les informations disponibles nécessaires pour permettre à l'autorité compétente de comprendre la nature, la cause et les conséquences possibles de l'incident, y compris afin de déterminer tout impact transfrontière de l'incident. Cette notification n'accroît pas la responsabilité des entités critiques.

[38] JO L 119 du 4.5.2016, p. 1.
[39] JO L 135 du 22.5.2019, p. 1.

2. Afin de déterminer l'importance de la perturbation ou de la perturbation potentielle des activités de l'entité critique résultant d'un incident, les paramètres suivants sont, en particulier, pris en compte:

(a) le nombre d'utilisateurs touchés par la perturbation ou la perturbation potentielle;

(b) la durée de la perturbation ou la durée escomptée d'une perturbation potentielle;

(c) la zone géographique touchée par la perturbation ou la perturbation potentielle.

3. Sur la base des informations fournies dans la notification par l'entité critique, l'autorité compétente, par l'intermédiaire de son point de contact unique, informe le point de contact unique des autres États membres touchés, si l'incident a ou est susceptible d'avoir une incidence significative sur les entités critiques et sur la continuité de la fourniture des services essentiels dans un ou plusieurs autres États membres.

Ce faisant, les points de contact uniques doivent, dans le respect du droit de l'Union ou de la législation nationale conforme au droit de l'Union, traiter les informations de manière à en respecter la confidentialité et à préserver la sécurité et les intérêts commerciaux de l'entité critique concernée.

4. Dès que possible après réception de la notification visée au paragraphe 1, l'autorité compétente fournit à l'entité critique notifiante des informations pertinentes concernant les suites données à sa notification, y compris des informations susceptibles de l'aider à réagir efficacement à l'incident.

CHAPITRE IV

SURVEILLANCE SPECIFIQUE DES ENTITES CRITIQUES REVETANT UNE IMPORTANCE EUROPEENNE PARTICULIERE

Article 14

Entités critiques revêtant une importance européenne particulière

1. Les entités critiques revêtant une importance européenne particulière font l'objet d'une surveillance spécifique, conformément au présent chapitre.

2. Une entité est considérée comme une entité critique revêtant une importance européenne particulière lorsqu'elle a été identifiée en tant qu'entité critique, qu'elle fournit des services essentiels à ou dans plus d'un tiers des États membres et qu'elle a fait l'objet d'une notification à ce titre adressée à la Commission conformément à l'article 5, paragraphes 1 et 6, respectivement.

3. Dans les meilleurs délais après réception de la notification visée à l'article 5, paragraphe 6, la Commission adresse une notification à l'entité concernée lui signalant qu'elle est considérée comme une entité critique revêtant une importance européenne particulière et l'informant de ses obligations au titre du présent chapitre et de la date à partir de laquelle ces obligations s'appliquent à elle.

Les dispositions du présent chapitre s'appliquent à l'entité critique revêtant une importance européenne particulière concernée à partir de la date de réception de ladite notification.

Article 15

Surveillance spécifique

1. À la demande d'un ou de plusieurs États membres ou de la Commission, l'État membre dans lequel se situe l'infrastructure de l'entité critique revêtant une importance européenne particulière informe, conjointement avec ladite entité, la Commission et le groupe sur la résilience des entités critiques des résultats de l'évaluation des risques effectuée conformément à l'article 10 et des mesures prises conformément à l'article 11.

Ledit État membre informe également, dans les meilleurs délais, la Commission et le groupe sur la résilience des entités critiques de toute mesure de surveillance ou de coercition, y compris toute évaluation de la conformité ou toute injonction émise, adoptée par son autorité compétente en vertu des articles 18 et 19 à l'égard de ladite entité.

2. À la demande d'un ou de plusieurs États membres, ou de sa propre initiative, et en accord avec l'État membre où se situe l'infrastructure de l'entité critique revêtant une importance européenne particulière, la Commission organise une mission de conseil afin d'évaluer les mesures mises en place par l'entité pour s'acquitter des obligations qui lui incombent en vertu du chapitre III. Au besoin, la mission de conseil peut demander une expertise spécifique dans le domaine de la gestion des risques de catastrophe par l'intermédiaire du Centre de coordination de la réaction d'urgence.

3. La mission de conseil communique ses constatations dans un rapport transmis à la Commission, au groupe sur la résilience des entités critiques et à l'entité critique revêtant une importance européenne particulière concernée dans un délai de trois mois à compter de la fin de la mission.

Le groupe sur la résilience des entités critiques analyse le rapport et, s'il y a lieu, indique à la Commission si l'entité critique revêtant une importance européenne particulière concernée respecte les obligations qui lui incombent en vertu du chapitre III et, le cas échéant, lui conseille les mesures qui pourraient améliorer sa résilience.

Sur cette base, la Commission communique à l'État membre dans lequel l'infrastructure de cette entité est située, au groupe sur la résilience des entités critiques et à l'entité, son avis concernant le respect par l'entité de ses obligations au titre du chapitre III et, le cas échéant, concernant les mesures susceptibles d'être prises pour améliorer sa résilience.

Cet État membre tient dûment compte de cet avis et fournit à la Commission et au groupe sur la résilience des entités critiques des informations sur les mesures qu'il a adoptées à la suite de la communication.

4. Chaque mission de conseil est composée d'experts des États membres et de représentants de la Commission. Les États membres peuvent proposer des candidats susceptibles de faire partie d'une mission de conseil. La Commission sélectionne et nomme les membres de chaque mission de conseil sur la base de leurs compétences professionnelles et en veillant à garantir une représentation géographique équilibrée entre les États membres. La Commission prend en charge les coûts liés à la participation à la mission de conseil.

   La Commission organise le programme de la mission de conseil, en consultation avec les membres de la mission concernée et en accord avec l'État membre où se situe l'infrastructure de l'entité critique ou de l'entité critique revêtant une importance européenne particulière.

5. La Commission adopte un acte d'exécution établissant les règles relatives aux modalités de procédure pour la conduite et les rapports des missions de conseil. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 20, paragraphe 2.

6. Les États membres veillent à ce que l'entité critique revêtant une importance européenne particulière concernée accorde à la mission de conseil l'accès à l'ensemble des informations, systèmes et installations relatifs à ses services essentiels, nécessaire à l'exécution de ses tâches.

7. La mission de conseil est menée dans le respect du droit national applicable de l'État membre dans lequel l'infrastructure est située.

8. Lorsqu'elle organise les missions de conseil, la Commission tient compte des rapports de toute inspection qu'elle a effectuée en vertu du règlement (CE) nº 300/2008 et du règlement (CE) nº 725/2004, ainsi que des rapports de tout suivi effectué en vertu de la directive 2005/65/CE à l'égard de l'entité critique ou de l'entité critique revêtant une importance européenne particulière, selon le cas.

CHAPITRE V

COOPERATION ET RAPPORTS

Article 16

Groupe sur la résilience des entités critiques

1. Un groupe sur la résilience des entités critiques est créé avec effet au [six mois après l'entrée en vigueur de la présente directive]. Il assiste la Commission et facilite la coopération stratégique et l'échange d'informations sur les questions relatives à la présente directive.

2. Le groupe sur la résilience des entités critiques est composé de représentants des États membres et de la Commission. Lorsque c'est utile pour l'exécution de ses tâches, le groupe sur la résilience des entités critiques peut inviter des représentants des parties intéressées à participer à ses travaux.

Le représentant de la Commission préside le groupe sur la résilience des entités critiques.

3. Le groupe sur la résilience des entités critiques est chargé des tâches suivantes:

(a) soutenir la Commission lorsqu'elle aide les États membres à renforcer leur capacité à garantir la résilience des entités critiques conformément à la présente directive;

(b) évaluer les stratégies en faveur de la résilience des entités critiques visées à l'article 3 et déterminer les bonnes pratiques en ce qui concerne ces stratégies;

(c) faciliter l'échange de bonnes pratiques pour le recensement des entités critiques par les États membres conformément à l'article 5, y compris en ce qui concerne les dépendances transfrontières et les risques et incidents;

(d) contribuer, sur demande, à l'élaboration des lignes directrices visées à l'article 6, paragraphe 3, et de tout acte délégué et d'exécution au titre de la présente directive;

(e) examiner chaque année les rapports de synthèse visés à l'article 8, paragraphe 3;

(f) échanger les bonnes pratiques concernant l'échange d'informations en rapport avec la notification des incidents visée à l'article 13;

(g) analyser les rapports des missions de conseil et prodiguer des conseils conformément à l'article 15, paragraphe 3;

(h) échanger des informations et les bonnes pratiques en matière de recherche et de développement dans le domaine de la résilience des entités critiques conformément à la présente directive;

(i) s'il y a lieu, procéder à des échanges d'informations sur des questions relatives à la résilience des entités critiques avec les institutions, organes ou organismes de l'Union concernés.

4. Au plus tard le [24 mois après l'entrée en vigueur de la présente directive], puis tous les deux ans, le groupe sur la résilience des entités critiques établit un programme de travail prévoyant les actions à entreprendre pour réaliser ses objectifs et ses tâches, qui est cohérent avec les exigences et les objectifs de la présente directive.

5. Le groupe sur la résilience des entités critiques se réunit régulièrement et au moins une fois par an avec le groupe de coopération institué en vertu de [la directive SRI 2] afin de promouvoir la coopération stratégique et l'échange d'informations.

6. La Commission peut adopter des actes d'exécution fixant les modalités de procédure nécessaires au fonctionnement du groupe sur la résilience des entités critiques. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 20, paragraphe 2.

7. La Commission remet au groupe sur la résilience des entités critiques un rapport faisant la synthèse des informations communiquées par les États membres conformément à l'article 3, paragraphe 3, et à l'article 4, paragraphe 4, au plus tard le [trois ans et six mois après l'entrée en vigueur de la présente directive], puis selon les besoins et au moins tous les quatre ans.

Article 17

Soutien de la Commission aux autorités compétentes et aux entités critiques

1. La Commission aide, s'il y a lieu, les États membres et les entités critiques à se conformer aux obligations qui leur incombent en vertu de la présente directive, notamment en établissant, au niveau de l'Union, une vue d'ensemble des risques transfrontières et transsectoriels pesant sur la fourniture de services essentiels, en organisant les missions de conseil visées à l'article 11, paragraphe 3, et à l'article 15, paragraphe 3, et en facilitant l'échange d'informations entre experts dans l'ensemble de l'Union.

2. La Commission complète les activités des États membres visées à l'article 9 en élaborant des bonnes pratiques et des méthodes, ainsi que des activités de formation transfrontières et des exercices pour tester la résilience des entités critiques.

CHAPITRE VI

SURVEILLANCE ET COERCITION

Article 18

Mise en œuvre et coercition

1. Afin d'évaluer le respect des obligations découlant de la présente directive par les entités recensées en tant qu'entités critiques conformément à l'article 5, les États membres veillent à ce que les autorités compétentes disposent des pouvoirs et des moyens nécessaires pour:

   (a) procéder à des inspections sur site des locaux utilisés par l'entité critique pour fournir ses services essentiels et à la surveillance hors site des mesures adoptées par les entités critiques conformément à l'article 11;

   (b) effectuer ou ordonner des audits portant sur ces entités.

2. Les États membres veillent à ce que les autorités compétentes disposent des pouvoirs et des moyens pour exiger, lorsque l'exécution de leurs tâches au titre de la présente directive le requiert, que toute entité recensée en tant qu'entité critique en vertu du paragraphe 5 fournisse, dans un délai raisonnable fixé par ces autorités:

(a) les informations nécessaires pour évaluer si les mesures qu'elle a adoptées pour assurer sa résilience satisfont aux exigences de l'article 11;

(b) la preuve de la mise en œuvre effective de ces mesures, y compris les résultats d'un audit effectué par un auditeur indépendant et qualifié sélectionné par ladite entité et réalisé à ses frais.

Au moment de formuler une telle demande d'informations, les autorités compétentes mentionnent la finalité de la demande et précisent les informations exigées.

3. Sans préjudice de la possibilité d'imposer des sanctions conformément à l'article 19, les autorités compétentes peuvent, à la suite des mesures de surveillance visées au paragraphe 1 ou de l'évaluation des informations visées au paragraphe 2, enjoindre aux entités critiques concernées de prendre les mesures nécessaires et proportionnées pour remédier à toute violation constatée de la présente directive, dans un délai raisonnable fixé par ces autorités, et de leur fournir des informations sur les mesures prises. Ces injonctions tiennent compte, notamment, de la gravité de la violation.

4. L'État membre veille à ce que les pouvoirs prévus aux paragraphes 1, 2 et 3 ne puissent être exercés que sous réserve de garanties appropriées. Ces garanties font en sorte, en particulier, que les pouvoirs soient exercés de manière objective, transparente et proportionnée et que les droits et les intérêts légitimes des entités critiques concernées soient dûment protégés, y compris leur droit d'être entendues, leurs droits de la défense et leur droit à un recours effectif devant une juridiction indépendante.

5. Les États membres veillent, lorsqu'une autorité compétente évalue si une entité critique respecte ses obligations, conformément au présent article, à ce que ladite autorité en informe les autorités compétentes de l'État membre concerné désignées en vertu de [la directive SRI 2] et à ce qu'elle puisse demander à ces autorités d'évaluer la cybersécurité de cette entité, et de coopérer et d'échanger des informations à cette fin.

Article 19

Sanctions

Les États membres déterminent le régime des sanctions applicables aux violations des dispositions nationales adoptées conformément à la présente directive et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. Ces sanctions doivent être effectives, proportionnées et dissuasives. Les États membres informent la Commission, au plus tard [deux ans après l'entrée en vigueur de la présente directive], du régime ainsi déterminé et des mesures ainsi prises, de même que, sans retard, de toute modification apportée ultérieurement à ce régime ou à ces mesures.

CHAPITRE VII

DISPOSITIONS FINALES

Article 20

Procédure de comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) nº 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nº 182/2011 s'applique.

Article 21

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 11, paragraphe 4, est conféré à la Commission pour une période de cinq ans à compter de la date d'entrée en vigueur de la présente directive ou de toute autre date fixée par les colégislateurs.

3. La délégation de pouvoir visée à l'article 11, paragraphe 4, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer».

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 11, paragraphe 4, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

Article 22

Rapports et réexamen

La Commission présente au Parlement européen et au Conseil, au plus tard le [54 mois après l'entrée en vigueur de la présente directive], un rapport évaluant dans quelle mesure les États membres ont pris les dispositions nécessaires pour se conformer à la présente directive.

La Commission réexamine périodiquement le fonctionnement de la présente directive et en rend compte au Parlement européen et au Conseil. Le rapport évalue en particulier l'incidence et la valeur ajoutée de la présente directive qui a pour objet de garantir la résilience des entités critiques et détermine si le champ d'application de la directive devrait être étendu à d'autres secteurs ou sous-secteurs. Le premier rapport est présenté le [six ans après l'entrée en vigueur de la présente directive] et évalue en particulier si le champ d'application de la directive devrait être étendu au secteur de la production, de la transformation et de la distribution des denrées alimentaires.

Article 23

Abrogation de la directive 2008/114/CE

La directive 2008/114/CE est abrogée avec effet au [date d'entrée en vigueur de la présente directive].

Article 24

Transposition

1. Les États membres adoptent et publient, au plus tard le [18 mois après l'entrée en vigueur de la présente directive], les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive. Ils communiquent immédiatement à la Commission le texte de ces dispositions.

   Ils appliquent ces dispositions à partir du [deux ans après l'entrée en vigueur de la présente directive + un jour].

   Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

2. Les États membres communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine couvert par la présente directive.

Article 25

Entrée en vigueur

La présente directive entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Article 26

Destinataires

Les États membres sont destinataires de la présente directive.

Fait à Bruxelles, le

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL

sur la résilience des entités critiques

1.2. Domaine(s) politique(s) concerné(s)

Sécurité

1.3. La proposition/l'initiative porte sur:

☐ **une action nouvelle**

☐ **une action nouvelle suite à un projet pilote/une action préparatoire**[40]

☑ **la prolongation d'une action existante**

☐ **une fusion ou une réorientation d'une ou de plusieurs actions vers une autre action/une action nouvelle**

1.4. Objectif(s)

1.4.1. Objectif général/objectifs généraux

Les opérateurs d'infrastructures critiques fournissent des services dans un certain nombre de secteurs (tels que les transports, l'énergie, la santé, l'eau, etc.) qui sont nécessaires à des fonctions sociétales et à des activités économiques vitales. Les opérateurs doivent donc être résilients, c'est-à-dire bien protégés, mais aussi être en mesure de relancer rapidement leurs activités en cas de perturbation.

L'objectif général de la proposition consiste à renforcer la résilience de ces opérateurs (dénommés «entités critiques») face à une série de risques naturels et d'origine humaine, intentionnels et accidentels.

1.4.2. Objectif(s) spécifique(s)

L'initiative entend répondre à quatre objectifs spécifiques:

— garantir un meilleur niveau de connaissance des risques et des interdépendances auxquels les entités critiques sont confrontées, ainsi que des moyens d'y remédier;

— veiller à ce que toutes les entités concernées soient recensées en tant qu'«entités critiques» par les autorités des États membres;

[40] Tel(le) que visé(e) à l'article 58, paragraphe 2, point a) ou b), du règlement financier.

— veiller à ce que l'éventail complet des activités de résilience soit inclus dans les politiques publiques et les pratiques opérationnelles;

— renforcer les capacités et améliorer la coopération et la communication entre les parties prenantes.

Ces objectifs contribueront à la réalisation de l'objectif général de l'initiative.

1.4.3. Résultat(s) et incidence(s) attendus

Préciser les effets que la proposition/l'initiative devrait avoir sur les bénéficiaires/la population visée.

L'initiative devrait avoir des effets positifs sur la sécurité des entités critiques, qui seraient davantage résilientes aux risques et aux perturbations. Elles seraient en mesure de mieux atténuer les risques, de faire face aux perturbations potentielles et de réduire au minimum les incidences négatives en cas d'incident.

Une meilleure résilience des entités critiques signifie également que leurs activités seront plus fiables et que les services qu'elles fournissent dans de nombreux secteurs vitaux le seront de manière continue, ce qui contribuera au bon fonctionnement du marché intérieur. Ce bon fonctionnement aura à son tour une incidence positive pour le grand public et les entreprises, étant donné qu'ils dépendent de ces services dans leurs activités quotidiennes.

Les pouvoirs publics tireraient également profit de la stabilité découlant du bon fonctionnement des principales activités économiques et de la fourniture constante de services essentiels à leurs citoyens.

1.4.4. Indicateurs de performance

Préciser les indicateurs permettant de suivre l'avancement et les réalisations.

Les indicateurs permettant de suivre l'avancement et les réalisations seront liés aux objectifs spécifiques de l'initiative:

— le nombre et la portée des évaluations des risques réalisées par les autorités et les entités critiques constitueront un indicateur de la meilleure connaissance des risques par les acteurs clés;

— le nombre d'«entités critiques» recensées par les États membres reflétera l'exhaustivité de la portée des mesures prises à l'égard des infrastructures critiques;

— l'intégration de la résilience dans les politiques publiques et les pratiques opérationnelles sera reflétée dans les stratégies nationales et les mesures de résilience adoptées par les entités critiques;

— les améliorations en termes de capacité et de coopération seront évaluées sur la base des activités de renforcement des capacités et des initiatives de coopération qui seront mises en place.

1.5. Justification(s) de la proposition/de l'initiative

1.5.1. Besoin(s) à satisfaire à court ou à long terme, assorti(s) d'un calendrier détaillé pour la mise en œuvre de l'initiative

Pour satisfaire aux exigences de l'initiative, les États membres devront élaborer une stratégie portant sur la résilience des entités critiques, dans le court à moyen terme, procéder à une évaluation nationale des risques, et identifier les opérateurs qui peuvent être qualifiés d'«entités critiques» sur la base des résultats de l'évaluation des risques et des critères spécifiques. Ces activités seront réalisées régulièrement, selon les besoins, et au moins une fois tous les quatre ans. Les États membres devront également mettre en place des mécanismes de coopération entre les parties prenantes concernées.

Les opérateurs désignés comme «entités critiques» seraient tenus de procéder à leur propre évaluation des risques dans le court à moyen terme, de prendre des mesures techniques et organisationnelles appropriées et proportionnées pour garantir leur résilience, et d'informer les autorités compétentes des incidents.

1.5.2. Valeur ajoutée de l'intervention de l'Union (celle-ci peut résulter de différents facteurs, par exemple gains de coordination, sécurité juridique, efficacité accrue, complémentarités, etc.). Aux fins du présent point, on entend par «valeur ajoutée de l'intervention de l'Union» la valeur découlant de l'intervention de l'Union qui vient s'ajouter à la valeur qui, sans cela, aurait été générée par la seule action des États membres.

Justification de l'action au niveau européen (ex ante):

L'objectif de cette initiative est de renforcer la résilience des entités critiques face à une série de risques. Cet objectif ne peut pas être réalisé de manière satisfaisante par la seule action des États membres: l'action de l'UE se justifie en raison de la nature commune des risques auxquels les entités critiques sont confrontées, du caractère transnational des services qu'elles fournissent, et des interdépendances et connexions entre elles (au-delà des secteurs et des frontières). Dès lors, une vulnérabilité ou une perturbation dans une installation est susceptible de provoquer des perturbations transsectorielles et transfrontières.

Valeur ajoutée escomptée de l'intervention de l'UE (ex post):

Par rapport à la situation actuelle, l'initiative proposée apportera une valeur ajoutée, en ce que:

— elle met en place un cadre général favorisant un rapprochement plus étroit des politiques des États membres (champ d'application sectoriel cohérent, critères de désignation des entités critiques, exigences communes en matière d'évaluation des risques),

— elle veille à ce que les entités critiques prennent des mesures de résilience appropriées,

— elle met en commun les connaissances et l'expertise présentes dans toute l'UE afin d'optimiser la réaction des entités critiques et des autorités,

— elle réduit les disparités entre les États membres et renforce la résilience des entités critiques dans l'UE.

1.5.3. Leçons tirées d'expériences similaires

La proposition s'appuie sur les enseignements tirés de la mise en œuvre de la directive sur les infrastructures critiques européennes (directive 2008/114/CE) et de son évaluation [SWD (2019) 308].

1.5.4. Compatibilité avec le cadre financier pluriannuel et synergies éventuelles avec d'autres instruments appropriés

La présente proposition est un élément fondamental de la nouvelle stratégie de l'UE pour l'union de la sécurité, visant à mettre en place un environnement de sécurité à l'épreuve du temps.

Des synergies peuvent être développées avec le mécanisme de protection civile de l'Union en matière de prévention, d'atténuation et de gestion des catastrophes.

1.6. Durée et incidence financière de la proposition/de l'initiative

☐ **durée limitée**

☐ en vigueur à partir de [JJ/MM]AAAA jusqu'en [JJ/MM]AAAA

☐ incidence financière de AAAA jusqu'en AAAA pour les crédits d'engagement et de AAAA jusqu'en AAAA pour les crédits de paiement

☑ **durée illimitée**

- Mise en œuvre avec une période de montée en puissance de 2021 jusqu'en 2027,
- puis un fonctionnement en rythme de croisière au-delà.

1.7. Mode(s) de gestion prévu(s)[41]

☑ **gestion directe** par la Commission

☑ dans ses services, notamment par l'intermédiaire de son personnel dans les délégations de l'Union;

☐ par les agences exécutives

☑ **gestion partagée** avec les États membres

☐ **gestion indirecte** en confiant des tâches d'exécution budgétaire:

☐ à des pays tiers ou aux organismes qu'ils ont désignés;

☐ à des organisations internationales et à leurs agences (à préciser);

☐ à la BEI et au Fonds européen d'investissement;

☐ aux organismes visés aux articles 70 et 71 du règlement financier;

☐ à des organismes de droit public;

☐ à des organismes de droit privé investis d'une mission de service public, pour autant qu'ils présentent les garanties financières suffisantes;

☐ à des organismes de droit privé d'un État membre qui sont chargés de la mise en œuvre d'un partenariat public-privé et présentent les garanties financières suffisantes;

☐ à des personnes chargées de l'exécution d'actions spécifiques relevant de la PESC, en vertu du titre V du traité sur l'Union européenne, identifiées dans l'acte de base concerné.

---

[41] Les explications sur les modes de gestion ainsi que les références au règlement financier sont disponibles sur le site BudgWeb: https://myintracomm.ec.europa.eu/budgweb/FR/man/budgmanag/Pages/budgmanag.aspx

Si plusieurs modes de gestion sont indiqués, veuillez donner des précisions dans la partie «Remarques».

Remarques

La gestion directe couvrira principalement: des dépenses administratives de la DG HOME, l'accord administratif avec le JRC, les subventions gérées par la Commission.

La gestion partagée couvrira les projets en gestion partagée, étant donné que les États membres devront élaborer une stratégie et une évaluation des risques et pourront utiliser leurs enveloppes nationales à cette fin.

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

Préciser la fréquence et les conditions de ces dispositions.

Conformément à la proposition de règlement du Parlement européen et du Conseil établissant, dans le cadre du Fonds pour la sécurité intérieure, l'instrument de l'Union consacré au domaine de la sécurité [COM(2018) 472 final]:

Gestion partagée:

Chaque État membre établit des systèmes de gestion et de contrôle pour son programme et assure la qualité et la fiabilité du système de suivi et des données sur les indicateurs, conformément au règlement portant dispositions communes (RDC). Afin de faciliter le démarrage rapide de la mise en œuvre, il est possible de «transférer» les systèmes de gestion et de contrôle existants qui fonctionnent bien à la prochaine période de programmation.

Dans ce contexte, les États membres seront invités à créer un comité de suivi auquel la Commission participe à titre consultatif. Le comité de suivi se réunit au moins une fois par an. Il examine toutes les questions qui ont une incidence sur les progrès du programme en vue de la réalisation de ses objectifs.

Les États membres envoient un rapport annuel sur l'exécution qui devrait fournir des informations sur les progrès réalisés dans la mise en œuvre du programme et sur la réalisation des objectifs intermédiaires. Il devrait également signaler tout problème affectant la performance du programme et décrire les mesures prises pour y remédier.

À la fin de la période, chaque État membre présente un rapport de performance final. Le rapport final devrait mettre l'accent sur les progrès accomplis dans la réalisation des objectifs du programme et donner un aperçu des principaux problèmes qui ont affecté la performance du programme, des mesures prises pour y remédier et de l'évaluation de l'efficacité de ces mesures. En outre, il devrait présenter la contribution du programme pour relever les défis identifiés dans les recommandations pertinentes de l'UE adressées à l'État membre, les progrès accomplis dans la réalisation des objectifs fixés dans le cadre de performance, les résultats des évaluations pertinentes et le suivi donné à ces constats et les résultats des actions de communication.

Selon le projet de proposition de RDC, les États membres envoient chaque année un dossier «assurance» comprenant les comptes annuels, la déclaration de gestion et l'avis d'audit sur les comptes, le rapport de contrôle annuel au titre de l'article 92, paragraphe 1, point d), du RDC, le système de gestion et de contrôle et la légalité et la régularité des dépenses déclarées dans les comptes annuels. Ce dossier «assurance» est utilisé par la Commission pour déterminer le montant à la charge du Fonds pour l'exercice comptable.

Une réunion de réexamen entre la Commission et chaque État membre est organisée tous les deux ans pour examiner la performance de chaque programme.

Les États membres envoient six fois par an des données concernant chaque programme, ventilées par objectif spécifique. Ces données concernent le coût des opérations et les valeurs des indicateurs communs de réalisation et de résultat.

En règle générale:

La Commission procède à une évaluation à mi-parcours et rétrospective des actions mises en œuvre dans le cadre de ce Fonds, conformément au règlement portant dispositions communes. L'évaluation à mi-parcours devrait s'appuyer notamment sur l'évaluation à mi-parcours des programmes soumis à la Commission par les États membres au plus tard le 31 décembre 2024.

2.2. Système(s) de gestion et de contrôle

2.2.1. Justification du (des) mode(s) de gestion, du (des) mécanisme(s) de mise en œuvre du financement, des modalités de paiement et de la stratégie de contrôle proposée

Conformément à la proposition de règlement du Parlement européen et du Conseil établissant, dans le cadre du Fonds pour la sécurité intérieure, l'instrument de l'Union consacré au domaine de la sécurité [COM(2018) 472 final]:

Tant les évaluations ex post des fonds de la DG HOME pour 2007-2013 que les évaluations provisoires des fonds actuels de la DG HOME montrent qu'une combinaison de modes de mise à disposition dans les domaines de la migration et des affaires intérieures a permis d'atteindre de manière efficace les objectifs des fonds. La conception holistique des mécanismes de mise à disposition est maintenue et comprend une gestion partagée, directe et indirecte.

Grâce à la gestion partagée, les États membres mettent en œuvre des programmes adaptés à leur contexte national qui contribuent aux objectifs politiques de l'Union. La gestion partagée garantit qu'un soutien financier est disponible dans tous les États participants. En outre, la gestion partagée permet une prévisibilité du financement et les États membres, qui connaissent le mieux les défis auxquels ils sont confrontés, peuvent planifier leurs dotations à long terme en conséquence. À titre de nouveauté, le Fonds peut également fournir une aide d'urgence grâce à une gestion partagée, en plus de la gestion directe et indirecte.

Par la gestion directe, la Commission soutient d'autres actions qui contribuent aux objectifs de politique commune de l'Union. Ces actions permettent d'apporter un soutien sur mesure aux besoins urgents et spécifiques des États membres («aide d'urgence»), de soutenir des réseaux et des activités transnationaux, de tester des activités innovantes qui pourraient être étendues dans le cadre de programmes nationaux et de couvrir des études dans l'intérêt de l'Union en tant qu'ensemble («actions de l'Union»).

Grâce à la gestion indirecte, le Fonds garde la possibilité de déléguer des tâches d'exécution du budget, notamment à des organisations internationales et des agences relevant du domaine des affaires intérieures à des fins spécifiques.

Compte tenu des différents objectifs et besoins, un mécanisme thématique est proposé dans le cadre du Fonds afin d'équilibrer la prévisibilité de l'allocation pluriannuelle des fonds aux programmes nationaux avec une flexibilité dans le

décaissement périodique de fonds pour des actions à forte valeur ajoutée pour l'Union. Le mécanisme thématique est utilisé pour des actions spécifiques dans les États membres et entre ceux-ci, les actions de l'Union et l'aide d'urgence. Il permettra que les fonds puissent être alloués et transférés au moyen des différentes modalités ci-dessus, sur la base d'une programmation biennale.

Les modalités de paiement pour la gestion partagée sont décrites dans le projet de proposition de RDC prévoyant un préfinancement annuel, suivi d'un maximum de quatre paiements intermédiaires par programme et par an sur la base des demandes de paiement envoyées par les États membres au cours de l'exercice. Conformément au projet de proposition de RDC, les préfinancements sont compensés au cours de l'exercice comptable final des programmes.

La stratégie de contrôle sera fondée sur le nouveau règlement financier et sur le règlement portant dispositions communes. Le nouveau règlement financier et le projet de proposition de RDC devraient étendre l'utilisation des formes simplifiées de subventions telles que les montants forfaitaires, les taux forfaitaires et les coûts unitaires. Il introduit également de nouvelles formes de paiements, basées sur les résultats obtenus au lieu du coût. Les bénéficiaires pourront recevoir une somme d'argent fixe s'ils apportent la preuve que certaines actions telles que des formations ou la fourniture d'une aide humanitaire ont été exécutées. Cela devrait simplifier la charge de contrôle tant au niveau des bénéficiaires que des États membres (par exemple, vérification des factures et des justificatifs pour les coûts).

Pour la gestion partagée, le projet de proposition de RDC s'appuie sur la stratégie de gestion et de contrôle appliquée pour la période de programmation 2014-2020, mais introduit certaines mesures visant à simplifier la mise en œuvre et à réduire la charge de contrôle tant au niveau des bénéficiaires que des États membres. Les nouveautés comprennent:

— la suppression de la procédure de désignation (ce qui devrait permettre d'accélérer la mise en œuvre des programmes);

— les vérifications de gestion (administratives et sur place) à effectuer par l'autorité de gestion en fonction des risques (par rapport aux contrôles administratifs à 100 % requis pour la période de programmation 2014-2020). En outre, sous certaines conditions, les autorités de gestion peuvent appliquer des modalités de contrôle proportionnées conformément aux procédures nationales;

— les conditions permettant d'éviter plusieurs audits sur la même opération ou dépense.

Les autorités responsables des programmes soumettront à la Commission des demandes de paiement intermédiaire fondées sur les dépenses engagées par les bénéficiaires. Le projet de proposition de RDC permet aux autorités de gestion d'effectuer des vérifications de gestion fondées sur le risque et prévoit également des contrôles spécifiques (contrôles sur place par l'autorité de gestion et audits des opérations ou dépenses par l'autorité d'audit) après que les dépenses correspondantes ont été déclarées à la Commission dans les demandes de paiement intermédiaire. Afin d'atténuer le risque de remboursement de coûts inéligibles, le projet de RDC prévoit que les paiements provisoires de la Commission soient plafonnés à 90 %,

étant donné qu'à ce jour, une partie seulement des contrôles nationaux ont été effectués. La Commission versera le solde restant après l'exercice annuel d'apurement des comptes, dès réception du dossier «assurance» de la part des autorités responsables du programme. Toute irrégularité détectée par la Commission ou la Cour des comptes européenne après la transmission du dossier «assurance» annuel peut entraîner une correction financière nette.

En ce qui concerne la partie mise en œuvre par **gestion directe** au titre du mécanisme thématique, le système de gestion et de contrôle s'appuiera sur l'expérience acquise au cours de la période 2014-2020 dans le cadre des actions de l'Union et de l'aide d'urgence. Un régime simplifié sera mis en place pour permettre le traitement rapide des demandes de financement tout en réduisant le risque d'erreurs: les demandeurs admissibles seront limités aux États membres et aux organisations internationales, le financement sera fondé sur des options simplifiées en matière de coûts, des modèles standard seront élaborés pour les demandes de financement, les accords de subvention/contribution et les rapports, et un comité d'évaluation permanent examinera les demandes dès leur réception.

2.2.2. Informations sur les risques recensés et sur le(s) système(s) de contrôle interne mis en place pour les atténuer

La DG HOME n'a pas été confrontée à d'importants risques d'erreurs dans ses programmes de dépenses. Cela est confirmé par l'absence récurrente de constatations significatives dans les rapports annuels de la Cour des comptes.

En gestion partagée, les risques généraux liés à la mise en œuvre des programmes actuels concernent l'insuffisance de la mise en œuvre du Fonds par les États membres et les erreurs possibles découlant de la complexité des règles et des faiblesses des systèmes de gestion et de contrôle. Le projet de RDC simplifie le cadre réglementaire en harmonisant les règles et les systèmes de gestion et de contrôle entre les différents fonds mis en œuvre dans le cadre de la gestion partagée. Il simplifie également les exigences de contrôle (par exemple, les vérifications de gestion fondées sur le risque, la possibilité de dispositions de contrôle proportionnées basées sur les procédures nationales, les limitations du travail d'audit en termes de calendrier et/ou d'opérations spécifiques).

2.2.3. Estimation et justification du rapport coût-efficacité des contrôles (rapport «coûts du contrôle ÷ valeur des fonds gérés concernés»), et évaluation du niveau attendu de risque d'erreur (lors du paiement et lors de la clôture)

Le rapport «coûts du contrôle/valeur des fonds gérés concernés» est établi par la Commission. Le RAA 2019 de la DG HOME indique un ratio de 0,72 % pour la gestion partagée, de 1,31 % pour les subventions en gestion directe et de 6,05 % pour les marchés en gestion directe. Le pourcentage relatif à la gestion partagée diminue généralement progressivement avec les gains d'efficacité dans la mise en œuvre des programmes et une augmentation des paiements aux États membres.

L'introduction, dans le projet de RDC, de l'approche fondée sur le risque dans le domaine de la gestion et des contrôles et l'existence d'une volonté accrue d'adopter des options de coûts simplifiés (OCS) devrait entraîner une nouvelle réduction du coût des contrôles pour les États membres.

Le rapport annuel d'activités 2019 faisait état d'un taux d'erreur résiduel cumulé de 1,57 % pour les programmes nationaux relevant du FAMI/FSI et d'un taux d'erreur résiduel cumulé de 4,11 % pour les subventions en gestion directe non liées à la recherche.

2.3. Mesures de prévention des fraudes et irrégularités

Préciser les mesures de prévention et de protection existantes ou envisagées, au titre de la stratégie antifraude par exemple.

La DG HOME continuera à appliquer sa stratégie de lutte contre la fraude conformément à la stratégie antifraude de la Commission (SAFC) afin de faire en sorte, entre autres, que ses contrôles internes de détection de la fraude soient pleinement conformes à la SAFC et que sa gestion des risques de fraude soit orientée sur la détection des domaines les plus exposés à ces risques et la détermination des moyens appropriés d'y faire face.

En ce qui concerne la gestion partagée, les États membres veillent à la légalité et à la régularité des dépenses inscrites dans les comptes présentés à la Commission. Dans ce contexte, les États membres prennent toutes les mesures nécessaires pour prévenir, détecter et corriger les irrégularités. Comme dans le cycle de programmation actuel 2014-2020, les États membres sont tenus de mettre en place des procédures de détection des irrégularités et de lutte contre la fraude, associées au règlement délégué spécifique de la Commission sur la notification des irrégularités. Les mesures de lutte antifraude resteront un principe et une obligation transversaux pour les États membres.

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

(1) Lignes budgétaires nouvelles

Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Type de dépense	Participation			
	Rubrique 5: résilience, sécurité et défense	CD/CND[42]	de pays AELE[43]	de pays candidats[44]	de pays tiers	au sens de l'article 21, paragraphe 2, point b), du règlement financier
5	12.02.01 – «Fonds pour la sécurité intérieure»	CD	NON	NON	OUI	NON
5	12 01 01 – Dépenses d'appui au «Fonds pour la sécurité intérieure»	CND	NON	NON	OUI	NON

Remarque:

Il convient de noter que les crédits opérationnels demandés dans le cadre de la proposition sont couverts par des crédits déjà prévus dans la fiche financière législative du règlement sur le FSI.

Des ressources humaines supplémentaires sont requises dans le cadre de cette proposition législative.

[42] CD = crédits dissociés / CND = crédits non dissociés.

[43] AELE: Association européenne de libre-échange.

[44] Pays candidats et, le cas échéant, candidats potentiels des Balkans occidentaux.

3.2. Incidence financière estimée de la proposition sur les crédits

3.2.1. Synthèse de l'incidence estimée sur les crédits opérationnels

☐ La proposition/l'initiative ne nécessite pas l'utilisation de crédits opérationnels

☑ La proposition/l'initiative nécessite l'utilisation de crédits opérationnels, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

Rubrique du cadre financier pluriannuel	5	Résilience, sécurité et défense

DG: HOME			2021	2022	2023	2024	2025	2026	2027	**Après 2027**	**TOTAL**
• Crédits opérationnels											
Ligne budgétaire 12 02 01 – Fonds pour la sécurité intérieure	Engagements	(1a)	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822
	Paiements	(2a)	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822
Crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques[45]											
Ligne budgétaire		(3)									
TOTAL des crédits	Engagements	= 1a + 1b + 3	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822

[45] Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

pour la DG HOME	Paiements	= 2a + 2b +3	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822

• TOTAL des crédits opérationnels	Engagements	(4)									
	Paiements	(5)									
• TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques		(6)									
TOTAL des crédits pour la RUBRIQUE 5 du cadre financier pluriannuel	Engagements	= 4 + 6	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822
	Paiements	= 5 + 6	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822

Si plusieurs rubriques opérationnelles sont concernées par la proposition/l'initiative, dupliquer la section qui précède:

• TOTAL des crédits opérationnels (toutes les rubriques opérationnelles)	Engagements	(4)									
	Paiements	(5)									
TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques (toutes les rubriques opérationnelles)		(6)									
TOTAL des crédits pour les RUBRIQUES 1 à 6 du cadre financier pluriannuel (Montant de référence)	Engagements	= 4 + 6	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822
	Paiements	= 5 + 6	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822

Rubrique du cadre financier pluriannuel	**7**	«Dépenses administratives»

Cette partie est à compléter en utilisant les «données budgétaires de nature administrative», à introduire d'abord dans l'annexe de la fiche financière législative (annexe V des règles internes), à charger dans DECIDE pour les besoins de la consultation interservices.

En Mio EUR (à la 3e décimale)

		2021	2022	2023	2024	2025	2026	2027	**TOTAL**
DG: HOME									
• Ressources humaines		0,152	0,228	0,499	0,813	0,932	0,932	0,932	**4,488**
• Autres dépenses administratives		0,033	0,085	0,109	0,109	0,109	0,109	0,109	**0,663**
TOTAL DG HOME	Crédits	**0,185**	**0,313**	**0,608**	**0,922**	**1,041**	**1,041**	**1,041**	**5,151**

TOTAL des crédits pour la RUBRIQUE 7 du cadre financier pluriannuel	(Total engagements = Total paiements)	**0,185**	**0,313**	**0,608**	**0,922**	**1,041**	**1,041**	**1,041**	**5,151**

En Mio EUR (à la 3e décimale)

		2021	2022	2023	2024	2025	2026	2027	**Après 2027**	**TOTAL**
TOTAL des crédits pour les RUBRIQUES 1 à 7 du cadre financier pluriannuel	Engagements	**0,309**	**4,661**	**6,178**	**7,642**	**8,061**	**8,061**	**8,061**	**—**	**42,973**
	Paiements	**0,725**	**4,636**	**5,965**	**6,325**	**6,444**	**6,444**	**6,444**	**5,989**	**42,973**

3.2.2. Réalisations estimées financées par des crédits opérationnels

Crédits d'engagement en millions d'euros (à la troisième décimale)

Indiquer les objectifs et les réalisations ⇩	Type	Coût moyen	Année 2021		Année 2022		Année 2023		Année 2024		Année 2025		Année 2026		Année 2027		TOTAL	
			Nombre	Coût	Nombre	Coût	Nombre	Coût	Nombre	Coût	Nombre	Coût	Nombre	Coût	Nombre	Coût	Nombre	Coût
OBJECTIF SPÉCIFIQUE N° 1: appui de la Commission aux autorités compétentes et aux entités critiques																		
Réalisation	Développer et maintenir la capacité en termes de connaissances et de soutien					2 000		2 000				2 000		2 000		2 000		12 000
Réalisation	Soutien aux autorités compétentes par le renforcement des échanges de bonnes pratiques et d'informations et par la réalisation d'évaluations des risques (coûts financiers couverts par les études ci-dessous)																	
Réalisation	Soutien aux autorités compétentes et aux entités critiques (c'est-à-dire aux opérateurs) par l'élaboration de matériels d'orientation et de méthodologies, par un appui à l'organisation d'exercices de simulation de scénarios d'incidents en temps réel et par des formations					0,500		0,850		1 200		1 500		1 500		1 500		7 050
Réalisation	Projets sur divers sujets liés aux activités d'appui susmentionnées (méthodes d'évaluation des risques, simulation de scénarios d'incidents en temps réel, formations...)	**0,400**			3	1 200	5	2 000	7	2 800		2 800	7	2 800	7		36	14 400
Réalisation	Études (évaluations des risques) et consultations (liées à la mise en œuvre de la directive)	**0,100**			4	0,400	4	0,400	4	0,400	4	0,400	4	0,400	4	0,400	24	2 400
Réalisation	Autres réunions, conférences	**0,031**		0,124	8	0,248	8	0,248	8	0,248	8	0,248	8	0,248	8	0,248	52	1 612
Sous-total objectif spécifique n° 1				0,124		4 348		5 498		6 648		6 948		6 948		6 948		37 462

OBJECTIF SPÉCIFIQUE N° 2: Équipes de conseil en résilience

Réalisation	Organisation d'équipes de conseil en résilience (membres: représentants des États membres) Organisation par la COM de l'appel à désignation de membres (pour																		
Réalisation	Organisation par la COM du programme et des missions de conseil Apport par la COM d'une contribution importante aux missions de conseil (orientations et surveillance des entités critiques d'importance européenne - avec les ÉM) Coordination quotidienne des équipes de conseil en résilience							0,072		0,072		0,072			0,072		0,072		0,360
Sous-total objectif spécifique n° 2								0,072		0,072		0,072			0,072		0,072		0,360
TOTAL objectifs 1 et 2				**0,124**		**4 348**		**5 570**		**6 720**		**7 020**			**7 020**		**7 020**		**37 822**

3.2.3. Synthèse de l'incidence estimée sur les crédits administratifs

☐ La proposition/l'initiative ne nécessite pas l'utilisation de crédits de nature administrative.

☑ La proposition/l'initiative nécessite l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

	2021	2022	2023	2024	2025	2026	2027	TOTAL
RUBRIQUE 7 du cadre financier pluriannuel								
Ressources humaines	0,152	0,228	0,499	0,813	0,932	0,932	0,932	4,488
Autres dépenses administratives	0,033	0,085	0,109	0,109	0,109	0,109	0,109	0,663
Sous-total RUBRIQUE 7 du cadre financier pluriannuel	**0,185**	**0,313**	**0,608**	**0,922**	**1,041**	**1,041**	**1,041**	**5,188**

Hors RUBRIQUE 7[46] du cadre financier pluriannuel								
Ressources humaines								
Autres dépenses de nature administrative								
Sous-total hors RUBRIQUE 7 du cadre financier pluriannuel								

TOTAL	**0,185**	**0,313**	**0,608**	**0,922**	**1,041**	**1,041**	**1,041**	**5,188**

Les besoins en crédits pour les ressources humaines et les autres dépenses de nature administrative seront couverts par les crédits de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

46 Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

3.2.3.1. Besoins estimés en ressources humaines

☐ La proposition/l'initiative ne nécessite pas l'utilisation de ressources humaines.

☑ La proposition/l'initiative nécessite l'utilisation de ressources humaines, comme expliqué ci-après:

Estimation à exprimer en équivalents temps plein

		Année **2021**	Année **2022**	Année **2023**	Année **2024**	2025	2026	2027
• Emplois du tableau des effectifs (fonctionnaires et agents temporaires)								
20 01 02 01 (au siège et dans les bureaux de représentation de la Commission)		1	2	4	5	5	5	5
XX 01 01 02 (en délégation)								
XX 01 05 01/11/21 (recherche indirecte)								
10 01 05 01/11 (recherche directe)								
•Personnel externe (en équivalents temps plein: ETP)[47]								
20 02 01 03 (AC, END, INT de l'enveloppe globale)				1	2	2	2	2
XX 01 02 02 (AC, AL, END, INT et JPD dans les délégations)								
XX 01 04 **aa** [48]	– au siège							
	– en délégation							
XX 01 05 02/12/22 (AC, END, INT – recherche indirecte)								
10 01 05 02/12 (AC, END, INT sur recherche directe)								
Autres lignes budgétaires (à préciser)								
TOTAL		**1**	**2**	**5**	**7**	**7**	**7**	**7**

XX est le domaine d'action ou le titre concerné.

Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

Description des tâches à effectuer:

Fonctionnaires et agents temporaires	La proposition prévoit 4 AD et 1 AST affectés à la mise en œuvre de la directive du côté de la Commission, dont 1 AD est déjà actif en interne, tandis que les autres ETP sont des ressources humaines supplémentaires qui devront être recrutées. Le plan de recrutement prévoit: 2022: + 1 AD: chargé de mission responsable de la mise en place du pôle de connaissances et des activités de soutien 2023: + 1 AD (chargé de mission responsable des équipes de conseil), 1 AST (assistant auprès des équipes de conseil en résilience) 2024: + 1 AD (chargé de mission contribuant aux activités de soutien aux autorités et aux opérateurs)
Personnel externe	La proposition prévoit 2 END chargés de la mise en œuvre de la directive du côté de la

[47] AC = agent contractuel, AL = agent local, END = expert national détaché, INT = intérimaire, JPD = jeune professionnel en délégation.

[48] Sous-plafonds de personnel externe financés sur crédits opérationnels (anciennes lignes «BA»).

	Commission. Le plan de recrutement prévoit: 2023: + 1 END (expert en résilience des infrastructures critiques/contribuant aux activités de soutien aux autorités et aux opérateurs) 2024: + 1 END (expert en résilience des infrastructures critiques/contribuant aux activités de soutien aux autorités et aux opérateurs)

3.2.4. Compatibilité avec le cadre financier pluriannuel actuel

La proposition/l'initiative:

☑ peut être intégralement financée par voie de redéploiement au sein de la rubrique concernée du cadre financier pluriannuel (CFP).

Dépenses opérationnelles couvertes par le FSI au titre du CFP 2021-2027

☐ nécessite l'utilisation de la marge non allouée sous la rubrique correspondante du CFP et/ou le recours aux instruments spéciaux comme le prévoit le règlement CFP.

Expliquez le besoin, en précisant les rubriques et lignes budgétaires concernées, les montants correspondants et les instruments dont le recours est proposé.

☐ nécessite une révision du CFP.

Expliquez le besoin, en précisant les rubriques et lignes budgétaires concernées et les montants correspondants.

3.2.5. Participation de tiers au financement

La proposition/l'initiative:

☑ ne prévoit pas de cofinancement par des tierces parties

☐ prévoit un cofinancement par des tiers, dont le montant est estimé ci-dessous:

Crédits en Mio EUR (à la 3e décimale)

	Année **N**[49]	Année **N+1**	Année **N+2**	Année **N+3**	Indiquer le nombre d'années correspondant à la durée de l'incidence (cf. point 1.6)			Total
Préciser l'organisme de cofinancement								
TOTAL crédits cofinancés								

[49] L'année N est l'année du début de la mise en œuvre de la proposition/de l'initiative. Veuillez remplacer «N» par la première année de mise en œuvre prévue (par exemple: 2021). Procédez de la même façon pour les années suivantes.

3.3. Incidence estimée sur les recettes

☑ La proposition/l'initiative est sans incidence financière sur les recettes.

☐ La proposition/l'initiative a l'incidence financière suivante:

☐ sur les ressources propres

☐ sur les autres recettes

veuillez indiquer si les recettes sont affectées à des lignes de dépenses ☐

En Mio EUR (à la 3e décimale)

Ligne budgétaire de recettes:	Montants inscrits pour l'exercice en cours	Incidence de la proposition/de l'initiative[50]						
		Année **N**	Année **N+1**	Année **N+2**	Année **N+3**	Indiquer le nombre d'années correspondant à la durée de l'incidence (cf. point 1.6)		
Article …….								

Pour les recettes affectées, préciser la(les) ligne(s) budgétaire(s) de dépenses concernée(s).

[…]

Autres remarques (relatives par exemple à la méthode/formule utilisée pour le calcul de l'incidence sur les recettes ou toute autre information).

[…]

[50] En ce qui concerne les ressources propres traditionnelles (droits de douane, cotisations sur le sucre), les montants indiqués doivent être des montants nets, c'est-à-dire des montants bruts après déduction de 20 % de frais de perception.