Informations de base

2020/0266(COD) COD - Procédure législative ordinaire (ex-procedure codécision) Règlement	Procédure terminée
Finance numérique: loi sur la résilience opérationnelle numérique (DORA) Modification Règlement 2009/1060 2008/0217(COD) Modification Règlement 2012/648 2010/0250(COD) Modification Règlement 2014/600 2011/0296(COD) Modification Règlement 2014/909 2012/0029(COD) **Subject** 2.50.03 Marchés financiers, bourse, OPCVM, investissements, valeurs mobilières 2.50.04 Banques et crédit 2.50.08 Services financiers, information financière et contrôle des comptes 2.50.10 Surveillance financière 3.30.06 Technologies de l'information et de la communication, technologies numériques **Priorités législatives** Déclaration commune 2021 Déclaration commune 2022	

Acteurs principaux

Parlement européen

Commission au fond	Rapporteur(e)	Date de nomination
ECON Affaires économiques et monétaires	KELLEHER Billy (Renew)	15/10/2020
	Rapporteur(e) fictif/fictive FITZGERALD Frances (EPP) SANT Alfred (S&D) PEKSA Mikuláš (Greens /EFA) RZOŃCA Bogdan (ECR) BECK Gunnar (ID)	

Commission pour avis	Rapporteur(e) pour avis	Date de nomination
ITRE Industrie, recherche et énergie	La commission a décidé de ne pas donner d'avis.	

	IMCO Marché intérieur et protection des consommateurs	La commission a décidé de ne pas donner d'avis.	
Conseil de l'Union européenne			
Commission européenne	**DG de la Commission**	**Commissaire**	
	Stabilité financière, services financiers et union des marchés des capitaux	MCGUINNESS Mairead	
Comité économique et social européen			

Evénements clés

Date	Evénement	Référence	Résumé
24/09/2020	Publication de la proposition législative	COM(2020)0595	Résumé
17/12/2020	Annonce en plénière de la saisine de la commission, 1ère lecture		
01/12/2021	Vote en commission,1ère lecture		
01/12/2021	Décision de la commission parlementaire d'ouvrir des négociations interinstitutionnelles à travers d'un rapport adopté en commission		
07/12/2021	Dépôt du rapport de la commission, 1ère lecture	A9-0341/2021	Résumé
13/12/2021	Décision de la commission parlementaire d'engager des négociations interinstitutionnelles annoncée en plénière (Article 71)		
15/12/2021	Décision de la commission parlementaire d'engager des négociations interinstitutionnelles confirmée par la plénière (Article 71)		
13/07/2022	Approbation en commission du texte adopté en négociations interinstitutionnelles de la 1ère lecture	PE734.260 GEDA/A/(2022)005010	
09/11/2022	Débat en plénière		
10/11/2022	Décision du Parlement, 1ère lecture	T9-0381/2022	Résumé
10/11/2022	Résultat du vote au parlement		
28/11/2022	Adoption de l'acte par le Conseil après la 1ère lecture du Parlement		
14/12/2022	Signature de l'acte final		
27/12/2022	Publication de l'acte final au Journal officiel		

Informations techniques

Référence de la procédure	2020/0266(COD)
Type de procédure	COD - Procédure législative ordinaire (ex-procedure codécision)
Sous-type de procédure	Note thématique
Instrument législatif	Règlement
Modifications et abrogations	Modification Règlement 2009/1060 2008/0217(COD)

	Modification Règlement 2012/648 2010/0250(COD) Modification Règlement 2014/600 2011/0296(COD) Modification Règlement 2014/909 2012/0029(COD)
Base juridique	Traité sur le fonctionnement de l'UE TFEU 114-p1
Autre base juridique	Règlement du Parlement EP 165
Consultation obligatoire d'autres institutions	Comité économique et social européen
État de la procédure	Procédure terminée
Dossier de la commission	ECON/9/04230

Portail de documentation

Parlement Européen

Type de document	Commission	Référence	Date	Résumé
Projet de rapport de la commission		PE689.801	17/03/2021	
Amendements déposés en commission		PE693.603	27/05/2021	
Rapport déposé de la commission, 1ère lecture/lecture unique		A9-0341/2021	07/12/2021	Résumé
Texte convenu lors de négociations interinstitutionnelles		PE734.260	07/07/2022	
Texte adopté du Parlement, 1ère lecture/lecture unique		T9-0381/2022	10/11/2022	Résumé

Conseil de l'Union

Type de document	Référence	Date	Résumé
Lettre de la Coreper confirmant l'accord interinstitutionnel	GEDA/A/(2022)005010	29/06/2022	
Projet d'acte final	00041/2022/LEX	14/12/2022	

Commission Européenne

Type de document	Référence	Date	Résumé
Document de base législatif	COM(2020)0595	24/09/2020	Résumé
Document annexé à la procédure	SEC(2020)0307	24/09/2020	
Document annexé à la procédure	SWD(2020)0198	24/09/2020	
Document annexé à la procédure	SWD(2020)0199	24/09/2020	
Réaction de la Commission sur le texte adopté en plénière	SP(2022)688	17/01/2023	

Parlements nationaux

Type de document	Parlement /Chambre	Référence	Date	Résumé
Contribution	CZ_CHAMBER	COM(2020)0595	16/12/2020	

Contribution	ES_PARLIAMENT	COM(2020)0595	22/02/2021	
Contribution	PT_PARLIAMENT	COM(2020)0595	09/03/2021	
Contribution	RO_SENATE	COM(2020)0595	10/05/2021	
Contribution	IT_CHAMBER	COM(2020)0595	27/10/2021	

Autres Institutions et organes

Institution/organe	Type de document	Référence	Date	Résumé
EESC	Comité économique et social: avis, rapport	CES5040/2020	24/02/2021	
EDPS	Document annexé à la procédure	N9-0035/2021 JO C 229 15.06.2021, p. 0016	10/05/2021	

Réunions avec des représentant(e)s d'intérêts, publiées conformément au règlement intérieur

Rapporteur(e)s, rapporteur(e)s fictifs/fictives et président(e)s des commissions

Transparence

Nom	Rôle	Commission	Date	Représentant(e)s d'intérêts
KELLEHER Billy	Rapporteur(e)	ECON	25/05/2022	Microsoft Corporation
KELLEHER Billy	Rapporteur(e)	ECON	15/03/2022	Capital Group
KELLEHER Billy	Rapporteur(e)	ECON	10/03/2022	BME
KELLEHER Billy	Rapporteur(e)	ECON	22/02/2022	Banking and Payments Federation Ireland
KELLEHER Billy	Rapporteur(e)	ECON	11/02/2022	European Banking Federation
KELLEHER Billy	Rapporteur(e)	ECON	19/01/2022	Digital Europe
KELLEHER Billy	Rapporteur(e)	ECON	25/10/2021	BIPAR - European Federation of Insurance Intermediaries
KELLEHER Billy	Rapporteur(e)	ECON	22/09/2021	PayPal Limited, Belgium Branch
KELLEHER Billy	Rapporteur(e)	ECON	21/09/2021	Federation Bancaire Francaise
KELLEHER Billy	Rapporteur(e)	ECON	09/09/2021	AWS
KELLEHER Billy	Rapporteur(e)	ECON	09/09/2021	UniCredit
KELLEHER Billy	Rapporteur(e)	ECON	08/09/2021	Bloomberg L.P.
KELLEHER Billy	Rapporteur(e)	ECON	08/09/2021	Microsoft Corporation

Acte final

Règlement 2022/2554
JO L 333 27.12.2022, p. 0001 Résumé

Actes délégués	
Référence	**Sujet**
2024/3006(DEA)	Examination of delegated act
2025/2574(DEA)	Examination of delegated act
2025/2623(DEA)	Examination of delegated act

Finance numérique: loi sur la résilience opérationnelle numérique (DORA)

2020/0266(COD) - 27/12/2022 - Acte final

OBJECTIF : renforcer la sécurité informatique des entités financières telles que les banques, les compagnies d'assurance et les entreprises d'investissement en vue de permettre au secteur financier européen de maintenir des opérations résilientes en cas de perturbation opérationnelle grave.

ACTE LÉGISLATIF : Règlement (UE) 2022/2554 du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) no 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.

CONTENU : le règlement sur la résilience opérationnelle numérique (**règlement DORA**) fixe des **exigences uniformes** pour la sécurité des réseaux et des systèmes d'information des entreprises et des organisations actives dans le secteur financier ainsi que des tiers critiques qui leur fournissent des services liés aux technologies de l'information et de la communication (TIC), tels que des plateformes d'informatique en nuage ou des services d'analyse de données.

DORA crée un **cadre réglementaire sur la résilience opérationnelle numérique** dans lequel toutes les entreprises doivent s'assurer qu'elles peuvent résister à tous les types de perturbations et de menaces liées aux TIC, y réagir et s'en remettre. Les nouvelles règles constitueront un cadre solide qui renforcera la sécurité informatique du secteur financier.

Exigences uniformes

DORA fixe des exigences uniformes pour la sécurité des réseaux et des systèmes d'information des entreprises et des organisations opérant dans le secteur financier, comme suit:

- les exigences applicables aux entités financières en ce qui concerne: i) la **gestion des risques** liés aux technologies de l'information et de la communication (TIC); ii) la **notification**, aux autorités compétentes, des incidents majeurs liés aux TIC et la notification, à titre volontaire, des cybermenaces importantes aux autorités compétentes; iii) la notification aux autorités compétentes, par les entités financières des incidents opérationnels ou de sécurité majeurs liés au paiement; iv) les **tests** de résilience opérationnelle numérique; v) le partage d'informations et de renseignements en rapport avec les cybermenaces et les cybervulnérabilités; vi) les mesures destinées à garantir la **gestion saine du risque** lié aux prestataires tiers de services TIC;

- les exigences relatives aux **accords contractuels conclus entre des prestataires tiers de services TIC et des entités financières**;

- les règles relatives à l'établissement du **cadre de supervision** applicable aux prestataires tiers critiques de services TIC lorsqu'ils fournissent des services à des entités financières, ainsi que celles liées à l'exercice des tâches dans ce cadre.

- les règles relatives à la **coopération** entre les autorités compétentes, et les règles relatives à la surveillance et à l'exécution par les autorités compétentes en ce qui concerne toutes les questions couvertes par le règlement.

Champ d'application

La nouvelle règlementation **s'appliquera à presque toutes les entités financières**. Elle ne s'appliquera pas aux intermédiaires d'assurance qui sont des microentreprises ou des petites ou moyennes entreprises. Les cabinets d'audit ne seront pas soumis au règlement DORA, mais feront partie d'un futur réexamen du règlement, dans le cadre duquel une éventuelle révision des règles pourrait être envisagée.

Principe de proportionnalité

Les efforts demandés aux entités financières seront proportionnels aux risques potentiels. Le règlement précise que les entités financières devront mettre en œuvre les règles relatives à la gestion des risques conformément au principe de proportionnalité, en tenant compte de leur taille et de leur profil de risque global ainsi que de la nature, de l'ampleur et de la complexité de leurs services, activités et opérations.

Gouvernance et organisation

Les entités financières devront :

- disposer d'un **cadre de gouvernance** et de contrôle interne garantissant une gestion efficace et prudente du risque lié aux TIC en vue d'atteindre un niveau élevé de résilience opérationnelle numérique;

- disposer d'un **cadre de gestion du risque** lié aux TIC solide, complet et bien documenté, qui leur permet de parer au risque lié aux TIC de manière rapide, efficiente et exhaustive et de garantir un niveau élevé de résilience opérationnelle numérique;

- mettre en place des mécanismes permettant de **détecter rapidement les activités anormales**. Tous les mécanismes de détection seront régulièrement testés.

Cadre de supervision des prestataires tiers critiques de services TIC

Les prestataires critiques établis dans un pays tiers qui fournissent des services informatiques aux entités financières dans l'UE seront tenus d'établir **une filiale dans l'UE**, afin que la supervision puisse être correctement mise en œuvre.

Afin que les prestataires tiers critiques de services TIC fassent l'objet d'une supervision appropriée et efficace à l'échelle de l'Union, le règlement prévoit que l'une des trois autorités européennes de surveillance (AES) pourra être désignée comme **superviseur principal**.

Les superviseurs principaux se verront confier les pouvoirs nécessaires pour mener des enquêtes, réaliser des inspections sur place et hors site des locaux et sites des prestataires tiers critiques de services TIC et obtenir des informations complètes et actualisées.

Afin de permettre la coordination des stratégies générales de supervision ainsi que des approches opérationnelles et des méthodes de travail cohérentes, les superviseurs principaux désignés devront mettre en place un **réseau de supervision commun** pour assurer la coordination de leurs activités au cours des phases préparatoires et durant l'exécution des activités de supervision de leurs prestataires tiers critiques de services TIC respectifs qui font l'objet d'une supervision.

Le superviseur principal sera également en mesure d'exercer ses pouvoirs de supervision dans les pays tiers.

Tests de résilience opérationnelle numérique

Afin d'évaluer l'état de préparation en vue du traitement d'incidents liés aux TIC, de recenser les faiblesses, les défaillances et les lacunes en matière de résilience opérationnelle numérique et de mettre rapidement en œuvre des mesures correctives, les entités financières, autres que les microentreprises, devront établir, maintenir et réexaminer un programme solide et complet de tests de résilience opérationnelle numérique, qui fait partie intégrante du cadre de gestion du risque lié aux TIC.

En vertu du règlement, des **tests de pénétration fondés sur la menace** seront effectués en mode fonctionnel et il sera possible d'inclure les autorités de plusieurs États membres dans les procédures de test. Le recours à des auditeurs internes ne sera possible que dans un certain nombre de circonstances strictement limitées, sous réserve de conditions de sauvegarde.

ENTRÉE EN VIGUEUR : 16.1.2023. Le règlement s'applique à partir du 17.1.2025.

Finance numérique: loi sur la résilience opérationnelle numérique (DORA)

2020/0266(COD) - 24/09/2020 - Document de base législatif

OBJECTIF : définir des exigences uniformes concernant la sécurité des réseaux et des systèmes d'information qui soutiennent les processus opérationnels des entités financières en vue d'atteindre un niveau élevé de résilience numérique opérationnelle pour le secteur financier.

ACTE PROPOSÉ : Règlement du Parlement européen et du Conseil.

RÔLE DU PARLEMENT EUROPÉEN : le Parlement européen décide conformément à la procédure législative ordinaire et sur un pied d'égalité avec le Conseil.

CONTEXTE : la présente proposition s'inscrit dans un nouvel ensemble de mesures sur la finance numérique visant à soutenir davantage le potentiel du financement numérique en termes d'innovation et de concurrence tout en atténuant les risques.

Le paquet sur le « financement numérique » comprend une nouvelle stratégie sur le financement numérique qui vise à garantir que la législation de l'Union sur les services financiers est adaptée à l'ère numérique et contribue à une économie tournée vers l'avenir en rendant l'utilisation de technologies innovantes plus accessible aux consommateurs et aux entreprises européennes. Il est de l'intérêt politique de l'Union de développer et de promouvoir l'adoption de technologies de transformation numérique dans le secteur financier, y compris la technologie des chaînes de blocs et des registres distribués (DLT).

Ce paquet comprend également une proposition de règlement visant à établir un nouveau cadre juridique européen en vue d'assurer le bon fonctionnement des marchés des crypto-actifs, une proposition de règlement sur un régime pilote pour les infrastructures de marché basé sur la technologie des registres distribués (DLT) et une proposition visant à clarifier ou à modifier certaines règles communautaires connexes en matière de services financiers.

Au cours des dernières décennies, l'utilisation des technologies de l'information et de la communication (TIC), a joué un rôle central dans la finance, et revêt aujourd'hui une importance cruciale dans le fonctionnement quotidien de toutes les entités financières. La numérisation couvre, par exemple, les paiements, qui sont de plus en plus passés de méthodes basées sur l'argent liquide et le papier à l'utilisation de solutions numériques. La finance est devenue largement numérique dans l'ensemble du secteur.

Cependant, l'accroissement de la numérisation et de l'interconnexion amplifie également les risques liés aux TIC, ce qui rend la société dans son ensemble - et le système financier en particulier - plus vulnérable aux cybermenaces.

Les risques liés aux TIC posent des défis pour les performances et la stabilité du système financier de l'UE. L'absence de règles détaillées et complètes sur la résilience opérationnelle numérique au niveau de l'UE a conduit à la prolifération d'initiatives réglementaires nationales (par exemple, en ce qui concerne les tests de résilience opérationnelle numérique) et d'approches de surveillance (par exemple, en ce qui concerne la dépendance à l'égard des fournisseurs d'infrastructures et de services tiers).

Cette situation fragmente le marché unique, porte atteinte à la stabilité et à l'intégrité du secteur financier de l'UE et compromet la protection des consommateurs et des investisseurs. La Commission estime donc nécessaire de mettre en place un cadre détaillé et complet sur la résilience opérationnelle numérique pour les entités financières de l'UE.

CONTENU : la proposition vise à mettre en place un cadre global qui améliorera la gestion des risques liés au numérique. En particulier, elle vise à renforcer et à rationaliser la conduite de la gestion des risques liés aux TIC par les entités financières, à imposer à toutes les entreprises de veiller à pouvoir résister à tous les types de perturbations et de menaces liées à l'informatique, à sensibiliser les superviseurs aux cyber-risques et aux incidents liés aux TIC auxquels sont confrontées les entités financières, ainsi qu'à introduire des pouvoirs permettant aux superviseurs financiers de surveiller les risques découlant de la dépendance des entités financières à l'égard des tiers fournisseurs de services TIC, tels que les prestataires de services d'informatique en nuage.

Champ d'application du règlement

Afin d'assurer la cohérence des exigences de gestion des risques liés aux TIC applicables au secteur financier, le règlement proposé couvrira une série d'entités financières réglementées au niveau de l'Union, à savoir, entre autres : i) les banques, ii) les établissements de paiement, iii) les établissements de monnaie électronique, iv) les entreprises d'investissement, les fournisseurs de services de cryptage, v) les dépositaires centraux de titres, vi) les contreparties centrales, vii) les bourses, viii) les référentiels centraux, ix) les agences de notation du crédit.

Une telle couverture devrait faciliter une application homogène et cohérente de tous les éléments de la gestion des risques dans les domaines liés aux TIC, tout en préservant l'égalité des conditions de concurrence entre les entités financières en ce qui concerne leurs obligations réglementaires en matière de risques liés aux TIC.

Exigences liées à la gouvernance

Dans la mesure où la proposition vise à mieux aligner les stratégies commerciales des entités financières et la conduite de la gestion des risques liés aux TIC, l'organe de direction devrait conserver un rôle crucial et actif dans le pilotage du cadre de gestion des risques liés aux TIC et veiller au respect d'une cyberhygiène rigoureuse.

Exigences en matière de gestion des risques liés aux TIC

La résilience opérationnelle numérique est ancrée dans un ensemble de principes et d'exigences clés sur le cadre de gestion des risques liés aux TIC, conformément aux conseils techniques conjoints des Autorités européennes de surveillance (AES). Ces exigences, inspirées des normes, lignes directrices et recommandations internationales, nationales et sectorielles pertinentes, tournent autour de fonctions spécifiques de la gestion des risques liés aux TIC (identification, protection et prévention, détection, réponse, apprentissage, évolution et communication).

Pour suivre l'évolution rapide du paysage des cybermenaces, les entités financières seraient tenues de mettre en place et de maintenir des systèmes et des outils TIC résilients qui minimisent l'impact des risques liés aux TIC.

Rapports d'incidents liés aux TIC

La proposition crée un mécanisme cohérent de notification des incidents qui contribuera à réduire les charges administratives des entités financières et à renforcer l'efficacité de la surveillance. La déclaration serait traitée à l'aide d'un modèle commun et selon une procédure harmonisée, telle que mise au point par les AES.

Test de résilience opérationnelle numérique

Les capacités et les fonctions incluses dans le cadre de gestion des risques liés aux TIC devraient être testées périodiquement pour vérifier l'état de préparation et identifier les faiblesses, les déficiences ou les lacunes, ainsi que pour mettre en œuvre rapidement des mesures correctives. La proposition permet une application proportionnée des exigences de test de résilience opérationnelle numérique en fonction de la taille, de l'activité et des profils de risque des entités financières.

Partage d'informations

Afin de sensibiliser au risque lié aux TIC, de minimiser sa propagation, de soutenir les capacités défensives des entités financières et les techniques de détection des menaces, le règlement proposé permet aux entités financières de mettre en place des arrangements pour échanger entre elles des informations et des renseignements sur la cybermenace. Tous les accords volontaires d'échange d'informations entre entités financières que la proposition encourage seraient menés dans des environnements de confiance, dans le respect total des règles de l'Union en matière de protection des données.

Implications budgétaires

Dès lors que le règlement prévoit un rôle accru pour les AES pour surveiller de manière adéquate les fournisseurs tiers de TIC critiques, la proposition impliquerait le déploiement de ressources accrues, notamment pour remplir les missions de surveillance (telles que les inspections et les audits sur site et en ligne) et le recours à du personnel possédant une expertise spécifique en matière de sécurité des TIC.

L'ampleur et la répartition de ces coûts dépendront de l'étendue des nouveaux pouvoirs de surveillance et des tâches (précises) à accomplir par les AES.

L'impact total des coûts est estimé à environ 30,19 millions d'euros pour la période 2022 - 2027. Par conséquent, aucune incidence sur les crédits du budget de l'UE n'est prévue (à l'exception du personnel supplémentaire), car ces coûts seront entièrement financés par les redevances.

Finance numérique: loi sur la résilience opérationnelle numérique (DORA)

2020/0266(COD) - 07/12/2021 - Rapport déposé de la commission, 1ère lecture/lecture unique

La commission des affaires économiques et monétaires a adopté le rapport de Billy KELLEHER (Renew Europe, IE) sur la 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.

La proposition de la Commission relative à un acte législatif sur la résilience opérationnelle numérique du secteur financier (DORA) vise à définir des exigences uniformes concernant la sécurité des réseaux et des systèmes d'information en vue de mettre en place un cadre global qui améliorera la gestion des risques liés au numérique par les entités financières.

La commission compétente a recommandé que la position du Parlement européen adoptée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition comme suit:

Exigences uniformes

Les exigences applicables aux entités financières concerneront : i) la gestion des risques liés aux technologies de l'information et de la communication (TIC); ii) la notification, aux autorités compétentes, des incidents majeurs liés à l'informatique; iii) la notification aux autorités compétentes, par les établissements de crédit, les établissements de paiement et les établissements de monnaie électronique, des incidents opérationnels ou de sécurité majeurs liés au paiement; iv) les tests de résilience opérationnelle numérique; v) le partage d'informations et de renseignements en rapport avec les cybermenaces et les cybervulnérabilités; vi) les mesures destinées à garantir la gestion solide du risque lié aux tiers prestataires de services informatiques par les entités financières.

Le règlement serait sans préjudice des compétences des États membres concernant la préservation de la sécurité publique, de la défense et de la sécurité nationale.

Champ d'application

La proposition s'appliquerait aux intermédiaires d'assurance, **qui ne sont pas des micro, petites ou moyennes entreprises**, à l'exception des entreprises qui dépendent exclusivement de systèmes de vente automatisés organisés. Les contrôleurs légaux des comptes et les cabinets d'audit de petite et moyenne taille seraient également exclus du champ d'application du règlement, sauf cas exceptionnels. Le règlement s'appliquerait aux prestataires de **services informatiques intra-groupe**, à l'exception du cadre de supervision visé au chapitre V.

Principe de proportionnalité

Le texte amendé précise que les entités financières devront mettre en œuvre les règles introduites par les chapitres II (gestion des risques), III (gestion, classification et notification des incidents liés à l'informatique) et IV (tests de résilience) conformément au principe de proportionnalité, **en tenant compte de leur taille, de la nature, de l'ampleur et de la complexité** de leurs services, activités et opérations et de leur profil de risque global.

Le règlement ne s'appliquerait pas aux petites entreprises d'investissement non interconnectées, aux établissements de crédit et aux établissements de monnaie électronique exemptés en vertu des directives européennes pertinentes. Il ne s'appliquerait pas non plus aux petites institutions de retraite professionnelle. Ces entreprises et entités exemptées devraient néanmoins mettre en place un cadre de gestion des risques informatiques solide et documenté, lequel serait réexaminé au moins une fois par an.

Gouvernance et organisation

Les entités financières devront disposer d'un **cadre de gouvernance et de contrôle interne** qui garantisse une gestion efficace et prudente de tous les risques informatiques en vue d'atteindre un niveau élevé de résilience opérationnelle numérique. L'organe de direction devra mettre en place des procédures et des stratégies visant à garantir le maintien de normes élevées en matière de sécurité, de confidentialité et d'intégrité des données.

Identification, protection, prévention, détection des risques

Les entités financières devront entre autres i) examiner si nécessaire, et au moins une fois par an, la criticité ou l'importance des fonctions opérationnelles liées à l'informatique, ii) garantir que les données sont protégées contre les risques informatiques internes, y compris les risques liés à une mauvaise administration ou à un mauvais traitement et à une erreur humaine; iii) consigner tous les incidents liés à l'informatique ayant des effets sur la stabilité, la continuité ou la qualité des services financiers.

La **politique de continuité** des activités informatiques devrait avoir pour but de gérer et d'atténuer les risques susceptibles d'avoir une incidence préjudiciable sur les systèmes et les services informatiques des entités financières ainsi que de faciliter leur rétablissement rapide si nécessaire.

Les **programmes de sensibilisation** à la sécurité informatique devraient s'appliquer à l'ensemble du personnel, tandis que les formations à la résilience opérationnelle numérique devraient s'appliquer, au minimum, à tous les employés disposant de droits d'accès direct aux systèmes informatiques.

Notification des incidents majeurs liés à l'informatique

Les entités financières pourraient notifier, **sur une base volontaire**, les cybermenaces importantes à l'autorité compétente concernée lorsqu'elles estiment que la menace est pertinente pour le système financier, les utilisateurs de services ou les clients.

L'autorité compétente devrait être informée en tout état de cause **dans les 24 heures** suivant la prise de connaissance d'un incident en ce qui concerne les incidents qui perturbent de manière significative la disponibilité des services fournis par l'entité ou qui ont une incidence sur l'intégrité, la confidentialité ou la sécurité des données à caractère personnel conservées par l'entité financière. En ce qui concerne les incidents qui ont une incidence significative autre que la disponibilité des services fournis par l'entité financière, l'autorité compétente devrait être informée dans les 72 heures.

Dès réception du rapport d'incident, l'autorité compétente devrait fournir, dans les meilleurs délais, des précisions sur l'incident majeur lié à l' informatique à l'ABE, à l'AEMF ou à l'AEAPP, ainsi qu'à la BCE, le cas échéant. Le Conseil de résolution unique (CRU) devrait être informé lorsque l' entité financière touchée relève du règlement relatif au mécanisme de résolution unique, tandis que les centres de réponse aux incidents de sécurité informatique (CSIRT) devraient être avisés lorsque les entités touchées relèvent de la directive sur la sécurité des réseaux et des systèmes d' information (SRI).

Tests

Les tests de pénétration fondés sur la menace devraient couvrir au minimum **les fonctions et les services critiques ou importants** d'une entité financière. En outre, le texte a été modifié pour ce qui est de la participation des tiers prestataires de services informatiques aux tests de pénétration fondés sur la menace. Lorsque la participation d'un tiers prestataire de services informatiques est susceptible de porter atteinte à la qualité du service fourni à d'autres clients, ledit tiers prestataire aurait la possibilité de conclure des accords contractuels au nom de l'ensemble des utilisateurs de l'entité financière qui ont recours à ses services en vue de mener des tests groupés.

À l'issue du test, une fois que les rapports et les plans de mesures correctives ont été approuvés, l'entité financière et les testeurs externes devraient fournir à l'autorité publique unique désignée, conformément au règlement, un rapport confidentiel des résultats du test et la documentation confirmant que le test a été effectué conformément aux exigences.

Bonne gestion des risques liés aux tiers prestataires de services informatiques

Les entités financières devraient tenir et mettre à jour **un registre d'informations en rapport avec tous les accords contractuels** portant sur l'utilisation de services informatiques fournis par des tiers prestataires de services informatiques qui appuient des fonctions critiques ou importantes. Les accords contractuels relatifs à l'utilisation de services informatiques devraient permettre aux entités financières de prendre les mesures correctives adéquates, qui pourront comporter **la résiliation complète des accords** si aucune rectification n'est possible ou la résiliation partielle des accords, dans certaines circonstances.

En vue de réduire les risques de perturbations au niveau de l'entité financière, dans des circonstances justifiées et en accord avec ses autorités compétentes, l'entité financière pourrait décider de ne pas résilier les accords contractuels conclus avec le tiers prestataire de services informatiques avant d'être en mesure de changer de tiers prestataire de services informatiques ou de recourir à des solutions sur site en fonction de la complexité du service fourni.

Enfin, lorsque des accords contractuels relatifs à l'utilisation de services informatiques qui appuient des fonctions critiques ou importantes sont conclus avec un **tiers prestataire de services informatiques établi dans un pays tiers**, les entités financières devraient également tenir compte du respect de la protection des données et de l'application effective des règles définies dans le présent règlement.

Finance numérique: loi sur la résilience opérationnelle numérique (DORA)

2020/0266(COD) - 10/11/2022 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté par 556 voix pour, 18 contre et 38 abstentions, une résolution législative sur la 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.

Le règlement sur la résilience opérationnelle numérique (DORA) vise à **atteindre un niveau élevé de résilience opérationnelle numérique** pour toutes les entités financières réglementées, telles que les banques, les compagnies d'assurance et les entreprises d'investissement.

DORA crée un cadre réglementaire sur la résilience opérationnelle numérique dans lequel toutes les entreprises doivent s'assurer qu'elles peuvent résister à tous les types de perturbations et de menaces liées aux TIC, y réagir et s'en remettre. Les nouvelles règles constitueront un cadre solide qui renforcera la sécurité informatique du secteur financier.

La position du Parlement européen arrêtée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition comme suit:

Exigences uniformes

DORA fixe des exigences uniformes pour la sécurité des réseaux et des systèmes d'information des entreprises et des organisations opérant dans le secteur financier, comme suit:

- les exigences applicables aux entités financières en ce qui concerne: i) la gestion des risques liés aux technologies de l'information et de la communication (TIC); ii) la notification, aux autorités compétentes, des incidents majeurs liés aux TIC et la notification, à titre volontaire, des cybermenaces importantes aux autorités compétentes; iii) la notification aux autorités compétentes, par les entités financières des incidents opérationnels ou de sécurité majeurs liés au paiement; iv) les tests de résilience opérationnelle numérique; v) le partage d'informations et de renseignements en rapport avec les cybermenaces et les cybervulnérabilités; vi) les mesures destinées à garantir la gestion saine du risque lié aux prestataires tiers de services TIC;

- les exigences relatives aux accords contractuels conclus entre des prestataires tiers de services TIC et des entités financières;

- les règles relatives à l'établissement du cadre de supervision applicable aux prestataires tiers critiques de services TIC lorsqu'ils fournissent des services à des entités financières, ainsi que celles liées à l'exercice des tâches dans ce cadre.

Champ d'application

La nouvelle règlementation s'appliquera à **presque toutes les entités financières**. Elle ne s'appliquera pas aux intermédiaires d'assurance qui sont des microentreprises ou des petites ou moyennes entreprises. Les **cabinets d'audit** ne seront pas soumis au règlement DORA, mais feront partie d'un futur réexamen du règlement, dans le cadre duquel une éventuelle révision des règles pourrait être envisagée.

Principe de proportionnalité

Le texte amendé précise que les entités financières devront mettre en œuvre les règles relatives à la gestion des risques conformément au principe de proportionnalité, en tenant compte de leur taille et de leur profil de risque global ainsi que de la nature, de l'ampleur et de la complexité de leurs services, activités et opérations.

Gouvernance et organisation

Les entités financières devront disposer d'un **cadre de gouvernance et de contrôle interne** garantissant une gestion efficace et prudente du risque lié aux TIC en vue d'atteindre un niveau élevé de résilience opérationnelle numérique. L'organe de direction de l'entité financière définira, approuvera, supervisera et sera responsable de la mise en œuvre de toutes les dispositions relatives au cadre de gestion du risque lié aux TIC.

Prestataires tiers critiques de services TIC établi dans un pays tiers

Les **autorités européennes de surveillance** (AES), agissant par l'intermédiaire du comité mixte et sur recommandation du forum de supervision établi conformément au règlement désigneront les prestataires tiers de services TIC qui sont critiques pour les entités financières, à l'issue d'une évaluation. Afin que la supervision puisse être correctement mise en œuvre, les entités financières ne pourront faire appel aux services d'un prestataire tiers de services TIC établi dans un pays tiers et ayant été désigné comme critique que si ce dernier a établi **une filiale dans l'Union** dans un délai de 12 mois à compter de la désignation.

Cadre de supervision

Les superviseurs principaux se verront confier les pouvoirs nécessaires pour mener des enquêtes, réaliser des inspections sur place et hors site des locaux et sites des prestataires tiers critiques de services TIC et obtenir des informations complètes et actualisées. Ces pouvoirs permettront au superviseur principal (à savoir l'AES désignée conformément au règlement) de se faire une idée précise du type, de la dimension et des incidences du risque que les prestataires tiers de services TIC représentent pour les entités financières et, en définitive, pour le système financier de l'Union.

Afin de garantir une approche cohérente en matière d'activités de supervision et en vue de permettre la coordination des stratégies générales de supervision ainsi que des approches opérationnelles et des méthodes de travail cohérentes, les superviseurs principaux désignés devront mettre en place **un réseau de supervision commun** pour assurer la coordination de leurs activités au cours des phases préparatoires et durant l'exécution des activités de supervision de leurs prestataires tiers critiques de services TIC respectifs qui font l'objet d'une supervision.

Le superviseur principal sera également en mesure d'exercer ses pouvoirs de supervision **dans les pays tiers.** L'exercice de ces pouvoirs dans les pays tiers lui permettra d'examiner les installations à partir desquelles les services TIC ou d'appui technique sont effectivement fournis ou gérés par le prestataire tiers critique de services TIC.

Tests de résilience opérationnelle numérique

Afin d'évaluer l'état de préparation en vue du traitement d'incidents liés aux TIC, de recenser les faiblesses, les défaillances et les lacunes en matière de résilience opérationnelle numérique et de mettre rapidement en œuvre des mesures correctives, les entités financières, autres que les microentreprises, devront établir, maintenir et réexaminer **un programme solide et complet de tests de résilience opérationnelle numérique,** qui fait partie intégrante du cadre de gestion du risque lié aux TIC.

En vertu du règlement amendé, des **tests de pénétration fondés sur la menace** seront effectués en mode fonctionnel et il sera possible d'inclure les autorités de plusieurs États membres dans les procédures de test. Le recours à des auditeurs internes ne sera possible que dans un certain nombre de circonstances strictement limitées, sous réserve de conditions de sauvegarde.

Protection des données

Les AES et les autorités compétentes ne seront autorisées à traiter des données à caractère personnel que lorsque cela est nécessaire à l'accomplissement de leurs obligations et missions respectives en vertu du présent règlement, en particulier en matière d'enquête, d'inspection, de demande d'informations, de communication, de publication, d'évaluation, de vérification, d'évaluation et d'élaboration de plans de supervision.