SECRÉTARIAT GÉNÉRAL

Notice décrivant le cadre de gestion des risques liés aux TIC au sens du règlement européen n°2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier (DORA)

Secteurs de l'assurance, de la réassurance et la retraite professionnelle supplémentaire

(Version du 18/12/2024)

Table des matières

1. Introduction

1 Le présent document (la « Notice » dans la suite) a pour objet de présenter le cadre de gestion des risques liés aux technologies de l'information et de la communication (TIC) au sens des dispositions du règlement (UE) n°2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier (ci-après, le « règlement DORA ») et des textes d'application associés. De manière concomitante, elle a aussi pour vocation à préciser les éléments y afférant qui devront être repris dans le Rapport régulier au contrôleur (RSR) pour les entités soumises au cadre prudentiel solvabilité 2 (cf. partie 2).

Selon la définition de l'article 3(5) du règlement DORA, on entend par « risque lié aux TIC », toute circonstance raisonnablement identifiable liée à l'utilisation des réseaux et des systèmes d'information qui, si elle se concrétise, peut compromettre la sécurité des réseaux et des systèmes d'information, de tout outil ou processus dépendant de la technologie, du fonctionnement et des processus ou de la fourniture de services en produisant des effets préjudiciables dans l'environnement numérique ou physique.

2 Outre le règlement DORA, la présente Notice se réfère au règlement délégué (UE) n°2024/1774 de la Commission du 13 mars 2024, complétant le règlement DORA par des normes techniques de réglementation précisant les outils, méthodes, processus et politiques de gestion du risque lié aux TIC et le cadre simplifié de gestion du risque lié aux TIC. Elle se réfère également au règlement délégué (UE) n°2024/1773 de la Commission du 13 mars 2024, complétant le règlement DORA par des normes techniques de réglementation précisant le contenu de la politique relative aux tiers.

3 La présente Notice vise les entités listées suivantes :

a. les entreprises d'assurance ou de réassurance relevant du régime « Solvabilité II » mentionnés aux articles L. 310-3-1 du code des assurances, L. 211-10 du code de la mutualité et L. 931-6 du code de la sécurité sociale ;
b. les organismes de retraite professionnelle supplémentaire (ORPS) mentionnés aux articles L. 381-1 du code des assurances, L. 214-1 du code de la mutualité et L. 942-1 du code de la sécurité sociale, qui comptent plus de quinze affiliés au total ;
c. les intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire mentionnés au paragraphe III de l'article L. 511-1 du code des assurances, qui ne sont ni des microentreprises, ni des petites ou moyennes entreprises[1].

Ces obligations précisent notamment les diligences à effectuer, afin de tenir compte de l'importance de la gestion du risque lié aux TIC, et de sa prise en compte par la gouvernance et en cas de recours à des prestataires externes.

4 Au vu des trois catégories d'entités différentes mentionnées au paragraphe 3, la présente Notice contient cinq parties, dont l'introduction, qui ne sont pas toutes applicables à l'ensemble de ces entités. Ainsi :
- la partie 2 relative aux informations à communiquer dans le cadre du RSR, ne concerne que les entités mentionnées au point a du paragraphe 3 ;
- la partie 3 relative aux outils, méthodes, processus et politiques de gestion du risque lié aux TIC, s'applique à toutes les entités mentionnées au paragraphe 3, sauf les petits ORPS[2] ;
- la partie 4 relative au cadre simplifié de gestion du risque lié aux TIC, ne concerne que les petits ORPS ;
- la partie 5 relative au rapport sur le réexamen du cadre de gestion du risque lié aux TIC, s'applique à toutes les entités mentionnées au paragraphe 3, sans exception.

5 La présente Notice vise à apporter des explications aux entités mentionnées au paragraphe 3, sur les modalités de mise en œuvre du règlement DORA dont l'entrée en application est prévue pour le 17 janvier 2025. Son contenu ne saurait toutefois épuiser toutes les questions soulevées par la mise en œuvre d'une obligation du règlement DORA, et sera ainsi amené à évoluer. Par ailleurs, ce document ne préjuge pas des décisions individuelles qui pourraient être prises par l'ACPR, sur la base des situations particulières qu'elle pourra être amenée à examiner.

6 Le règlement DORA ayant réaffirmé, notamment à son article 4, un principe d'application des mesures de gestion du risque informatique proportionnelle à la nature, à l'ampleur et à

[1] Au regard des seuils mentionnés au point 64 de l'article 3 du règlement DORA.
[2] Petit ORPS : un ORPS qui gère des régimes de retraite qui, ensemble, comptent moins de cent affiliés au total.

la complexité des risques inhérents à l'activité des entreprises assujetties concernées, les indications fournies par la Notice doivent être lues dans le respect de ce principe. À ce titre, l'ACPR tiendra compte de l'organisation interne des entreprises assujetties, de la nature, du périmètre et de la complexité des produits et services que ces entreprises fournissent ou comptent fournir. Pour les entités financières du secteur des assurances n'entrant pas dans le périmètre de DORA, il est à noter que des mesures doivent être prises pour gérer de manière adéquate les risques informatiques et cybernétique dans le cadre d'une gestion saine et prudente de l'activité de l'entreprise.

7 Sauf mention contraire, dans cette Notice, « l'entreprise » désigne les entités mentionnées au paragraphe 3.

8 La présente notice est applicable à compter du jour de sa publication au registre officiel de l'ACPR mais ne prendra ses effets qu'à compter de l'entrée en vigueur du règlement DORA (17 janvier 2025).

2. Informations à communiquer dans le cadre du RSR[3]

9 Les entités soumises au cadre réglementaire Solvabilité 2 remettent un rapport destiné au superviseur, nommé « rapport régulier au contrôleur » dont le principe est posé au 1 de l'article 304 du règlement délégué modifié et contenu détaillé aux articlées 307 et suivants du même texte.

10 Sous le principe des orientations précisées ci-après, l'entité se réfère aux précisions qui ont vocation à être apportées à la notice « *Communication d'informations à l'autorité de contrôle et informations à destination du public (RSR/SFCR) pour les entreprises et groupes d'assurance soumis à la Directive Solvabilité 2* » dans sa version du 17/07/2023.

11 L'entreprise fournit des informations sur le cadre de gouvernance des risques liés aux TIC et à la sécurité des réseaux et des systèmes d'information (article 5 du règlement DORA).

12 L'entreprise fournit des informations sur sa stratégie de résilience opérationnelle numérique (cf. art. 6.8 du règlement DORA) et sur l'organisation de son cadre de gestion des risques associés aux TIC (articles 5.1, 6.1, et 16.1.a du règlement DORA).

3. Outils, méthodes, processus et politiques de gestion du risque lié aux TIC

13 Cette partie s'adresse à l'ensemble des entités listées au paragraphe 3, sauf les petits ORPS.

3.1. Stratégie de résilience opérationnelle numérique et gouvernance

14 L'entreprise documente sa stratégie de résilience opérationnelle numérique en précisant notamment sa gouvernance et son intégration dans le système de gestion des risques liés

[3] Il convient d'entendre RSR solo et RSR groupe : l'article 372 du règlement délégué n°2015-35 prévoit que « *les articles 304 à 311 du présent règlement s'appliquent aux informations que doivent soumettre au contrôleur du groupe les entreprises d'assurance et de réassurance participantes, les sociétés holding d'assurance ou les compagnies financières holding mixtes*. »

aux technologies de l'information et de la communication (TIC), ainsi que les moyens qui lui sont dédiées[4].

15 L'entreprise documente sa stratégie de résilience opérationnelle numérique précisant les méthodes pour parer aux risques qui pèsent sur les actifs informationnels et les actifs de TIC, y compris les logiciels, le matériel informatique, les serveurs, ainsi que toutes les composantes et infrastructures physiques pertinentes, afin de garantir que tous les actifs informationnels et actifs de TIC sont correctement protégés contre les risques, y compris les dommages et les accès ou utilisations non autorisés, selon les méthodes mentionnées à l'article 6 (8) du règlement Dora.

La stratégie de résilience opérationnelle numérique peut comprendre le cas échéant la stratégie globale multifournisseurs intégrant notamment les principales relations de dépendance à l'égard de prestataires tiers de service TIC et exposant les raisons qui sous-tendent la combinaison de prestataires tiers de services TIC choisis conformément au point 9 de l'article précité.

16 L'entreprise documente la gestion efficace et prudente du risque lié aux TIC par son cadre de gouvernance et de contrôle interne conformément à l'article 5 (1) du règlement DORA. À cet égard, son organe de direction définit, approuve, supervise et est responsable de la mise en œuvre de toutes les dispositions relatives au cadre de gestion du risque lié aux TIC, conformément au point 2 de l'article précité. La documentation comprend l'ensemble des éléments précisés à l'article 3 du règlement délégué UE n°2024/1774.

3.2. Gestion des risques liés aux TIC

17 En vue de satisfaire les objectifs assignés par les articles 5 et 6 du règlement DORA sur la résilience opérationnelle numérique du secteur financier, l'entreprise élabore, documente, met à jour régulièrement, met en œuvre et tient à disposition du superviseur les politiques et procédures de gestion du risque lié aux TIC qui contiennent l'ensemble des éléments définis à l'article 3 du règlement (UE) n°2024/1774.

Elle traite en particulier les éléments suivants :

- l'indication de l'approbation du niveau de tolérance au risque lié aux TIC ;
- une procédure et une méthode d'évaluation des vulnérabilités et des menaces qui affectent ou peuvent affecter les fonctions opérationnelles soutenues et les systèmes de TIC et actifs de TIC qui les soutiennent, ainsi que les indicateurs quantitatifs ou qualitatifs requis ;
- la procédure de détermination, de mise en œuvre et de documentation des mesures de traitement du risque lié aux TIC ;
- les éléments requis au titre des risques résiduels liés aux TIC ;
- les dispositions de suivi ;
- la prise en compte de toute modification de la stratégie commerciale et de la stratégie de résilience opérationnelle numérique de l'entreprise.

[4] Sont également compris les programmes de sensibilisation à la sécurité des TIC et des formations à la résilience opérationnelle numérique qu'elles intègrent à leurs programmes de formation du personnel au sens du paragraphe 6 de l'article 13 du règlement DORA n°2022-2554 (cf. également l'article 5.2.g du même règlement).

3.3. Sécurité des réseaux et des systèmes de TIC

18 En vue de satisfaire les objectifs assignés par l'article 9 du règlement DORA sur la résilience opérationnelle numérique du secteur financier, l'entreprise élabore, documente, met à jour régulièrement, met en œuvre et tient à disposition du superviseur les politiques de sécurité des TIC, la sécurité de l'information et les procédures, protocoles et outils y afférents qui :

- garantissent la sécurité des réseaux ;
- comportent des garanties contre les intrusions et les utilisations abusives des données ;
- préservent la disponibilité, l'authenticité, l'intégrité et la confidentialité des données, y compris en recourant à des techniques cryptographiques ;
- garantissent une transmission précise et rapide des données sans perturbation majeure et sans retard injustifié.

Elle s'assure que ces politiques respectent les conditions mentionnées au 2 de l'article 2 du règlement délégué n°2024/1774.

19 Aux fins des garanties de sécurité des réseaux mentionnées au paragraphe précédent, l'entreprise élabore, documente, met à jour régulièrement, met en œuvre et tient à disposition du superviseur les protocoles et les outils de gestion de la sécurité des réseaux définis à l'article 13 du règlement délégué précité.

20 Aux fins des garanties visant à préserver la disponibilité, l'authenticité[5], l'intégrité et la confidentialité des données, l'entreprise élabore, documente, met à jour régulièrement, met en œuvre et tient à disposition du superviseur les politiques, procédures, protocoles et outils de protection des informations en transit (cf. en ce sens l'article 14 du règlement délégué n°2024-1774).

Tel est notamment le cas de la politique en matière de chiffrement et de contrôles cryptographiques et de la politique de gestion des clés cryptographiques, au sens des dispositions des articles 6 et 7 du règlement délégué précité.

3.4. Gestion des opérations de TIC

3.4.1. Politique et procédure de gestion des actifs de TIC

21 L'entreprise doit disposer d'une politique de gestion des actifs de TIC conformément aux article 4(2) du règlement délégué (UE) n°2024/1774.

22 L'entreprise élabore, documente et met en œuvre une procédure de gestion des actifs de TIC (article 5 du règlement délégué précité). Cette procédure précise les critères utilisés pour évaluer la criticité des actifs de TIC en fonction :

a du risque lié aux TIC associé à ces fonctions « métiers » et de leur dépendance à l'égard des actifs informationnels ou des actifs de TIC ;
b de l'incidence que la perte de confidentialité, d'intégrité et de disponibilité de ces actifs informationnels et ces actifs de TIC aurait sur les processus opérationnels et les activités de l'entreprise.

[5] Au sens des définitions de la CNIL.

3.4.2. Politique de ressources humaines et de contrôle d'accès

23 L'entreprise inclut dans sa politique en matière de ressources humaines ou dans d'autres politiques pertinentes des éléments liés à la sécurité des TIC (article 19 du règlement délégué n°2024/1774) :

- l'identification et l'attribution de toute responsabilité spécifique en matière de sécurité des TIC ;
- l'obligation pour les membres du personnel de l'entreprise et des prestataires tiers de services TIC qui utilisent des actifs de TIC de l'entreprise ou qui y ont accès :
    - d'être informés des politiques, procédures et protocoles de sécurité des TIC de l'entreprise et de les respecter ;
    - de connaitre les canaux de notification mis en place par l'entreprise pour la détection des comportements anormaux y compris le cas échéant les canaux de signalement établis conformément à la directive (UE) n°2019/1937 du Parlement européen et du Conseil ;
    - de restituer à l'entité financière après la cessation de leur emploi, tous les actifs de TIC et tous les actifs informationnels matériels en leur possession qui appartiennent à l'entreprise.

24 L'entreprise élabore, documente et met en œuvre des politiques et procédures de gestions de l'identité conformément à l'article 20 (1) du règlement délégué n°2024/1774. Celles-ci doivent contenir l'ensemble des éléments cités au point 2 du même article.

25 L'entreprise élabore, documente et met en œuvre une politique sur le contrôle des droits de gestion des accès aux actifs de TIC (article 21 du règlement délégué n°2024/1774). En particulier, cette politique doit inclure :

- l'attribution des droits d'accès aux actifs de TIC selon les principes du besoin d'en connaitre du besoin d'en disposer et du moindre privilège y compris pour l'accès à distance et l'accès d'urgence ;
- une séparation des tâches visant à empêcher un accès injustifié à des données critiques ou à empêcher l'attribution de combinaisons de droits d'accès susceptibles d'être utilisées pour contourner les contrôles ;
- des dispositions sur la responsabilité des utilisateurs, en limitant, dans la mesure du possible, l'utilisation de comptes utilisateurs génériques ou partagés et en veillant à ce que les utilisateurs soient à tout moment identifiables pour les actions effectuées dans les systèmes de TIC ;
- des dispositions sur les restrictions d'accès aux actifs de TIC, prévoyant des contrôles et des outils pour empêcher tout accès non autorisé ;
- des procédures de gestion de comptes permettant d'accorder, de modifier ou de révoquer des droits d'accès pour les comptes d'utilisateurs et les comptes génériques, y compris les comptes génériques d'administrateur comportant les dispositions relatives aux éléments cités à l'article 21(e) du règlement délégué n°2024/1774 ;
- les protocoles et procédures relatifs aux mécanismes d'authentification forte (article 9(4)(d) du règlement DORA et article 21 (f) du règlement délégué n°2024/1774) ;
- toute information relative aux mesures de contrôle de l'accès physique aux actifs de TIC (article 21(g) du règlement délégué n°2024/1774).

3.4.3. Politiques et procédures couvrant l'exploitation, la surveillance et le contrôle des systèmes et services informatiques

35 En vue de de garantir la confidentialité, l'intégrité et la disponibilité des systèmes, l'entreprise élabore, documente et met en œuvre des politiques et procédures définissant la manière dont elle exploite, surveille, contrôle et restaure les systèmes et les services de TIC, en particulier ceux qui soutiennent des fonctions critiques ou importantes[6] (article 9(2) du règlement DORA et article 8(1) du règlement délégué n°2024/1774).

36 Les documents mentionnés au paragraphe 35 incluent des procédures de planification et de surveillance des performances et des capacités permettant de prévenir, détecter et résoudre tout problème de performance important dans les systèmes de TIC, ainsi que toute limite de capacité (article 9 du règlement délégué n°2024/1774).

37 Les documents mentionnés au paragraphe 35 incluent des procédures de gestion des vulnérabilités qui prévoient notamment diverses revues et évaluations en matière de sécurité de l'information, afin de garantir une identification efficace des vulnérabilités présentes au sein de ses systèmes et services de TIC, y compris quand ces services sont fournis par un prestataire tiers (article 10(1) et article 10(2) du règlement délégué n°2024/1774).

38 Les documents mentionnés au paragraphe 35 incluent des procédures de gestion des correctifs qui prévoient notamment l'identification et l'évaluation des correctifs et mises à jour logiciels et matériels disponibles, la définition des procédures d'urgence pour l'application des correctifs et des mises à jour des actifs de TIC, la fixation des délais pour l'installation des correctifs et mises à jour logiciels et matériels, ainsi que des procédures de remontée d'informations lorsque ces délais ne peuvent pas être respectés (article 10(3) et article 10(4) du règlement délégué 2024/1774).

39 Les documents mentionnés au paragraphe 35 incluent une procédure de sécurité des données et des systèmes de TIC qui contient tous les éléments mentionnés à l'article 11(2) du règlement délégué 2024/1774.

40 L'entreprise établit, maintient et réexamine un programme de tests de résilience opérationnelle numérique afin d'évaluer l'état de préparation en vue du traitement d'incidents liés aux TIC (article 24 du règlement DORA). Les résultats de ces tests font partie des informations incluses dans le rapport sur le réexamen du cadre de gestion du risque lié aux TIC (cf. partie 5). L'entreprise veille à soumettre, au moins une fois par an, tous les systèmes et applications de TIC qui soutiennent des fonctions critiques ou importantes à des tests appropriés.

3.4.4. Politique de gestion des incidents liés aux TIC

[6] « fonction critique ou importante » : une fonction dont la perturbation est susceptible de nuire sérieusement à la performance financière d'une entité financière, ou à la solidité ou à la continuité de ses services et activités, ou une interruption, une anomalie ou une défaillance de l'exécution de cette fonction est susceptible de nuire sérieusement à la capacité d'une entité financière de respecter en permanence les conditions et obligations de son agrément, ou ses autres obligations découlant des dispositions applicables du droit relatif aux services financiers (définition du point 22 de l'article 3 du règlement DORA).

41 L'entreprise élabore, documente et met en œuvre une politique décrivant les principes de détection et de gestion des incidents liés aux TIC (article 17 et article 10 du règlement DORA). Ces principes incluent notamment :

- une stratégie de communication interne et externe en cas d'incidents liés aux TIC (article6 (8)(h) du règlement DORA) ;
- des mécanismes techniques, organisationnels et opérationnels de détection rapide des activités et comportements anormaux (y compris les problèmes de performance réseaux de TIC et les incidents) et mécanismes d'analyse des incidents importants et récurrents (article 22(c) et article 22(e) du règlement délégué n°2024/1774) ;
- la conservation des éléments de preuve relatifs aux incidents liés aux TIC dans le respect des dispositions prévues par le règlement (UE) n°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 (article 22(d) du règlement délégué n°2024/1774) ;
- l'utilisation d'outils générant des alertes pour les activités et comportements anormaux, au moins pour les actifs de TIC et les actifs informationnels qui soutiennent des fonctions critiques et journalisent l'ensemble des activités anormales (article 23(2)(b) et article 23(4) du règlement délégué n°2024/1774) ;
- la communication, sur demande, aux autorités compétentes, des changements mis en œuvre suite à l'examen post-incident (article 13(2) du règlement DORA).

3.4.5. Politiques et procédures de gestion du changement et des projets

42 L'entreprise élabore, documente et met en œuvre des politiques de gestion des changements dans les TIC (article 9(4)(e) du règlement DORA). Ces politiques comprennent notamment les documents mentionnés aux paragraphes 43 à 45.

43 L'entreprise élabore, documente et met en œuvre une politique de gestion des projets TIC conformément aux dispositions de l'article 15 du règlement délégué n°2024/1774. Cette politique doit notamment prévoir que les projets ayant une incidence sur les fonctions critiques ou importantes de l'entreprise soient notifiés à l'organe de direction individuellement ou de façon groupée, ainsi que périodiquement et, si nécessaire, chaque fois qu'un évènement l'exige

44 L'entreprise élabore, documente et met en œuvre :

- une politique régissant l'acquisition, le développement et la maintenance des systèmes de TIC (article 16 du règlement délégué n°2024/1774). En particulier, cette politique précisera les mesures visant à atténuer le risque d'altération involontaire ou de manipulation intentionnelle des systèmes de TIC lors de l'acquisition, du développement, de la maintenance et du déploiement des systèmes dans l'environnement de production (article 16(1)(c) du règlement délégué précité) ;
- une procédure d'acquisition, de développement et de maintenance des systèmes de TIC pour les tests et d'approbation de tous les systèmes de TIC avant leur utilisation et après les opérations de maintenance (article 16(2) du règlement délégué n°2024/1774). Cette procédure comprend notamment :
    - i) la réalisation d'examens du code source des systèmes et applications (notamment des tests statiques et dynamiques incluant des tests de sécurité

pour les systèmes et applications exposés à l'internet) (article 16(3) du règlement délégué précité)
    - ii) des tests de sécurité des progiciels au plus tard lors de la phase d'intégration (article 16(4) du même règlement délégué).

45 L'entreprise élabore, documente et met en œuvre des procédures de gestion des changements TIC (article 17(1) du règlement délégué n°2024/1774). En particulier, ces procédures comprennent :
- i) des mécanismes visant à garantir l'indépendance des fonctions de mise en œuvre et de validation des changements liées aux TIC ainsi que la clarté des rôles et responsabilités (points b et c de l'article précité) ;
- ii) des procédures de repli dans le cas de changements qui n'ont pas été mis en œuvre avec succès (point e de l'article précité)
- iii) des procédures d'évaluation, d'approbation et de réévaluation des changements d'urgence après leur mise en œuvre (point g du même article).

3.5. Gestion de la continuité d'activité

3.5.1. Description du maintien en condition opérationnelle des systèmes et solutions de TIC (continuité des activités de TIC)

46 L'entreprise élabore, documente et met en œuvre une politique de continuité des activités de TIC (article 11(2) du règlement DORA) incluant notamment (article 24 du règlement délégué n°2024/1774) :
- une description des rôles et responsabilités concernant la gestion de la continuité des activités de TIC ;
- les fonctions critiques ou importantes, les actifs informationnels et les actifs de TIC (y compris lorsque gérés par des prestataires) qui les soutiennent ainsi que leurs interdépendances , ;
- les objectifs et modalités de tests de continuité des activités de TIC ;
- l'interaction et l'alignement entre la continuité des activités de TIC et la continuité globale des activités.
- les scénarios de perturbation couverts (incidents opérationnels et de sécurité).

La politique de continuité des activités TIC est alignée sur la politique de communication visée à l'article 14, paragraphe 2, du règlement (UE) n°2022/2554 et les mesures de communication et de communication de crise visées à l'article 11, paragraphe 2, point e), du règlement (UE) n°2022/2554.

47 L'entreprise élabore, documente et met en œuvre les plans de réponse aux différents scénarios de perturbation pour les différents actifs de TIC supportant les processus critiques ou importants, y compris lorsqu'ils sont gérés par des prestataires, ainsi que sur l'indication des durées maximales d'interruption de service tolérées et de perte de données (article 26 du règlement délégué n°2024/1774). La construction de ces plans de réponse prend en compte les spécifications mentionnées dans le règlement délégué n°2024/1774.

48 L'entreprise élabore, documente et met en œuvre des tests de continuité des activités de TIC réalisés sur l'exercice (objectif, périmètre, champ couvert, calendrier), ainsi que leurs résultats et plans d'action associés (article 25 du règlement délégué n°2024/1774.

49 Le plan de réponse et de rétablissement des TIC mis en œuvre par l'entreprise fait l'objet de revues indépendantes de l'audit interne, dont les résultats sont documentés (article 11(3) du règlement DORA).

3.5.2. Description du dispositif de gestion de crise

50 L'entreprise élabore, documente et met en œuvre une procédure de gestion de crise (cf. point 41) qui inclut notamment :
- une description des rôles et responsabilités concernant la gestion de crise (article 11(7) du règlement DORA) ;
- une description du dispositif de gestion de crise (organisation, éléments déclencheurs des différents stades d'activation) ;
- une description des procédures et méthodes de rétablissement ;
- une présentation des cas d'activation du dispositif de gestion de crise au cours de l'exercice (exemple : grippe A [H1N1], Covid, panne informatique ou attaque cyber).

3.6. Gestion des risques liés aux prestataires tiers de services TIC

51 La gestion des risques liés aux tiers prestataires de services informatiques dans le cadre du règlement DORA complète les règles sectorielles existantes en matière d'externalisation qui continuent à devoir être respectées.

52 L'entreprise est tenue d'adopter, comme partie intégrante de son cadre de gestion du risque lié aux TIC, une stratégie en matière de risques liés aux prestataires tiers de services TIC, et de réexaminer régulièrement cette stratégie en tenant compte le cas échéant de la stratégie multi-fournisseurs visée à l'article 6(9) du règlement DORA. Conformément à l'article 28(2) du règlement DORA, la stratégie en matière de risques liés aux prestataires tiers de services TIC doit inclure une politique relative à l'utilisation des services TIC soutenant des fonctions critiques ou importantes qui sont fournis par des prestataires tiers de services TIC. Les principes généraux sont décrits au sein de l'article 28 du Règlement.

53 Le contenu détaillé de la politique mentionnée au paragraphe précédent, est précisé par le règlement délégué (UE) n°2024/1773. Les paragraphes suivants reprennent les principaux éléments attendus dans cette politique.

54 L'entreprise fournit des informations sur l'attribution de la fonction qui doit être mise en place pour assurer le suivi des accords conclus avec des prestataires tiers de services TIC qu'elle soit dévolue ou non à un membre de la direction générale, et définir les modalités de coopération entre cette fonction et les fonctions de contrôle.(article 5(3) du règlement DORA et article 3(5) du Règlement délégué n°2024/1773)

55 L'entreprise fournit des informations sur les critères de classification pour déterminer si le service TIC fourni soutient une fonction critique ou importante (article 3(22) du règlement DORA et article 3(2) du Règlement délégué 2024/1773).

56 L'entreprise précise les éléments justifiant le recours à des prestataires tiers de services TIC en fournissant une analyse préalable menée sur la criticité des fonctions critiques ou importantes,

ou des parties importantes de celles-ci, soutenues, une évaluation des risques associés et une description des critères de sélection des prestataires tiers potentiels (article 5 et 6 du Règlement délégué n°2024/1773).

57 L'entreprise fournit des informations sur les adaptations prises, au niveau de l'entité et aux niveaux sous-consolidé et consolidé, pour se conformer à l'exigence de tenue d'un registre d'informations en rapport avec tous les accords contractuels portant sur l'utilisation de services TIC fournis par des prestataires tiers de services TIC (article 28(3) du règlement DORA).

58 L'entreprise fournit une description des contrôles effectués dans le cadre d'un processus de diligence raisonnable, appliqué pour sélectionner et évaluer les prestataires tiers de services TIC avant la conclusion de tout accord contractuel, particulièrement pour les services soutenant des fonctions critiques ou importants.

59 L'entreprise fournit une description du dispositif de contrôle permanent et périodique qui porte sur les prestataires tiers, particulièrement pour les services TICS qui soutiennent une ou plusieurs fonctions critiques ou importantes.

60 L'entreprise fournit une description de la méthodologie d'évaluation de la qualité de la prestation (article 9 §2 du Règlement délégué n°2024/1773).

61 L'entreprise fournit une description du dispositif spécifique d'identification, de gestion et de suivi des risques associés à l'externalisation vers des prestataires tiers de services TIC, particulièrement pour les services qui portent sur des fonctions critiques ou importantes.

62 L'entreprise fournit une description des dispositifs mis en œuvre par l'établissement pour disposer de l'expertise nécessaire[7] à une supervision effective des accords contractuels qui permettent la réalisation des audits auprès des prestataires TIC, particulièrement pour les services TIC qui soutiennent une ou plusieurs fonctions critiques ou importantes.

63 L'entreprise fournit une description des procédures d'identification, d'évaluation et de gestion des conflits d'intérêts potentiels dans le cadre de la gestion des relations avec les prestataires de services TIC, y compris les conflits d'intérêt entre entités du même groupe (article 28(4) du règlement et article 7 du Règlement délégué n°2024/1773).

64 S'il existe des risques de concentration liés aux prestataires de services TIC, l'entreprise fournit une évaluation des avantages et des coûts des solutions alternatives envisageables (article 29(1) du règlement DORA.

65 L'entreprise fournit une description des plans de poursuite d'activité et de la stratégie de sortie qui porte sur les prestataires tiers, particulièrement pour les services TICS qui soutiennent une ou plusieurs fonctions critiques ou importantes.

66 L'entreprise fournit une description, formalisation et date(s) de mise à jour des procédures sur lesquelles s'appuie le contrôle permanent et périodique qui porte sur les prestataires tiers,

[7] Au sens des dispositions combinées des articles 3.3 et 6.1.e du règlement délégué 2024/1773.

particulièrement pour les services TICS qui soutiennent une ou plusieurs fonctions critiques ou importantes.

67 Lors de chaque réexamen du cadre de gestion du risque lié aux TIC, l'entreprise fournit une appréciation des résultats des contrôles de 2ème niveau qui portent sur les prestataires tiers, particulièrement pour les services TIC qui soutiennent une ou plusieurs fonctions critiques ou importantes.

68 Toutefois, les obligations d'information, notamment en ce qui concerne le registre d'information et la notification des accords contractuels ne sont pas couvertes par la présente Notice.

4. Cadre simplifié de gestion du risque lié aux TIC

69 La définition, à l'article 16 du règlement DORA, d'un cadre simplifié de gestion du risque lié aux TIC fait partie des mesures relatives à l'application du principe de proportionnalité mentionné au paragraphe 5 du présent document.

70 Ce cadre simplifié, détaillé aux articles 28 à 40 du règlement délégué (UE) n°2024/1774, s'applique aux petits ORPS mentionnés au paragraphe 6 du présent document (moins de cent affiliés).

5. Rapport sur le réexamen du cadre de gestion du risque lié aux TIC

71 Le cadre de gestion du risque lié aux TIC doit être documenté et réexaminé au moins une fois par an, ou périodiquement pour les microentreprises et les entités pour lesquelles le cadre simplifié s'applique. Il l'est également en cas de survenance d'incidents majeurs liés aux TIC.

72 Le réexamen s'inscrit dans un processus d'amélioration permanente sur la base des enseignements tirés de la mise en œuvre et du suivi. Il tient compte des conclusions tirées des tests de résilience opérationnelle numérique ou des processus d'audit pertinents.

73 Il est matérialisé par un rapport « sur le réexamen du cadre de gestion du risque lié aux TIC » qui est présenté à l'ACPR à sa demande, dans un format électronique interrogeable[8].

Excepté pour les petits ORPS mentionnés au paragraphe 6 du présent document, le rapport précité (article 6(5) du règlement DORA) respecte le format et le contenu définis à l'article 27 du règlement délégué (UE) 2024/1774 (pour une vision schématique de la structure et du contenu, cf. annexe 1 au présent document).

74 Pour les petits ORPS mentionnés au paragraphe 6 du présent document, le rapport précité (article 16(2) du règlement DORA) respecte le format et le contenu définis à l'article 41 du règlement délégué (UE) 2024/1774. Ce rapport contient notamment :

- Les principales insuffisances relevées, risques et anomalies détectées ;

[8] C'est-à-dire : word ou PDF autre que format « image ».

- Les mesures correctives engagées pour remédier aux insuffisances relevées, date de réalisation prévisionnelle de ces mesures et état d'avancement de leur mise en œuvre à la date de rédaction du présent rapport ;
- Les modalités de suivi des recommandations résultant des contrôles permanents (outils, personnes en charge) ;
- Les modalités de vérification de l'exécution dans des délais raisonnables des mesures correctrices décidées au sein de l'entreprise par les personnes compétentes.

75 Le rapport établi au titre de la première année d'entrée en vigueur du cadre réglementaire DORA (2025) décrit les éléments du cadre de gestion des risques liés aux TIC et souligne les sujets encore en développement ou qui restent à approfondir.

Annexe 1 : Structure et contenu du rapport sur le réexamen[9] du cadre de gestion du risque lié aux TIC

La structure ci-après, détaillée à l'article 27 du règlement délégué 2024-1774, s'applique aux entités relevant du cadre général.

Les organismes qui établissent le « rapport sur le réexamen du cadre simplifié de gestion du risque lié aux TIC » sont invitées à se référer aux dispositions de l'article 41 du même règlement.

Introduction

- Identité de l'organisme
- Description du contexte du rapport en ce qui concerne :
  - la nature, l'échelle et la complexité des services, activités et opérations de l'entité financière,
  - son organisation,
  - ses fonctions critiques recensées,
  - sa stratégie,
  - ses grands projets ou activités en cours,
  - ses relations et sa dépendance à l'égard de services et systèmes de TIC internes ou sous-traités,
  - ou les conséquences qu'une perte totale ou une dégradation grave de ces systèmes engendrerait en ce qui concerne les fonctions critiques ou importantes et l'efficience du marché ;
- Résumé, s'il y a lieu, des changements majeurs dont le cadre de gestion du risque lié aux TIC a fait l'objet depuis le rapport précédent;
- Synthèse du profil de risque lié aux TIC actuel et à court terme, en fonction de l'éventail des menaces recensées, de l'évaluation de l'efficacité des contrôles et de la posture de sécurité de l'organisme.

Date d'approbation du rapport par l'organe de direction de l'organisme

Mention du motif du réexamen du cadre de gestion du risque lié aux TIC, selon le cas :

- Réexamen annuel ou périodique
- Suite à incident majeur lié aux TIC

Dates de début et de fin de la période examinée

Mention de la fonction responsable du réexamen

Description des principales modifications et améliorations dont le cadre de gestion du risque lié aux TIC a fait l'objet depuis le réexamen précédent :

- Le rapport établi au titre de la première année d'entrée en vigueur du cadre réglementaire DORA décrit les éléments du cadre de gestion des risques liés aux TIC qui ont été définis en conformité avec le cadre réglementaire et ceux qui resteraient à mener ou à compléter.

[9] Au sens des points 71 et 72 de cette notice.

- L'analyse de l'incidence des modifications sur la stratégie de résilience opérationnelle numérique de l'entité financière, sur le cadre de contrôle interne des TIC de l'entité financière et sur la gouvernance de la gestion du risque lié aux TIC de l'organisme.

Résumé des conclusions du réexamen ainsi qu'une analyse et une évaluation détaillées de la gravité des faiblesses, des défaillances et des lacunes du cadre de gestion du risque lié aux TIC au cours de la période examinée

Description des mesures prises face aux faiblesses, défaillances et lacunes constatées, comprenant :

- Résumé des mesures prises pour remédier aux faiblesses, défaillances et lacunes constatées ;
- Date prévue pour la mise en œuvre des mesures et des dates relatives au contrôle interne de la mise en œuvre, y compris des informations sur l'état d'avancement de la mise en œuvre de ces mesures à la date de rédaction du rapport, en expliquant, le cas échéant, s'il existe un risque que les délais ne soient pas respectés ;
- Outils à utiliser et identification de la fonction responsable de l'exécution des mesures, en précisant si les outils et les fonctions sont internes ou externes ;
- Description de l'incidence des modifications envisagées dans les mesures sur les ressources budgétaires, humaines et matérielles de l'entité financière, y compris sur les ressources consacrées à la mise en œuvre de toute mesure corrective ;
- Informations sur le processus d'information de l'ACPR, le cas échéant ;
- Si les faiblesses, défaillances ou lacunes recensées ne font pas l'objet de mesures correctives, une explication détaillée des critères appliqués pour analyser leur incidence et évaluer le risque résiduel lié aux TIC qui leur est associé, ainsi que des critères appliqués pour accepter ce risque résiduel.

Informations, s'il y a lieu, sur les nouvelles évolutions prévues du cadre de gestion du risque lié aux TIC

Conclusions résultant du réexamen du cadre de gestion du risque lié aux TIC

Suites, s'il y a lieu, des réexamens ultérieurs

- Liste, état d'avancement, appréciation critique des mesures correctives

Sources d'information utilisées pour l'élaboration du rapport

- Résultats des audits internes des évaluation s de la conformité, des tests de résilience opérationnels numériques (voire des tests avancés – TLPT)