Décembre 2024

Rapport sur le contrôle interne
Annexe sur la gestion des risques liés aux Technologies de l'Information et de la Communication –TIC-

(Annexe établie en application de l'arrêté du 3 novembre 2014 modifié et du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier)

Préambule

La présente annexe a pour objet de compléter le canevas de RACI avec les éléments prévus par le règlement (UE) 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 ». Cette annexe est applicable aux entités remettant un rapport de contrôle interne, visées à l'article 2 du règlement DORA. Les éléments demandés aux entités se rapportent au cadre de gestion du risque lié aux technologies de l'information et de la communication (TIC) prévu par l'article 6 du règlement DORA dont les règles de réexamen sont définies par l'article 6(5). Les obligations applicables aux entités soumises au cadre simplifié de gestion du risque lié aux TIC prévu par l'article 16 du règlement DORA font l'objet d'un encadré dans la présente annexe.

L'annexe doit être transmise à l'ACPR sous format bureautique, dans les conditions prévues par l'instruction n° 2017-I-24 modifiée relative à la transmission à l'ACPR de documents comptables, prudentiels et d'informations diverses.
Elle doit être remise au SGACPR au plus tard le 30 avril suivant la fin de chaque exercice. Pour le premier exercice de remise de cette annexe, cette dernière est attendue au plus tard le 30 juin 2025.

La rédaction est en français. Par exception, les rapports des établissements soumis à la supervision directe de la BCE peuvent être rédigés en anglais.

Informations attendues en matière d'activités informatiques

Table des matières

1. Stratégie informatique et gouvernance

- Présentation de la stratégie informatique de l'établissement (organisation, articulation avec la stratégie globale, objectifs prioritaires et plans d'action fixés, cadre d'appétence aux risques…) et des moyens alloués pour la mettre en œuvre (procédures mises en place pour veiller à son respect, budget alloué et sa procédure de pilotage, nombre et nature des effectifs consacrés à la gestion des opérations informatiques, à la sécurité du système d'information ainsi qu'à la continuité d'activité) ;
- Présentation du cadre de gouvernance (rôles des dirigeants effectifs, de l'organe de surveillance et le cas échéant du comité des risques dans la définition, le contrôle et la révision du cadre de gestion du risque lié aux TIC) (article 5 du règlement DORA).

2. Gestion du risque lié aux TIC

- Présentation de la stratégie de résilience opérationnelle numérique et des moyens alloués pour la mettre en œuvre (article 6(8) du règlement DORA) ;
- Présentation des politiques et procédures de gestion du risque lié aux TIC contenant l'ensemble des éléments visés à l'article 3 du règlement délégué (UE) 2024/1774 de la Commission du 13 mars 2024 complétant le règlement (UE) 2022/2554 du Parlement européen et du Conseil 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 (ci-après, le « règlement délégué 2024/1774 »)[1] ;
- Présentation de l'organisation du cadre de gestion[2] du risque lié aux TIC (articles 5(1), 6(1), et 16(1)(a) du règlement DORA) comprenant les éléments suivants :
    i) Dispositif d'évaluation du profil de risque lié aux TIC et ses résultats ;
    ii) Seuil de tolérance au risque lié aux TIC ;
    iii) Processus d'audit, plan d'audit de TIC (article 5(2)(f) et article 6(6) du règlement DORA) et processus de suivi formel sur la base des conclusions de l'audit interne (article 6(7) du règlement DORA) ;

[1] Le règlement délégué 2024/1774 se fonde sur les projets de normes techniques de réglementation soumis à la Commission par l'Autorité bancaire européenne, l'Autorité européenne des assurances et des pensions professionnelles et l'Autorité européenne des marchés financiers, en concertation avec l'Agence de l'Union européenne pour la cybersécurité.

[2] Ce cadre de gestion devant être revu a minima annuellement.

iv) Modalités et périodicité d'information des dirigeants effectifs et de l'organe de surveillance sur l'exposition de l'établissement au risque lié aux TIC[3].

Disposez-vous des éléments suivants :	Oui/non/ partiellement	Commentaires
Mesures de réduction des risques informatiques majeurs et de contrôle pour surveiller l'efficacité de ces mesures et description du processus d'information des dirigeants effectifs et de l'organe de surveillance ;	Choisissez un élément.	
Description du suivi et du contrôle permanent de la sécurité et du fonctionnement des systèmes et outils de TIC (article 9(1) du règlement DORA, voir partie 2)	Choisissez un élément.	
Présentation des risques liés aux TIC incluant les risques pour la résilience, la continuité et la disponibilité des systèmes de TIC, en particulier ceux qui soutiennent des fonctions critiques ou importantes (article 9(2) du règlement DORA) ;	Choisissez un élément.	

– Pour les entités visées à l'article 16(1) du règlement DORA pour lesquelles le cadre simplifié de gestion du risque lié aux TIC[4] s'applique, présentation des :

  i) principales insuffisances relevées, risques et anomalies détectées ;

  ii) 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 ;

  iii) modalités de suivi des recommandations résultant des contrôles permanents (outils, personnes en charge) ;

  iv) modalités de vérification de l'exécution dans des délais raisonnables des mesures correctrices décidées au sein des entreprises par les personnes compétentes (articles 11 f) et 26 a) de l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution).

3. Sécurité des réseaux et des systèmes de TIC

Disposez-vous de l'élément suivant :	Oui/non/ partiellement	Commentaires
Politique de sécurité des systèmes d'information[5]– cf. art. 9 §4.a du règlement DORA ?	Choisissez un élément.	
Date de création ou de mise à jour		
Nom du responsable de la sécurité informatique		

[3] Joindre le dernier tableau dédié à les informer

[4] Ce cadre devra être revu périodiquement.

[5] Une politique de sécurité de l'information qui définit des règles visant à protéger la disponibilité, l'authenticité, l'intégrité et la confidentialité des données, des actifs informationnels et des actifs de TIC, y compris ceux de leurs clients, le cas échéant

Disposez-vous des éléments suivants :	Oui/non/ partiellement	Commentaires
Politiques de sécurité des TIC (article 9(2) du règlement DORA) ? Rappel : les politiques de sécurité des TIC doivent être conformes aux dispositions prévues par l'article 2 du règlement délégué 2024/1774	Choisissez un élément.	
Procédures, protocoles, politiques et outils de gestion de la sécurité des réseaux (article 13(1) du règlement délégué 2024/1774) ?	Choisissez un élément.	
Procédures, protocoles, politiques et outils de sécurisation de l'information en transit (article 14(1) du règlement délégué 2024/1774) ?	Choisissez un élément.	

- Description des procédures mises en place pour détecter, prévenir et répondre aux incidents liés aux TIC (article 6(8)(a) et article 11(2)(b) du règlement DORA) et aux incidents majeurs liés[6]aux TIC ;
- Présentation de la procédure de déclaration des incidents majeurs liés aux TIC et de notification volontaire des cyber menaces importantes à l'autorité compétente (article 19 du règlement DORA) ;

Disposez-vous des éléments suivants :	Oui/non/ partiellement	Commentaires
Programmes de sensibilisation à la sécurité des TIC (sensibilisation des collaborateurs et des prestataires tiers de services de TIC le cas échéant) et de formations à la résilience opérationnelle numérique (article 13(6) du règlement DORA).	Choisissez un élément.	
Politique de sécurité physique et environnementale conformément à l'article 18 du règlement délégué 2024/1774	Choisissez un élément.	
Politique de sécurité logique, de préservation de l'intégrité et de la confidentialité des données, mesures spécifiques mises en place pour l'activité de banque en ligne, description des tests d'intrusion effectués au cours de l'exercice, plan de secours informatique…)	Choisissez un élément.	

4. Gestion des opérations de TIC

4.1. Présentation de la gestion des actifs informationnels

Disposez-vous des éléments suivants :	Oui/non/ partiellement	Commentaires
Politique de gestion des actifs de TIC (articles 4(1) et 8(1)(2)(a) du règlement délégué 2024/1774) ;	Choisissez un élément.	

[6] - Un incident lié aux TIC est défini comme un évènement ou une série d'évènements liés entre eux que l'entité financière n'a pas prévu qui compromet la sécurité des réseaux et des systèmes d'information, et a une incidence négative sur la disponibilité, l'authenticité, l'intégrité et la confidentialité des données ou sur les services fournis par l'entité financière (article 3(8) du règlement DORA).;

Registre des actifs de TIC (article 4(2) points i) à ix) du règlement délégué 2024/1774)	Choisissez un élément.	

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

- Description des grands principes de la politique des ressources humaines (article 19 du règlement délégué 2024/1774

Par ailleurs, disposez-vous des éléments suivants :	Oui/non/ partiellement	Commentaires
Politique comprenant des mesures de contrôle de l'accès physique aux actifs de TIC (article 21(g) du règlement délégué 2024/1774)	Choisissez un élément.	
Politiques et procédures de gestion de l'identité (article 20 du règlement délégué 2024/1774)	Choisissez un élément.	
Politique relative au contrôle des droits de gestion des accès aux actifs de TIC article 21 du règlement délégué 2024/1774)	Choisissez un élément.	
Politiques et protocoles pour des mécanismes d'authentification forte (article 9(4)(d) du règlement DORA et article 21 (f) du règlement délégué 2024/1774)	Choisissez un élément.	

4.3. Processus de gestion des opérations informatiques : présentation des procédures couvrant l'exploitation, la surveillance et le contrôle des systèmes et services informatiques ;

Disposez-vous de procédures de sécurité des opérations de TIC suivantes :	Oui/non/ partiellement	Commentaires
Politiques et procédures pour les opérations de TIC (article 9(2) du règlement DORA et article 8(1) du règlement délégué 2024/1774)	Choisissez un élément.	
Procédures de gestion des capacités et des performances (article 9 du règlement délégué 2024/1774)	Choisissez un élément.	
Procédures de gestion des vulnérabilités (article 10(1) et article 10(2) du règlement délégué 2024/1774)	Choisissez un élément.	
Procédure de gestion des correctifs et des mises à jour (article 9(4)(f) du règlement DORA et articles 10(3) et 10(4) du règlement délégué 2024/1774).	Choisissez un élément.	
Procédure de sécurité des données et des systèmes de TIC (article 11 du règlement délégué 2024/1774)	Choisissez un élément.	

Procédures, protocoles et outils de journalisation (article 12 du règlement délégué 2024/1774)	Choisissez un élément.	

- Description du 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)

4.4. Processus de détection et de gestion des incidents opérationnels ou de sécurité, dont :

Description des grands principes de gestion des incidents liés aux TIC et mécanismes permettant de détecter rapidement les activités anormales (article 17 et article 10 du règlement DORA).

Pour plus de détails, disposez-vous des éléments suivants :	Oui/non/ partiellement	Commentaires
Stratégie de communication en cas d'incidents liés aux TIC qui doivent être divulgués en vertu de l'article 14 du règlement DORA (article 6(8)(h)).	Choisissez un élément.	
Politique de gestion des incidents liés aux TIC (dont liste de contacts pertinents internes/externes) (article 22 du règlement délégué 2024/1774)	Choisissez un élément.	
Mécanismes techniques, organisationnels et opérationnels de détection rapide des activités et comportements anormaux (y compris les problèmes de performance des 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 2024/1774)	Choisissez un élément.	
Procédure de conservation des éléments de preuve relatifs aux incidents liés aux TIC dans le respect des dispositions prévues par le 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 (article 22(d) du règlement délégué 2024/1774)	Choisissez un élément.	
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 2024/1774)	Choisissez un élément.	
Procédure de communication des changements mis en œuvre suite à l'examen post-incident (article 13(2) du règlement DORA).	Choisissez un élément.	

4.5. Gestion du changement et des projets

- Description des politiques pour la gestion des changements dans les TIC (article 9(4)(e) du règlement DORA) ;
- Description du cadre de conduite des projets et programmes informatiques :

Disposez-vous des éléments suivants :	Oui/non/ partiellement	Commentaires
Politique pour la gestion des projets de TIC (article 15 du règlement délégué 2024/1774)	Choisissez un élément.	
Politique régissant l'acquisition, le développement et la maintenance des systèmes de TIC (article 16 du règlement délégué 2024/1774)	Choisissez un élément.	
Procédures de gestion des changements TIC (article 17 du règlement délégué 2024/1774).	Choisissez un élément.	

5. Gestion de la continuité d'activité

5.1. Description du dispositif de gestion de la continuité d'activité requis par l'arrêté du 3 novembre 2014 relatif au contrôle interne

- Rôles et responsabilités concernant la gestion de la continuité d'activité ;
- Politique de continuité des activités, notamment ses objectifs, les scénarios retenus, l'organisation devant être mise en œuvre par les unités organisationnelles de l'établissement ou pour les différents processus opérationnels ;
- Dispositif d'analyse des incidences sur les activités de l'exposition à de graves perturbations de l'activité (*Business impact analysis* – BIA), notamment l'organisation retenue pour sa réalisation au sein de l'établissement. Présentation des principales conclusions de l'analyse, et des résultats pour les processus critiques ou importants ;
- Présentation du (ou des) plan(s) d'urgence et de poursuite d'activité, scénarios retenus, architecture globale (un plan unique ou un plan par métier ou processus, cohérence globale en cas de plans multiples), responsabilités *(*périmètre des activités couvertes par le (ou les) plan(s) d'urgence et de poursuite d'activité, activités traitées en priorité en cas de crise, risques résiduels non couverts par le plan d'urgence et de poursuite d'activité, délais de mise en œuvre du plan d'urgence et de poursuite d'activité ;
- Audit et résultats des contrôles permanents du plan d'urgence et de poursuite d'activité.

5.2. Description du maintien en condition opérationnelle des systèmes et solutions de TIC (continuité informatique), cf. article 11du règlement DORA

- Rôles et responsabilités concernant la gestion de la continuité informatique ;
- Présentation de la politique de continuité informatique visée à l'article 11.2 du règlement DORA et à l'article 39 du règlement délégué 2024/1774) dont notamment :
  - i) Scénarios de perturbation couverts (incidents opérationnels et de sécurité),
  - ii) Capacité d'identification des actifs de TIC supportant les processus critiques ou importants, y compris lorsque gérés par des prestataires ;

iii) Objectifs et modalités des tests de continuité informatique.

- Présentation des plans de réponse aux différents scénarios de perturbation pour les différents actifs de TIC supportant les processus critiques ou importants, y compris lorsque gérés par des prestataires. Indication des durées maximales d'interruption de service tolérées et de perte de données ;
- Présentation des tests de continuité informatique (article 40 du règlement délégué 2024/1774) réalisés sur l'exercice (objectif, périmètre, champ couvert, calendrier), et explication de leurs résultats et plans d'action associés.
- Audit et résultats des contrôles permanents du plan de réponse et de rétablissement des TIC.

5.3. Dispositif de gestion de crise (cf. article 11 du règlement DORA)

- Rôles et responsabilités concernant la gestion de crise[7] (cf. art. 11.7 du règlement DORA) ;
- Présentation du dispositif de gestion de crise (organisation, éléments déclencheurs des différents stades d'activation) ;
- Description des procédures et méthodes de rétablissement ;
    - Présentation des cas d'activation du dispositif de gestion de crise au cours de l'exercice (exemple : grippe A [H1N1], Covid, panne informatique ou cyber attaque).

- Pour les entités visées à l'article 16(1) du règlement DORA pour lesquelles le cadre simplifié de gestion du risque lié aux TIC s'applique, les entités doivent assurer la continuité des fonctions critiques ou importantes, au moyen de plans de continuité des activités et de mesures de réponse et de rétablissement (point f), qui comprennent au moins des mesures de sauvegarde et de restauration, et tester régulièrement les plans et mesures visés au point f), ainsi que l'efficacité des contrôles mis en œuvre conformément aux points a) et c) (point g).

6. Externalisation des activités informatiques

- Attribution du rôle de suivi des accords conclus avec des prestataires tiers de services TIC (article 5(3) du règlement DORA)[8] ;
- Concernant les modalités d'utilisation des services TIC fournis par des prestataires tiers de services TIC (article 5(2)(h) et article 28(2) du règlement DORA) : présentation de la politique de l'établissement et de la stratégie en matière de risques liés à ces prestataires incluant notamment la description des dispositions existantes pour éclairer la prise de décision d'externalisation *(analyse préalable menée sur la criticité de l'activité à externaliser et l'évaluation des risques associés…)* avant que celle-ci ne soit effective ;
- adaptations prises 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) ;
- description de la procédure et des contrôles effectués avant la conclusion de tout accord contractuel avec des prestataires tiers de services TIC ;
- description du dispositif de contrôle permanent et périodique des activités externalisées ;
- descriptif de la méthodologie d'évaluation de la qualité de la prestation et sa fréquence de revue ;
- description du dispositif d'identification, de gestion et de suivi des risques associés à l'externalisation ;

[7] Microentreprises exemptées.

[8] Microentreprises exemptées. Est une microentreprise une entité financière, autre qu'une plate-forme de négociation, une contrepartie centrale, un référentiel central ou un dépositaire central de titres, qui emploie moins de dix personnes et dont le chiffre d'affaires annuel et/ou le total de bilan n'excède pas 2 millions d'euros (article 3(60) du règlement DORA).

- description des dispositifs mis en œuvre par l'établissement pour conserver l'expertise nécessaire afin de contrôler effectivement les activités externalisées et de gérer les risques associés à l'externalisation ;
- description des procédures d'identification, d'évaluation et de gestion des conflits d'intérêts liés au dispositif d'externalisation de l'établissement, y compris entre entités du même groupe ;
- description des plans de poursuite d'activité et de la stratégie de sortie définis pour les activités critiques ou importantes externalisées : formalisation des scénarios et objectifs retenus ainsi que des mesures alternatives envisagées, présentation des tests réalisés (fréquence, résultats…), reporting à la direction (sur les tests, les mises à jour apportées aux plans ou à la stratégie de sortie) ;
- description, formalisation et date(s) de mise à jour des procédures sur lesquelles s'appuie le contrôle permanent et périodique des activités externalisées (dont les procédures d'examen de la conformité) ;
- résultats des contrôles permanents de 2ème niveau menés sur les activités externalisées : principales insuffisances relevées et mesures correctives engagées pour y remédier (date de réalisation prévisionnelle et état d'avancement de leur mise en œuvre à la date de rédaction du présent rapport), modalités de suivi des recommandations résultant des contrôles permanents *(outils, personnes en charge)* ;
- résultats des contrôles périodiques menés sur les activités externalisées : principales insuffisances relevées et mesures correctives engagées pour y remédier (date de réalisation prévisionnelle et état d'avancement de leur mise en œuvre à la date de rédaction du présent rapport), modalités de suivi des recommandations résultant des contrôles périodiques.