

LE REGLEMENT DORA

Novembre 2024



L'article L. 122-5 de la propriété intellectuelle n'autorisant pas les représentations ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de l'ayant droit ou ayant cause, sauf exception stricte (« copies ou reproductions réalisées à partir d'une source licite et strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective », analyses et les courtes citations dans un but d'exemple et d'illustration, etc.), toute représentation ou reproduction, par quelque procédé que ce soit du présent document sans autorisation préalable du Clusif constituerait une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

Table des matières

LE REGLEMENT DORA	1
1 INTRODUCTION	8
2 PRESENTATION DE DORA	9
2.1 Contexte	9
2.2 Calendrier d’application	10
2.3 Champ d’application	10
2.4 Les obligations	11
2.5 Les sanctions	11
2.6 Les consultations	11
2.7 La contractualisation avec les TIC	12
3 LES ENTITES FINANCIERES.....	13
3.1 Direction générale	14
3.2 DSI	15
3.3 RSSI	16
3.4 Responsable juridique et conformité.....	17
3.5 Responsable d’actif TIC/Chef de projet TIC.....	18
3.6 Responsable PCA et gestion de crise.....	19
3.7 Gestion des tiers.....	20
4 LES PRESTATAIRES DE SERVICES TIC.....	21
4.1 Suis-je concerné par DORA ?.....	21
4.2 Le partage des responsabilités.....	22
4.2.1 Spécification et utilisation d’un service.....	22
4.2.2 RACI	22
4.2.3 Les audits et tests de résilience.....	23
4.3 Les exigences des clients et implication des prestataires	24
4.3.1 Obligations des prestataires.....	24
4.3.2 Les tests d’intrusion fondés sur les menaces	25
4.3.3 Les stratégies de sortie et de réversibilité	29
4.3.4 Comment obtenir les informations nécessaires de la part d’un prestataire ?	29
4.4 Les contrats	30
4.4.1 Avant le contrat : pré-évaluation	30
4.4.2 Phase de contractualisation	31
4.4.3 Phase après contrat : résiliation et stratégie de sortie	32
4.5 Le cas des prestataires tiers critiques (article 31).....	32
4.5.1 Régulation des prestataires tiers critiques de services informatiques	32
4.5.2 Rôle des AES et du superviseur principal	32
4.5.3 Critères de désignation	33

4.5.4	Redevance de supervision.....	34
4.5.5	Mode de supervision.....	34
4.5.6	Pouvoirs du superviseur principal.....	35
4.5.7	Sanctions.....	36
4.5.8	Mise en conformité du fournisseur.....	36
4.6	Le partage d'informations	37
5	ANNEXES	38
5.1	Annexe 1 - Chronologie et responsabilités détaillées des tests d'intrusion fondés sur les menaces... 38	38
5.2	Annexe 2 – Autres réglementations du secteur financier sur la résilience et la gestion des tiers (liste non exhaustive)	40
5.3	Annexe 3 – Partage des responsabilités	42
5.4	Annexe 4 – Glossaire	46
	BIBLIOGRAPHIE	47

Remerciements

Le Clusif tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Les responsables du groupe de travail :

Odile	DUTHIL	Caisse des dépôts et consignations
Garance	MATHIAS	Mathias Avocat
Thiébaut	MEYER	Google

Les contributeurs :

Hanane	ABBASSI	PwC
Xavier	AGHINA	Orange
Camille	ANDRE	Scalesquad
Nicolas	ANDREU	Coface
Gérald	AROULANDA	Ymunit
Eva	ASPE	Mathias Avocat
Eric	AVET	Manika Consulting
Simon	BALLOUHEY	TNP Consultants
Ludovic	BARBIER	Groupe Uneo
Delphine	BARON	Macif
Pierre	BARRIERE	Sopra Banking
Roxane	BAUDUIN	Groupe Uneo
Julien	BEAUSSART	Cyber BRG
Hend	BIBI	OVH Cloud
Isaac	BOCCARA	Sigasec
Inès	BOUTAR	SoSafe
Tatiana	BOYER	Garance Mutuelle
Maryan	BRUNEL	Klesia
Etienne	BUSNEL	Besse
Justine	CABANIS	La Robe Numérique
Jean-Luc	CAMBOT	Carte Blanche Partenaires
Alban	CAOUREN	Selceon
Laurent	CRUZ-MERMY	Elcem-com
Stanislas	De TRUCHIS	Harfanglab
Luc	DECLERCK	Board of Cyber
Florence	DEVAMBEZ	Albingia
Arnaud	DUFURNET	The Green Bow
Gilles	FAVIER	Board of Cyber
Marc	GARDETTE	Microsoft
Christophe	GIRAULT	IRP Auto
Denis	HAVE	SCC France
Yoann	JAGUENEAU	Groupe IMA
Romuald	JUEST	On X

Le règlement DORA

Arnaud	JUMELET	Microsoft
Olivier	LAISNEY	Groupe Uneo
Thibault	LAPEDAGNE	Cybervadis
François	LOREK	Trax Solutions
Thierry	LORHO	Sopra Steria
Grégoire	LUNDI	FTI Consulting
Julien	MALVAUX	Mutuelle nationale des hospitaliers
Clotilde	MARCHETTI	Grand Thornton
Bertrand	MASIUS	Own
Loïc	MENGUY	CCR
Pierre	NICOLAS	SCASSI
Thibaud	PAYAN	WLF
Patrick	PITON	Sopra Banking
Bastien	RIZZA	Blackfox Partners
Laurent	ROUSSEAU	Infoblox
Jean-Baptiste	ROUX	SoSafe
Hervé	SCHAUER	HS2
Dylan	SEBBANE	S2H Group
Lucie	SHEN	Capgemini
Patrick	SONOU	RAPID 7
Ulrich Landry	TAGNE LELE	Manika Consulting
Stéphane	VALLOIS	Swiss Life
Emmanuel	VANDANGEON	PwC
Cécile	VERNUDACHI	Anders Avocats
Ariane	YAÏCH	Blackfox Partners

Le Clusif remercie également les adhérents ayant participé à la relecture.

1 Introduction

Pour renforcer et homogénéiser, au niveau européen, la sécurité et la résilience informatiques, trois textes européens ont été publiés. Il s'agit de :

- La directive dite « NIS 2 » qui classe les entités entrant dans son périmètre d'application entre « entités essentielles » et « entités importantes » et introduit des exigences plus strictes par rapport à NIS 1 en matière de gestion des risques, de notification des incidents et de mesures de sécurité.
- La directive sur la résilience des entités critiques, dite « REC », qui vise à réduire les vulnérabilités et à renforcer la résilience physique des entités critiques qui sont définies par ladite directive (en annexe) et qui, plus généralement, « fournissent des services indispensables pour maintenir les fonctions sociétales vitales, les activités économiques, la santé et la sécurité publiques ainsi que l'environnement ».
- Le règlement « DORA » sur la résilience opérationnelle numérique du secteur financier.

Ce livable a pour objectif de présenter le nouveau règlement européen pour la résilience opérationnelle du secteur financier en Europe (« DORA »). Il débute par une présentation du texte et le situe dans le paysage réglementaire. Il aborde ensuite les exigences des entités financières et positionne, sous forme de « Mind Map », les rôles et responsabilités de différents acteurs pour la mise en conformité de l'entreprise. Enfin, il aborde le rôle et les exigences des prestataires de service IT, et notamment ceux qui seront identifiés comme prestataires critiques pour le secteur financier européen.

2 Présentation de DORA

Contexte

Le règlement européen sur la résilience opérationnelle numérique du secteur financier, dit « DORA »¹ (*Regulation (EU) 2022/2554 - Digital Operational Resilience Act*) s'inscrit dans la stratégie européenne visant à développer une approche harmonisée de la finance numérique au sein de l'Union européenne (UE).

Il fait partie du paquet législatif (Digital Financial Package, DFP) qui comprend aussi le règlement européen sur les marchés de cryptoactifs (MiCA) et le régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués (DLT).

Il vise à « atteindre un niveau commun élevé de résilience opérationnelle numérique ». À cette fin, il fixe des exigences uniformes pour la sécurité des réseaux et des systèmes d'information des entreprises et des organisations opérant dans le secteur financier. Il fixe notamment des exigences de gestion des risques liés aux TIC. L'objectif étant de rendre le secteur financier, au niveau de l'UE, plus résilient, afin de garantir sa sûreté technologique et son bon fonctionnement, ainsi que son rétablissement rapide après des atteintes à la sécurité des technologies de l'information et de la communication (TIC) et des incidents liés aux TIC.

Le règlement DORA a été adopté le même jour, le 14/12/2022, que la **directive NIS 2** qui renforce les exigences en matière de cybersécurité au sein de l'UE, pour les entités qualifiées d'essentielles ou importantes, notamment les banques et les infrastructures des marchés financiers. DORA est considéré comme une « *lex specialis* » de la directive NIS 2 pour le secteur financier.

Il a également été adopté en même temps qu'une directive² sur le même thème, qui vise à modifier certaines directives du secteur financier, telles que Solvabilité 2, DSP2 (sur les services de paiement), IORP2 (sur les activités et la surveillance des institutions de retraite professionnelle), MiFID2 (sur les marchés d'instruments financiers), AIFM (sur les gestionnaires de fonds d'investissement alternatif), UCITS IV (sur les organismes de placement collectif en valeurs mobilières), CRD IV (concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement) et BRRD (établissant un cadre européen pour le redressement et la résolution des établissements de crédit et des entreprises d'investissement), afin de les mettre en cohérence avec les nouvelles dispositions du règlement DORA.

Toutefois, il n'y a pas d'étanchéité pure et parfaite entre ces deux textes, les lignes directrices de la Commission européenne du 14 septembre 2023 sur l'application de l'article 4, paragraphes 1 et 2 de la directive 2022/2555 rappelant à ce sujet que les actions de supervision des autorités désignées par des textes sectoriels (dont DORA), peuvent se dérouler avec « l'assistance » de celles compétentes en vertu de NIS 2, ce qui laisse augurer de l'émergence de « doctrines de supervision » inspirées de ces deux textes.

Par ailleurs, la stratégie nationale de cybersécurité « doit comprendre » un cadre sur lequel reposent « la coopération et la coordination » entre autorités compétentes, y compris pour les secteurs soumis à des règles sectorielles (III.2-32 in fine des lignes directrices et article 7.1-c de la directive NIS 2). Voir note de bas de page, appendice, page 9 sur le cadre de l'application de DORA et NIS2 pour les entités financières (cadre de gestion des risques et de déclaration

¹ https://eur-lex.europa.eu/legal-content/FR/TXT/?toc=OJ%3AL%3A2022%3A333%3ATOC&uri=uriserv%3AOJ.L_.2022.333.01.0001.01.FRA

² <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32022L2556>

des incidents)³. Il convient de préciser que la directive NIS 2 s'applique également aux prestataires de services TIC et que ces prestataires auront un double cadre de supervision par des autorités différentes (ACPR, AMF et ANSSI).

Calendrier d'application

Le règlement DORA et la directive associée sont entrés en vigueur le 16 janvier 2023. Les États membres ont démarré le processus de transposition concernant la directive, processus qui devra être terminé avant le 17 janvier 2025, date de l'entrée en application du règlement DORA. Les entités concernées devront être conformes à cette date.

Champ d'application

Le règlement DORA s'applique à 21 catégories d'entités du secteur financier qui représenteraient plus de 22 000 entités au sein de l'UE :

- Établissements de crédit
- Établissements de paiement
- Établissements de paiement électronique
- Établissements de monnaie électronique
- Entreprises d'investissement
- Prestataires de services fournisseurs de services de cryptoactifs
- Émetteurs de jetons référencés comme actifs
- Dépositaires centraux de titres
- Contreparties centrales
- Plateformes de négociation
- Référentiels centraux
- Gestionnaires de fonds d'investissement alternatifs et sociétés de gestion
- Prestataires de services d'information de données
- Entreprises d'assurance
- Intermédiaires d'assurance, intermédiaires de réassurance et Intermédiaires d'assurance à titre accessoire
- Institutions de retraite professionnelle
- Agences de notation de crédit
- Administrateurs de benchmark
- Prestataires de services de crowdfunding
- Référentiels de titrisation

Le règlement DORA s'applique aussi aux fournisseurs de services TIC (Technologies de l'information et de la communication) des entités financières. Un mécanisme de surveillance et de supervision direct des prestataires de services TIC « critiques »⁴ est mis en place au niveau de l'UE : évaluation des règles, procédures et mécanismes mis en place pour gérer les risques informatiques susceptibles d'impacter les entités financières.

Les prestataires « critiques » au sens de DORA seront désignés par les autorités européennes de surveillance (autorité bancaire européenne, autorité européenne des marchés financiers et autorité européenne des assurances et des pensions professionnelles) (AES) sur le

³ [https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52023XC0918\(01\)](https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52023XC0918(01))

⁴ <https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/operational-resilience/joint-regulatory-technical-standards-harmonisation-conditions-enabling-conduct-oversight-activities>

fondement de plusieurs critères (dépendance des entités financières, degré de substituabilité, etc.). Les prestataires désignés devront payer une contribution pour la supervision par les AES (article 43).

Les obligations

Les règles prévues par le règlement DORA peuvent être regroupées en 6 catégories :

- Gouvernance renforcée avec en particulier 3 fonctions prépondérantes
 - Suivi de l'externalisation (art. 5.3)
 - Gestion de crise (art. 11.7)
 - Communication sur incident (art. 14.3)
- Gestion des risques liés aux TIC
- Gestion, classification et notification des incidents
- Conduites de tests de la résilience opérationnelle numérique
- Encadrement des prestataires de services de TIC
- Partage d'informations en matière de cybersécurité

Les obligations liées aux contrats des prestataires TIC

Dans la mesure où le règlement DORA imposera un suivi complet du risque (de la conclusion du contrat à son exécution ou à sa résiliation, y compris lors de la phase post-contractuelle), il est nécessaire pour les entités du secteur financier de mettre à jour les éléments contractuels pour tous les contrats conclus avec un fournisseur de services TIC. Les droits d'accès, d'inspection et d'audit par l'entité financière ou un tiers désigné.

Les sanctions

En ce qui concerne les prestataires de services TIC, l'AES compétente pourra procéder à des contrôles sur pièces ou sur place (articles 33 à 35) et aura également le pouvoir de prononcer des sanctions en cas de non-conformité, notamment des pénalités financières et des astreintes journalières à un taux de 1% du chiffre d'affaires mondial de la précédente année d'exercice réalisé par le prestataire de services TIC concerné, et ce pendant une période totale de 6 mois maximum (article 31).

Concernant les entités du secteur financier, le régulateur pourra également leur demander de mettre fin à leurs accords avec le prestataire en question (« prestataire tiers critique de services TIC », article 39.7). Si la responsabilité des tiers est engagée, le règlement DORA ne supprime ou ne réduit en aucun cas les responsabilités des entités financières.

Les consultations

Les AES ont lancé deux vagues de consultations à partir du 8 décembre 2023, consultations publiques à destination des entités du secteur financier et des prestataires de services TIC sur le deuxième volet de mesures dans le cadre du règlement DORA. Les consultations sont restées ouvertes jusqu'à l'été 2024. Le paquet réglementaire en question comprenait :

- Un projet de normes techniques réglementaires (RTS) et un ensemble de projets de normes techniques d'exécution (ITS) sur le contenu, les délais et les modèles des rapports d'incident.
- Un projet de normes techniques (RTS) sur les critères de classification des incidents liés aux TIC.
- Des lignes directrices sur l'agrégation des coûts et des pertes résultant d'incidents majeurs.

- Un projet de RTS sur la sous-traitance de fonctions critiques ou importantes.
- Un projet de RTS sur l'harmonisation du contrôle des entités du secteur financier et des prestataires de services TIC.
- Des lignes directrices sur la coopération en matière de surveillance entre les AES et les autorités nationales compétentes.
- Un projet de RTS sur les tests d'intrusion fondés sur la menace (Threat-Led Penetration Tests - TLPT).
- Un projet de normes techniques d'implémentation (RTI) sur le modèle de registre d'information sur les accords contractuels des services TIC fournis par les tiers prestataires.
- Un projet de normes techniques de réglementation (RTS) sur les outils, méthodes et politiques de gestion du risque et le cadre simplifié de gestion du risque lié aux TIC.

La contractualisation avec les TIC

Le règlement dispose, dans son considérant 62, qu'« *afin d'assurer un suivi efficace du risque lié aux prestataires de services TIC dans le secteur financier, il convient d'établir un ensemble de règles destinées à guider les entités financières lors du suivi des risques engendrés par l'externalisation des fonctions à des prestataires de TIC (...)* ». Dans ce contexte, le chapitre V du règlement encadre la gestion des risques liés aux prestataires tiers de services TIC, notamment en encadrant, dans son article 30, les principales dispositions contractuelles. Les détails des obligations contractuelles sont indiqués dans la partie III du document.

En d'autres termes, toute entité financière doit soumettre son prestataire de service TIC à une analyse de risque et devra être très attentive à la contractualisation.

(Art. 15-e) Un point de vigilance dans le cadre des scénarios de continuité d'activité et de tests des activités de TIC qui soutiennent les fonctions critiques ou importantes : tenir compte des impacts en cas d'insolvabilité ou autres défaillances des prestataires tiers de service TIC et, le cas échéant, les risques politiques dans les juridictions des prestataires.

3 Les entités financières

Après avoir présenté les principales exigences du règlement DORA, se pose la question de leur mise en œuvre par les entités financières. Par où commencer ? Quelles fonctions impliquer ? Quelles sont les actions prioritaires ?

L'objectif de cette partie est de fournir au responsable du programme DORA au sein de l'entité financière des outils pratiques pour guider chacune des fonctions impliquées dans les chantiers de mise en œuvre.

Les fonctions les plus à même d'être parties prenantes sur un programme DORA sont les suivantes :

- Direction générale (DG)
- Directeur des systèmes d'information (DSI)
- Responsable de la sécurité des systèmes d'information (RSSI)
- Directeur juridique / conformité
- Responsable d'actif TIC / Chef de projet TIC
- Responsable du plan de continuité d'activité (RPCA) / gestion de crise
- Responsable de la gestion des tiers informatiques / maîtrise de l'externalisation

La liste des fonctions ci-dessus est fournie à titre indicatif et doit être adaptée au contexte organisationnel de chaque entité financière, en particulier concernant la mise en œuvre du modèle dit des trois lignes de défense (art. 6) ou la gestion des tiers TIC.

Les exigences de sécurité listées pour chaque fonction doivent être mises en œuvre en prenant en compte le principe de proportionnalité (voir art. 4), c'est-à-dire en tenant compte de la taille, du profil de risque et de la complexité des opérations de l'entité financière.

Direction générale

Définit les rôles et les responsabilités pour les fonctions TIC et met en place une gouvernance appropriée (art. 5)
(DSI, Dir. Risques | Organigramme, fiches de poste)

Assume la responsabilité ultime de la gestion du risque lié aux TIC (art. 5). Accepte le risque résiduel.
(RSSI | Analyse de risques)

Approuve la stratégie de résilience opérationnelle numérique, y compris le niveau de tolérance aux risques liés aux TIC (art. 5 et 6)
(Métiers, DSI, RSSI, RPCA | Stratégie de résilience)

Approuve et supervise la mise en œuvre de la politique de continuité des activités de TIC de l'entité financière et des plans de réponse et de rétablissement des TIC (art. 5 et 11)
(DSI, RSSI, RPCA | Stratégie de résilience)

Approuve et examine périodiquement les plans internes d'audit des TIC (art. 5)
(Audit interne, RSSI | Plan d'audit des TIC)



Direction générale

Actions
(Interlocuteurs | Livrables)

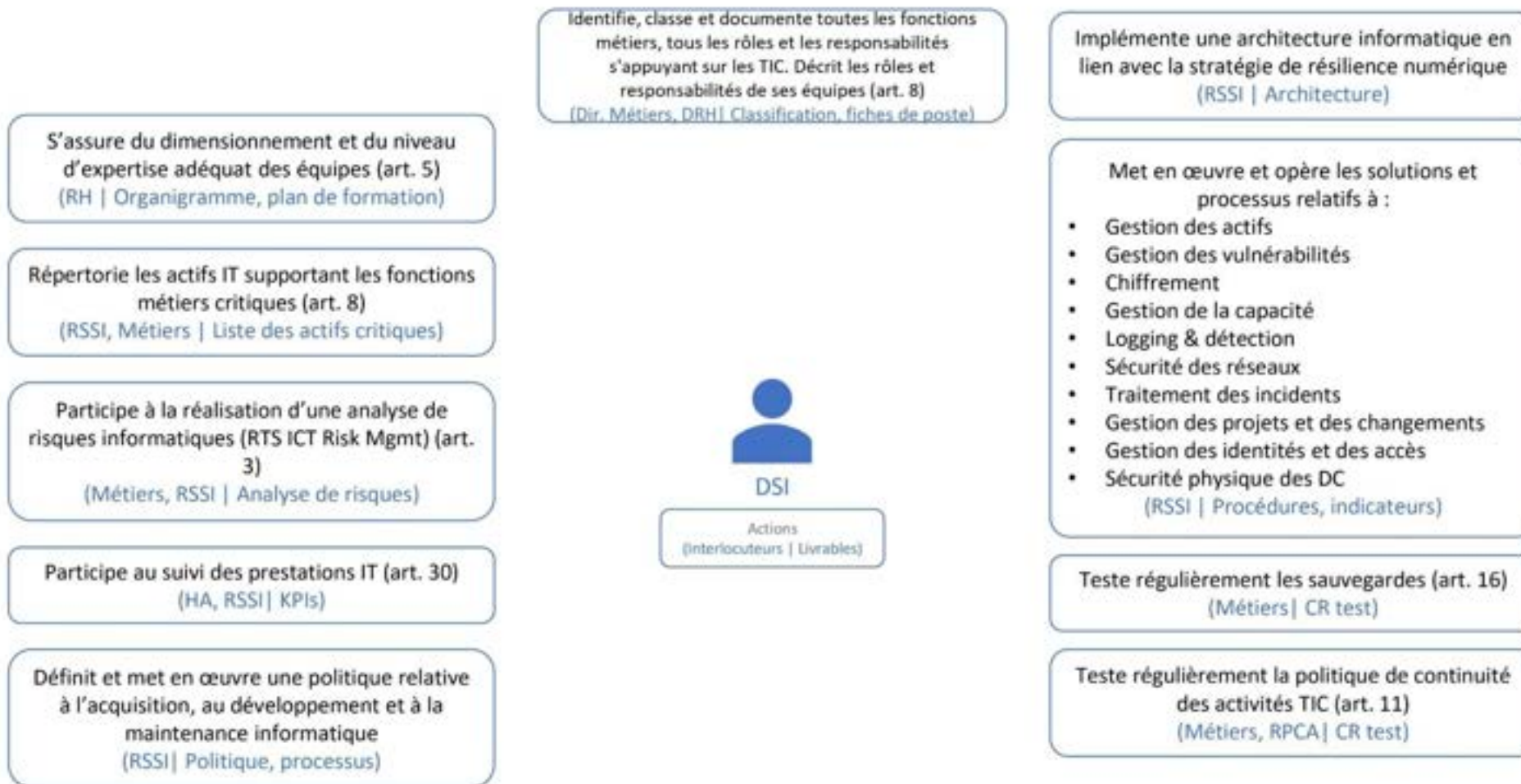
Alloue le budget approprié pour satisfaire les besoins en matière de résilience opérationnelle numérique pour tous les types de ressources, y compris pour la sensibilisation et la formation (art. 5 et 13)
(Métiers, DSI, RSSI | Budget)

Met en place des canaux de notification pour être informé des accords avec les prestataires de services TIC et des incidents majeurs liés aux TIC (art. 5)
(DSI | Reportings)

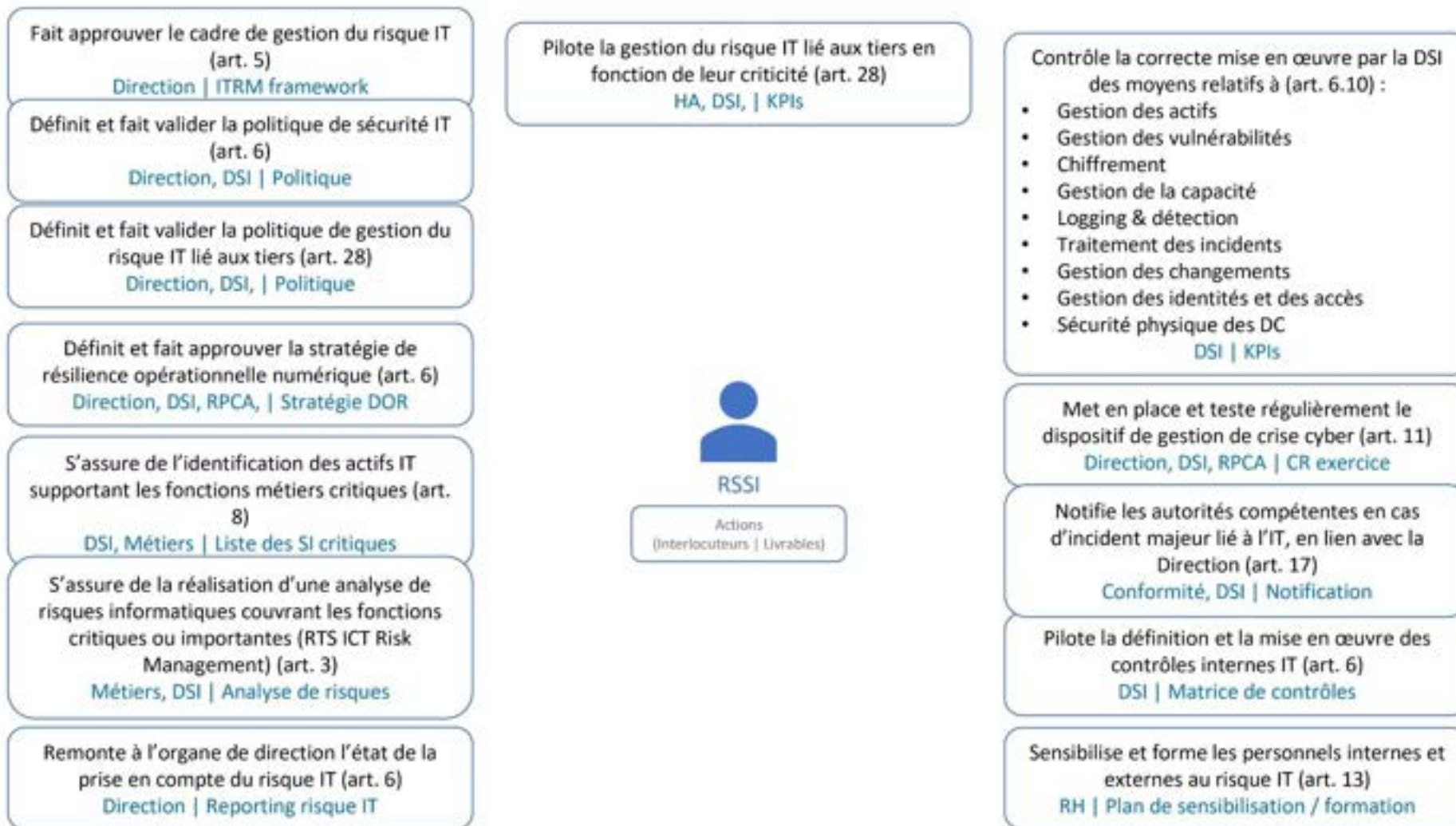
S'assure de la désignation d'un responsable du suivi des accords conclus avec les prestataires de services TIC (art. 5)
(DSI | Fiche de poste)

Suit régulièrement une formation proportionnée au risque lié aux TIC gérés (art. 5)
(RSSI | Formation)

DSI



RSSI



Responsable juridique et conformité

- Étudier le règlement UE 2022/2554, la directive UE 2022/2556 et identifier le cadre d'application
- Connaître le droit applicable aux services financiers (art. 28.1-a)
- Évaluer les interactions avec d'autres textes pouvant avoir un impact en matière de résilience ou cybersécurité

(Équipe juridique et autre à définir en fonction des législations applicables à l'entité | document de synthèse)

- Réaliser une analyse précontractuelle sur les services TIC (considérant 66) (art. 28.4 et 29)
- Identifier et évaluer le risque de concentration, de la criticité des services et des conflits d'intérêts (considérant 66) (art. 28.4)

(DSI, équipe prestataire | une fiche d'évaluation par prestataire, KPI)

S'informer et tenir compte des éléments suivants lors de l'analyse préliminaire du risque de concentration en cas de sous-traitance de fonctions importantes et critiques (art 29.2) :

- Avantages et risques liés à la sous-traitance et éventuels sous-traitants établis dans un pays tiers
- Dispositions législatives en matière d'insolvabilité et contraintes liées à la récupération urgente des données
- Respect des règles de l'Union en matière de protection des données et de l'application effective de la législation dans ce pays tiers
- La capacité à suivre une chaîne de sous-traitance et la capacité de surveillance par l'autorité de l'entité

(Métiers, RSSI, équipe prestataire | fiche d'évaluation par prestataire)

- Effectuer une veille juridique
- Anticiper, prévenir et sensibiliser aux risques juridiques (sanction pécuniaire, retrait ou suspension d'agrément, etc.)

(DSI, métiers, RSSI, achats | document de présentation et sensibilisation)



Métier juridique et conformité

(Interlocuteur | Livrable)

- Vérifier que les principales dispositions contractuelles sont bien intégrées aux contrats de prestation de service TIC (art. 30)
- Adapter les clauses juridiques en fonction de la nature du service TIC et son importance
- Recourir au modèle de clauses types (RTS) pour améliorer le niveau de sécurité juridique (art. 30.4 et considérant 75)

(Métiers, RSSI, équipe prestataire | contrat)

- Adapter les accords contractuels conclus avec des prestataires tiers critiques de services TIC dans le cadre du suivi effectué par les autorités (art. 42.8)
- Exiger la résiliation du contrat, sur demande de l'autorité de contrôle, pour les prestataires critiques en cas d'opposition à une inspection (art. 39.7)

(Métiers, service achats, équipe prestataire | contrat, liste des non-conformités et plan d'action)

Répondre aux demandes des autorités

(interlocuteur : à définir en fonction du contenu du mandat de l'autorité | politique de gestion des audits des autorités)

- Communiquer aux autorités des éléments nécessaires sur les nouveaux accords relatifs à l'utilisation de services TIC (art. 28.3)
- Informer les autorités, en temps utile, des projets d'accords contractuels sur les services TIC supportant les fonctions critiques ou lorsque la fonction est devenue critique (art. 28.3)

(Métiers, service achats | registre d'information ou document projet sur l'accord contractuel)

Maintenir un suivi permanent des accords contractuels conclus avec des prestataires tiers critiques de services TIC (ex. : évolution de service TIC, nouvelles dispositions législatives, etc.) (considérant 92)

(Métiers, RSSI, équipe prestataire | KPI, contrat)

Responsable d'actif TIC/Chef de projet TIC

S'assurer de la conformité à DORA lors des changements et mettre à jour :

- La cartographie des risques
- Le dossier applicatif
- Le Plan d'assurance sécurité, les processus et procédures des sous-traitants
- Les procédures de résilience
- Le programme de test

(Acteurs en fonction du sujet | Documents à jour)

- Classifier les activités et identifier les risques de son périmètre (art. 6.2)
- Inventorier et cartographier les actifs matériels et immatériels de son périmètre (art. 8)
- Mettre en œuvre des systèmes, protocoles et outils résilients en cas de tension sur les marchés (art. 7.d)

(Métiers, RSSI | Cartographie des risques et inventaires)

- S'assurer que les sous-traitants de son périmètre présentent les qualités requises avant et pendant le contrat, notamment sa substituabilité et l'absence de concentration du marché sur un seul acteur (art. 29.1)
- Utiliser les clauses DORA dans les CCTP (art. 30)
- Maintenir l'inventaire de la chaîne de sous-traitant (art. 8.5 et 28.3)
- Gérer les sous-traitants par les risques (art. 28.1 et 29)
- Pouvoir déconnecter instantanément un sous-traitant (art. 9)
- Collecter et contrôler les KPI des sous-traitants : incidents, continuité d'activité, performance, etc. (art. 5.3)

(Métiers, DSI, RSSI, Achats | Plan d'assurance sécurité, processus et procédures de gestion des sous-traitants)

Maintenir les référentiels de l'application :

- Classification des actifs et de l'activité (critique ou non) (art. 8.1)
- Chaîne d'alerte en cas d'incident (art. 9 et 17)
- Dossier technique de l'application (art. 8.6)
- Chaîne de sous-traitance (art. 8.5)
- Programme d'audit (art. 21 à 24)
- Plan de correction des vulnérabilités (art. 8)
- Plan d'action de traitement des risques (art. 6.7)

(Métiers, DSI, RSSI | Dossier applicatif)



Responsable d'actif de TIC
Chef de projet IT
(interlocuteur | Livrable)

Préparer la résilience applicative avec les autres acteurs :

- Prise en compte de l'efficacité du marché financier (art. 12.6)
- Coûts et pertes occasionnés par des perturbations informatiques et des incidents liés à l'informatique (art. 11.10)
- Communication interne et externe (art. 14, 17 et 19)
- Contrôles et rapprochements post-incident (art. 12.7)
- Registre des actions de réponse à incident (art. 11.8)

(Métiers, Communication, DSI | Procédures)

- Informer la Direction des accords et changements de sous-traitants informatiques (art. 5.2-i)
- Rapporter à l'encadrement sous forme de tableau de bord (art. 5.2, 6.5 et 13)
- Informer la Direction sur les incidents majeurs et leur résolution (art. 17.3-e)

(Direction, DSI | Procédures et tableaux de bord)

- Réaliser une analyse de risques (RTS ICT Risk Mgmt, art 3)
- Programmer, superviser et documenter les tests de continuité et les audits de Sécurité (art. 21 à 24)
- S'assurer que le plan de vérification et correction des vulnérabilités est mis en œuvre (art. 24.5)
- Adapter le programme de tests lors des changements (art. 11.4)

(Équipe prestataire | Pilotage du programme de tests)

Responsable PCA et gestion de crise



Gestion des tiers

Tient à jour un registre d'information sur les tiers IT
(HA, Métiers, DSI | registre)

Met en œuvre la politique de gestion du risque IT lié aux tiers (RSSI | n/a)

Évalue le risque de concentration
(DSI, RSSI | Rapport d'analyse)

Définit une stratégie multi-vendeurs
(DSI, RSSI | Stratégie multi-tiers)

Met en place des stratégies de sortie des tiers IT critiques
(DSI, RSSI | Stratégies de sortie)

Réalise les diligences précontractuelles
(RSSI | rapports d'analyse)

Réalise les diligences postcontractuelles
(RSSI | rapports d'analyse)



Responsable
Gestion des tiers

Actions
(interlocuteurs | Livrables)

4 Les prestataires de services TIC

En tant que prestataire TIC d'entités financières, plusieurs questions se posent :

1. Suis-je concerné par DORA en tant que prestataire ?
2. Comment gérer le partage de responsabilité avec mes clients et la tenue des audits et des tests de sécurité ?
3. Quelles seront les exigences des clients et notamment mon implication dans les tests avancés et les plans de sortie, les demandes d'informations ?
4. Quels sont les points contractuels les plus importants ?
5. Quelles sont les exigences en cas de désignation comme prestataire critique ?
6. Quel est mon rôle dans le partage d'information ?

Suis-je concerné par DORA ?

La prestation de services dans le secteur financier fait souvent référence à la notion de « criticité » du prestataire. Il semble important de clarifier deux notions de criticité à ne pas confondre et qui sont indépendantes l'une de l'autre.

D'une part, un prestataire peut être critique pour une entité financière du fait de l'externalisation d'une prestation de services ou autres tâches opérationnelles critiques ou importantes. Par exemple, dans le secteur de la banque, cette notion est prise au sens de l'article 10.r 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 (ACPR)⁵ – mis à jour le 25 février 2021 pour aligner le droit français aux orientations de l'Autorité bancaire européenne (ABE).

Le règlement DORA donne une définition d'une fonction critique ou importante⁶ et impose aux entités financières plusieurs exigences. Parmi celles-ci, nous pouvons citer :

- L'article 28.2 : l'entité financière doit adopter une stratégie de gestion des risques liés aux prestataires de services TIC. Cette stratégie inclut une politique relative à l'utilisation des services TIC qui soutiennent des fonctions critiques ou importantes fournies par des prestataires.
- L'article 28.4-a : avant de conclure un accord contractuel, les entités financières doivent déterminer si les services TIC auxquels ils vont souscrire supportent des fonctions critiques ou importantes.
- L'article 28.8 : une stratégie de sortie doit être préparée pour les fonctions critiques ou importantes.

D'autre part, un prestataire peut être considéré comme critique au sens de l'article 31 de DORA (CTPP - prestataires tiers critiques de services TIC). Il s'agit des prestataires qui ont une criticité systémique pour le secteur financier européen dans son ensemble. Des exigences particulières sont prévues par DORA pour ces prestataires, notamment une surveillance directe par les autorités européennes de supervision (voir chapitre V).

⁵ <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000029700770>

⁶ Article 3.22 : fonction dont la perturbation est susceptible de nuire sérieusement à la performance financière d'une entité financière ou à la solidité ou la continuité de ses services et activités, ou dont l'exécution interrompue, défectueuse ou défaillante 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.

Un prestataire TIC d'entités financières est donc concerné par DORA pour accompagner ses clients pour leur propre conformité – et en particulier dans le cas d'une activité critique – et potentiellement en tant que prestataire critique pour le secteur financier européen.

Le partage des responsabilités

La sous-traitance de certains services par un prestataire au profit d'une entité financière pose immédiatement la question du partage des responsabilités, aussi bien pour la spécification et l'utilisation du service que pour les tests nécessaires pour la garantie d'un bon niveau de résilience et de sécurité.

Ces enjeux devront être établis contractuellement, en particulier lorsque ces services soutiennent des activités critiques ou importantes. Dans ce cas, les accords contractuels précisent notamment les descriptions complètes des niveaux de service (art. 30.3-a) ainsi que les obligations du prestataire en matière de plans d'urgence (art. 30.3-c).

4.1.1 Spécification et utilisation d'un service

Les exigences de DORA imposent que les entités financières, quel que soit leur modèle de service, mettent en œuvre des cadres efficaces de gestion des risques liés aux TIC, établissent des pratiques de gouvernance saines et maintiennent la résilience opérationnelle. Chaque modèle de service modifie l'équilibre des responsabilités, mais ne change pas le besoin fondamental d'une gestion approfondie des risques, d'un traitement des incidents et d'une conformité aux normes réglementaires.

À titre d'illustration, l'application des exigences DORA à différents modèles de services tels que SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) et les environnements sur site est présentée dans l'annexe 3.

4.1.2 RACI

Afin de déterminer ce partage de responsabilité entre l'entité financière et le prestataire, une bonne pratique peut consister à établir un tableau « RACI » (Réalisateur - Approbateur - Consulté - Informé).

Sans être exhaustif, voici une liste de points à étudier, qui seront autant de lignes de ce tableau.

- **La spécification du service** (options de configuration, localisation, limitations, etc.)
- **La mise à disposition du service** (installation, configuration, etc.)
- **L'utilisation du service**
 - Opérations usuelles (contrôles de sécurité, application des correctifs, modifications matérielles ou logicielles, sauvegardes, etc.)
 - Gestion des accès (aussi bien pour le client que pour le fournisseur de service)
 - Surveillance (capacité matérielle, performances matérielles et logicielles, événements de production et de sécurité, etc.)
 - Stockage (capacité, chiffrement, etc.)
 - Réseau (plan d'adressage, filtrage des accès, contrôles de sécurité réseau, etc.)
 - Maintien en condition de sécurité (cartographie, sécurité de la couche matérielle, sécurité des logiciels, etc.)
 - Continuité d'activité (maintien du PCA en définissant les périmètres relatifs à chaque partie)

- **La gestion des événements**
 - Gestion des changements (nouvelles versions de firmware, mises à jour logicielles, etc.)
 - Gestion des incidents (ouverture de tickets, remplacement du matériel défectueux, restaurations, etc.)
- **La réversibilité**
 - Définition du modèle de réversibilité (planification, choix des infrastructures de repli, etc.)
 - Récupération des données
- **La fin de service**
 - Destruction des configurations
 - Destruction des données (destruction logique, effacement des supports de stockage, etc.)

Bien entendu, les exemples donnés ci-dessus sont génériques et devront être adaptés à chaque service.

4.1.3 Les audits et tests de résilience

Ce partage des responsabilités est également nécessaire pour les tests et audits de résilience, dès lors que le prestataire opère tout ou partie du service évalué.

En effet, les articles 30.3-d et 30.3-e prévoient que les accords contractuels relatifs aux services TIC qui soutiennent des fonctions critiques ou importantes incluent l'obligation pour le prestataire de participer et de coopérer aux tests d'intrusion fondés sur les menaces (décrits aux articles 26 et 27), ainsi que « *les droits illimités d'accès, d'inspection et d'audit par l'entité financière ou par une tierce partie désignée* » (art. 30.3-e-i).

Pour autant, certains tests sont difficilement réalisables par l'entité financière elle-même. C'est notamment le cas lorsqu'elle utilise une ressource mutualisée avec d'autres clients, y compris hors du secteur financier. Ces tests doivent alors être réalisés directement par le prestataire. C'est par exemple le cas de l'arrêt complet d'un data center d'une infrastructure de cloud public, ou de l'évaluation d'une menace interne chez le prestataire par l'utilisation d'un compte à privilèges.

De plus, dans le cadre de la prestation au profit d'une entité financière, l'autorité compétente joue également un rôle dans ces tests puisqu'il peut exercer un contrôle :

- Soit directement dans le cas de prestataires tiers critiques (via le forum de supervision)
- Soit indirectement dans le cadre d'une inspection d'une entité financière cliente du prestataire

Les tests de sécurité d'un service sous-traité peuvent donc se répartir en 3 groupes :

- Les tests dont le périmètre est défini par l'entité financière ou l'autorité de supervision et qui sont exécutés par eux. Cela peut être le test d'un attaquant externe qui vise l'environnement hébergé par le prestataire, ou l'évaluation d'une menace interne – avec ou sans privilège – sur les données hébergées. Pour une entité financière, le test doit être réalisé uniquement sur le périmètre du ou des services auxquels elle a souscrit et dans le respect des conditions d'utilisation. En aucun cas le test ne doit être réalisé sur le périmètre d'un service des autres clients.

- Les tests dont le périmètre est défini par l'entité financière ou l'autorité de supervision mais qui sont exécutés par le prestataire, directement ou par un testeur tiers. Il peut s'agir par exemple de tester la solidité des mesures de sécurité du prestataire ou l'isolation des services sous-traités entre plusieurs clients.
- Les tests dont le périmètre est défini par le prestataire et qui sont exécutés par celui-ci. C'est par exemple le cas d'utilisation de comptes à privilèges en interne chez le prestataire.

Les exigences des clients et implication des prestataires

4.1.4 Obligations des prestataires

Dans le cas où l'entité financière aura contractualisé avec un prestataire tiers de services l'usage d'une application critique ou importante, elle imposera des exigences contractuelles à son prestataire pour pouvoir répondre à ses propres obligations, dans une démarche de responsabilité partagée, comme cela est déjà le cas aujourd'hui dans les contrats inspirés par les orientations de l'ABE sur la sous-traitance⁷.

Les obligations des prestataires pourront concerner notamment les thématiques mentionnées dans les articles 5 à 14 du règlement DORA, à savoir :

- La gouvernance et l'organisation des TIC
- La gestion des risques
- La gestion des actifs informationnels et TIC et leur protection
- La détection des activités anormales
- La continuité du service rendu et les activités connexes de sauvegarde et de restauration
- La veille cyber, les examens post-incidents et l'amélioration continue au sens large
- La notification des incidents majeurs liés au TIC
- La gestion de crise

Les prestataires seront mis à contribution **selon le type de prestations**⁸, notamment pour :

- La mise en œuvre d'une gestion du risque efficace permettant de protéger les actifs informationnels et TIC (article 6 « Cadre de gestion du risque lié aux TIC »)
- L'identification, la classification et la documentation de ces mêmes actifs (article 8.1), ainsi que le suivi de leur exposition aux risques (menaces, vulnérabilités, obsolescence...) (article 8.2)
- L'évaluation annuelle des risques liés aux TIC (article 8.7)
- Les contrôles d'accès physiques et logiques aux actifs (article 9.4-c « Protection et prévention ») et sur les environnements de production
- La gestion des changements, qui s'entend jusqu'au niveau le plus bas de l'infrastructure TIC sous-tendant les services (article 9 « Protection et prévention »)
- La mise en œuvre et le test régulier de plans de continuité (article 11 « Réponse et rétablissement »)

⁷ <https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf>

⁸ Annexe 3 du RTS JC 2023 85 : https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_85_-_Final_report_on_draft_ITS_on_Register_of_Information.pdf

- Les obligations liées aux sauvegardes et restaurations (article 12 « Politiques et procédures de sauvegarde, procédures et méthodes de restauration et de rétablissement »)
- La surveillance du risque à travers la mise en place d'une organisation classique en trois lignes de défense (article 6.4)
- La surveillance des infrastructures et des réseaux (article 10) en mettant en place les moyens nécessaires
- L'évaluation des services et de l'infrastructure fournis (article 25) à travers une large palette de tests comme :
 - Les scans de vulnérabilités de l'infrastructure TIC
 - Les audits d'infrastructure
 - Les audits de sécurité des solutions logicielles au sens large : code source et composants tiers embarqués via une solution de type Software Bill Of Material (SBOM) – il s'agit de prouver que les applications sont exemptes de vulnérabilités applicatives et technologiques connues
 - Les tests de sécurité applicative
 - Les tests d'intrusion
- La réalisation de tests d'intrusion fondés sur les menaces (article 26) tous 3 les ans
- La remontée vers l'entité des incidents majeurs de sécurité selon le contenu attendu (articles 17 à 19)

Spécifiquement, les prestataires devront :

- Renforcer leur gouvernance sécurité si elle n'est pas au niveau attendu (politique de sécurité, comités internes et externes).
- Rendre compte de manière formelle et régulière de leurs activités « sécurité » à l'entité financière, sous forme de rapports, d'évaluations internes et externes, d'indicateurs de suivi et, indirectement, aux autorités.
- Prouver une gouvernance de sécurité et que celle-ci est maintenue durant toute la durée du contrat, cela à travers la fourniture de certifications et de rapports (ISO27001⁹, ISO22301¹⁰, ISAE3402¹¹, etc.) à renouveler au fil du temps.

4.1.5 Les tests d'intrusion fondés sur les menaces

En anglais : Threat-Led Penetration Tests (TLPT)

Les autorités compétentes désigneront les entités financières qui sont tenues de réaliser des tests d'intrusion fondés sur la menace (art. 26.8).

Les prestataires de services offrant à ces entités financières un ou des services critiques seront obligatoirement enrôlés dans les travaux menés pour réaliser les tests d'intrusion fondés sur la menace.

Les tests d'intrusion fondés sur les menaces font l'objet d'un document spécifique de type « Norme technique de réglementation » (NTR) (en anglais : Regulatory Technical Standards – RTS). Le présent chapitre s'appuie sur le document final « *JC 2024-29 – Final report DORA RTS on TLP* »¹². Ce texte s'inscrit dans le cadre de la description des critères de sélection des

⁹ Norme définissant les exigences pour la mise en place d'un système de management de la sécurité de l'information.

¹⁰ Norme définissant les exigences pour la mise en place d'un système de management de la continuité d'activité.

¹¹ Standard de fiabilité du contrôle interne de prestations de services externalisées.

¹² https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-29_-

entités financières devant effectuer des tests d'intrusion fondés sur les menaces et la manière d'implémenter ces tests.

Il découle de l'article 26-11 de DORA que le document de norme technique sur les tests d'intrusion fondés sur la menace doit être conforme au cadre européen TIBER-EU (Threat Intelligence-Based Ethical Red Teaming).

Mais DORA n'intègre pas toutes les exigences de TIBER-EU, car DORA reste une norme avancée de test de résilience opérationnelle numérique applicable aux entités financières suffisamment matures du point de vue des technologies de l'information et de la communication.

TIBER-EU est adopté par certains pays européens sur la base du volontariat, donc nous ne traiterons pas de la coexistence des implémentations nationales de TIBER-EU avec DORA. Mais si une entité financière est soumise aux tests d'intrusion fondés sur les menaces par DORA, elle ne doit suivre que les exigences DORA.

Résumé du contenu du document final de norme technique de réglementation.

Le document de norme technique sur les tests d'intrusion fondés sur les menaces a été rédigé en accord avec le cadre TIBER-EU et reflète la méthode, les process et la structure du test d'intrusion décrit dans ce cadre.

Une autorité publique (nommée « TLPT authority » dans le document) est désignée pour traiter les sujets de tests d'intrusion fondés sur les menaces au niveau national. Chacune de ces autorités nationales s'assure que les entités financières qui opèrent dans le secteur des services financiers « cœur » (nommées « core financial subservice sector » dans le document) effectuent des tests d'intrusion fondés sur les menaces quand les critères indiquant leur impact systémique sont remplis.

Cependant, une telle entité peut être écartée par l'autorité si les tests d'intrusion fondés sur les menaces ne sont pas justifiés, en raison d'une évaluation globale sur la maturité des TIC, des caractéristiques des technologies concernées, du profil de risque lié au TIC spécifique, de l'impact des tests d'intrusion ou des préoccupations en matière de la stabilité financière (les tests étant réalisés sur les systèmes de production).

A contrario, des tests d'intrusion peuvent être demandés en raison de l'impact, du caractère systémique et du profil de risque de l'entité financière.

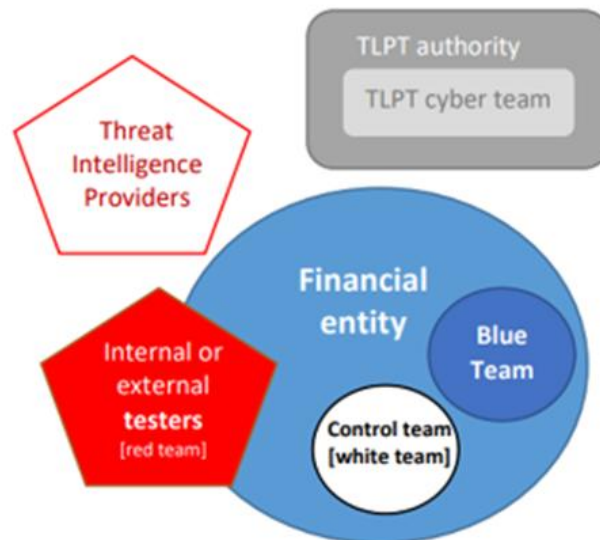
Se reporter au Chapitre II - Article 2 du document de norme technique de réglementation pour le détail des critères.

La méthodologie des tests d'intrusion fondés sur les menaces de DORA est similaire au TIBER-EU et demande l'engagement de plusieurs parties :

- L'entité financière avec une équipe de contrôle / équipe blanche (**Control team / White team**¹³) et une équipe bleue (**Blue team**) (*Chapitre III - Article 4*)
- La **TLPT authority** déjà citée supra
- Un **Threat Intelligence Provider**
- Des **testeurs** de l'équipe rouge (Red team) encadrés par un ou deux responsables (**tests managers**) de préférence

[Final report DORA RTS on TLPT.pdf](#)

¹³ Dans un souci de clarté et de cohérence avec les pratiques, les termes anglophones liés aux tests d'intrusion « Blue team », « Red team », etc., ont été utilisés et n'ont pas fait l'objet d'une traduction systématique.



Le test est secret/confidentiel afin qu'il soit réaliste, c'est-à-dire afin que les conditions de déroulement ne soient pas altérées par la connaissance du test par l'équipe sécurité de l'entité.

En conséquence, des précautions doivent être prises : communication sur le test d'intrusion limitée et sous l'autorisation de la Control team / White team. La Control team doit être réduite au strict nécessaire et son responsable doit être bien choisi (connaissance approfondie de l'entité, position, séniorité, accès au management), l'opération de test d'intrusion est désignée sous un nom de code, etc.

En raison du caractère sensible des tests d'intrusion fondés sur les menaces pour l'entité (possibilité de déni de service, crash en environnement de production, etc.), le document de norme technique DORA insiste sur la prise de conscience des risques par l'entité financière (*Chapitre III - Article 5 et notamment 2.*), la recherche d'atténuations et le contrôle des tests tout au long de leur déroulement.

Dans cet esprit, la sélection des testeurs et du Threat Intelligence Provider est également essentielle (*Chapitre III - Article 5.2 pour les détails*), car leurs missions sont différentes d'un « simple » test d'intrusion réalisé dans un environnement isolé : dans le cas d'un test d'intrusion fondé sur les menaces, il s'agit de cibler une entité financière dans son ensemble dans le monde réel : ses process, ses technologies et ses employés.

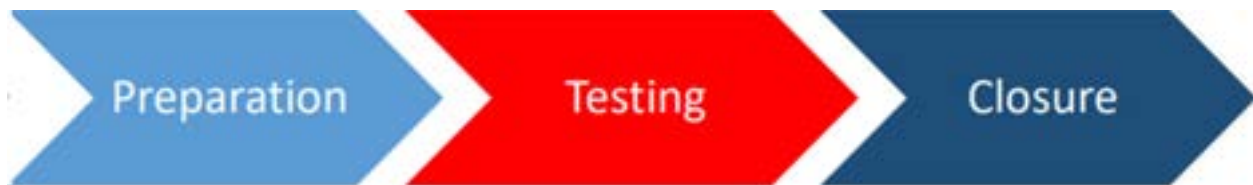
De plus, à la fin du test, les testeurs externes et le Threat Intelligence Provider doivent effectuer des procédures de restauration pour nettoyer les systèmes (virus, backdoor, désactivation...) et supprimer de façon sécurisée toutes les informations sensibles collectées (secrets, identifications, etc.) (*Chapitre III - Article 5.2-g et 5.2-h*).

La norme technique de réglementation sur les tests d'intrusion fondés sur les menaces introduit la possibilité de mener des tests groupés (« Pooled tests ») et des tests conjoints (« Joint tests ») associant plusieurs entités financières qui ont recours au même prestataire tiers pour obtenir certains services TIC soutenant des fonctions critiques ou importantes.

Le test conjoint d'intrusion fondé sur les menaces est un test d'intrusion groupé particulier, car englobant plusieurs entités financières qui utilisent le même fournisseur de service TIC « intra-groupe » ou bien qui appartiennent au même groupe et utilisent un système TIC commun.

Dans ces deux types de tests d'intrusion, des conditions et des exigences spécifiques sont dictées sur l'organisation, la conduite et le contenu des tests.

Les tests d'intrusion fondés sur la menace sont découpés en phases successives dont le déroulement est très encadré (durée, validation).



Préparation

Cette phase a pour but de lancer les tests d'intrusion fondés sur les menaces à la manière d'un « projet » avec un cadrage, la sélection des acteurs et la constitution des équipes, la spécification du périmètre ainsi que l'organisation du pilotage.

Phase de test

La phase de test commence par une étape de « Threat Intelligence » qui doit proposer des scénarii d'attaque pour chaque fonction critique ou importante identifiée dans le périmètre des tests. Elle est confiée à un Threat Intelligence Provider, externe à l'entité financière.

Les tests sont ensuite préparés par la Red team sur la base des éléments validés en amont, périmètre et rapport de Threat Intelligence. Ils sont ensuite menés par la même équipe sous la supervision de la Control team de l'entité et de la TLPT Authority : gestion des changements du plan, avancement des travaux, et prononcé de la fin des tests.

Clôture

La fin des tests donne lieu à des rapports croisés entre Red team et Blue team, à un exercice de « re-jeu » avec la participation des deux équipes, au partage d'expérience et à la production d'un rapport final soumis à la TLPT Authority.

Ensuite, la remédiation est assurée par l'entité financière, sur la base d'un plan de remédiation fourni à la TLPT Authority et qui couvre chaque vulnérabilité découverte.

Sur la préparation et le déroulement des tests d'intrusion fondés sur les menaces, le DORA met en avant un ensemble de recommandations :

- Tenir des réunions en présentiel ou à distance entre toutes les parties prenantes, et tout au long des tests pour fluidifier la communication.
- Obtenir un exposé clair des attentes de la TLPT authority sur le test : l'information est destinée à la Control team de l'entité financière, mais concerne aussi le Threat Intelligence Provider et les testeurs.
- À propos des responsabilités du Threat Intelligence Provider :
 - Identifier au moins deux zones d'intérêt, les cibles, afin de fournir les informations aux testeurs pour simuler des attaques réalistes et réelles sur les systèmes de production des fonctions critiques ou importantes.
 - À travers la production de deux documents – le « Threat Intelligence Report » (possibles scénarii de menace) et le plan de test de travail de l'équipe rouge « draft Red-team test plan » –, le Threat Intelligence Provider échange sur la pertinence de ses propositions avec les autres acteurs opérationnels : Control team et tests managers.
 - Enfin, le Threat Intelligence Provider doit tenir compte du paysage des menaces dressé par la TLPT authority pour le secteur financier du pays.
- Informer de façon précise les testeurs de la Red team sur les rapports du Threat Intelligence Provider afin de finaliser le test plan.
- Laisser un temps suffisant à la Red team pour conduire les tests de façon réaliste et complète afin de conduire toutes les phases d'attaque et atteindre les cibles. Le temps dépend du périmètre, des ressources de l'entité, des informations fournies par l'entité et d'éventuelles exigences externes.
- User des Tactiques, techniques et procédures (TTPs) de la Red team : la reconnaissance, l'armement, le lancement de l'attaque, l'exploitation, la prise de contrôle et la latéralisation, l'action sur la cible.

- Pour les testeurs, prendre en compte le temps alloué aux tests, les ressources disponibles et le cadre légal et éthique (*Chapitre III - Article 5 et notamment 2.i cite les actions interdites*). Quand les testeurs sont « bloqués », ils peuvent bénéficier d'un « coup de pouce » de la Control team, sous réserve d'accord de la TLPT Authority. Ce coup de pouce prendra la forme d'un accès au réseau, au système, etc., pour progresser dans le test.
- Saisir les tests d'intrusion fondés sur les menaces comme une opportunité d'apprentissage pour l'entité : en conséquence les Blue team et Red team doivent rejouer l'attaque ensemble et revoir les étapes pour apprendre du test. En complément, monter une équipe « Purple » et faire des exercices dédiés. Enfin, les équipes doivent se faire des retours sur le test.
- À la clôture du test, partager le rapport de test et le plan de remédiation avec l'autorité (TLPT Authority) pour présenter les vulnérabilités et leur interprétation.

Tous les 3 tests, confier les tests à l'extérieur de l'entité financière. Pour mémoire, les équipes mixtes (testeurs internes et externes) sont considérées comme étant internes.

4.1.6 Les stratégies de sortie et de réversibilité

Les prestataires offrant aux entités financières des services supportant des fonctions critiques ou importantes sont parties prenantes dans la conformité aux exigences DORA décrites dans le RTS « *JC 2023 84 - Final report on draft RTS to specify the policy on ICT services supporting critical or important functions* »¹⁴.

Si les implications du RTS sont présentées dans le chapitre « Les contrats » plus avant dans ce document, il convient de faire un focus sur les exigences relatives au plan de sortie (article 10 du RTS).

En effet, pour chaque service supportant une fonction critique ou importante fourni par un prestataire tiers, un plan de sortie est demandé et il doit être :

- Compatible avec le contrat
- Documenté
- Revu à intervalle régulier
- Réaliste, faisable et plausible
- *Et testé*

Ce dernier point est épineux, car il peut demander un effort important à renouveler selon l'évolution du service.

4.1.7 Comment obtenir les informations nécessaires de la part d'un prestataire ?

Pour pouvoir remplir leurs obligations de conformité, les entités financières ont besoin d'informations de la part de leurs prestataires, en particulier de ceux qui participent à une activité jugée importante ou critique par l'entreprise. Il leur est demandé de déterminer (voir article 6 section 3 du RTS sur les services TIC supportant les fonctions critiques) le processus de due diligence pour sélectionner et évaluer les prestataires de services TIC potentiels, et déterminer en particulier lesquels parmi les éléments suivants doivent être utilisés pour obtenir un niveau d'assurance adapté (plusieurs peuvent être requis) :

- Les audits ou évaluations indépendantes effectués par l'entité financière elle-même ou en son nom
- L'utilisation par l'entité financière de rapports d'audit indépendants réalisés au nom du prestataire TIC

¹⁴ https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_84_-_Final_report_on_draft_RTS_to_specify_the_policy_on_ICT_services_supporting_critical_or_important_functions.pdf

- L'utilisation par l'entité financière des rapports d'audit de la fonction d'audit interne du prestataire TIC
- L'utilisation par l'entité financière de certifications tierces pertinentes et appropriées
- L'utilisation par l'entité financière d'autres informations pertinentes disponibles ou d'autres informations fournies par le prestataire de services tiers en TIC

Ainsi, il peut être attendu des prestataires TIC de mettre à disposition :

- Des éléments de politique de sécurité interne
- Des programmes de conformité
- Des tables de correspondance entre des mesures de sécurité présentes dans leurs solutions et les exigences réglementaires de leurs clients
- Des certificats de conformité à des référentiels de sécurité, ainsi que leur domaine d'applicabilité
- Des résultats d'évaluation effectuées par des tiers
- Etc.

Toutes ces informations sont soit disponibles librement sur ces portails, soit à la demande. L'accès à certains documents peut nécessiter un accord de confidentialité (NDA - Non-Disclosure Agreement) préalable.

On note qu'une entreprise peut demander à son prestataire de remplir un questionnaire ad hoc sur sa gouvernance et ses pratiques de sécurité. Dans ce domaine, il est primordial de mutualiser au maximum les efforts, et l'utilisation de formulaires harmonisés est à privilégier.

Les contrats

Dans le cadre de la gestion des risques liés aux prestataires de services TIC, les entités financières doivent évaluer les risques liés à la sous-traitance, adopter une stratégie de contractualisation, d'exécution, de pilotage de la prestation, et enfin une stratégie de sortie, le tout dans un principe de proportionnalité.

4.1.8 Avant le contrat : pré-évaluation

(Article 28.4) Avant de conclure un contrat, une évaluation préliminaire doit être établie par l'entité financière sur le caractère critique ou important de la fonction sous-traitée, les conditions de surveillance et conclusion du contrat, le risque de sous-traitance et de concentration, diligence des prestataires durant la phase de sélection et identification des conflits d'intérêts.

(Article 28.5) L'entité financière doit s'assurer avant de conclure un accord contractuel que le prestataire respecte les normes adéquates en matière de sécurité de l'information. Ces obligations sont renforcées pour les services supportant les fonctions importantes ou critiques avec l'utilisation des normes les plus actualisées et les plus élevées en matière de sécurité de l'information.

Les certifications de sécurité portent sur un périmètre précis, il convient donc de vérifier que le service souscrit est couvert par les normes et dans le périmètre des certifications adoptées par le prestataire.

(Article 29.1) Lors de l'identification et l'évaluation des risques, et en particulier du risque de concentration, si l'accord contractuel soutient des fonctions critiques ou importantes débouchant sur des services qui ne sont pas facilement substituables (telle qu'une technologie unique sur le marché ou fournie par une minorité de tiers prestataires de service TIC) ou qu'il y ait plusieurs contrats avec le même prestataire ou des prestataires étroitement liés, l'entité doit recourir à des solutions alternatives en tenant compte des avantages et coûts, faire appel à plusieurs prestataires et prendre en compte la compatibilité des solutions en fonction des besoins et objectifs (départ chez un autre prestataire ou migration en interne).

Le critère de réversibilité de la solution est donc à prendre en compte ainsi que la possibilité

d'héberger la solution en interne. La maîtrise ou les compétences nécessaires liées à l'utilisation de la solution en interne sont un élément à envisager dans ce cas-là.

4.1.9 Phase de contractualisation

(Article 30.2) Dans la phase de contractualisation, les principales dispositions contractuelles sont définies dans l'article 30.2 du règlement.

Ces accords doivent contenir principalement les éléments suivants :

- La description du service TIC
- Si le service soutient des fonctions importantes ou critiques
- Le ou les lieux où les services sont fournis et où les données sont traitées, y compris le lieu de stockage (avec obligation d'informer l'entité préalablement s'il est envisagé de changer ces lieux)
- Les dispositions sur la disponibilité, l'authenticité, l'intégrité et la confidentialité en ce qui concerne la protection des données, y compris les données à caractère personnel
- Les garanties d'accès, de récupération et de restitution des données dans un format accessible (la réversibilité des données)
- La description des niveaux de services (SLA)
- L'obligation d'assistance aux incidents
- L'obligation du prestataire de coopérer avec les autorités compétentes et les autorités de résolution de l'entité financière
- Les droits de résiliation et les délais de préavis
- Les conditions de participation du prestataire aux programmes de sensibilisation à la sécurité des TIC élaborées par l'entité financière

Point d'attention sur les services supportant des fonctions importantes ou critiques :

(Article 30.3) Des accords contractuels types sont à établir en cas d'utilisation de services qui soutiennent les fonctions importantes ou critiques, en plus de ceux listés précédemment, avec des engagements supplémentaires :

- (SLA) Description complète des niveaux de services avec les objectifs de performance quantitatifs et qualitatifs pour permettre le suivi efficace par l'entité financière, associé à un droit de suivi permanent par celle-ci.
 - Des niveaux de supports peuvent donc être proposés avec un cadre de gouvernance ou une comitologie pour apporter l'assistance en fonction des besoins.
 - Des mesures correctives sont prises si ces SLAs ne sont pas atteints.
- Notification par le prestataire, avec préavis, de tout développement susceptible d'avoir une incidence significative sur le service (ex. : migration importante ou mise à jour, etc.).
- Obligation du prestataire de mettre en œuvre et tester des plans d'urgences avec mise en place de mesures, outils et politiques de sécurité des TIC.
- Obligation du prestataire de participer et de coopérer pleinement au test d'intrusion fondé sur la menace effectué par l'entité financière.
 - Ce test doit être réalisé sur le périmètre du service souscrit et ne pas engendrer de perturbation sur le service s'il est consommé par d'autres clients (cas des services en mode public cloud) : point à cadrer avec un mode opératoire et un code de conduite à respecter.
- Obligation du prestataire de fournir des indicateurs de performance, de notification des incidents, de reporting sur les incidents, de reporting sur la continuité d'activité et la sécurité des TIC.
- Droit d'assurer le suivi permanent des performances du prestataire avec des droits illimités d'audits, d'accès et d'inspection, droits de convenir d'autres niveaux d'assurances si les droits des autres clients sont affectés (ex. : cas d'un service en mode public cloud), obligation du prestataire de coopérer pleinement aux inspections sur place et audits par les autorités compétentes, l'entité financière ou un tiers désigné.

- Pour traiter le point précédent, les prestataires peuvent développer une politique ou un mode opératoire pour gérer les audits avec les différents acteurs.
- Obligation de fournir des précisions sur les modalités d'inspection et audit à distance (ex. : questionnaire ou fourniture d'autres preuves documentaires comme les rapports d'audits, etc.).

N.B. : (Article 28.10 et article 30.4) Un RTS¹⁵ précise davantage le contenu détaillé de la stratégie visée au paragraphe 2 en ce qui concerne les accords contractuels relatifs à l'utilisation de services TIC qui soutiennent des fonctions critiques ou importantes fournis par des prestataires tiers de services TIC.

4.1.10 Phase après contrat : résiliation et stratégie de sortie

(Article 28.7) Cet article précise les circonstances de résiliation d'un contrat. Il pourrait s'agir de non-respect des législations applicables ou de l'accord contractuel, d'un changement significatif du service, de faiblesses avérées dans sa gestion globale du risque lié aux TIC par le prestataire, ou de l'incapacité de l'autorité compétente à surveiller efficacement l'entité financière en raison des conditions contractuelles.

(Article 28.8) Pour les services TIC qui soutiennent des fonctions critiques ou importantes, les entités financières mettent en place des stratégies de sortie. Pendant le retrait de l'accord contractuel, l'entité financière doit veiller à ce que les activités ne soient pas perturbées, sans restriction du respect des exigences réglementaires et sans porter atteinte à la continuité et à la qualité des services fournis aux clients.

(Article 30.3-f) Dans le cadre de la stratégie de sortie, il est fixé une période de transition adéquate obligatoire au cours de laquelle le prestataire doit continuer à fournir le même service et permettre à l'entité financière de migrer vers un autre prestataire tiers de services TIC ou de recourir à des solutions en interne adaptées à la complexité du service fourni.

Un tel point dépend des besoins et objectifs fixés par l'entité financière et du modèle fourni par le prestataire pour garantir la migration des données (réversibilité du service, technologie utilisée sur le marché pour migrer chez un tiers prestataire ou en interne, coûts associés, etc.).

Le cas des prestataires tiers critiques (article 31)

4.1.11 Régulation des prestataires tiers critiques de services informatiques

Les pratiques d'externalisation et la concentration des services informatiques dépendant de tiers peuvent générer des risques systémiques pour le secteur financier. Or, les autorités nationales chargées de la surveillance financière ne disposent pas des moyens nécessaires pour mesurer et gérer les risques informatiques liés aux tiers prestataires de services informatiques critiques pour les entités financières.

Le règlement DORA établit donc, au niveau de l'Union, un cadre de supervision adapté pour pouvoir contrôler en permanence les activités des tiers prestataires critiques de services informatiques (TPCSI) pour les entités financières.

4.1.12 Rôle des AES et du superviseur principal

Les trois autorités européennes de surveillance (AES) sont :

1. L'Autorité bancaire européenne (ABE)
2. L'Autorité européenne des assurances et des pensions professionnelles (AEAPP)

¹⁵ https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_84_-_Final_report_on_draft_RTS_to_specify_the_policy_on_ICT_services_supporting_critical_or_importa nt_functions.pdf

3. L'Autorité européenne des marchés financiers (AEMF)

Le forum de supervision se compose des présidents des AES et d'un représentant à haut niveau du personnel en poste de l'autorité compétente concernée de chaque État membre. Les directeurs exécutifs de chaque AES et un représentant de la Commission européenne, du CERS, de la BCE et de l'ENISA participent au forum de supervision en qualité d'observateurs.

- Les AES, agissant par l'intermédiaire du comité mixte et sur recommandation du forum de supervision, désignent les tiers prestataires critiques de services informatiques, en tenant compte des critères précisés dans la section suivante ;
- désignent une des trois AES (l'ABE, l'AEMF ou l'AEAPP) comme superviseur principal pour chaque tiers prestataire critique de services informatiques.

L'AES désignée comme superviseur principal pour chacun de ces tiers prestataires critiques de services informatiques se voit conférer des pouvoirs lui permettant de veiller à ce que ces prestataires fassent l'objet d'un suivi adéquat à l'échelle paneuropéenne.

Les superviseurs principaux devraient disposer des moyens nécessaires pour réaliser des enquêtes, des contrôles sur place et à distance, d'accéder à tous les lieux et sites significatifs et obtenir des informations exhaustives et à jour afin de leur permettre d'évaluer le type, l'ampleur et les conséquences du risque que les fournisseurs tiers de services informatiques posent aux entités financières et, en fin de compte, au système financier de l'Union.

4.1.13 Critères de désignation

Étant donné que seuls les tiers prestataires critiques de services nécessitent un traitement particulier, un mécanisme de désignation aux fins de l'application du cadre de supervision devrait être mis en place pour tenir compte de la dimension et de la nature de la dépendance du secteur financier à l'égard de ces tiers prestataires de services informatiques.

Ce mécanisme consiste en un ensemble de critères quantitatifs et qualitatifs qui définissent les paramètres de criticité.

- Les conséquences globales sur la stabilité, la continuité ou la qualité de la fourniture de services financiers si le tiers prestataire de services informatiques concerné subissait un dysfonctionnement opérationnel majeur dans la prestation de ses services, en tenant compte du nombre d'entités financières qui bénéficient des services du tiers prestataire de services informatiques concerné.
- La taille et le rôle systémique des entités financières qui utilisent les services informatiques fournis par le tiers, évalués selon les critères suivants :
 - Le nombre d'établissements qualifiés d'importance systémique mondiale (EISm) ou d'autres établissements considérés comme systémiques (autres EIS) qui ont recours aux services informatiques du tiers.
 - Les liens entre les EISm ou les autres EIS mentionnés au point 1 et d'autres entités financières, y compris les cas où les EISm ou les autres EIS assurent des services d'infrastructure financière à d'autres entités financières.
- La dépendance des entités financières à l'égard des services fournis par le tiers prestataire de services informatiques concerné en ce qui concerne les fonctions critiques des entités financières, que les entités financières dépendent de ces services directement ou indirectement, par des moyens ou par des accords de sous-traitance.
- Le degré de substituabilité du tiers prestataire de services informatiques, en tenant compte des paramètres suivants :
 - L'impossibilité de trouver des alternatives, même partielles, à cause du faible nombre de tiers prestataires de services informatiques qui opèrent sur un marché donné, ou de la position dominante du tiers prestataire de services informatiques concerné, ou de la complexité ou du niveau de technicité requis,

y compris en ce qui concerne toute technologie propriétaire, ou des particularités de l'organisation ou de l'activité du tiers prestataire de services informatiques.

- Des obstacles pour transférer partiellement ou totalement les données et les charges de travail pertinentes du tiers prestataire de services informatiques concerné vers un autre, à cause soit de coûts financiers élevés, de limites de temps ou d'autres types de ressources que le processus de transfert peut demander, soit de risques informatiques accrus ou d'autres risques opérationnels auxquels l'entité financière peut être confrontée à cause de ce transfert.
- Le nombre d'États membres dans lesquels le tiers prestataire de services informatiques concerné fournit des services.
- Le nombre d'États membres dans lesquels opèrent des entités financières faisant appel au tiers prestataire de services informatiques concerné.

La Commission est habilitée à adopter un acte délégué pour préciser davantage les critères applicables aux fournisseurs de services tiers critiques de services informatiques.

Les tiers prestataires critiques de services informatiques qui ne sont pas automatiquement désignés par suite de l'application des critères susmentionnés ont la possibilité d'adhérer volontairement au cadre de supervision.

4.1.14 Redevance de supervision

Les AES perçoivent, auprès des tiers prestataires critiques de services informatiques, des redevances qui couvrent intégralement les dépenses qu'elles doivent engager pour exercer les tâches de supervision que leur assigne le présent règlement, y compris le remboursement de tous les coûts pouvant résulter des travaux effectués par les autorités compétentes qui participent aux activités de supervision.

Le montant de la redevance perçue auprès d'un tiers prestataire critique de services informatiques couvre tous les frais administratifs et est proportionnel à son chiffre d'affaires.

La Commission est habilitée à adopter un acte délégué pour compléter le règlement DORA en déterminant le montant des redevances et leurs modalités de paiement.

4.1.15 Mode de supervision

Le superviseur principal détermine si chaque tiers prestataire critique de services informatiques a mis en place des règles, des procédures, des mécanismes et des dispositifs complets, solides et efficaces pour gérer les risques informatiques qu'il est susceptible de faire peser sur les entités financières.

L'évaluation comprend :

- Des exigences en matière de TIC pour garantir, en particulier, la sécurité, la disponibilité, la continuité, l'extensibilité et la qualité des services que le tiers prestataire critique de services informatiques fournit aux entités financières, ainsi que la capacité à maintenir à tout moment des normes élevées de sécurité, de confidentialité et d'intégrité des données.
- La sécurité physique qui contribue à assurer la sécurité informatique, y compris la sécurité des locaux, des installations et des centres de données.
- Les processus de gestion des risques, y compris les politiques de gestion des risques informatiques, la continuité des activités informatiques et les plans de rétablissement après sinistre dans le domaine informatique.

- Les modalités de gouvernance, notamment une structure organisationnelle comportant des lignes de responsabilité et des règles de reddition de comptes claires, transparentes et cohérentes permettant une gestion efficace des risques informatiques.
- Le recensement et le suivi des incidents liés à l'informatique, ainsi que leur notification rapide aux entités financières, la gestion et la résolution de ces incidents, en particulier les cyberattaques.
- Les mécanismes relatifs à la portabilité des données, à la portabilité des applications et à l'interopérabilité, qui garantissent un exercice effectif des droits de résiliation par les entités financières.
- Les tests des systèmes, des infrastructures et des contrôles informatiques.
- Les audits informatiques.
- L'utilisation des normes nationales et internationales pertinentes applicables à la fourniture de ces services informatiques aux entités financières.

Le superviseur principal adopte un plan de supervision individuel clair, détaillé et motivé pour chaque tiers prestataire critique de services informatiques. Ce plan est communiqué chaque année au tiers prestataire critique de services informatiques.

4.1.16 Pouvoirs du superviseur principal

Le superviseur principal dispose des pouvoirs suivants :

- Il peut, sur simple demande ou par voie de décision, exiger des tiers prestataires critiques de services informatiques qu'ils fournissent toutes les informations nécessaires à l'exécution des tâches qui lui incombent, notamment tous les documents commerciaux ou opérationnels, contrats, documents stratégiques, rapports d'audit de sécurité informatique, rapports d'incidents liés à l'informatique, ainsi que toute information relative aux parties auxquelles le tiers prestataire critique de services informatiques a externalisé des fonctions ou activités opérationnelles.
- Il peut mener les enquêtes nécessaires auprès des tiers prestataires de services informatiques et est habilité à :
 - examiner les dossiers, données, procédures et tout autre document pertinent pour l'exécution de ses tâches, quel qu'en soit le support.
 - prendre ou obtenir des copies certifiées conformes ou prélever des extraits de ces dossiers, données, procédures et autres documents.
 - convoquer les représentants du tiers prestataire de services informatiques et leur demander de fournir oralement ou par écrit des explications sur des faits ou des documents en rapport avec l'objet et le but de l'enquête, et enregistrer leurs réponses ;
 - interroger toute autre personne physique ou morale qui accepte de l'être aux fins de recueillir des informations concernant l'objet d'une enquête.
 - demander les enregistrements des échanges téléphoniques et de données.
- Le superviseur peut pénétrer dans tout local commercial, sur tout terrain ou sur toute propriété des tiers prestataires de services informatiques, tels que les sièges sociaux, les centres d'exploitation et les locaux secondaires, et y effectuer toutes les inspections sur place nécessaires, ainsi que procéder à des inspections hors site. Les inspections couvrent l'ensemble des systèmes, réseaux, dispositifs, informations et données informatiques pertinents utilisés pour la fourniture de services aux entités financières ou contribuant à cette fourniture.

- Il peut formuler des recommandations dans différents domaines, notamment en ce qui concerne :
 - le recours à des exigences ou à des processus spécifiques de sécurité et de qualité en matière de TIC, comme le déploiement de mises à jour, de mesures de chiffrement et d'autres mesures de sécurité que le superviseur principal juge pertinentes.
 - le recours à des conditions et des modalités, y compris leur mise en œuvre technique, pour prévenir l'émergence de points uniques de défaillance ou leur amplification, ou pour réduire au maximum l'effet systémique éventuel en cas de risque de concentration informatique.
 - des accords de sous-traitance, y compris les accords d'externalisation lorsque le superviseur principal estime que la poursuite de la sous-traitance ou que la conclusion d'un nouvel accord peut entraîner des risques.
- Le superviseur peut demander, au terme des activités de supervision, des rapports dans lesquels sont précisées les mesures qui ont été prises ou les solutions qui ont été mises en œuvre par les tiers prestataires critiques de services informatiques en ce qui concerne les recommandations émises.

4.1.17 Sanctions

Les autorités compétentes peuvent exiger des entités financières qu'elles suspendent temporairement, en partie ou en totalité, l'utilisation ou le déploiement d'un service fourni par le tiers prestataire critique de services informatiques, jusqu'à ce que les risques identifiés dans les recommandations adressées aux tiers prestataires critiques de services informatiques aient été écartés. Le cas échéant, elles peuvent exiger des entités financières qu'elles résilient, en partie ou en totalité, les accords contractuels concernés conclus avec les tiers prestataires critiques de services informatiques.

Le superviseur principal peut imposer une astreinte pour obliger le tiers prestataire critique de services informatiques à se conformer à ses obligations.

L'astreinte visée est imposée sur une base journalière jusqu'à ce que la conformité soit atteinte et pendant une période maximale de six mois à compter de la notification au tiers prestataire critique de services informatiques.

Le montant de l'astreinte, calculé à partir de la date indiquée dans la décision d'astreinte, est égal à 1 % du chiffre d'affaires quotidien moyen réalisé au niveau mondial par le tiers prestataire critique de services informatiques au cours de l'exercice précédent.

Avant d'imposer une astreinte, le superviseur principal donne aux représentants du tiers prestataire critique de services informatiques faisant l'objet de la procédure la possibilité d'être entendus sur les conclusions et ne fonde ses décisions que sur les conclusions sur lesquelles le tiers prestataire critique de services informatiques faisant l'objet de la procédure a eu la possibilité de formuler des observations. Les droits de la défense des personnes faisant l'objet de la procédure sont pleinement assurés au cours de la procédure. Elles disposent d'un droit d'accès au dossier, sous réserve de l'intérêt légitime d'autres personnes à ce que leurs secrets d'affaires ne soient pas divulgués. Le droit d'accès au dossier ne s'étend pas aux informations confidentielles ni aux documents préparatoires internes du superviseur principal.

Les AES rendent publique toute astreinte infligée, sauf dans les cas où cette publication perturberait gravement les marchés financiers ou causerait un préjudice disproportionné aux parties en cause.

4.1.18 Mise en conformité du fournisseur

Les tiers prestataires critiques de services informatiques seront officiellement désignés à partir de la date d'entrée en application de DORA le 17 janvier 2025.

Les TPCSI devront donc :

- Désigner une personne morale comme point de coordination pour le superviseur.
- Mettre en place un plan de gouvernance, des processus et une structure de traitement de l'information pour assurer une gestion correcte des demandes de documentation, d'inspections ou d'enquêtes du superviseur principal.
- À la suite de l'évaluation du superviseur désigné et conformément à ses plans de surveillance, mettre en œuvre des règles, procédures, mécanismes et arrangements complets, solides et efficaces pour gérer les risques TIC qu'ils peuvent présenter pour les entités FSI.
- Payer des honoraires au superviseur principal pour couvrir ses coûts liés à l'exécution des tâches de supervision.
- Si elle n'existe pas encore, établir une filiale dans l'UE dans les 12 mois suivant la désignation.

DORA introduit des exigences contractuelles supplémentaires entre les fournisseurs de services tiers TIC et les entités FSI. Ces exigences contractuelles devraient adopter une approche similaire à celle des instruments réglementaires préexistants au niveau européen, à l'instar des lignes directrices de l'ABE sur les accords d'externalisation, des lignes directrices de l'AEAPP (Autorité européenne des assurances et des pensions professionnelles) sur l'externalisation du cloud, ou encore des lignes directrices de l'AEMF (Autorité européenne des marchés financiers) sur l'externalisation aux fournisseurs de services cloud.

En vue de la mise en conformité avec les dispositions pertinentes de DORA, les fournisseurs de cloud devront tenir compte de la nécessité d'un examen de toute nouvelle exigence concernant les fournisseurs de services tiers dans le domaine des TIC et examiner l'impact de ces exigences sur les documents contractuels existants et s'aligner sur les principaux éléments et dispositions contractuels tels que prévus par DORA, si nécessaire. Ces modifications contractuelles devront être mises en œuvre d'ici la date d'application de DORA.

Le partage d'informations

Les entités financières peuvent échanger entre elles des informations sur les menaces, par exemple des indicateurs de compromissions (IoC), des tactiques, techniques et procédures de groupes d'attaquants (TTP) ou des alertes de cybersécurité (article 45).

Bien qu'aucune exigence ni recommandation dans ce domaine ne porte sur les prestataires – qu'ils soient critiques ou non –, ces derniers peuvent participer à ces échanges pour contribuer à une meilleure prise en compte des bonnes pratiques et à une réactivité accrue en cas de menace ou d'attaque.

5 Annexes

Annexe 1 - Chronologie et responsabilités détaillées des tests d'intrusion fondés sur les menaces

La chronologie et les responsabilités des acteurs des tests d'intrusion fondés sur les menaces sont précisées dans le document « Norme technique de réglementation » (NTR) (en anglais : Regulatory Technical Standards - RTS), déjà cité précédemment.

Préparation

1. La phase de préparation est lancée dès réception par l'entité financière de la notification de la demande par la TLPT Authority et les documents d'initialisation (annexe I) doivent être remis **dans les 3 mois** (*Chapitre III - Section II - Article 8.1*).
2. **La TLPT Authority évalue et valide** les documents d'initialisation.
3. Une fois la validation obtenue, l'entité financière constitue une Control team avec, à sa tête, un responsable chargé de la communication interne et externe, de la sélection des acteurs (Threat Intelligence provider, testeurs externes et/ou internes), de la conformité avec le règlement DORA et de la production du document de spécification du périmètre (fonctions critiques ou importantes sélectionnées et écartées, raisons, description générale des systèmes sous-tendant les fonctions retenues, description des cibles).
4. La Control team de l'entité financière doit conduire une **analyse de risque** des tests d'intrusion et identifier les mesures à prendre, puis consulter la **TLPT Authority** qui **peut « objecter »**.
5. La Control team doit **évaluer la conformité des acteurs externes**, Threat Intelligence provider et testeurs, avec le règlement DORA et le document de norme technique de réglementation (NTR/RTS) consacré aux tests d'intrusion fondés sur la menace, fournir les preuves à la **TLPT Authority** qui **peut « objecter »**.
6. Le document de spécification du périmètre est cadré par l'annexe II du document de norme technique de réglementation (NTR/RTS), doit être approuvé par le management de l'entité financière puis soumis à la validation de la TLPT Authority **dans les 6 mois** après la réception de la notification initiale.
7. **La TLPT Authority approuve le document** de spécification du périmètre.

Threat Intelligence

8. La phase de Threat Intelligence débute après l'approbation du périmètre ; elle est conduite par le Threat Intelligence Provider qui, sur la base des menaces et vulnérabilités potentielles ou identifiées sur l'entité financière, doit proposer **des scénarii d'attaque pour chaque fonction critique ou importante du périmètre**.
9. La Control team de l'entité financière doit **sélectionner au moins 3 scénarii** selon des recommandations précisées au *Chapitre III - Section II - Article 9.3 et 9.4* du document de norme technique de réglementation (NTR/RTS).
10. Le Threat Intelligence Provider doit fournir à l'équipe de contrôle (Control team) le rapport de Threat Intelligence avec les scénarii sélectionnés au modèle décrit en annexe III du document de norme technique de réglementation (NTR/RTS).
11. La Control team **soumet le rapport de Threat Intelligence à la TLPT authority**.

Tests de la Red team

12. La phase de test débute après **l'approbation du rapport de Threat Intelligence**.
13. Les testeurs doivent prendre en compte le rapport de Threat Intelligence, le document de spécification du périmètre et consulter les autres parties (équipe de contrôle de l'entité financière, Threat Intelligence Provider et test managers de la TLPT

Authority) pour la préparation du plan de test ; son contenu doit s'aligner sur les exigences de l'annexe IV du document de norme technique de réglementation (NTR/RTS) et être **soumis à la TLPT Authority pour approbation**.

14. Une fois l'approbation du plan de test reçue par l'entité financière, le test d'intrusion fondé sur les menaces peut débuter pour une durée proportionnelle au périmètre et à la complexité de l'entité, mais **au moins de 12 semaines**.
15. Tout changement au plan est soumis à l'approbation conjointe de l'équipe de la Control team de l'entité et de la TLPT Authority.
16. Le traitement des cas exceptionnels (découverte des tests, risque d'impact sur les biens/fonctions/services, blocage de l'équipe rouge) est prévu dans le document de norme technique de réglementation (NTR/RTS).
17. **Au moins un point hebdomadaire** est nécessaire entre la Red team, la Control team et les tests managers de la TLPT Authority pour rendre compte de l'avancement – le Threat Intelligence Provider doit être disponible pour consultation.
18. La **fin de la phase active des tests** doit être prononcée **avec l'accord de toutes les parties** : Control team, Threat Intelligence Provider, testeurs et TLPT Authority.
19. À noter que le recours à des testeurs internes à l'entité est encadré par l'article 13 du document de norme technique de réglementation (NTR/RTS) (politique dédiée en particulier).

Clôture

20. À la fin des tests de l'équipe rouge, l'équipe bleue **de l'entité est informée** que les tests d'intrusion fondés sur les menaces ont eu lieu.
21. **Dans les 4 semaines qui suivent la fin des tests**, les testeurs de l'équipe rouge fournissent leur rapport à l'équipe de contrôle, suivant les directives de l'annexe V du document de norme technique de réglementation (NTR/RTS) ; sans délai, cette dernière le transmet à l'équipe bleue et aux tests managers de la TLPT Authority.
22. De même **dans les 10 semaines qui suivent la fin des tests** de l'équipe rouge, l'équipe bleue fournit son propre rapport à l'équipe de contrôle suivant les directives de l'annexe VI du RTS ; sans délai, cette dernière le transmet à l'équipe rouge et aux tests managers.
23. **Dans les 10 semaines qui suivent la fin des tests** de l'équipe rouge, l'équipe bleue et les testeurs de l'équipe rouge rejouent l'attaque et la défense réalisées pendant le test ; en complément, l'équipe de contrôle doit conduire un exercice de type « Purple team » sur des sujets ou problèmes identifiés pendant les tests.
24. Une fois que la TLPT Authority a notifié à l'équipe de contrôle que les rapports des équipes rouges et bleues ont été évalués et qu'ils contiennent les informations attendues conformément aux annexes V et VI du NTR/RTS, alors le rapport final contenant les failles relevées par les tests d'intrusion fondés sur les menaces est rédigé par l'équipe de contrôle de l'entité financière sans information sensible et selon les directives de l'annexe VII, puis soumis à la TLPT Authority **dans les 8 semaines**.

Remédiation

25. L'entité financière doit fournir un plan de remédiation à la TLPT Authority **dans les 8 semaines après la notification reçue de la TLPT Authority** avec un traitement de chaque vulnérabilité comme décrit au *Chapitre III - Article 12* du document de norme technique de réglementation (NTR/RTS).

Annexe 2 – Autres réglementations du secteur financier sur la résilience et la gestion des tiers (liste non exhaustive)



Le BCBS (Basel Committee on Banking Supervision) est à l'origine de la plupart des orientations ou réglementations sur la résilience opérationnelle. En effet, beaucoup de ces approches sont inspirées par les principes de résilience opérationnelle¹⁶ publiés par le BCBS en mars 2021.



États-Unis

La SEC a adopté fin 2023 de nouvelles règles concernant la gestion du risque de cybersécurité et la déclaration des incidents¹⁷. Les agences de supervision américaines (BGFRS - Board of Governors of the Federal Reserve System, OCC - Office of the Comptroller of the Currency et FDIC - Federal Deposit Insurance Corporation) avaient déjà publié en 2020 des orientations sur les bonnes pratiques en matière de résilience opérationnelle¹⁸.



Canada

Le BSIF (Bureau du Surintendant des Institutions Financières / OSFI - Office of the Superintendent of Financial Institutions) a publié pour consultation une nouvelle version de la ligne directrice E-21 sur la résilience opérationnelle et la gestion du risque opérationnel¹⁹. Elle établit notamment de nouvelles attentes à l'égard de la gestion de la continuité des activités, de la gestion de crise, de la gestion du changement et de la gestion du risque lié aux données.



Royaume-Uni

La Banque d'Angleterre (BoE), la PRA (Prudential Regulation Authority) et la FCA (Financial Conduct Authority), ont publié conjointement le 7 décembre 2023 une consultation²⁰ pour établir les règles concernant la gestion des prestataires critiques des entités financières au Royaume-Uni. L'objectif du régulateur est de définir les exigences nécessaires pour gérer les risques de stabilité du système financier britannique dus à une interruption ou à une perturbation d'un service fourni par un prestataire.

Ce papier fait suite à la publication en mars 2021 de règles en matière de résilience opérationnelle (*Policy Statement PS6/21 - Operational resilience : Impact tolerances for important business services*²¹).



Australie

L'APRA (Australian Prudential Regulation Authority) a publié le 18 juillet 2023 le standard prudentiel CPS 230²² dont les 3 piliers principaux sont (1) la gestion du risque opérationnel,

¹⁶ <https://www.bis.org/bcbs/publ/d516.pdf>

¹⁷ <https://www.sec.gov/files/rules/final/2023/33-11216.pdf>

¹⁸ <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-144a.pdf>

¹⁹ <https://www.osfi-bsif.gc.ca/Fra/fi-if/rg-ro/gdn-ort/gl-ld/Pages/e21-dft.aspx>

²⁰ <https://www.bankofengland.co.uk/prudential-regulation/publication/2023/december/operational-resilience-critical-third-parties-to-the-uk-financial-sector>

²¹ <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/policy-statement/2021/march/ps621.pdf>

²² <https://www.apra.gov.au/sites/default/files/2023-07/Prudential%20Standard%20CPS%20230%20Operational%20Risk%20Management%20-%20clean.pdf>

(2) les plans de continuité d'activité et la capacité à fournir les services critiques y compris face à des incidents majeurs et (3) la bonne gestion des risques liés aux sous-traitants.



Le Conseil de stabilité financière (FSB - Financial Stability Board) a publié le 4 décembre 2023 un guide pratique à l'usage des institutions financières et des autorités de régulation sur la gestion du risque et la surveillance des fournisseurs de services tiers²³. L'objectif de cette publication est de réduire la fragmentation dans la réglementation et les pratiques de supervision entre les juridictions.



Inde

La RBI (Reserve Bank of India) a publié en novembre 2023 une directive pour la gestion du risque TIC²⁴. Ce document précise notamment les attendus en matière de gouvernance informatique, de gestion des infrastructures et des services TIC, de gestion des sous-traitants, de politique et contrôles de sécurité et de plans de continuité d'activité.



Japon

La FSA (Financial Services Agency) a publié un document de réflexion sur la résilience opérationnelle pour les entités financières²⁵ dont l'objectif est d'assurer la continuité de service face à des incidents majeurs, aussi bien naturels (tremblements de terre, inondations) que d'origine cyber.

²³ <https://www.fsb.org/wp-content/uploads/P041223-1.pdf>

²⁴

<https://rbidocs.rbi.org.in/rdocs/notification/PDFs/107MDITGOVERNANCE3303572008604C67AC25B84292D85567.PDF>

²⁵ <https://www.fsa.go.jp/news/r4/ginkou/20230427/04.pdf>

Annexe 3 – Partage des responsabilités

À titre d'illustration, l'application des exigences DORA à différents modèles de services tels que SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) et les environnements sur site est présentée ici. Elle nécessite une approche différenciée basée sur le niveau de contrôle et de responsabilité inhérent à chaque modèle.

		SaaS	PaaS	IaaS	On-Premise
Responsabilité toujours assumée par le client	Gouvernance et stratégie	<ul style="list-style-type: none"> S'assurer que des mesures appropriées de classification, de traitement et de protection des données sont en place. Gérer les contrôles d'accès des utilisateurs et la vérification de l'identité. Effectuer régulièrement des analyses d'impact relatives à la protection des données. 	<ul style="list-style-type: none"> Sécuriser le code et les données de l'application. Gérer les paramètres de configuration de l'environnement. Effectuer des évaluations des risques au niveau de l'application. 	<ul style="list-style-type: none"> Sécuriser le système d'exploitation et les configurations réseau. Gérer l'accès au réseau virtualisé et aux ressources de calcul. Implémenter un chiffrement fort pour les données au repos et en transit. 	<ul style="list-style-type: none"> Gérer et sécuriser l'ensemble de la pile technologique, de la sécurité physique à la couche applicative. Effectuer des évaluations complètes des risques. Assurance que toutes les obligations en matière de conformité et de déclaration sont respectées sans dépendre d'un fournisseur de services.
	Évaluation du risque				
	Gestion des incidents				
	Gestion de la continuité des activités				
	Tests et amélioration continue				
Responsabilité partagée	Protection des données	<ul style="list-style-type: none"> Collaborer à la définition des rôles et des privilèges d'accès. Élaborer des procédures conjointes d'intervention en cas d'incident et de notification des atteintes à la protection des données. 	<ul style="list-style-type: none"> Travailler ensemble sur des stratégies de gestion des risques au niveau de la plateforme. Coordonner la planification de la continuité des activités au niveau des applications et des plateformes. 	<ul style="list-style-type: none"> Aligner les pratiques de gestion de l'infrastructure sur les exigences de gestion des risques. Élaborer des plans complets de continuité d'activité et de reprise après sinistre, qui couvrent à la fois l'infrastructure et les données des clients. 	<p>Bien que la plupart des responsabilités incombent au client, lors de l'utilisation de logiciels ou de services tiers, la collaboration est nécessaire pour la réponse aux incidents et la planification de la continuité.</p>
	Gestion du risque				
	Réponse aux incidents				
	Surveillance de la conformité				
	Stratégie de sortie				
Responsabilité transférée au fournisseur de cloud	Fournir des services transparents	<ul style="list-style-type: none"> Maintenir la sécurité et la disponibilité des applications. Fournir des fonctionnalités robustes de sécurité et de chiffrement des données. Proposer des mécanismes de signalement des incidents et aider les clients à se conformer aux exigences en matière de rapports. 	<ul style="list-style-type: none"> Assurer la sécurité et la résilience de la plateforme. Fournir des fonctionnalités de conformité et de sécurité pour le déploiement d'applications. Soutenir les efforts des clients dans la détection et la gestion des incidents. 	<ul style="list-style-type: none"> Assurer la sécurité du matériel et des installations du centre de données. Fournir une infrastructure de virtualisation robuste. Offrir des outils de surveillance de l'intégrité et des performances de l'infrastructure. 	<ul style="list-style-type: none"> Fournir des mises à jour de sécurité et des correctifs pour les logiciels locaux. Offrir des conseils et une assistance pour maintenir la conformité des logiciels.
	Maintenir une infrastructure résiliente				
	Soutenir la conformité des clients				

5.1.1.1 SaaS

Pour le Software as a Service, le fournisseur de services gère la majorité de l'infrastructure et des logiciels, tandis que la responsabilité du client est principalement axée sur la gestion des données et de l'accès des utilisateurs.

Responsabilités du client :

- S'assurer que des mesures appropriées de classification, de traitement et de protection des données sont en place.
- Gérer les contrôles d'accès des utilisateurs et la vérification de l'identité.
- Effectuer des analyses d'impact relatives à la protection des données.

Responsabilités du fournisseur de services :

- Maintenir la sécurité et la disponibilité des applications.
- Fournir des fonctionnalités robustes de sécurité et de chiffrement des données.
- Proposer des mécanismes de signalement des incidents et aider les clients à se conformer aux exigences en matière de rapports.

Responsabilités partagées :

- Collaborer à la définition des rôles et des privilèges d'accès.
- Élaborer des procédures conjointes d'intervention en cas d'incident et de notification des atteintes à la protection des données.

5.1.1.2 PaaS

Dans Platform as a Service, le client a le contrôle sur les applications déployées et éventuellement sur les paramètres de configuration de l'environnement d'hébergement.

Responsabilités du client :

- Sécuriser le code et les données de l'application.
- Gérer les paramètres de configuration de l'environnement.
- Effectuer des évaluations des risques au niveau de l'application.

Responsabilités du fournisseur de services :

- Assurer la sécurité et la résilience de la plateforme.
- Fournir des fonctionnalités de conformité et de sécurité pour le déploiement d'applications.
- Soutenir les efforts des clients dans la détection et la gestion des incidents.

Responsabilités partagées :

- Travailler ensemble sur des stratégies de gestion des risques au niveau de la plateforme.
- Coordonner la planification de la continuité des activités au niveau des applications et des plateformes.

5.1.1.3 IaaS

Avec l'infrastructure as a Service, le client est responsable de la gestion du système d'exploitation, du stockage et des applications déployées.

Responsabilités du client :

- Sécuriser le système d'exploitation et les configurations réseau.
- Gérer l'accès au réseau virtualisé et aux ressources de calcul.
- Mettre en œuvre un chiffrement fort pour les données au repos et en transit.

Responsabilités du fournisseur de services :

- Assurer la sécurité du matériel et des installations du centre de données.
- Fournir une infrastructure de virtualisation robuste.
- Offrir des outils de surveillance de l'intégrité et des performances de l'infrastructure.

Responsabilités partagées :

- Aligner les pratiques de gestion de l'infrastructure sur les exigences de gestion des risques.
- Élaborer des plans complets de continuité d'activité et de reprise après sinistre qui couvrent à la fois l'infrastructure et les données des clients.

5.1.1.4 Sur site

Pour les déploiements sur site, le client conserve toutes les responsabilités en matière de gestion et de sécurisation de l'infrastructure, des applications et des données.

Responsabilités du client :

- Gérer et sécuriser l'ensemble de la pile technologique, de la sécurité physique à la couche applicative.
- Effectuer des évaluations complètes des risques.
- S'assurer que toutes les obligations en matière de conformité et de déclaration sont respectées sans dépendre d'un fournisseur de services.

Responsabilités du fournisseur de services (le cas échéant, par exemple dans le cas d'un logiciel tiers) :

- Fournir des mises à jour de sécurité et des correctifs pour les logiciels.
- Offrir des conseils et une assistance pour maintenir la conformité des logiciels.

Responsabilités partagées :

Bien que la plupart des responsabilités incombent au client, lors de l'utilisation de logiciels ou de services tiers, la collaboration est nécessaire pour la réponse aux incidents et la planification de la continuité.

Annexe 4 – Glossaire

ABE	Autorité bancaire européenne (EBA - European Banking Authority)
AEAPP	Autorité européenne des assurances et des pensions professionnelles (EIOPA - European Insurance and Occupational Pensions Authority)
AEMF	Autorité européenne des marchés financiers (ESMA - European Securities and Markets Authority)
AES	Autorités européennes de surveillance
DORA	Digital Operational Resilience Act
SOC2	Service Organisation Control
ISAE 3402	International Standard on Assurance Engagement 3402
CTTP	Critical Third Party Provider
PCI-DSS	Payment Card Industry Data Security Standard
FSB	Financial Stability Board (https://www.fsb.org)
TLPT	Threat-Led Penetration Testing – Test fondé sur l'analyse de la menace
IAAS	Infrastructure as a Service
PAAS	Platform as a Service
SAAS	Software as a Service
PSEE	Prestation de service essentielle externalisée

Bibliographie

- Règlement délégué 2024/1502 du 22 février 2024 : définition des critères de désignation de prestataires tiers de services TIC comme critiques pour les entités financières (DORA, art. 31). À lire en contemplation des RTS relatives à l'article 28.10).
- Règlement délégué 2024/1505 du 22 février 2024 : détermination du montant des redevances de supervision à percevoir par le superviseur principal auprès des prestataires tiers critiques de services TIC et les modalités de paiement de ces redevances (DORA, art. 43).
- Règlement délégué 2024/1772 du 13 mars 2024 : normes techniques de réglementation précisant les critères de classification des incidents liés aux TIC et des cybermenaces, fixant des seuils d'importance significative et précisant les détails des rapports d'incidents majeurs (DORA, art. 18.3).
- Règlement délégué 2024/1773 du 13 mars 2024 : normes techniques de réglementation précisant le contenu détaillé de la politique relative aux accords contractuels sur l'utilisation de services TIC soutenant des fonctions critiques ou importantes fournis par des prestataires tiers de services TIC (DORA, art. 28.10).

Règlement délégué 2024/1774 du 13 mars 2024 : 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 (DORA, art. 16.3).

Le règlement DORA



Tour Eria, 5 rue Bellini
92821 Puteaux Cedex
France

☎ +33 1 53 25 08 80

clusif@clusif.fr

clusif.fr