racine AVOCATS

Les RDV Experts

DORA | La série décryptage Banque – Finance – Assurance & IP/IT

DORA #6 : Gestion et notification des incidents liés aux TIC

Le Règlement (UE) 2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier (« **DORA** ») définit l'incident lié aux TIC comme suit :

- L'« **incident lié aux TIC** » : un événement ou une série d'événements liés entre eux que l'entité financière n'a pas prévu qui compromet la sécurité des réseaux et des systèmes d'information, et a une incidence négative sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données ou sur les services fournis par l'entité financière ; de

- L'« **incident majeur lié aux TIC** » : un incident lié aux TIC qui a une incidence négative élevée sur les réseaux et les systèmes d'information qui soutiennent les fonctions critiques ou importantes de l'entité financière.

DORA met à la charge des entités assujetties une obligation de **prévention** (article 9), de **détection** (article 10) et de **réponse** (article 11) aux incidents liés aux TIC qui nécessite de définir un **processus de gestion des incidents liés aux TIC afin de les détecter, de les gérer et de les notifier** (article 17).

Ce processus doit permettre de classer les incidents liés aux TIC (**1**) puis de notifier les incidents majeurs au régulateur (**2**).

1. Classification des incidents liés aux TIC

a. Critères de classification des incidents liés aux TIC

La classification des incidents s'opère sur la base d'un **ensemble de critères** dont une première liste est fixée par l'article 18 de DORA et qui sont précisés par les **normes techniques** contenues dans un

projet de Règlement délégué de DORA (Règlement délégué de la Commission complétant le règlement (UE) 2022/2554 en ce qui concerne les normes techniques de réglementation précisant les critères de classification des incidents liés aux TIC et des cybermenaces, établissant des seuils d'importance relative et précisant les détails des rapports sur les incidents majeurs).

Ces critères sont notamment les suivants :

• **Clients, contreparties financières et transactions :**
- Nombre de clients affectés dans l'incapacité d'utiliser le service fourni ;
- Nombre de contreparties financières ayant conclu un accord contractuel avec l'établissement ayant subi un préjudice du fait de l'incident ;
- Nombre et montant des transactions affectées par l'incident.

• **Impact réputationnel :**
- Incident porté à la connaissance des médias ;
- Réception de plaintes répétées du fait de l'incident ;
- Risque ou impossibilité de satisfaire aux exigences réglementaires ;
- Risque de pertes de clients et/ou contreparties financières entrainant un impact significatif sur l'activité.

• **Durée et temps d'arrêt du service :**
- La durée de l'incident se mesure à partir du moment où l'incident se produit et jusqu'au moment où l'incident est résolu ;
- Le temps d'indisponibilité du service se mesure à partir du moment où le service est totalement ou partiellement indisponible pour les clients et/ou contreparties financières.

• **Etendue géographique :** impact dans d'autres Etats membres (clients, contreparties financières, succursales, infrastructures de marché ou fournisseurs tiers dans d'autres Etats membres).

• **Pertes de données :**
- si l'incident les a rendues temporairement ou définitivement inaccessibles ou inutilisables ;
- si l'incident a compromis la fiabilité de la source des données ;
- si l'incident a entraîné une modification non autorisée des données qui les a rendues inutilisables ;
- si l'incident a entraîné l'accès à des données ou leur divulgation à des tiers.

• **Criticité des services affectés :**
- affecte ou a affecté des services TIC ou des systèmes de réseau et d'information qui soutiennent des fonctions critiques ou importantes de l'entité ;
- affecte ou a affecté les services financiers fournis par l'entité ;
- constitue ou a constitué un accès réussi, malveillant et non autorisé au réseau et aux systèmes d'information de l'entité.

• **Impact économique de l'incident :**
Prise en compte des types de coûts et de pertes, directs et indirects, subis à la suite de l'incident relatifs notamment aux :
- Fonds ou actifs financiers expropriés y compris ceux perdus à la suite d'un vol ;
- Coûts de remplacement des logiciels, du matériel, etc. ;

- Coûts de personnel associés au remplacement, à l'embauche de personnel supplémentaire, etc. ;
- Frais liés au non-respect des obligations contractuelles ;
- Coûts de réparation ou d'indemnisation des clients ;
- Coûts liés à la communication interne ou externe ;
- Coûts de conseil y compris ceux relatifs aux services de conseil juridique.

b. Seuils de matérialité permettant d'identifier les incidents majeurs à notifier aux autorités compétentes

Un incident est considéré comme **majeur** dès lors qu'il affecte des services critiques tels que décrits ci-dessus et que deux ou plusieurs seuils de matérialité parmi les suivants sont atteints :

• **Concernant les clients, contreparties financières et transactions :**
- La proportion de clients affectés est supérieure à 10 % du nombre de clients utilisant le service ;
- Le nombre de clients affectés dépasse 100 000 clients ;
- La proportion de contreparties financières affectées est supérieur à 30 % ;
- La proportion de transactions affectées est supérieur à 10 % de la moyenne journalière des transactions effectuées par l'entité en nombre ;
- La proportion de transactions affectées est supérieur à 10 % de la moyenne journalière des transactions effectuées par l'entité en valeur ;
- Les clients ou contreparties financières ont été identifiées comme pertinents.

• **Concernant l'impact réputationnel :**
- Tout incident relatif à l'impact réputationnel est considéré comme atteignant le seuil de matérialité.

• **Concernant la durée et le temps d'arrêt du service :**
- La durée de l'incident est supérieure à 24h ;
- Le temps d'indisponibilité du service est supérieur à 2h pour les services TIC qui soutiennent des fonctions critiques ou importantes.

• **Concernant l'impact économique de l'incident :**
- Lorsque les coûts et les pertes encourus par l'entité financière du fait de l'incident majeur ont dépassé ou risquent de dépasser 100 000 euros.

2. Notification des incidents liés aux TIC

Les entités financières adressent à l'autorité compétente les éléments suivants :

- **une notification initiale** ;
- un **rapport intermédiaire** après la notification initiale visée au point a), dès que la situation de l'incident initial a sensiblement changé ou que le traitement de l'incident majeur lié aux TIC a

changé sur la base des nouvelles informations disponibles, suivi, le cas échéant, de notifications actualisées chaque fois qu'une mise à jour pertinente de la situation est disponible, ainsi que sur demande spécifique de l'autorité compétente ;

- un **rapport final**, lorsque l'analyse des causes originelles est terminée, que des mesures d'atténuation aient déjà été mises en œuvre ou non, et lorsque les chiffres relatifs aux incidences réelles sont disponibles en lieu et place des estimations.

Un projet de Règlement délégué complétant DORA précise le **contenu**, les **délais** et le **modèle** des rapports d'incidents liés aux TIC.

La **notification initiale** est soumise dès que possible dans les **quatre heures suivant la classification de l'incident comme majeur** et au maximum **vingt-quatre heures après la détection** de l'évènement.

Le **rapport intermédiaire** est adressé dans les soixante-douze heures suivant le classement de l'incident comme majeur, ou lorsque les activités habituelles ont été rétablies et que les affaires ont repris leur cours normal.

Le **rapport final** est présenté au plus tard **un mois** après que l'incident a été classé comme majeur, sauf si l'incident n'a pas été résolu. Dans ce dernier cas, le rapport final est présenté le jour suivant la résolution définitive de l'incident.

Voir nos précédents épisodes

DORA #5 : Les prestataires tiers
DORA #4 : La gestion du risque lié aux TIC, il ne vous reste qu'un an !
DORA #3 : Le cadre répressif
DORA #2 : Le champ d'application
DORA #1 : La genèse

IP/IT Banque – Finance – Assurance

Eric Barbry
Avocat Associé
ebarbry@racine.eu

Lena Chemla
Avocat
lchemla@racine.eu