RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE

ÉTAT DES LIEUX HUIT MOIS APRÈS L'ENTRÉE EN VIGUEUR DE DORA

09/10/2025

1. Introduction
2. Point d'étape sur la mise en œuvre du cadre règlementaire
3. RoI et incidents : premiers constats après six mois de reporting
4. De l'accompagnement en 2025 à une supervision progressivement renforcée à partir de 2026

1 INTRODUCTION

INTRODUCTION

- **DORA : « accélérateur » en faveur d'une résilience opérationnelle accrue**
  - Un cadre de gestion du risque informatique renforcé nécessitant une formalisation des politiques et procédures mises en place et une structuration de l'organisation de chaque entité financière
  - Un programme de test ambitieux et proportionné avec, pour les entités les plus importantes, un suivi par l'autorité compétente des tests d'intrusion fondés sur la menace (TLPT)
  - Une obligation de déclaration des incidents majeurs : incitation pour toutes les entités à mettre en place une un process efficace de détection des incidents ; permet une plus grande réactivité des autorités en cas d'incident critique
  - Un nouveau cadre de surveillance des fournisseurs de services TIC critiques: en assurant une plus grande résilience de ces tiers, ce cadre doit également accroitre la résilience des entités financières

- **DORA : un cadre qui simplifie et harmonise**
  - Ce règlement fixe des exigences communes à tout le secteur financier et s'applique à 20 catégories différentes d'entités et permet ainsi de limiter la « fragmentation » règlementaire dans le domaine de la résilience opérationnelle
  - DORA est *lex specialis* de NIS2 : étant donné que les dispositions de DORA ont un effet au moins équivalent à celle de NIS2, les entités essentielles et importantes au sens de NIS2 ne sont soumises qu'aux dispositions de DORA en matière de gestion du risque cyber et de notification des incidents
  - Des orientations ont été supprimées ou fortement réduites : par exemple, c'est le cas des lignes directrices de l'EIOPA et de l'ESMA sur la gestion du risque *Cloud* ou encore des lignes directrices de l'EBA et de l'EIOPA sur la gestion du risque TIC
  - La simplification de certaines orientations toujours en cours : les lignes directrice de l'EBA sur l'externalisation ou encoure les orientations de l'EBA sur le risque opérationnel des IORP.

2

POINT D'ÉTAPE SUR LA MISE EN ŒUVRE DU CADRE RÈGLEMENTAIRE

A. CORPUS RÈGLEMENTAIRE

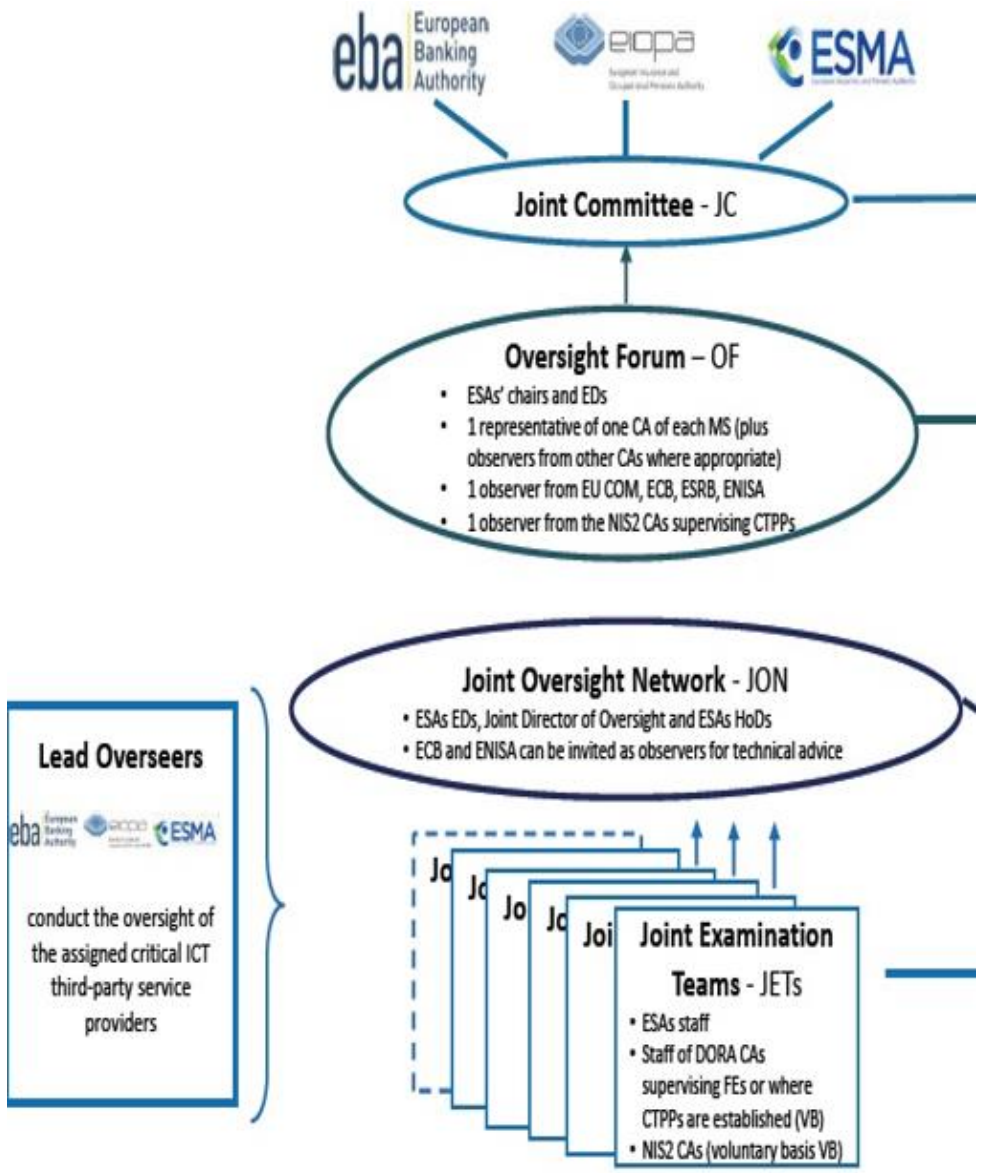
- **Niveau européen**
  - Malgré le retard, l'ensemble des textes de niveau 2 ont été adoptés. Le dernier texte adopté et entré en vigueur est le règlement délégué 2025/532 sur la sous-traitance. L'ensemble des textes est consultable sur Eurlex (ici)
  - C'est une règlementation vivante qui fait également l'objet de plusieurs Q&A déjà adoptées ou en cours de finalisation
  - Une clause de revoyure au 17 janvier 2028

- **Niveau français (PJL résilience)**
  - Examen au Sénat: commission spéciale le 4 mars 2025 et en séance publique les 11 et 12 mars 2025
  - Examen à l'Assemblée nationale: une commission spéciale a eu lieu la semaine du 8 septembre et en séance publique la semaine du 22 septembre
  - L'adoption du texte ainsi que sa transposition au niveau réglementaire (ajustement à la marge de l'arrêté du 03/11/2014 sur le contrôle interne des entités du secteur « bancaire ») est attendue d'ici la fin de l'année

B. UNE SURVEILLANCE DES PRESTATAIRES CRITIQUES (CTPP) QUI SE MET PROGRESSIVEMENT EN PLACE

- **Corpus méthodologique en cours d'élaboration : un contexte nouveau**
  - Une méthodologie qui doit être tournée vers la surveillance des CTPP
  - Une méthodologie de surveillance qui identifie des points de contrôle clé

- **Gouvernance : une nouvelle organisation en cours de stabilisation**
  - Suite à la clôture de la première campagne de remise des registres d'information, l'Oversight Forum a pleinement entamé ses travaux, avec notamment pour objectif la désignation des CTTP, qui seront soumis à la surveillance des équipes conjointes, les JET, en cours de constitution



3

R.O.I. ET INCIDENTS : PREMIERS CONSTATS APRÈS 6 MOIS DE REPORTING

A. R.O.I. : UNE REMISE COMPLEXE QUI NÉCESSITE DE L'ANTICIPATION

- **84% des entités ont fait une remise sur Onegate mais pour seulement 39% d'entre elles le RoI a pu être traité au niveau européen**

- **Plusieurs facteurs peuvent contribuer à l'expliquer, à l'instar de :**
  - Un calendrier très resserré pour tous les acteurs
  - Des règles de validation non stabilisées et modifiées en cours de période de remise du côté des autorités compétentes ainsi qu'un volume inhabituellement élevé de sollicitations du support technique
  - Un format de remise inhabituel et nécessitant une appropriation parfois sous-estimée du côté des remettants (faible participation observée à l'exercice de dry-run, faible utilisation de l'environnement de test, défaut d'anticipation de l'ampleur de la gouvernance nécessaire en interne)

A. R.O.I. : UNE REMISE COMPLEXE QUI NÉCESSITE DE L'ANTICIPATION

- **Et maintenant ? Les solutions**

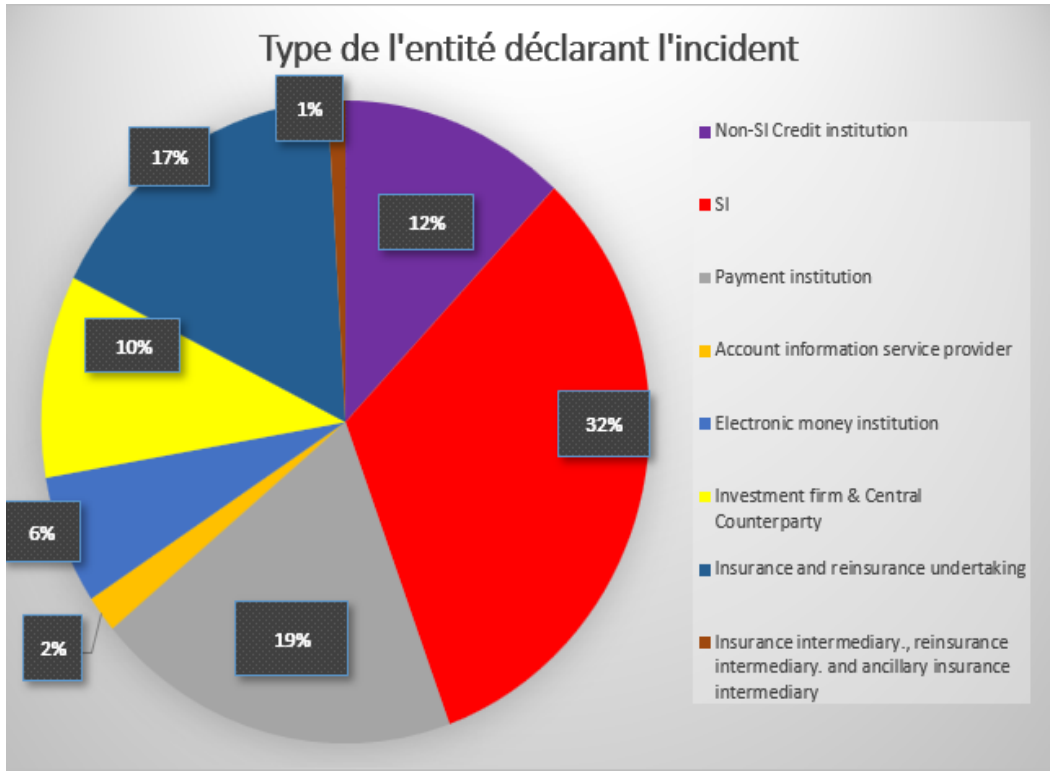
- En prévision de la prochaine remise, l'ACPR va accroitre ses efforts en termes de communication et d'accompagnement des remettants, de manière bilatérale chaque fois que nécessaire
- Alignement des règles de validation Onegate avec celles des AES (à l'exception de la vérification de l'EUID lorsqu'il est utilisé par les entité). Une automatisation de la production et de la communication des CRT devraient être mises en place d'ici la fin de l'année.
- Les entités remettantes sont, quant à elle, invitées à anticiper les prochaines remises, par exemple 1) en développant un outil interne et en mettant an place une véritable *gouvernance projet* en se basant sur tous les éléments de validation et autres retours d'expériences déjà à disposition et 2) en procédant à des remises test sur l'espace homologation dans les mois précédents la période de remis
- Discussion avec les autorités européennes pour faire un bilan de cette première remise

Plus globalement, le RoI doit être pleinement intégré dans le cadre de gestion du risque de tiers des entités (cf. slides 14)

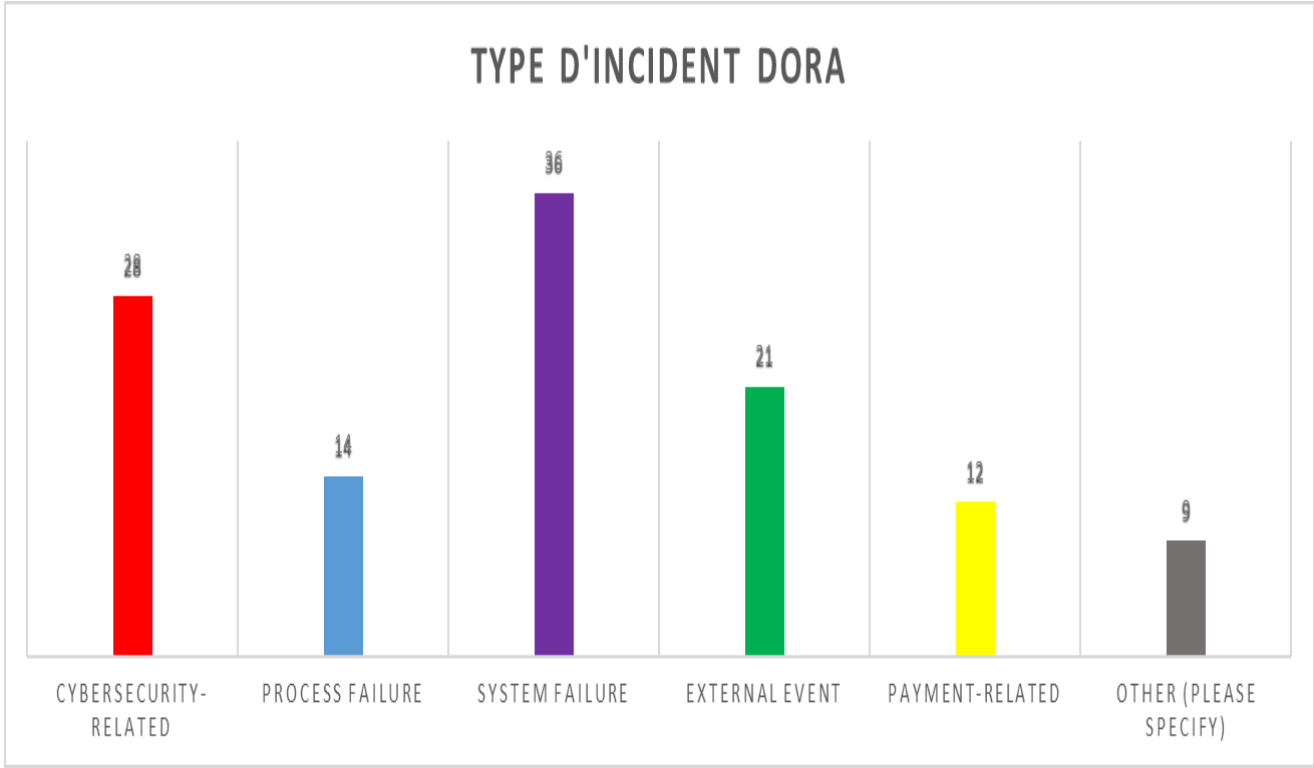
Précisions techniques en annexe à cette présentation

B. INCIDENTS : UN NOMBRE IMPORTANT DE NOTIFICATIONS

Entités notifiantes : majoritairement des EC et assurances



Type d'incidents : essentiellement des failles dans les SI. Le chiffre sur les incidents cyber est élevé du fait d'un incident ayant affecté plusieurs entités



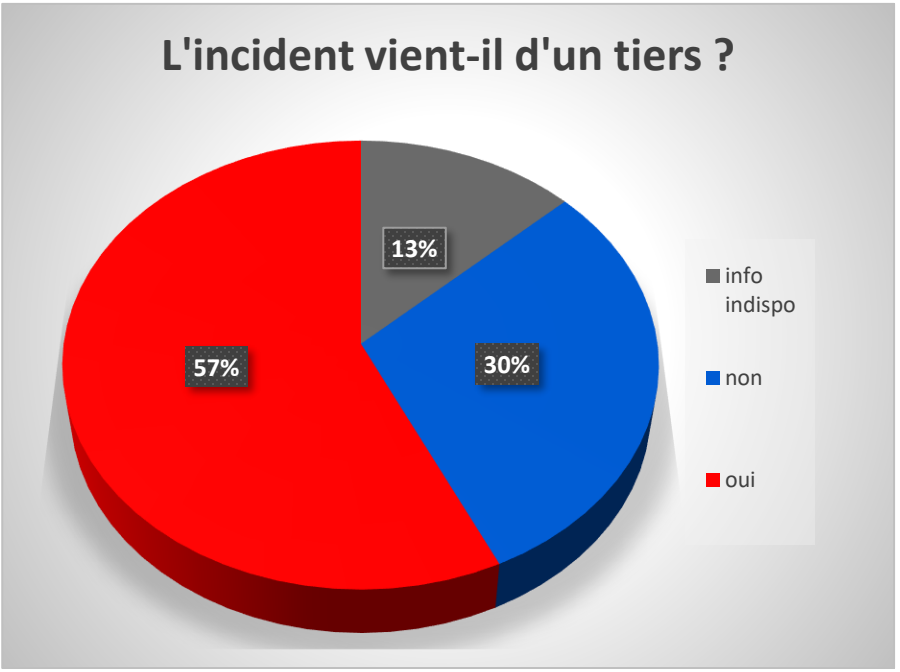
Chiffres au 23/08/2025

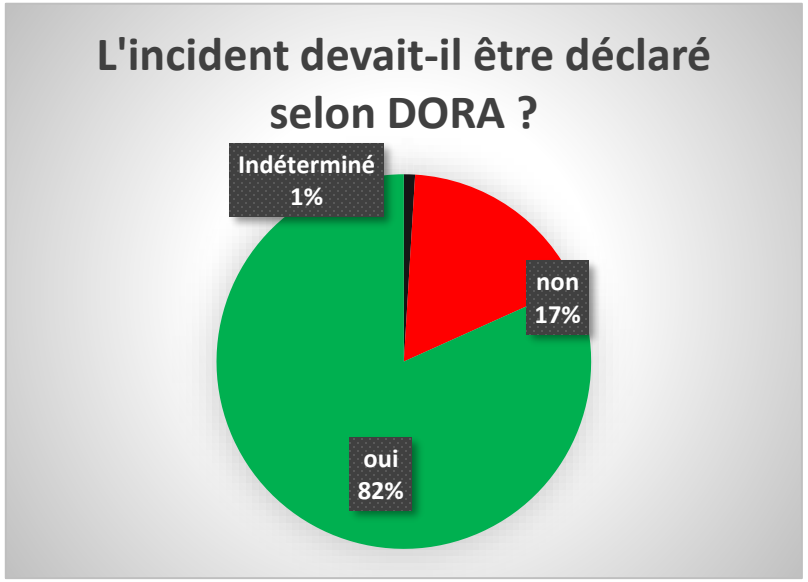
B. INCIDENTS : UN NOMBRE IMPORTANT DE NOTIFICATIONS

- **Tiers impliqués : oui dans plus de la moitié des cas (impact important de l'incident Harvest)**

Dans près 60% des cas l'incident est déjà clos au moment de la notification initiale (les activités ont repris normalement et/ou l'analyse des causes a été terminée)

- **[analyse préliminaire] dans les majorités des cas les notifications sont justifiées**





B. INCIDENTS : UN NOMBRE IMPORTANT DE NOTIFICATIONS

- **Difficultés :**
  - Retard des remises : un incident doit être notifié maximum 4h après sa classification comme majeur, et maximum 24h après sa détection (art5 du règlement délégué (UR) 2025/301). Ces délais sont encore rarement respectés.
  - Le format .Json et les remises sur OneGate : des outils internes pas toujours opérationnels; manque d'anticipation sur les accréditations
  - Non-remplissage de certains champs obligatoires ou erreurs dans leur remplissage

La FAQ DORA de l'ACPR, avec la maquette annotée, est visible ici (partie B, Reporting). Il convient de la lire attentivement afin de disposer de toutes les informations nécessaires au reporting correct des incidents.

- Mécompréhension et/ou omission de certains critères de classification des incidents (règlement délégué (UE) 2024/1772)

Un incident est majeur dans 3 cas possibles :

1) **L'incident est une cyberattaque (art6c + 9.5b)**
2) **L'incident touche ou a touché, quelle que soit l'ampleur de l'impact, des services TIC/réseaux/SI soutenant des FCI (critère primaire) + il remplit au moins 2 critères secondaires**
3) **L'incident touche ou a touché, quelle que soit l'ampleur de l'impact, des services financiers nécessitant un agrément, un enregistrement ou étant surveillés par l'ACPR (critère primaire) + il remplit au moins 2 critères secondaires**

- Prise en compte erronée des mesures compensatoires mises en place après détection d'un incident dans l'évaluation des critères de classification : un incident doit être classifié indépendamment de la mise en place d'éventuelles mesures compensatoires

C. R.O.I. ET INCIDENTS : DES REMISES QUI DOIVENT ÊTRE PLEINEMENT INTÉGRÉES DANS LES PROCESS INTERNES DES ENTITÉS (1/2)

- **ROI**
  - Le registre s'intègre pleinement au cadre de gestion des risques, notamment les risques liés aux TIC et d'externalisation
  - Son utilisation doit être conjointe aux autres outils internes, notamment les inventaires 1) des actifs ICT, 2) de la criticité des actifs et processus ou 3) des dépendances et interdépendances
  - Ainsi, toute évolution des critères de criticité et/ou d'interdépendance doit générer une revue de l'analyse de risques effectuée lors de la conclusion du contrat (indépendamment de sa révision à fréquence régulière)
  - Ces éléments contribuent également aux processus de gestion de crise et de continuité d'activité
  - En outre, le registre doit être tenu à jour de manière constante et revu régulièrement afin de s'assurer de la conformité constante des contrats aux obligations contractuelless pour les accords conclus portant sur des services TIC
  - Le registre contribue également à l'évaluation du risque de concentration
  - Permet d'identifier des problématiques avec des prestataires pour lesquels la renégociation des contrats est difficile et d'en référer aux autorités de contrôle

C. R.O.I. ET INCIDENTS : DES REMISES QUI DOIVENT ÊTRE PLEINEMENT INTÉGRÉES DANS LES PROCESS INTERNES DES ENTITÉS (2/2)

- **IR**
  - Les déclarations d'incidents s'intègrent également dans le cadre de gestion des risques
  - Ainsi, tout incident majeur lié aux TIC doit entrainer la revue et, si nécessaire, l'actualisation des processus internes pertinents de gestion des risques sur la base des enseignements tirés de la survenance et de la gestion de cet incident
  - Dès lors, a minima, le cadre de gestion du risque lié aux TIC et la politique de continuité des activités TIC de même que les processus de gestion de crise (y compris en termes de communication), doivent tenir compte des incidents majeurs
  - Ces évolutions doivent également contribuer à l'amélioration des formations et actions de sensibilisation mises en place, en interne comme en externe

4

DE L'ACCOMPAGNEMENT EN 2025 À UNE SUPERVISION PROGRESSIVEMENT RENFORCÉE À COMPTER DE 2026

DE L'ACCOMPAGNEMENT À UNE SUPERVISION RENFORCÉE

- **Un accompagnement de l'ensemble des entités financières en 2025**
  - De nombreuses présentations auprès des acteurs de la place depuis le mois d'octobre 2024
  - Un support technique sur le pont (plus de 700 questions auxquelles des réponses ont été apportées)
  - Organisation d'entretiens bilatéraux lorsque cela était nécessaire, incluant le support technique et les services de contrôle
  - La création d'une FAQ plusieurs fois mis à jour et mettant à disposition une documentation visant à faciliter la compréhension des attendus

- **Une supervision renforcée à compter de 2026**
  - Identification des priorités de contrôle sur la base : i) des ESR menés par les services de contrôle ; ii) des conclusions issues de l'analyse des réponses au questionnaire transsectoriel relatif à la mise en œuvre de DORA ; iii) la qualité des RoI et les premières conclusions issues d'analyses horizontales ; iv) les notifications d'incidents majeurs
  - Le lancement d'analyses transversales sectorielles et transsectorielles
  - Des contrôles sur place pour les entités les plus à risque

annexes

REGISTRE D'INFORMATIONS – LIENS UTILES

Quelques liens EBA utiles

ESAs Decision on reporting of information for CTPP designation	Décision des AES concernant la remise annuelle des RoI pour les besoins de désignation des CTPPs précisant les modalités de cette remise
ITS on the registers of information - Adopted and published in the Official Journal of the EU	Texte réglementaire précisant les standards techniques concernant les RoI
Data Model for DORA RoI	Illustration graphique du la correspondance des données entre les différents 'onglets' du RoI et précisions pratiques concernant le format de remise attendu pour chaque donnée
Reporting technical package ○ Validation rules - Please download the file and search for DORA under 'Frameworks' ○ Data Point Model Dictionary (updated 21 March 2025) ○ Data Point Model table layout and data point categorisation - Please download and search for '20241217 Annotated Table Layout DORADORA 4.0' ○ Sample files for taxonomy under taxonomy architecture v2.0 - Please download the folder, under "instances xBRL-CSV", search for the DORA file (DUMMYLEI123456789012.CON_FR_DORA010100_DORA_2024-12-31_20241213174803429) ○ Taxonomy package under taxonomy architecture v2.0 (updated 21 March 2025_- Please download the folder and search for DORA file ○ EBA reporting filing rules v5.5 ○ Preparing plain csv reporting package for DORA (explanatory slides)	Documentation technique et taxonomique détaillée permettant l'élaboration du package xBRL-CSV à remettre
List of possible values for all data fields with drop downs (updated 3 March 2025)	Détails des valeurs possibles pour les champs proposant une liste fermée de réponses
ITS on RoI - Annex 2 list of licensed activities for data point model updated to reflect DPM V4.0	Détail des data points en fonction du type d'agrément des entités déclarantes / déclarés
Overview of technical checks, validation rules and business checks to be applied by the EBA for RoI reporting (updated 28 April 2025)	Détail des règles de validation appliquées par l'EBA
Explanations of the data quality feedback to the registers of information from the validations (explanatory slides)	Explications des contrôles de validation effectués par l'EBA
DORA Sample data quality responses	Exemple de CRT
Observations from testing of RoI reporting to the ESAs – key common issues identified (presentation slides update 16 May 2025)	Observations détaillées des erreurs les plus communes constatées dans les CRT
Frequently asked question on reporting of the registers of information (updated on 28 March 2025)	Q&A EBA portant sur les RoI

ACCRÉDITATION DANS ONEGATE

- Pour déposer vos remises, une accréditation au portail des remettants OneGate est requise
  - Elle est à demander dans un premier temps sur le site du portail Onegate
  - La demande peut être effectuée sur les portails production et homologation/test (Portail OneGate – Production et Portail OneGate - Environnement de test)
  - Il conviendra de s'accréditer avec son LEI via la collecte « SOLVA ».
  - Pour ceux qui ont déjà un compte, vous devez effectuer une demande d'autorisation en vous connectant, dans votre profil Onegate. Les domaines nécessaires pour la collecte DORA sont répertoriés dans le tableau ci-dessous :

Déclaration	Domaines OneGate
Déclaration des registres d'information (ROI)	**DRA**
Déclaration des incidents (IR)	DSA
Déclaration des cyber menaces (CT)	DSA

A noter:

Afin de tester la validité de votre remise, nous vous invitons à la déposer en amont de la date limite, dans la plateforme homologation de OneGate.

DÉPÔT DANS ONEGATE

- La remise ROI (domaine DRA) s'effectue directement par dépôt de fichier sur la page d'accueil (cf. copie écran)

- Nous vous précisons que les ROI DORA ne constituent pas un rapport bureautique, c'est la raison pour laquelle, vous ne retrouverez pas le domaine DRA sous l'onglet rapport dans OneGate.
- Il s'agit d'une remise xBRL-CSV dit "plain CSV" par l'EBA pour DORA. Elle doit être remise dans une « enveloppe » au format XML.

ENCODAGE 64

- L'instance xBRL-CSV, consistant en une archive zip, est contenue dans les balises après encodage en base 64. (cf. copie écran : balise <csv>)

```
<XbrlDelivery>
    <XbrlDeclarationReport xmlns="http://www.onegate.eu/2010-01-01">
      <Administration creationTime="AAAA-MM-JJTHH:MM:SS.CCC">
       <From declarerType="LEI">XXXXX</From>
       <To>BDF</To>
       <Domain>XXX</Domain>
       <Response feedback="true">
              <Email>mail_emetteur@xxxx.fr</Email>
              <Language>FR</Language>
       </Response>

      </Administration>
      <Report  action="replace" >
        <csv>instance xBRL-CSV au format zip encodée en base 64</csv>
      </Report>
    </XbrlDeclarationReport>
</XbrlDelivery>
```

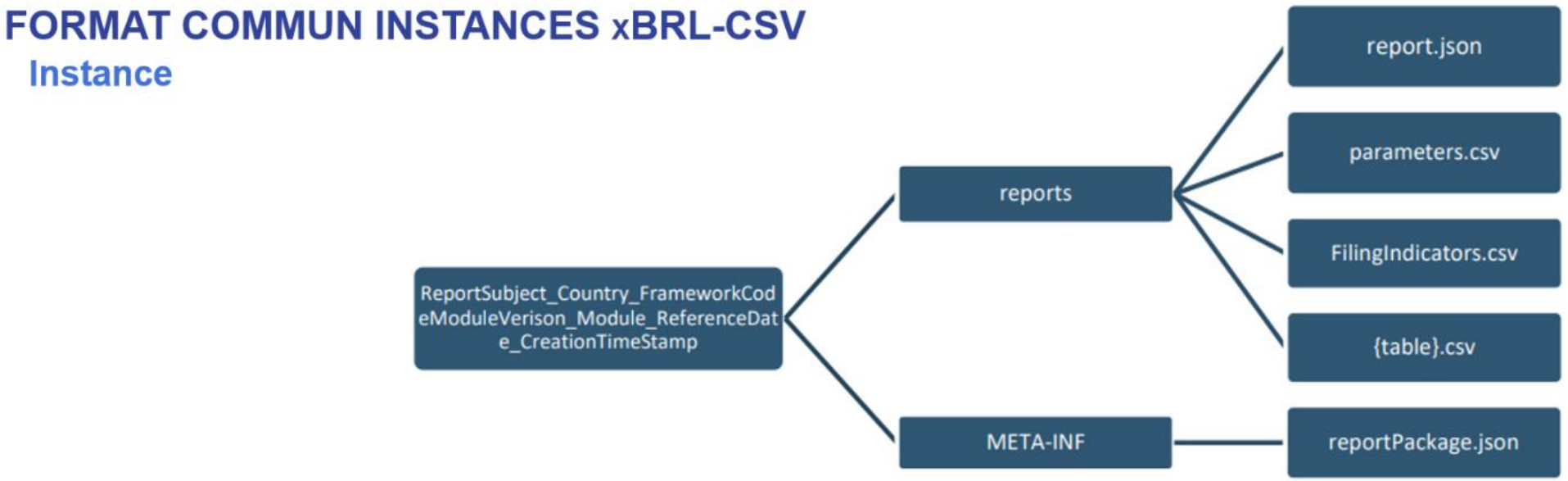
- Source e-surfi assurance: information techniques/documentations techniques/format de remise assurance/ NOTE TECHNIQUE 2025_Formats de fichier (cf. page 5)

Cet encodage en base 64 doit respecter la norme des fichiers attendus par l'EBA :

- Pour la conception de votre instance XBRL-CSV au format zip à encoder en base 64 en vue de son intégration dans votre remise de type XML, vous pouvez vous inspirer d'une instance de test disponible depuis le site de l'EBA : Preparations for reporting of DORA registers of information | European Banking Authority
- Cette étape d'encodage est "**technique**". Il est important d'identifier en amont en interne ou en externe les personnes qui peuvent le réaliser.

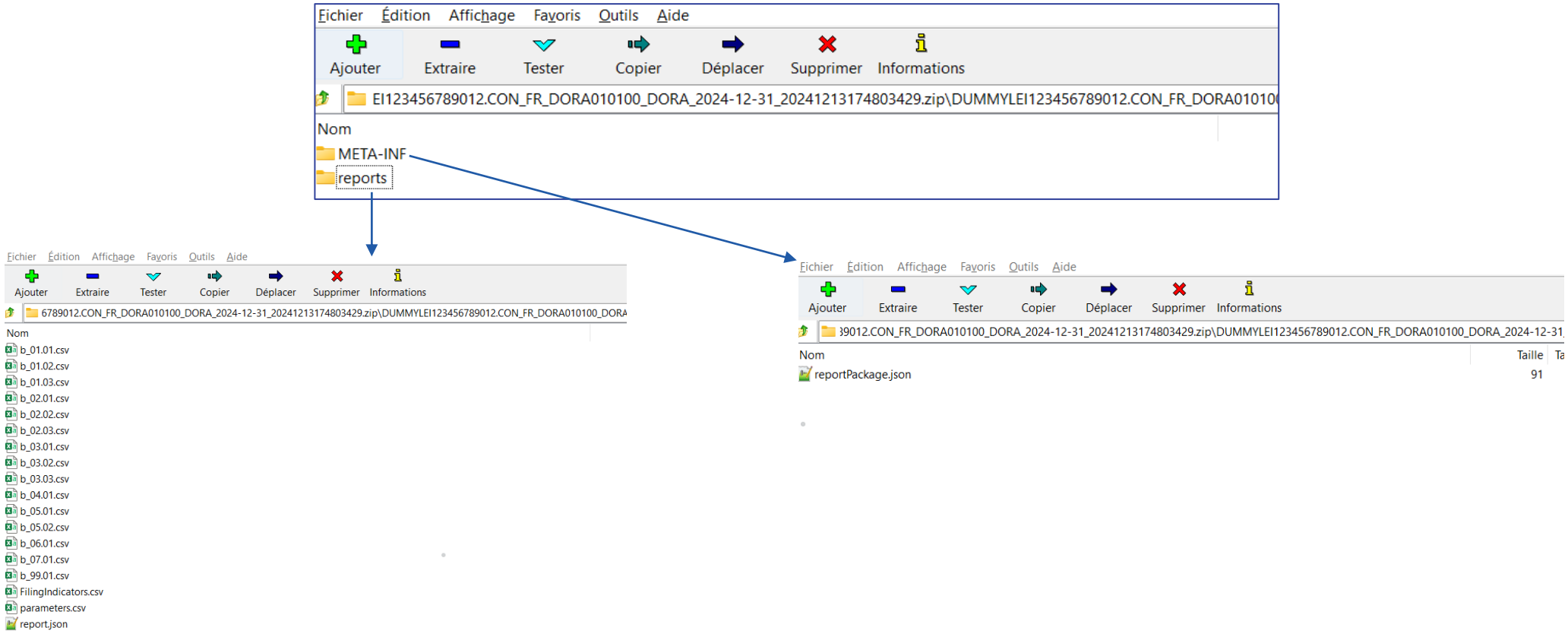
ARBORESCENCE DES FICHIERS À RESPECTER

- Vous devez respecter l'arborescence des fichiers zip attendus pour les remises ROI, conformément aux normes de l'EBA (cf. copie écran) et respecter la nomenclature de tous les nommages.



ARBORESCENCE DES FICHIERS À RESPECTER

- Sous le lien suivant: Sample files for taxonomy under taxonomy architecture v2.0 veuillez télécharger le dossier, sous « instances xBRL-CSV », recherchez le fichier DORA (DUMMYLEI123456789012. CON_FR_DORA010100_DORA_2024-12-31_20241213174803429), pour avoir accès au format zip attendu, ainsi qu'aux fichiers .csv et .json intégrés dans les dossiers META-INF et reports (cf. détail des fichiers ci-dessous)



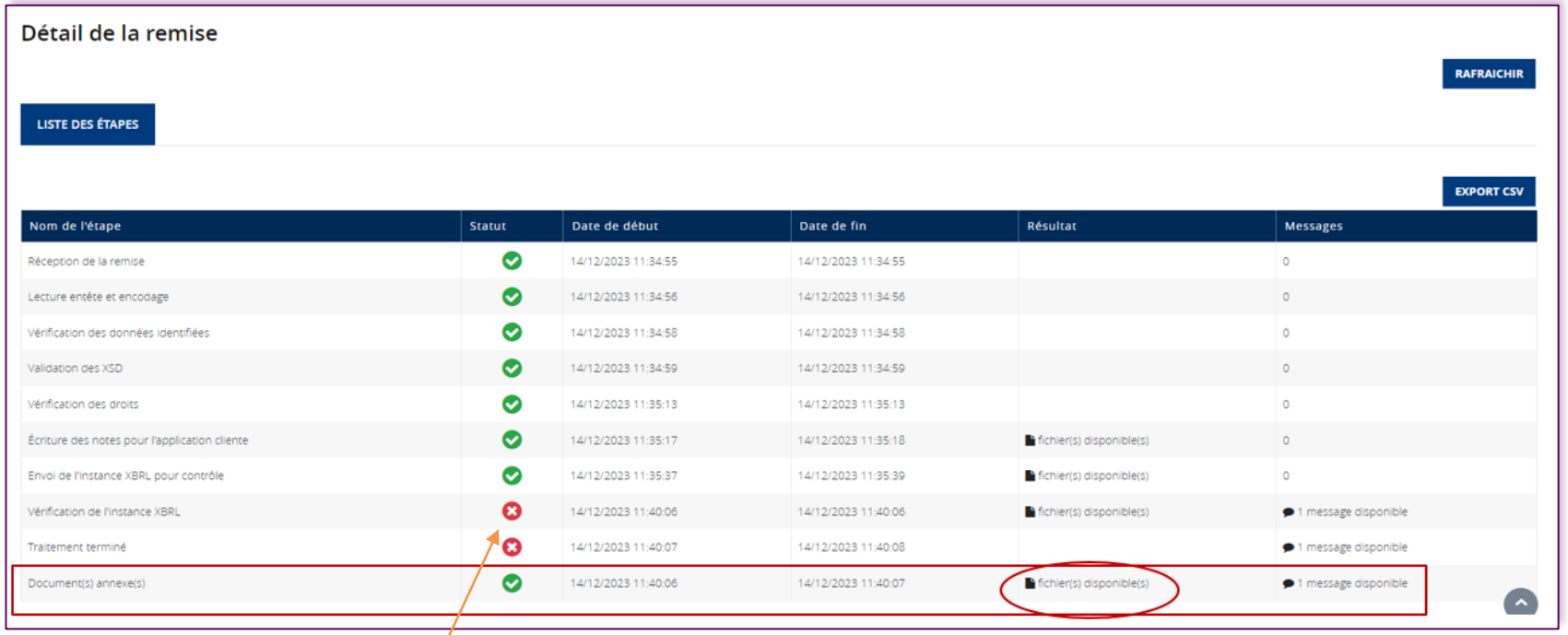
COMPTES RENDUS DE TRAITEMENT

Pour s'assurer de la bonne réception de la remise par l'ACPR, vous devez consulter le compte rendu de traitement.

Le CRT est accessible dans le menu Suivi->Remises->Détail, à l'étape des « Document(s) annexe(s) »

Si tous les contrôles dans Onegate sont validés un CRT avec 3 fichiers seront affichés

- Un fichier au format HTML avec la restitution des anomalies et de leur sévérité
- Un fichier au format XML qui correspond au CRT brut
- Un fichier au format Excel du ROI avec les anomalies



Cette croix rouge indique le rejet de la remise

Pour la collecte de l'année prochaine, il y aura deux CRT dans ONEGATE pour les ROI : le CRT du portail ONEGATE puis le CRT de l'EBA. Pour avoir la vision complète des anomalies identifiées, veuillez attendre l'apparition du second CRT.

RETOUR SUR LES PRINCIPALES CAUSES DE REJET TECHNIQUE

#	Rejet/ message affiché	Analyse du rejet	Solution
1	Erreur calendrier et format de date	La période '15/04/2025' n'est pas encore attendue. Le fichier ne peut pas être remis	Il convient de renseigner la date d'arrêté au format AAAA-MM-JJ ex : 2025-03-31 et non la date limite de remise.
2	MISSING_DATA_REPORT_DATE : Données manquantes dans l'instance : reportDate ERREUR MISSING_DATA_DECLARER_CODE : Données manquantes dans l'instance : declarerCode ERREUR MISSING_DATA_SCHEMA_REF : Données manquantes dans l'instance : schemaRef	Il manque un niveau dans l'arborescence de la remise	L'arborescence des fichiers doit être respectée, comme dans l'exemple fourni par l'EBA : https://www.eba.europa.eu/sites/default/files/2024-12/f4519b45-d6c2-4e7d-a8d4-4bee91a9c530/sample_documents.zip
3	Une erreur est survenue lors de la conversion CSV vers XML. Erreur lors de la lecture de l'instance CSV : error: invalidCSVFileFormat ; In Table b_99.01.csv : This table is invalid	Utilisation de l'encodage ANSI au lieu de UTF-8	L'encodage UTF-8 (avec ou sans BOM) afin de respecter la filing rule 1.4 de l'EBA : "All XBRL reports must use the UTF-8 character encoding (regardless of with or without BOM) in order to ensure that the receiver is able to process it. " : EBA Filing Rules (page 13) Il faut une uniformisation de l'encodage dans tous les fichiers = tous en UTF8 ou tous UTF8 - BOM.