FAQ sur la directive et le règlement DORA

Dernière mise à jour de la FAQ : 25 mars 2025

A. Questions générales

Q-A1 : Y-a-t-il eu des évolutions majeures qui amènent à actualiser certaines informations transmises lors des réunions de Place de l'ACPR du 9 octobre 2024 ?

Oui. Des corrections apparaissent en rouge dans les supports de présentation sur cette page. Elles sont apportées afin de prendre en compte l'évolution des travaux conduits au niveau européen sur les normes techniques de réglementation (RTS) et normes techniques d'exécution (ITS).

Q-A2 : L'adresse email de contact *2760-DORA-UT@acpr.banque-france.fr* est-elle toujours valable après l'entrée en application de DORA au 17 janvier 2025 ?

À partir du 17 janvier 2025, l'adresse email de contact ne sera plus utilisée pour les échanges entre l'ACPR et les entités financières. Les échanges devront passer nécessairement par les services de contrôle habituels *via* le **portail de l'ACPR**.

Q-A3 : En attendant l'examen et l'adoption du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité visant à transposer la Directive (UE) 2022/2556 du 14 décembre 2022 (DORA) ainsi que la révision de l'Accord monétaire entre l'Union européenne et la Principauté de Monaco, quelles sont les entités devant se conformer aux obligations réglementaires découlant de DORA au 17 janvier 2025 ?

Le calendrier d'examen du projet de loi Résilience est sans conséquence sur les exigences du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier (DORA) qui s'appliquent en l'état aux entités visées à l'article 2 de ce règlement dès le 17 janvier 2025.

En l'absence d'adoption du projet de loi Résilience, les succursales de pays tiers d'entreprise d'investissement au sens du L. 532-48 du Code monétaire et financier, les sociétés de financement au sens du II du L. 511-1 du même code, ainsi que les entités financières établies en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis et Futuna et à Saint-Pierre-et-Miquelon ne sont pas tenues d'appliquer les exigences du règlement DORA au 17 janvier 2025. Dans ce contexte, l'annexe sur la gestion des risques liés aux Technologies de l'Information et de la Communication (TIC) ne sera pas à communiquer au moment de la remise à l'ACPR du rapport relatif au contrôle interne établi en application des articles 258 et 266 de l'arrêté du 03 novembre 2014.

Dans l'attente d'une révision de l'Accord monétaire entre l'Union européenne et la Principauté de Monaco, les établissements financiers monégasques ne sont pas tenues d'appliquer les exigences du règlement DORA au 17 janvier 2025.

L'application du règlement DORA aux succursales de pays tiers d'établissement de crédit fait l'objet d'une Q&A en cours d'examen par la Commission européenne.

Q-A4 : Quels types de services doivent être considérés comme des services TIC ?

Une réponse à cette question a été apportée par la Commission européenne : **Question ID : 2999 – DORA030**.

B. Reporting

Q-B1 : À partir de quelle date et selon quelles modalités les entités financières doivent-elles déclarer les incidents majeurs liés aux TIC et les incidents opérationnels ou de sécurité majeurs liés au paiement ?

Les entités financières visées à l'article 2 du règlement (UE) 2022/2554 DORA relevant de la compétence de l'ACPR ainsi que les établissements de crédit classés comme importants doivent déclarer sur base individuelle, **à l'ACPR**, à partir du **17 janvier 2025** :

- **tous les incidents majeurs liés aux TIC** visés à l'article 19(1) du règlement DORA. Les critères de significativité permettant d'identifier ces incidents sont prévus à l'article 8 et 9 du **Règlement délégué (UE) 2024/1772 de la Commission du 13 mars 2024** ;
- **tous les incidents opérationnels ou de sécurité liés au paiement** concernant les établissements de crédit, les établissements de paiement, les prestataires de services d'information sur les comptes et les établissements de monnaie électronique visés à l'article 23 du règlement DORA.

En attendant la publication au journal officiel de l'Union européenne du règlement d'exécution de la Commission européenne définissant des normes techniques d'exécution (ITS) concernant les formats de déclaration des incidents qui sera le texte de référence dès son entrée en application, il est attendu que les entités financières, de manière temporaire, remettent leurs déclarations d'incidents selon les modalités prévues par le projet d'ITS (notamment à son Annexe I et II) présenté au lien suivant : **JC 2024-33 - Final report on the draft RTS and ITS on incident reporting**.

Les entités financières peuvent s'appuyer sur les modèles disponibles aux liens suivants :

- Pour le domaine Banque : **17/01/2025 - Mise en place de la collecte DORA pour la Banque**
- Pour le domaine Assurance : **17/01/2025 - Mise en place de la collecte DORA pour l'Assurance**

Ces incidents doivent être transmis au format .json et ne sont pas revêtus d'une signature électronique. En cas de besoin, les entités peuvent faire le choix de recourir à des logiciels facilitant la manipulation des fichiers en format .JSON (par exemple : XMLSpy, .NET Developer, IntelliJ, Eclipse, etc.). Des solutions en ligne – à n'utiliser que pour des besoins de test – existent également (**https://www.jsonschemavalidator.net** ; **https://jsonformatter.org**).

Les déclarations sont à effectuer via le portail OneGate de l'ACPR. Toutefois, lors de la période d'indisponibilité de OneGate entre minuit et 04h00 ainsi que le dimanche, les déclarations devront exceptionnellement être adressées à l'ACPR par courriel à l'adresse suivante : **2760-INCIDENTS-DORA-UT@acpr.banque-france.fr**

Externalisation des obligations de déclaration :

Les entités financières peuvent externaliser les obligations de déclaration à un prestataire tiers de services dans les conditions prévues à l'article 19(5) du règlement DORA. Elles doivent toutefois impérativement en informer l'ACPR dès la signature de l'accord d'externalisation, et au plus tard avant la première notification de ce type. Les entités financières doivent, en cette occasion, communiquer à l'ACPR le nom, les informations de contact et un code permettant d'identifier le prestataire tiers de services qui déclarera les incidents. Les demandes sont à adresser par courriel à l'adresse suivante : **2760-INCIDENTS-DORA-UT@acpr.banque-france.fr**, en complétant le formulaire de déclaration d'externalisation de déclaration des incidents majeurs.

Un seul espace où apparaîtra l'ensemble des déclarations faites par ou pour le compte d'une entité sera mis à disposition de chaque entité. L'accès à cet espace pourra être octroyé par l'entité à un ou des prestataires auxquels elle aura choisi d'externaliser les obligations de déclaration comme mentionné ci-dessus après information de l'ACPR.

L'ACPR ne prévoit pas de donner la possibilité à un prestataire tiers auquel les obligations de déclaration mentionnées ci-dessus auraient été externalisées de remettre un reporting agrégé conformément à l'article 7 du projet d'ITS sur le reporting des incidents (**JC 2024-33 - Final report on the draft RTS and ITS on incident reporting**).

Q-B2 : À partir de quelle date et selon quelles modalités les entités financières peuvent-elles notifier les cybermenaces importantes ?

Les cybermenaces importantes sont définies à l'article 3 point 13) du règlement DORA. Elles peuvent être notifiées, à titre volontaire, conformément à l'article 19(2) de DORA. Comme pour les incidents majeurs liés aux TIC, les entités financières visées à l'article 2 du règlement (UE) 2022/2554 DORA relevant de la compétence de l'ACPR ainsi que les établissements de crédit classés comme important peuvent notifier, sur base individuelle, ces cybermenaces importantes **à l'ACPR** à partir du **17 janvier 2025**.

En attendant la publication au journal officiel de l'Union européenne du règlement d'exécution de la Commission européenne définissant des normes techniques d'exécution (ITS) concernant les formats de déclaration des incidents, qui sera le texte de référence dès son entrée en application, il est attendu que les entités financières, de manière temporaire, notifient les cybermenaces selon les modalités prévues par le projet d'ITS (notamment à son Annexe III et IV) présenté au lien suivant : **JC 2024-33 - Final report on the draft RTS and ITS on incident reporting**.

Les entités financières peuvent s'appuyer sur les modèles disponibles aux liens suivants :

- Pour le domaine Banque : **17/01/2025 - Mise en place de la collecte DORA pour la Banque**
- Pour le domaine Assurance : **17/01/2025 - Mise en place de la collecte DORA pour l'Assurance**

Ces incidents doivent être transmis au format .json et ne sont pas revêtus d'une signature électronique.

Les déclarations sont à effectuer via le portail OneGate de l'ACPR. Toutefois, lors de la période d'indisponibilité de OneGate entre minuit et 04h00 ainsi que le dimanche, les déclarations devront exceptionnellement être adressées à l'ACPR par courriel à l'adresse suivante : **2760-INCIDENTS-DORA-UT@acpr.banque-france.fr**.

Q-B3 : Quelle est la date de la première remise à l'ACPR du registre d'informations (RoI) contenant les accords contractuels relatifs à l'utilisation des services TIC ? (hors entités relevant de la supervision directe de la BCE)

Le RoI est non seulement un outil essentiel pour la gestion des risques portés par les tiers mais il permet également aux autorités européennes de surveillances (AES) de désigner les prestataires tiers critiques de services TIC (CTPP) qui feront l'objet d'une surveillance au niveau européen prévue au chapitre V section II du règlement DORA. À cette fin, l'ACPR doit transmettre aux AES, sur base annuelle, les registres remis par les entités financières.

La date des premières remises annuelles des RoI par l'ACPR aux AES a été fixée par une décision de ces autorités du 8 novembre 2024 (ESA 2024 22) au 30 avril 2025, avec une date de référence au 31 mars 2025. **Il est donc attendu des entités financières pertinentes (cf. Q-B6 de la FAQ) qu'elles remettent leur registre à l'ACPR avant le 15 avril 2025**.

Q-B4 : Quelles sont les modalités de remise du registre d'informations ? (hors entités sous supervision directe de la BCE)

Les entités financières tiennent leur registre d'information conformément aux modèles prévus par le règlement d'exécution (UE) 2024/2956 de la Commission du 29 novembre 2024 définissant des normes techniques d'exécution pour l'application du règlement (UE) 2022/2554 du Parlement européen et du Conseil en ce qui concerne les modèles types pour le registre d'informations.

Ces registres devront être déposés par les entités pertinentes sur le portail OneGate de l'ACPR au format Plain CSV dans un dossier .zip et ne sont pas revêtues d'une signature électronique. L'ensemble des informations techniques est disponible sur les sites des AES (ici).

Q-B5 : À quelles entités s'appliquent en principe l'obligation de remettre un registre à l'ACPR ?

En lien avec l'obligation faite à l'ACPR de remonter aux Autorités européennes de supervision les informations nécessaires à l'identification des prestataires tiers critiques de services tics, il est demandé à l'ensemble des entités financières soumises à DORA et entrant dans le champ de compétence de l'ACPR tel que défini à l'article L. 612-2 du Code monétaire et financier de remettre un registre d'informations à l'ACPR.

Secteur de la banque, des services de paiement et des services d'investissement	1. les établissements de crédit qui ne sont pas classés comme importants, conformément à l'article 6, paragraphe 4, du règlement (UE) no 1024/2013 ; 2. les établissements de paiement ; 3. les prestataires de services d'information sur les comptes ; 4. les établissements de monnaie électronique ; 5. les entreprises d'investissement telles que définies à l'article L. 531-4 du Code monétaire et financier ; 6. les émetteurs de jetons se référant à un ou des actifs agréés en vertu du règlement (UE) 2023/1114 ;

	7. les contreparties centrales ; 8. les plates-formes de négociation ;
Secteur de l'assurance	1. les organismes d’assurance et de réassurance relevant du régime dit “Solvabilité II” mentionnés aux articles L. 310-3-1 du Code des assurances, L. 211-10 du Code de la mutualité et L. 931-6 du Code de la Sécurité sociale ; 2. les sociétés de groupe d’assurance et sociétés de groupe d’assurance mutuelle mentionnées aux articles L. 322-1-2 et L. 322-1-3 du Code des assurances ; les unions mutualistes de groupe mentionnées à l’article L. 111-4-2 du Code de la mutualité ; 3. les sociétés de groupe assurantiel de protection sociale mentionnées à l’article L. 931-2-2 du Code de la Sécurité sociale ;

4. les compagnies financières holding mixte mentionnées à l'article L. 517-4 du Code monétaire et financier, incluses dans le contrôle de groupe au sens de l'article L. 356-2 du Code des assurances ;
5. les organismes de retraite professionnelle supplémentaire, à savoir les fonds de retraite professionnelle supplémentaire (FRPS) mentionnés à l'article .L. 381-1 du Code des assurances, les mutuelles ou unions de retraite professionnelle supplémentaire (MRPS ou URPS) mentionnées à l'article L. 214-1 du Code de la mutualité et les institutions de retraite professionnelle supplémentaire (IRPS) mentionnées à l'article L. 942-1 du Code de la Sécurité sociale, selon les modalités prévus par le règlement (UE) 2022/2554 dans son article 2, al.3 c).

	6. les intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire qui ne sont pas des microentreprises ou des petites et moyennes entreprises conformément au e) de l'article 2(3) du règlement (UE) 2022/2554

En pratique, certaines entités n'auront pas à remettre leur RoI dès lors que leur maison-mère est sujette à l'obligation de procéder à une remise sur une base consolidée selon les modalités décrites en Q-B6. Concrètement, lorsqu'une entité ne se trouve dans aucun des cas envisagés en Q-B6, elle ne procède elle-même à aucune remise à l'ACPR.

Q-B6 : Quel est le niveau de remise du registre d'informations ?

Conformément à la décision des AES du 8 novembre 2024 susmentionnée (ESA 2024 22), il est demandé à une entité de procéder à une remise sur base individuelle lorsqu'elle se trouve dans l'une ou l'autre de ces situations :

1. Elle ne fait pas partie d'un groupe d'entités financières ;

2. Elle fait partie d'un groupe d'entités financières dont la maison mère dans l'Union européenne ou l'Espace économique européen est établie en France mais n'exerce pas d'activité dans l'un des secteurs mentionnés à l'article 1 ;
3. Elle fait partie d'un groupe d'entités financières dont la maison-mère n'est pas établie dans l'Union européenne ou l'Espace économique européen.

Pour ce qui est des remises au niveau consolidé, ce sont les deux critères mis en avant par les AES dans leur décision du 08 novembre 2024 ainsi que dans la foire aux questions mise en ligne sur leurs sites internet le 14 février 2025 qui sont pris en compte, à savoir : le périmètre de consolidation et le champ de compétence de l'ACPR. Sur cette base, une maison mère en France doit remettre un RoI au plus haut niveau de consolidation dès lors qu'elle est la mère dans l'Union. Ce RoI doit uniquement contenir les informations relatives aux entités du même secteur (au sens de l'article L. 612-2 du CMF) établies en France et au sein de l'Union européenne ou de l'Espace économie européenne ainsi que les informations relatives aux entités en France d'un autre secteur pour lequel l'ACPR est compétente. Le RoI n'inclut aucune information sur les entités localisées dans un pays tiers.

Enfin, pour des raisons pratiques, lorsque la tête de groupe dans l'UE est une holding (ex : compagnie financière holding, compagnie financière holding mixte, compagnie holding d'investissement, société holding d'assurance, société holding mixte d'assurance), il est attendu que cette holding remette le RoI pour le compte de ses entités.

Attention : les règles concernant les niveaux de remise ne s'appliquent bien qu'aux obligations de remise aux autorités. L'obligation de tenue et de mise à jour des registres d'informations s'applique à tous les niveaux de l'entité (niveau individuel, sous-consolidé et consolidé) (cf. article 28(3) du règlement DORA).

Q-B7 : comment puis-je savoir si mon entité doit remettre un RoI à l'ACPR et les informations qui doivent y figurer ?

En complément des informations fournies dans les questions précédentes, vous pouvez utiliser les tableaux récapitulatifs disponibles **ici**. Le tableau n°1 permet de déterminer si une entité est soumise à l'obligation de remettre un registre d'informations à l'ACPR et sur quel périmètre de consolidation. Dans le cas d'une remise sur base consolidée, le tableau n°2 précise pour quelles entités des informations doivent être incluses dans le registre.

Attention : ces tableaux permettent d'identifier un nombre important de situations sans pour autant viser l'exhaustivité. En cas de doute, les entités peuvent toujours solliciter leurs services de contrôle.

En complément, les entités remettantes pourront voir leur nouvelle obligation de reporting *via* la mise à jour de leur carte de visite fonctionnelles.

Q-B8 : Quelles sont les modalités d'information de l'ACPR de tout projet d'accord contractuel portant sur l'utilisation de services TIC qui soutiennent des fonctions critiques ou importantes ainsi que lorsqu'une fonction est devenue critique ou importante conformément au dernier alinéa de l'article 28(3) DORA ? (hors entités relevant de la supervision directe de la BCE)

Afin de se conformer à l'obligation pour les entités financières d'informer en temps utile l'autorité compétente de tout projet d'accord contractuel portant sur l'utilisation de services TIC qui soutiennent des fonctions critiques ou importantes ainsi que lorsqu'une fonction est devenue critique ou importante, et dans l'attente de l'adoption par l'ACPR d'une instruction spécifique, il est pour le moment demandé aux entités financières de procéder à cette information en reprenant les informations pertinentes du formulaire de notification détaillé en annexe de l'instruction n°2019-I-06 telle que modifiée par l'instruction n°2020-I-09. Ce formulaire devra être remis au service de contrôle habituel au plus tard 6 semaines avant l'entrée en vigueur de la sous-traitance à l'adresse suivante : https://acpr-portail.banque-france.fr, en saisissant le type de demande « Notifications prévues par la règlementation » pour les entités relevant du secteur de la banque et « Externalisation » pour les entités relevant du secteur de l'assurance.

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

Q-C1 : Quelles sont les dispositions contractuelles qui doivent figurer dans un contrat entre une entité financière et un prestataire tiers de services TIC ?

L'article 30(2) de DORA fournit une liste minimale d'éléments qui doivent figurer dans tous les accords contractuels relatifs à l'utilisation de services TIC.

L'article 30(3) de DORA prévoit des éléments additionnels qui ne sont obligatoires que lorsque les services TIC concernés soutiennent des fonctions critiques ou importantes.

Afin d'identifier les obligations applicables à chaque contrat, il est essentiel que l'entité financière, avant de négocier un contrat - ou d'en demander la révision -, détermine si l'accord contractuel couvre l'utilisation de services TIC qui soutiennent une fonction critique ou importante. Les fonctions critiques ou importantes sont définies au point 22 de l'article 3 de DORA de la manière suivante : « *une fonction dont la perturbation est susceptible de nuire sérieusement à la performance financière d'une entité financière, ou à la solidité ou à la continuité de ses services et activités, ou une interruption, une anomalie ou une défaillance de l'exécution de cette fonction est susceptible de nuire sérieusement à la capacité d'une entité financière de respecter en permanence les conditions et obligations de son agrément, ou ses autres obligations découlant des dispositions applicables du droit relatif aux services financiers.* ».

Par ailleurs, ce travail d'identification est un prérequis afin de gérer les risques liés aux prestataires tiers de services TIC dans le respect du principe de proportionnalité comme cela est prévu par l'article 28(1) de DORA.

D. Tests d'intrusion avancés (TLPT)

Ces éléments de réponses préparés par la TCT-FR (Banque de France, ACPR et AMF) n'engagent nullement la Banque centrale européenne en sa qualité d'autorité TLPT pour les établissements de crédit classés comme significatifs.

La TCT-FR reste à la disposition des entités financières et des prestataires de TI/RT pour répondre à leurs questions complémentaires sur les TLPT DORA et sur TIBER-FR. Les questions peuvent être adressées à tiber-fr@banque-france.fr.

Q-D1 : À quelle date la liste des entités soumises aux TLPT sera-t-elle communiquée ?

La liste des entités soumises aux TLPT DORA est confidentielle et ne sera pas rendue publique. La/les autorité(s) TLPT compétente(s) (en France, la Banque de France, l'ACPR et l'AMF, ainsi que la Banque centrale européenne pour les établissements de crédit classés comme significatifs, dits « *Significant Institutions* ») entreront en contact avec les entités concernées de manière bilatérale par l'envoi d'un courrier d'identification. Ces courriers seront émis après l'entrée en application définitive du règlement délégué sur les TLPT, adopté le 13 février par la Commission européenne et dorénavant soumis à un droit de regard (« *scrutiny period* ») du Parlement européen d'une durée de 3 mois (voir état d'avancement de l'adoption du règlement délégué).

Q-D2 : Les entités non concernées seront-elles officiellement informées ?

Tout d'abord, il convient de préciser que l'identification des entités à tester, par la/les autorité(s) TLPT compétente(s), se fait dans le cadre d'un plan/cycle triennal (sauf exceptions, la fréquence et le planning des tests étant fixés par la/les autorité(s) TLPT compétente(s)). Le fait qu'une entité en principe éligible au regard des critères quantitatifs du RTS DORA TLPT ne soit pas désignée sur le 1er cycle triennal ne signifie pas qu'elle ne le sera pas sur les cycles suivants.

Les entités en principe éligibles au regard des critères quantitatifs de l'article 2(2) règlement délégué sur les TLPT, qui ne se verraient pas désignées par leur autorité TLPT pour être soumises à l'exigence de TLPT DORA, seront averties par courrier de cette non-désignation.

Les autres entités non désignées pour faire l'objet d'un TLPT sur le 1er cycle triennal n'en seront pas notifiées par la/les autorité(s) TLPT compétente(s).

Q-D3 : Pour les groupes d'entreprises, les notifications et échanges avec la TCT s'effectueront-ils au niveau du groupe ou des entités individuellement ?

La désignation des entités à tester se fait au niveau entité et non groupe. Chaque entité devra donc former une équipe dédiée (une *Control Team*) avec laquelle la TCT-FR interagira. Dans certains cas, lorsqu'un *Joint* TLPT se justifie (c'est-à-dire regrouper plusieurs entités désignées d'un même groupe pour réaliser un seul test) alors une seule *Control Team* sera formée pour le test.

Q-D4 : En cas de sous-traitance partielle ou totale du système d'information à une filiale, qui sera soumise à l'exigence de TLPT DORA ?

Si plusieurs entités d'un même groupe sont désignées et qu'elles partagent un même prestataire intra-groupe (une filiale dédiée aux services informatiques pour tout ou partie du groupe)/une même infrastructures technique/des applicatifs communs, alors l'autorité TLPT compétente pourra décider d'organiser un *Joint* TLPT regroupant toutes ces entités.

Q-D5 : Existe-t-il des formations ou certifications spécifiques sur TIBER-EU ?

Le règlement DORA stipule : "*Financial entities shall only use testers for the carrying out of TLPT, that: are of the highest suitability and reputability*" et "*are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks*" (article 27.1c). En parallèle, les recommandations TIBER-EU mentionnent : "*RT testers provide copies of certifications that are appropriate according to recognised market standards*". Par conséquent, ni DORA ni TIBER-EU ne spécifient les certifications attendues pour les testeurs. Toutefois, nous vous rappelons que l'ANSSI requiert des prestataires qu'ils soient qualifiés PASSI LPM pour intervenir sur les systèmes d'importance vitale (SIIV) des opérateurs d'importance vitale (OIV) et conseille, dans les autres cas, le recours à des prestataires qualifiés PASSI RGS.

Q-D6 : Quel budget est-il recommandé d'allouer à ces tests ?

Les prestations de renseignement sur la menace (TI) et de *red teaming* (RT) font l'objet d'une négociation bilatérale entre le(s) prestataire(s) et l'entité testée. Nous vous recommandons de prendre connaissance des **bonnes pratiques TIBER-EU** relatives à l'acquisition de ces prestations.

Q-D7 : Une campagne annuelle de tests d'intrusion internes et externes peut-elle être considérée comme une équivalence aux TLPT ?

Non, en aucun cas : un TLPT est un exercice bien spécifique qui doit se faire avec l'accompagnement de l'autorité TLPT compétente.

Q-D8 : Est-il opportun de réaliser des tests à blanc avant l'évaluation officielle ?

Nous laissons cela à l'appréciation des entités. Néanmoins, pour les entités désignées, cela pourrait éveiller les soupçons de la *Blue Team* et accroître le risque de détection durant le test officiel. Pour les entités non désignées, un tel exercice, qu'elles peuvent intégrer à leur programme de tests de résilience (voir article 24 du règlement DORA), reste une opportunité d'améliorer leur cybersécurité mais cela ne pourra faire office de TLPT officiel car non accompagné par les autorités.

Q-D9 : En tant que RSSI d'une filiale d'un groupe, dois-je informer le RSSI du groupe en cas de notification ou serais-je le point de contact principal ?

Les TLPT étant confidentiels, vous ne pouvez échanger qu'avec les membres de la *Control Team*. Si le RSSI du groupe n'a pas été intégré à cette équipe dédiée alors il n'a pas à en connaître.

Q-D10 : Ni la profondeur, ni le nombre d'itérations et les conditions pour un statut de réussite ou d'échec ne sont définis. Seule existe une fourchette de durée. L'impact repose par conséquent sur un risque « d'acharnement » pour pénétrer dans le système d'information et un allongement non maitrisé de la durée du test, voire de mouvements latéraux non acceptés.

Toutes ces affirmations sont inexactes et nécessitent d'être clarifiées. Tout d'abord, la notion d'échec ou de réussite d'un TLPT n'existe pas. La/les autorité(s) TLPT compétente(s) se basent strictement sur le respect des exigences du règlement DORA par l'entité testée (respect de la méthodologie) afin de délivrer l'attestation et non sur les conclusions du test. Il ne s'agit pas d'attester du niveau de résilience cyber de l'entité (les vulnérabilités éventuellement décelées et les actions requises dans le plan de remédiation font l'objet d'un suivi à posteriori).

Autre incompréhension s'agissant de la « fourchette de durée » : chaque TLPT fait l'objet en phase de Préparation de l'élaboration d'un planning prévisionnel par la *Control Team* (CT) et validé par le *Test Manager* (TM) qui est nommé par la/les autorité(s) TLPT compétente(s). Comme pour tout autre projet il y a une maîtrise du temps. Ce planning prend en compte les exigences du RTS DORA TLPT sur les durées maximales (ou parfois minimales) de chaque étape/livrable du processus de test. Concernant la phase active de test, sa durée est également définie en amont (minimum 12 semaines et inclut la réalisation du plan de test). Pas de risque d'un allongement non maîtrisé du test ou de mouvements latéraux non acceptés puisque les testeurs ne devront appliquer que ce plan de test préalablement validé par la CT et la TM. Lors de l'exécution des scénarios de test, les testeurs vont tenter d'atteindre les « trophées » (objectifs) dans les délais impartis/validés. S'ils n'y parviennent pas il y aura des discussions/priorisations avec la CT et le TM qui décideront s'il convient ou non de persévérer. Le cas échéant, les tests sont arrêtés sans atteinte des trophées mais cela ne sera pas considéré comme un échec car il y aura malgré tout des enseignements à en tirer. A contrario, si les testeurs venaient à terminer le plan de test avant la durée minimale de 12 semaines, des actions de *purple teaming* pourraient être autorisées jusqu'à l'atteinte des 12 semaines réglementaires.

Mise à jour le 25 Mars 2025