TNP
HARNESS THE UNPREDICTABLE

HUB
INSTITUTE

LES 12 TRAVAUX DE DORA : GUIDE PRATIQUE POUR UNE MISE EN CONFORMITÉ OPÉRATIONNELLE ET RÉALISTE

SOMMAIRE

LES 12 TRAVAUX DE DORA

00. PRÉAMBULE : POURQUOI DORA ?

UNE RÉPONSE TECHNIQUE ET JURIDIQUE À LA CRISE DE 2008

Digital Operational Resilience ou résilience opérationnelle numérique : c'est la raison d'être du règlement DORA[1]. Ce règlement s'inscrit dans la volonté de l'Union Européenne de rendre le système financier européen "plus résilient, notamment d'un point de vue opérationnel, afin de garantir sa sûreté technologique et son bon fonctionnement, ainsi que son rétablissement rapide après des atteintes à la sécurité des TIC[2] et des incidents liés aux TIC"[3]. En d'autres termes, les entités régulées par le règlement DORA doivent s'organiser pour être en mesure de poursuivre leurs activités si elles subissent des cyberattaques ou des interruptions de fonctionnement de leurs systèmes d'information.

Les ravages des virus NotPetya et WannaCry en 2017 ont démontré la "vulnérabilité systémique" du secteur financier en matérialisant les craintes de l'UE envers les "cyber-incidents [qui] pourraient rapidement se propager de l'une des quelques 22.000 entités financières de l'UE à l'ensemble du système financier"[4]. C'est contre ces menaces mondiales que l'Union Européenne souhaite protéger son système financier.

La menace indirecte pesant sur les entités financières se comprend par le phénomène des attaques de la supply-chain IT (voir chapitre 10), longuement traité dans DORA par un sévère alourdissement de l'encadrement des relations techniques et contractuelles des entités financières avec leurs "15.000"[5] prestataires TIC. A ce titre, les "prestataires TIC" sont soumis à DORA comme les entités financières auxquelles ils fournissent leurs services.

LE CHANGEMENT DE STRATÉGIE CYBERSÉCURITÉ DE L'UNION EUROPÉENNE

Le nombre dérisoire de condamnations judiciaires de "hackers" démontre à lui seul que la réponse judiciaire des États de l'UE est manifestement inopérante pour endiguer

1 Règlement UE "Digital Operational Resilience Act" n°2022/2554 du 14 décembre 2022. Nous utiliserons l'acronyme anglais DORA dont l'usage est largement répandu dans le monde professionnel

2 TIC pour "Technologie de l'Information et de la Communication"

3 DORA Considérant n°6

4 DORA Considérant n°3

5 chiffre publié par les AES (EBA + EIOPA + ESMA) le 27 septembre 2023

le phénomène des cyberattaques. Partant de ce constat, l'UE a opéré un changement de paradigme complet dans sa politique de régulation. Puisqu'il n'est pas possible de réprimer de façon effective les cyber-attaquants, la pression est mise sur les opérateurs économiques auxquels sont imposées des règles de cybersécurité. Et si une entité financière n'est pas à l'état de l'art en termes de sécurité de ses réseaux et de ses systèmes d'information, elle pourra faire l'objet de sanctions administratives et de mesures correctives.

L'UE l'a bien compris : imposer des règles de résilience opérationnelle fiables à 100 % relève de l'utopie. Le règlement DORA comme la Directive NISv2[6] reposent donc chacun sur le principe de gestion continue et proactive du risque, par cycles le plus souvent annuels en lieu et place de la traditionnelle sécurité informatique défensive et passive. C'est un premier changement de paradigme opéré par DORA.

LE CONCEPT DE "RÉSILIENCE OPÉRATIONNELLE"

L'UE franchit une seconde étape avec le concept de "résilience opérationnelle" : en cas de "dysfonctionnement des TIC"[7] ("erreur humaine"[8], panne ou attaque cyber), priorité doit être donnée "à la continuité des fonctions critiques ou importantes" de l'entité financière et "à la reprise des activités"[9].

Plutôt que de décrire de manière traditionnelle (organisation / fonctionnel / technique et juridique) l'ensemble du dispositif de résilience opérationnelle imposé par DORA, nous proposons aux entités financières et à leurs prestataires TIC un mode d'emploi pragmatique de mise en conformité. C'est l'objet de ce Livre Blanc, voulu comme un guide de déploiement opérationnel des obligations légales qui entreront en application le 17 janvier 2025.

6 Directive UE "sécurité des réseaux et des système d'information" (Network and Information system security ou "NIS" pour l'acronyme anglais) dite "NISv2" n°2022/2555 du 14 décembre 2022. La Directive "NISv2" constitue la règlementation générale qui impose des règles de cyber sécurité aux réseaux et systèmes d'information des "entités régulées", dont DORA constitue une exception sectorielle pour les "entités financières" dont la liste est détaillée à l'article 2.1 de DORA.

7 DORA article 6.8.b

8 DORA article 9.3.d

9 DORA article 11.2

Conservant à l'esprit que DORA est un cadre règlementaire sectoriel spécifique pour le secteur financier, nous nous référerons ponctuellement à la Directive NISv2 lorsque ses dispositions permettent d'éclairer le sens de celles prévues dans le règlement DORA.

UNE RÉGLEMENTATION PRUDENTIELLE

DORA est la pièce centrale de la réglementation prudentielle dont l'objectif est d'uniformiser la prise en compte et la gestion du risque cyber dans l'ensemble des pays de l'UE et pour l'ensemble des acteurs économiques du "secteur financier". En plus de ce règlement, l'UE a publié le même jour la Directive UE n°2022/2556 qui amende huit précédentes directives[10] relatives à la solvabilité des institutions financières (Solvabilité II, CDR4 etc.) "en ce qui concerne la résilience opérationnelle numérique du secteur financier".

10 Directive (UE) 2022/2556 du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE)2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier

Retour au sommaire

01. "DOMPTER LE TAUREAU DE MINOS" : PRIORISEZ VOS ACTIONS POUR GÉRER VOTRE RISQUE DE NON-CONFORMITÉ

À l'instar d'Hercule domptant le taureau du roi Minos, les institutions financières doivent traquer et maîtriser leurs risques de non-conformité. Cette section détaillera comment hiérarchiser les actions et les ressources pour cibler efficacement les zones les plus critiques, en évitant que le risque ne s'emballe et ne cause des ravages incontrôlables dans le système financier global.

LE PREMIER ÉCUEIL : ”MON EXISTANT EST SUFFISANT POUR ÊTRE CONFORME”

Depuis la Directive de 2014[11] et les règles de l’EBA sur l’externalisation de 2019[12], les professionnel(le)s des entités financières ont déjà mis en place de nombreux dispositifs organisationnels, techniques et juridiques en matière de résilience[13]. Les "organes de direction" des entités financières sont de ce fait largement convaincus que DORA n’est que la ré-écriture compilée des règlementations qui les impactent depuis plus de 10 ans. Tel n’est pourtant pas le cas.

A l’inverse, il serait vain, voire contre-productif, pour les entités financières de vouloir faire table rase du passé pour démarrer un process raisonnable de mise en conformité DORA.

UN CALENDRIER LÉGAL TENDU...

DORA impose aux entités financières de gérer de manière "efficace et prudente"[14] le risque de dysfonctionnement de leurs infrastructures et outils numériques.

DORA s’appliquera de manière effective le 17 janvier 2025[15]. Cette date couperet est à tempérer du fait du calendrier de production par les Autorités Européennes de Surveillance (AES)[16] des normes techniques additionnelles prévues dans DORA pour le 17 janvier 2024[17] et le 17 juillet 2024[18].

Mais vu l’ampleur et la complexité du dispositif légal à déployer, il est illusoire d’espérer que la totalité des entités financières et de leurs prestataires TIC soient prêts dans les délais prévus par DORA. Si l’on prend l’exemple du régime spécifique applicable aux prestataires critiques pour

11 Directive 2014/59/UE du 15 mai 2014 établissant un cadre pour le redressement et la résolution des établissements de crédit et des entreprises d’investissement

12 European Banking Association "Orientations relatives à l’externalisation" 25 février 2019

13 Par exemple en France 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’ACPR

14 DORA article 5.1

15 DORA article 64

16 European Banking Association (EBA) + European Securities and Market Authority (ESMA) + European Insurance and Occupational Pensions Authority (EIOPA)

17 DORA articles 15, 16.3, 18.3, 28.9 et 28.10

18 DORA articles 11.11, 20, 26.11, 30.5, 31, 32.8, 41 et 43

l'UE[19], il n'est objectivement pas raisonnable d'attendre de ces derniers qu'ils puissent matériellement mettre en place les mesures techniques et de supervision en moins de six mois après le 17 juillet 2024.

... AVEC UN RISQUE IMPORTANT DE SANCTION

Le calendrier d'application de DORA conduit nécessairement les entités financières à envisager d'abord leur risque de non-conformité dans les délais légaux.

L'article 50 de DORA prévoit la possibilité pour les AES "d'adopter tout type de mesure, y compris de nature pécuniaire, propre à garantir que les entités financières continueront à respecter leurs obligations légales". Cependant, à la différence du RGPD[20] ou de NISv2, aucun plancher ni aucun plafond de sanction pécuniaire ne sont prévus.

Ce qui pourrait paraître comme une mesure de clémence est à mettre en balance avec le fait que chacun des 20 types d'entités financières régulées[21] est soumis à un agrément préalable d'exercice, délivré en France par la Banque de France, l'Autorité des Marchés Financiers (AMF) ou l'Autorité de Contrôle Prudentiel et de Résolution (ACPR). Et - c'est précisé dans DORA - la législation cybersécurité fait maintenant partie intégrante du bloc légal soumis au contrôle des AES. Ne pas être conforme aux obligations imposées par DORA fait donc courir aux entités régulées le risque de suspension (avec sursis ?) ou de retrait (temporaire ?) de leur agrément d'exercice. Le risque de non-conformité est donc majeur, notamment en termes d'impact financier et d'image.

PRIORISEZ VOS ACTIONS DE MISE EN CONFORMITÉ

Afin de réduire au maximum le risque de non-conformité, une entité financière devrait commencer par identifier clairement ses fonctions métiers et ses actifs, en distinguant ceux considérés comme critiques ou importants des autres. Cela permettrait de prioriser les actions de mise en conformité.

19 Le régime encadrant les "prestataires tiers critiques de services TIC" figure aux articles 31 et suivants de DORA

20 Règlement UE "RGPD" n°2016/679 du 27 avril 2016

21 Voir la liste des types d'entités financières à l'article 2 DORA et les Directives et Règlements UE encadrant leurs activités dans les définitions de l'article 3 DORA

> **“**Identifier clairement ses fonctions métier et ses actifs, en distinguant ceux considérés comme critiques ou importants des autres**”**

Les "fonctions critiques ou importantes" sont définies dans DORA comme celles dont "la perturbation [est] susceptible de nuire sérieusement à la performance financière, à la solidité ou à la continuité [des] services [d'une entité financière]"[22]. Cette définition est bien plus large que celle des "fonctions critiques"[23] imposée par la Directive de 2014.

Cette priorité d'action passe par l'identification des "fonctions critiques ou importantes" concernées en tenant compte de deux particularités :

(i) les "actifs de TIC" (les matériels et les logiciels) dont l'obsolescence pose aujourd'hui un véritable problème : les "systèmes de TIC hérités". La dette technique ("legacy" en anglais), encore très lourde dans les banques et les assurances, désigne tout "système de TIC qui a atteint la fin de son cycle de vie..., qui ne se prête pas à des mises à jour ou des corrections, ... ou qui n'est plus pris en charge... par un prestataire [TIC] mais qui est toujours

22 *DORA article 3.22*

23 *article 2.1.35 Directive n°2014/59 : "les activités, services ou opérations dont l'interruption est susceptible, dans un ou plusieurs États membres, d'entraîner des perturbations des services indispensables à l'économie réelle ou de perturber la stabilité financière en raison de la taille ou de la part de marché de l'établissement ou du groupe, de son interdépendance interne et externe, de sa complexité ou des activités transfrontières qu'il exerce..."*

utilisé et soutient les fonctions de l'entité financière"[24];

(ii) les fonctions critiques ou importantes qui seraient externalisées au profit de prestataires TIC.

Cette priorisation est une manière concrète de mettre en œuvre le "principe de proportionnalité"[25] rappelé à plusieurs reprises dans DORA.

DÉSIGNEZ UN RESPONSABLE DE LA CONDUITE DU CHANGEMENT DORA

Dès le lancement du projet de mise en conformité, il est nécessaire qu'un membre de la direction de l'entité financière prenne la charge et centralise les actions de mise en conformité DORA. Le DORA Chief Compliance Officer sera le responsable global de la "stratégie de résilience opérationnelle numérique"[26] à élaborer puis à implémenter.

24 DORA article 3.3

25 DORA articles 4 et 9.3

26 DORA article 5.2.d

DOCUMENTEZ VOS ACTIONS VERS L’ÉTAT DE L’ART DORA

Dès le début du projet de mise en conformité, l’entité financière doit prendre soin de documenter ses actions, pour être en mesure de prouver, de manière documentée (écrite et justifiée), son respect des règles légales et de l’état de l’art technique. Car lorsque DORA impose à une entité de "garantir la sécurité des réseaux et systèmes d’information... qui sous-tendent la fourniture continue de leurs services... et leur qualité"[27], il s’agit indéniablement pour les juristes, non d’une obligation de résultat, mais bien d’une obligation de moyens renforcée, dont la charge repose sur l’entité.

27 DORA article 3.1

Retour au sommaire

02. "TUER L'HYDRE DE LERNE" : LISTEZ VOS ÉCARTS ENTRE L'EXISTANT ET LES DISPOSITIFS CIBLES

La légendaire hydre de Lerne, monstre aux multiples têtes, symbolise les différentes non-conformités qui peuvent surgir simultanément. L'identification précise de ces écarts est essentielle, chaque tête de l'hydre représentant un écart qui, s'il n'est pas correctement considéré, peut se multiplier et aggraver le risque global.

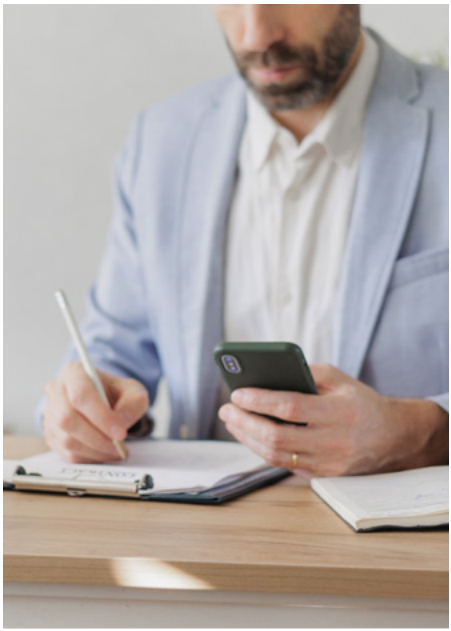
PARTEZ DU SOCLE DE SÉCURITÉ : LES 42 MESURES D’HYGIÈNE NUMÉRIQUE INDISPENSABLES

Le "guide d’hygiène informatique"[28] de l’ANSSI constitue une base peu contestable pour démarrer un état des lieux des mesures de cybersécurité à déployer. Ce guide constitue le "socle de sécurité" de l’atelier n°1 de la méthode d’analyse de risque EBIOS-RM[29] utilisée en France pour la cybersécurité des Opérateurs d’Importance Vitale[30] auxquels s’imposent des contraintes largement similaires à celles aujourd’hui prévues par DORA.

RETENEZ LA VISION OPÉRATIONNELLE DU DIFFÉRENTIEL : DE L’ENTITÉ AU GROUPE

Lors de la réalisation de l’état des lieux (le "gap analysis"), les entités financières devraient distinguer l’écart entre l’existant et le "à faire" (i) pour chacun des métiers de l’entité et (ii) au niveau de chaque entité régulée, parfois au niveau "sous-consolidé" et certainement au niveau "consolidé"[31].

L’identification des écarts permettra à chaque entité financière de planifier concrètement son projet de mise en conformité, de manière documentée comme le veut DORA, via une feuille de route arrêtée par le responsable de la conformité DORA et validée par son "organe de direction".

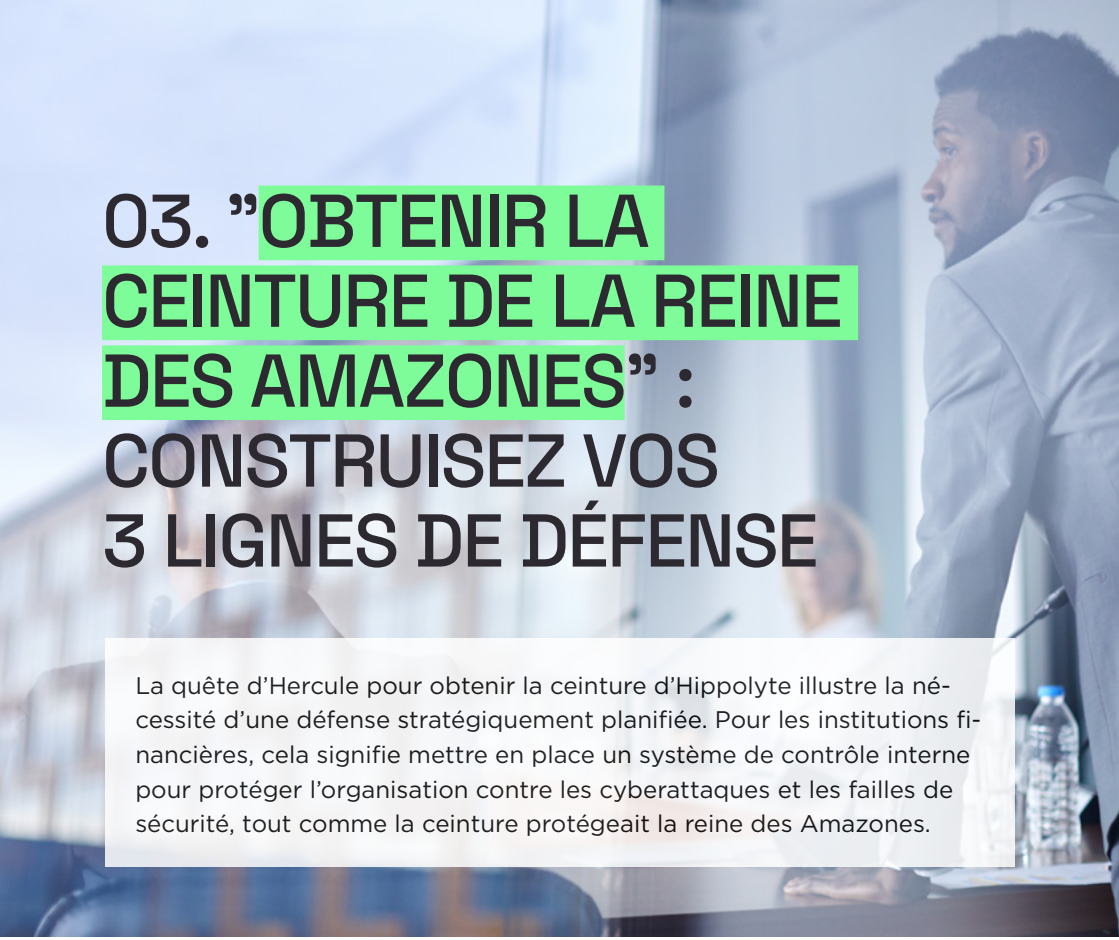


28 guide d’hygiène informatique v2.0 septembre 2017

29 ANSSI-PA-048 méthode EBIOS Risk Manager v1.1 décembre 2018

30 Loi de Programmation Militaire n°2013-1168 du 18 décembre 2013

31 DORA article 6.9 par exemple



03. "OBTENIR LA CEINTURE DE LA REINE DES AMAZONES" : CONSTRUISEZ VOS 3 LIGNES DE DÉFENSE

La quête d'Hercule pour obtenir la ceinture d'Hippolyte illustre la nécessité d'une défense stratégiquement planifiée. Pour les institutions financières, cela signifie mettre en place un système de contrôle interne pour protéger l'organisation contre les cyberattaques et les failles de sécurité, tout comme la ceinture protégeait la reine des Amazones.

ORGANISEZ LA GESTION DE VOS RISQUES TIC EN TROIS LIGNES DE DÉFENSE

L'article 6 de DORA est tout entier consacré à l'organisation du contrôle de la gestion des risques cyber "afin de garantir que tous les actifs informationnels et actifs de TIC sont correctement protégés"[32]. Les 4 objectifs de cette protection sont regroupés dans l'acronyme D.A.I.C. pour Disponibilité, Authenticité, Intégrité et Confidentialité[33].

A ce titre, DORA "recommande" aux entités financières d'organiser leur cadre de gestion du risque TIC selon

32 DORA article 3.2

33 DORA article 5.2.b, article 9.2, article 12.2, etc.

le modèle des trois lignes de défense, en vue d’assurer l’application effective des politiques et des procédures imposées par DORA.

La première ligne de défense doit instaurer un cadre formel et "documenté" de la gestion des risques par "des stratégies, des politiques, des procédures, des protocoles et des outils de TIC adéquats" qui sont réexaminés "au moins une fois par an". Cet examen annuel fera l’objet de contrôle par les autorités compétentes (qui pourront être, selon le secteur d’activité, la Banque de France, l’Autorité des Marchés Financiers ou l’Autorité de Contrôle Prudentiel et de Résolution...).

> **“**Chaque entité financière doit organiser son cadre de gestion du risque TIC selon le modèle des trois lignes de défense**”**

STRUCTUREZ VOS CONTRÔLES INTERNES

La deuxième ligne de défense doit permettre de s’assurer de la bonne exécution du travail de la première ligne. DORA précise que cette fonction de contrôle interne, pour être effective, doit être indépendante "afin d’éviter les conflits d’intérêt".

PRÉVOYEZ VOS AUDITS INTERNES ET LE SUIVI DE LEURS CONCLUSIONS

La troisième ligne de défense nécessite l’organisation d’audits internes ou externalisés, dont les conclusions doivent faire l’objet d’un "processus de suivi formel" qui doit prévoir "la vérification et la correction en temps utile des constatations d’importance critique de l’audit". A titre d’exemple, les "membres de l’encadrement supérieur" seront tenus, au moins une fois par an, de rendre compte à leur direction des "enseignements tirés des tests et des incidents" et de formuler des "recommandations" permettant d’améliorer la résilience opérationnelle de leur entité[34].

34 DORA article 13.5

04. "CUEILLIR LES POMMES D'OR DU JARDIN DES HESPÉRIDES" : SENSIBILISEZ VOTRE DIRECTION ET VOS ÉQUIPES AUX RISQUES CYBER

Tel Hercule cherchant les pommes d'or, les membres de la direction doivent suivre des formations afin d'être sensibilisés aux bonnes pratiques et aux risques cyber. Cela doit permettre à la direction de prendre des décisions éclairées en matière de risques et, in fine, d'étendre la culture cybersécurité à l'ensemble de l'entreprise et de protéger ses actifs informationnels les plus précieux.

FORMEZ VOS DIRECTIONS MÉTIERS ET VOS ÉQUIPES

A quoi sert de déployer des process et des outils logiciels sophistiqués si les collaborateurs de l’entité financière ne savent pas s’en servir ? Et si le risque cyber n’est pas véritablement compris, comment espérer que la direction d’une entité financière débloque les budgets nécessaires au projet de mise en conformité DORA ? C’est une petite révolution qu’instaure DORA en imposant des "programmes de sensibilisation à la sécurité des TIC et [des] formations à la résilience opérationnelle numérique"[35] afin de développer une véritable culture professionnelle de la cybersécurité. Il appartiendra à la direction des entités financières de prévoir des budgets spécifiques dédiés notamment aux "programmes de formation du personnel sous forme de modules obligatoires"[36], afin de réduire le risque d’attaque lié à l’erreur humaine (phishing, etc.).

SENSIBILISEZ LES ”ORGANES DE DIRECTION”

DORA précise que "les membres de la direction" de l’entité financière sont tout autant concernés par cette obligation nouvelle de sensibilisation, ainsi que les prestataires[37] qui sont tenus de participer aux programmes de sensibilisation mis en œuvre par leurs clients entités financières.

35 DORA article 5.2.al.2.g

36 DORA article 13.6

37 DORA article 30.2.i

Retour au sommaire

05. "CAPTURER LE SANGLIER D'ÉRYMANTHE" : ANALYSEZ VOS RISQUES PUIS CARTOGRAPHIEZ VOS ACTIFS

Dompter le taureau sauvage de Minos nécessitait d'abord de comprendre et de maîtriser sa nature imprévisible. De même, dans le secteur financier, une cartographie précise des risques est la première étape avant de pouvoir analyser et gérer efficacement les risques liés aux TIC.

ANALYSEZ VOS RISQUES AVÉRÉS

La première mission de la direction de l’entité financière est "la détermination du niveau approprié de tolérance au risque lié aux TIC[38]" auquel elle estime raisonnable de devoir résister.

Qui dit niveau de tolérance au risque, dit connaissance des risques, qui passe nécessairement par une identification de la menace, qu’elle soit d’origine naturelle (incendie, inondation) ou technique (panne, cyberattaque). La méthode d’analyse de risque EBIOS-RM de l’ANSSI permet de se livrer à cet exercice, en se basant sur des scenarii d’attaque probables. Sur ce point, DORA assure la continuité des obligations prévues dans les recommandations EBA "externalisation" de 2019.

38 DORA article 5.2.al.2.d

INVENTORIEZ VOS ACTIFS MATÉRIELS ET LOGICIELS

DORA impose une identification des "actifs de TIC" et des "actifs informationnels", ainsi que la cartographie "décrivant l'architecture des TIC".

Les "actifs de TIC"[39] sont les "actifs matériels ou logiciels dans les réseaux et les systèmes d'information utilisés par l'entité financière". Les "actifs informationnels"[40], quant à eux, désignent "l'ensemble d'informations, matérielles ou immatérielles, justifiant d'une protection".

De manière pragmatique, DORA impose l'identification des actifs de manière exhaustive, régulière et pour chaque "fonction métier"[41] de l'entité financière.

DORA opère un second changement de paradigme notable comparé à la Directive NISv2 : ce ne sont pas tant les "réseaux et systèmes d'information" que chaque entité financière doit protéger, mais bien les actifs informationnels, autrement dit les données qui y sont traités. En effet, DORA impose l'obligation de mettre en place une "politique de sécurité de l'information"[42], là où la Directive NISv2 impose la rédaction d'une "politique de sécurité du système d'information"[43].

> **"**DORA impose l'obligation de mettre en place une politique de sécurité de l'information**"**

Évidemment, les actifs de TIC, "y compris ceux situés sur des sites extérieurs" comme les actifs informationnels devront être classés selon leur criticité. Un actif de TIC devrait être considéré comme critique lorsqu'il est utilisé pour accomplir une fonction critique ou importante : les données des relevés de compte bancaire, par exemple, étant manifestement plus critiques pour une entité financière que les informations des badges magnétiques du service de restauration de ses collaborateurs.

39 DORA article 3.7

40 DORA article 3.6

41 DORA article 8.1

42 DORA article 9.4

43 NISv2 article 21.2

PROTÉGEZ VOS ACTIFS INFORMATIONNELS

DORA impose l’obligation de protéger les actifs informationnels "au repos, en cours d’utilisation ou en transit"[44] : il faut ici comprendre l’obligation de chiffrement des données en base active, des sauvegardes et des communications électroniques avec priorité pour les données traitées par les "fonctions critiques ou importantes" (données de production) comme celles susceptibles de les remplacer en cas de sinistre (données des back-up). Cette précision dans DORA est à rapprocher de la définition même de "cybersécurité" qui porte sur les "données stockées, transmises ou faisant l’objet d’un traitement"[45].

C’est une constante centrale dans DORA : la stratégie de gestion des risques cyber, comme la politique de sécurité de l’information, doit être construite "selon une approche fondée sur les risques"[46].

Rappelons que les risques prioritaires sont ceux pesant sur les "fonctions critiques ou importantes" de l’entité (voir chapitre 1.4), ceux provenant de ses "systèmes de TIC hérités" (voir chapitre 11.1) et ceux des services rendus par ses prestataires TIC (voir chapitre 10).

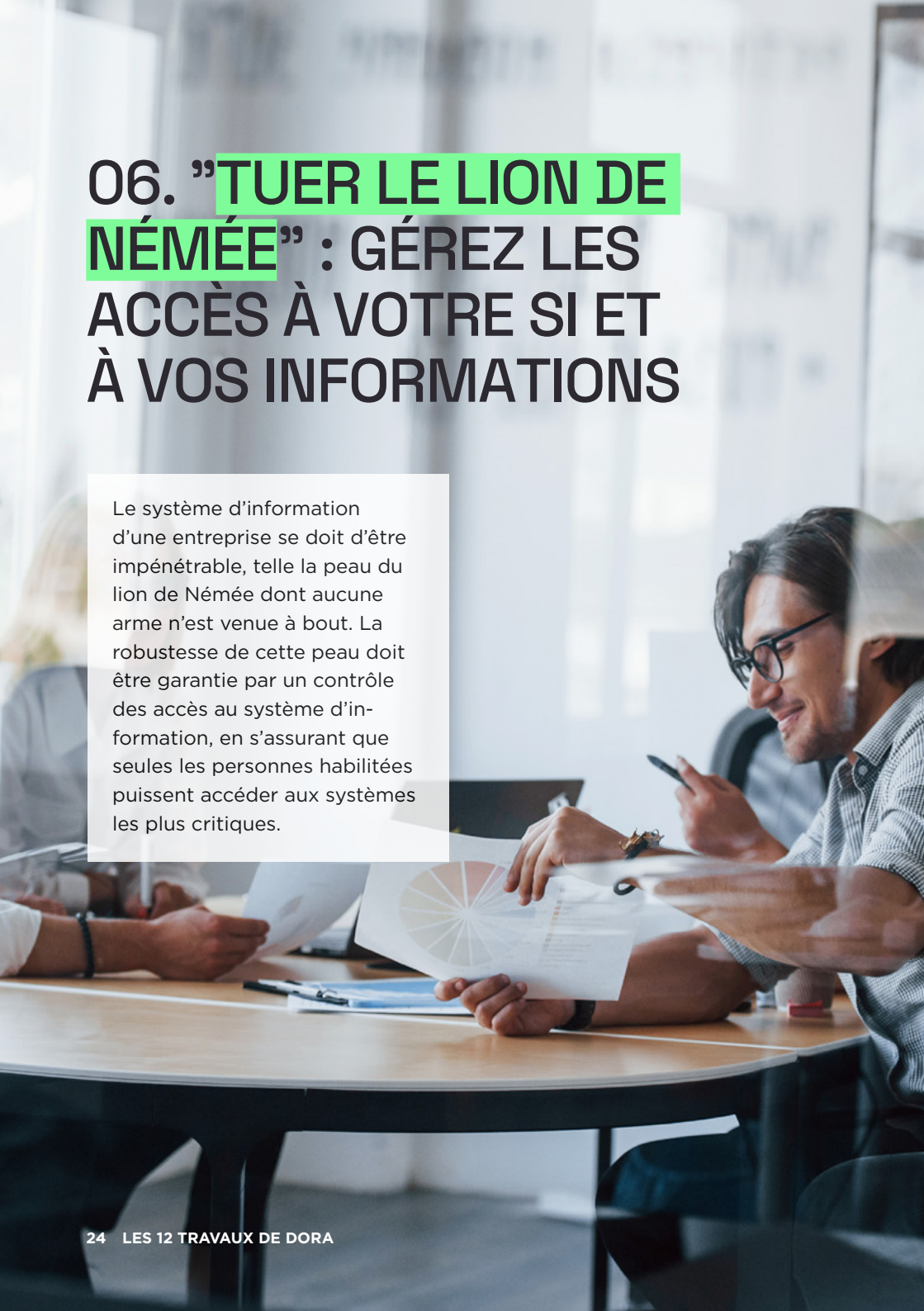
44 DORA article 9.2

45 DORA article 3.4 qui renvoie à la définition de l’article 6.2 de la Directive NISv2

46 DORA article 9.4.b

06. "TUER LE LION DE NÉMÉE" : GÉREZ LES ACCÈS À VOTRE SI ET À VOS INFORMATIONS

Le système d'information d'une entreprise se doit d'être impénétrable, telle la peau du lion de Némée dont aucune arme n'est venue à bout. La robustesse de cette peau doit être garantie par un contrôle des accès au système d'information, en s'assurant que seules les personnes habilitées puissent accéder aux systèmes les plus critiques.



DÉPLOYEZ UNE POLITIQUE D’ACCÈS AU SYSTÈME D’INFORMATION ET AUX ACTIFS INFORMATIONNELS

La base de la cybersécurité repose sur le contrôle de l’accès par les utilisateurs aux seules informations pertinentes au regard de leur activité professionnelle. De manière classique, cette sécurisation repose sur la mise en œuvre, effective et documentée, des principes du "moindre privilège" et du "besoin d’en connaître" rappelés à l’article 9.4.c de DORA.

IMPOSEZ L’AUTHENTIFICATION FORTE ET LA GESTION DE LA CRYPTOGRAPHIE

La cybersécurité doit être renforcée par l’usage d’un mécanisme "d’authentification forte"[47] (mise en œuvre d’un deuxième, voire d’un troisième facteur d’authentification d’accès au système d’information), au moins pour les utilisateurs bénéficiant de privilèges d’administration du système d’information de l’entité financière.
Il est pour le moins curieux de constater que DORA envisage la gestion de la cryptographie dans ce même article 9.4.d alors que la Directive NISv2 et le référentiel ISO 27001 y consacrent chacun un chapitre à part entière. Les RTS[48] ne manqueront pas de détailler les impératifs techniques à déployer à ce titre.

SURVEILLEZ L’ACTIVITÉ DE VOS UTILISATEURS

Curieusement, DORA n’évoque que de manière elliptique à l’article 10.3 l’obligation de mettre en œuvre des outils logiciels de traçabilité des actions des utilisateurs du système d’information via la collecte et la conservation des fichiers log. Ces logs sont pourtant essentiels dans la vérification des droits d’accès, comme pour identifier toute éventuelle intrusion d’un cyberattaquant via l’exploitation d’une vulnérabilité ou après un phishing. Les RSSI des entités financières ne manqueront pas de systématiser le déploiement de ces outils, qui impliquent par nature un traitement de données à caractère personnel au sens du RGPD, dans le strict respect en France de la délibération CNIL "journalisation" de 2021[49].

47 DORA article 9.4.d

48 "Regulatory Technical Standards" (RTS) et "Implemention Technical Standards" (ITS) désignent les documents détaillant les obligations de DORA et dont le rapport officiel par les AES est prévue soit pour le 17 janvier 2024, soit pour le 17 juillet 2024 (par exemple pour le détail de la notification des incidents de sécurité)

49 CNIL délibération n°2021-122 du 14 octobre 2021

07. "VAINCRE LE GÉANT GÉRYON" : ASSUREZ LA CONTINUITÉ DE VOTRE ACTIVITÉ PAR LA REDONDANCE

Le géant Géryon, doté de trois corps, incarnait la capacité à poursuivre son but en cas de dysfonctionnement de l'un d'entre eux. Une entité financière doit, de la même façon, être capable de poursuivre ses activités si l'un de ses systèmes principaux tombe en panne, par exemple, grâce à une politique de sauvegarde testée et éprouvée et un plan de reprise après sinistre documenté.

ASSUREZ LA CONTINUITÉ OPÉRATIONNELLE DES MÉTIERS...

La redondance des capacités de traitement des actifs de TIC est l’essence même du concept de résilience opérationnelle afin d’assurer "la fourniture en continu des services financiers et leur qualité"[50] pour garantir la "disponibilité des données"[51]. Il est donc nécessaire pour les entités financières de se doter "d’une politique de continuité des activités de TIC complète"[52]. Cette politique doit viser en priorité les fonctions critiques ou importantes[53] et passe par la rédaction de "plans de réponse et de rétablissement" (PRA) et d’un "plan de continuité"[54] (PCA) qui doit faire l’objet de tests[55] effectifs.

50 DORA article 3.1

51 DORA article 5.2.al.2.b les "données" étant les actifs informationnels

52 DORA article 11.1

53 DORA article 11.2.a

54 DORA article 11.3

55 DORA article 11.4

… "EN GARANTISSANT… LA REDONDANCE DE TOUTES LES COMPOSANTES CRITIQUES"…

C'est un point extrêmement important de DORA : l'obligation de "garantir de manière appropriée la redondance des composantes critiques"[56] du système d'information de chaque métier de l'entité financière. En pratique, cette obligation impose aux entités financières de disposer d'une infrastructure IT "principale" et d'une infrastructure "redondante", au moins pour ses fonctions critiques ou importantes[57], dont le basculement de l'une vers l'autre doit faire l'objet de tests basés sur des scénarios de cyberattaque.

A noter que cet objectif de redondance n'exclut pas le droit pour les entités financières de "permettre une déconnexion instantanée ou segmentée" de leur "infrastructure de connexion au réseau", pour le cas où il serait nécessaire "d'isoler les actifs informationnels affectés [par une] cyberattaque"[58].

56 DORA article 11.5 : les "composantes critiques" étant sans doute possible "les actifs de TIC supportant des fonctions critiques ou importantes"

57 DORA article 11.6.al.2

58 DORA article 9.4.b alinéas 1 et 2

... GRÂCE À UNE POLITIQUE DE SAUVEGARDE TESTÉE ET À JOUR

Basculer la production informatique depuis un site principal vers un site de secours nécessite des actifs informationnels disponibles. Et cette disponibilité ne peut être assurée que via des sauvegardes viables (donc testées). C’est en ce sens que DORA impose aux entités financières d’adopter des "politiques et procédures de sauvegarde, procédures et méthodes de restauration et de rétablissement"[59].

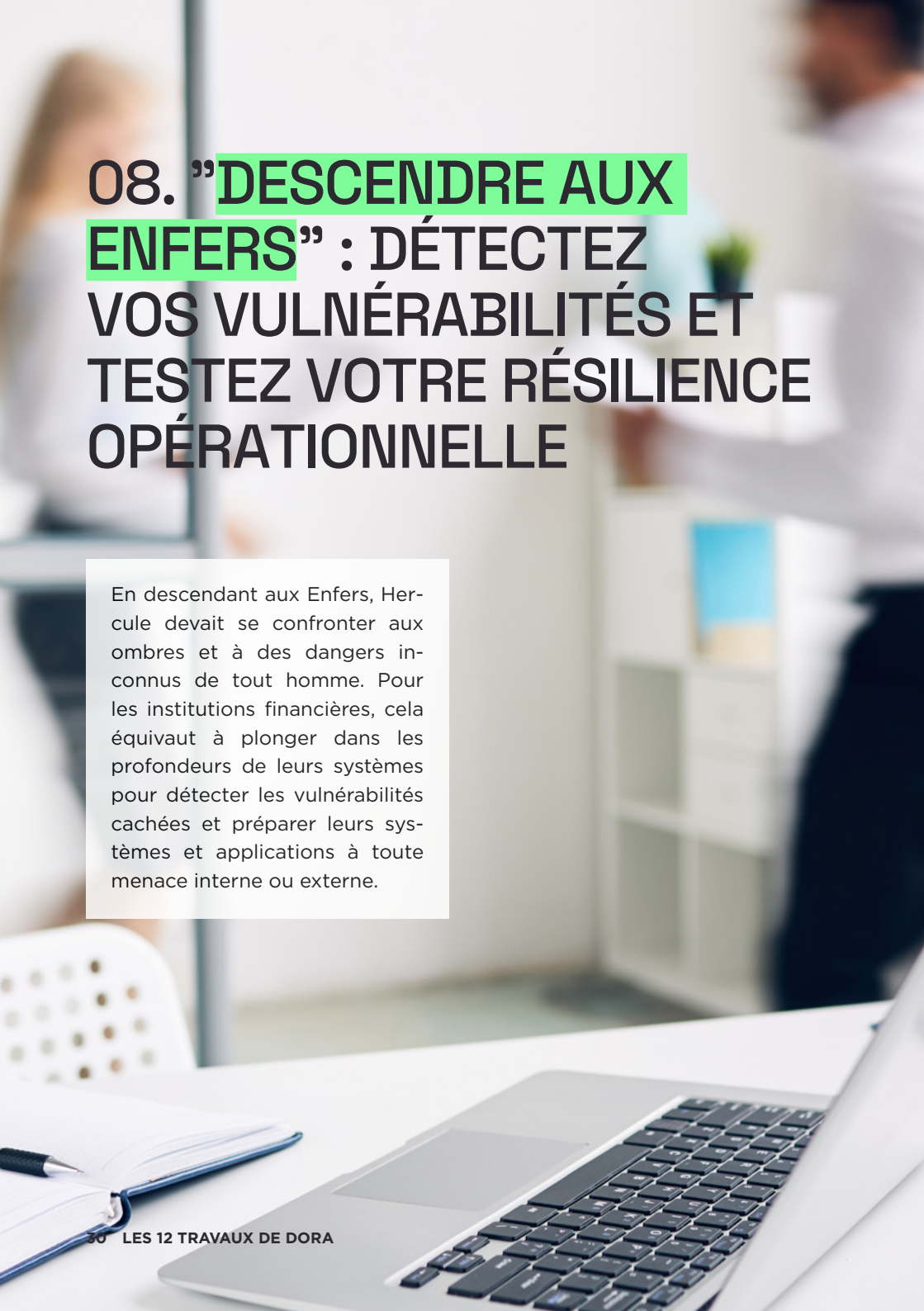
Pour donner un aperçu des détails techniques parfois imposés par DORA, l’article 12.3 al.1er mérite d’être cité : "Lorsqu’elles restaurent des données de sauvegarde à l’aide de leurs propres systèmes, les entités financières utilisent des systèmes de TIC qui sont séparés physiquement et logiquement du système de TIC source".

59 *DORA article 12*

Retour au sommaire

08. "DESCENDRE AUX ENFERS" : DÉTECTEZ VOS VULNÉRABILITÉS ET TESTEZ VOTRE RÉSILIENCE OPÉRATIONNELLE

En descendant aux Enfers, Hercule devait se confronter aux ombres et à des dangers inconnus de tout homme. Pour les institutions financières, cela équivaut à plonger dans les profondeurs de leurs systèmes pour détecter les vulnérabilités cachées et préparer leurs systèmes et applications à toute menace interne ou externe.



DÉTECTEZ VOS VULNÉRABILITÉS ET LES ACTIVITÉS ANORMALES...

Cet aspect essentiel de la résilience opérationnelle est traité de manière éparpillée dans DORA, ce qui en rend la compréhension difficile. DORA impose d’abord aux entités financières l’identification "continue"[60] des sources de risques et l’obligation de détection des "activités anormales"[61].

Déclinée de manière opérationnelle, la surveillance de "l’apparition d’anomalies et d’incident... en particulier les cyber-attaques"[62] passe nécessairement par la mise en place d’outils logiciel (i) de détection des "malwares" via, par exemple, des pare-feu/firewall et (ii) de détection des vulnérabilités[63] connues, notamment via des scans de port[64].

C’est aujourd’hui, indéniablement, l’état de l’art auquel il faudrait ajouter la détection et l’analyse des bibliothèques logicielles sous licence open source "embarquées" avec leurs propres vulnérabilités et dont la correction peut s’avérer extrêmement problématique[65].

60 DORA article 8.2

61 DORA article 10

62 DORA article 10.3

63 DORA article 3.16 : "une faiblesse, une susceptibilité ou un défaut d’un actif, d’un système, d’un processus ou d’un contrôle qui peuvent être exploités" [par un "acteur de la menace"]

64 DORA article 25.1 "des solutions logicielles de balayage"

65 Voir par exemple (parmi tant d’autres) la vulnérabilité "Log4j" en décembre 2021 et le podcast NoLimitSecu du 13 décembre 2021

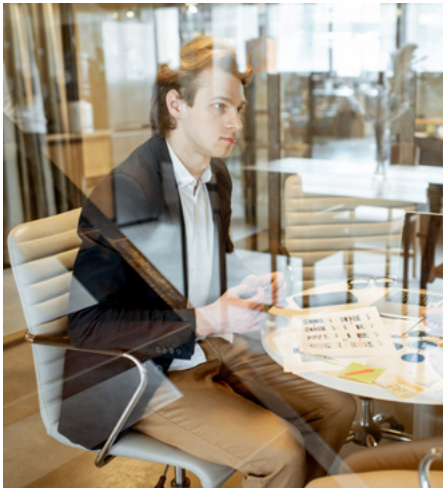
... ET TESTEZ LES SOLUTIONS TECHNIQUES DÉPLOYÉES

Simultanément avec l'obligation de détection a priori des vulnérabilités, DORA impose des tests dynamiques des solutions logicielles déployées[66]. Il est surprenant que les "tests de pénétration" (ou "pentests") soient cités en dernier dans la liste de l'article 25.1 de DORA alors qu'il s'agit d'une technique éprouvée de détection des vulnérabilités logicielles ou réseaux, qui peut être mise en œuvre lors des opérations de "redteam" aussi bien par les équipes internes d'une entité que par celles d'un prestataire spécialisé.

> **"**DORA précise que les fonctions critiques ou importantes doivent être testées au moins une fois par an**"**

Quelle que soit la nature des tests, DORA précise que les fonctions critiques ou importantes doivent être testées "au moins une fois par an"[67], qu'elles soient ou non confiées à un prestataire TIC.

Attention à l'analyse "de sources ouvertes" qui désignent les leaks (données volées puis mises à disposition en plus ou moins libre accès via un darknet) : si techniquement, l'analyse de ces fichiers et de leurs contenus peuvent donner de précieuses indications sur le mode opératoire des pirates, la collecte et le traitement de ces données posent de sérieux problèmes en droit pénal et il convient de n'y recourir qu'avec la plus grande prudence juridique.



66 DORA article 10.1. al.2

67 DORA article 24.6

L’EXCEPTION DES ”TESTS AVANCÉS DE PÉNÉTRATION FONDÉ SUR LA MENACE” (TLPT)

Nous ne ferons qu’évoquer les "tests avancés... de pénétration fondé sur la menace"[68] qui doivent être effectués "sur des systèmes en environnement de production en direct" et doivent porter sur les fonctions critiques ou importantes, internalisées ou confiées à un prestataire TIC. En effet, il revient aux AES de désigner les entités financières qui y seront soumises, en principe "au moins tous les trois ans". A noter enfin que les "testeurs" susceptibles de mener ces tests avancés doivent remplir un certain nombre de conditions détaillées à l’article 27 de DORA.

68 DORA article 26

Retour au sommaire

09. ”CAPTURER LES JUMENTS DE DIOMÈDE” : NOTIFIEZ VOS ”INCIDENTS MAJEURS” ET COMMUNIQUEZ EN TEMPS DE CRISE

Capturer les juments féroces et carnivores de Diomède nécessitait grande prudence et force. De manière analogue, la gestion des "incidents majeurs" dans le secteur financier exige une vigilance constante et la capacité à communiquer efficacement en temps de crise.

COLLECTEZ LES IOC IDENTIFIANT UN ”INCIDENT MAJEUR” ET PARTAGEZ-LES AVEC LES AES

La cybersécurité repose sur le partage d’informations relatives aux attaquants et à leurs modes opératoires[69]. Outre l’obligation de notifier aux AES les incidents majeurs de sécurité, DORA organise aussi tout un process de partage volontaire des informations techniques dont disposeraient les entités financières "pour veiller à ce que les causes originelles [ayant permis la réussite d’une cyberattaque] soient identifiées et documentées et qu’il y soit remédié pour éviter que de tels incidents ne se produisent"[70].

Ce mouvement de "remontée" puis de "redescente" des informations techniques nécessaires à la cyberprotection des entités financières passent d’abord par la connaissance des "incidents liés aux TIC" définis par DORA comme tout "événement... 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"[71].

RETENEZ LA DÉFINITION DES ”INCIDENTS MAJEURS” À NOTIFIER

Il faut insister ici sur la notion "d’incidents majeurs" de cybersécurité : l’obligation de notification aux AES ne concernera que les incidents ayant "une incidence négative élevée sur les réseaux et les systèmes d’information qui soutiennent les fonctions critiques ou importantes de l’entité"[72]. Le régulateur européen a manifestement tiré profit de l’expérience du RGPD qui impose la notification des violations de données à caractère personnel, quelle qu’en soit l’importance.

GÉREZ VOS INCIDENTS ET LEUR NOTIFICATION

Si le nombre d’incidents à remonter obligatoirement aux AES sera limité, le process de notification est, lui, sévèrement alourdi : l’article 17 de DORA impose tout un "processus de gestion des incidents liés aux TIC" et l’article

69 TTPs pour "Technique, Tactique et Procédure"

70 DORA article 17.2

71 DORA article 3.8

72 DORA article 3.10

18 traite longuement de la "classification des incidents". Nous insisterons seulement sur quelques points clé de l'article 19 "déclaration des incidents majeurs".

DORA impose une "notification initiale" des incidents majeurs aux AES (probablement dans les 4 heures après classification et/ou dans les 24 heures après détection d'après le projet de RTS[73] du 8 décembre 2023), puis un "rapport intermédiaire" (probablement dans les 72 heures), puis enfin un "rapport final, lorsque l'analyse des causes originelles [de l'incident] est terminée, que des mesures d'atténuation aient déjà été mises en œuvre ou non"[74] (probablement dans les 30 jours). A noter que ce process est identique à celui mis en place à l'article 23.4 de la Directive NISv2 : "alerte précoce" dans les 24 heures, puis notification dans les 72 heures, puis rapport final dans les 30 jours.

LES NOUVELLES OBLIGATIONS DE COMMUNICATION AUX CLIENTS

La nouveauté de DORA est d'imposer aux entités financières de communiquer "sans retard… dès leur connaissance" à l'égard de leurs clients sur l'existence de l'incident majeur et les "mesures prises pour [en] atténuer les effets préjudiciables". Les entités financières devront également les informer "en cas de cybermenace importante" des "mesures de protection appropriée que ces derniers pourraient envisager de prendre"[75]. En termes juridiques, c'est ici l'apparition d'une nouvelle obligation d'information et de conseil qui va s'imposer aux entités financières, donc une nouvelle source de risque de mise en cause de leur responsabilité en cas de non-respect de cette obligation spécifique.

73 "Regulatory Technical Standard" (RTS) désigne les documents détaillant les obligations de DORA et dont le rapport officiel par les AES est prévue soit pour le 17 janvier 2024, soit pour le 17 juillet 2024 (par exemple pour le détail de la notification des incidents de sécurité)

74 DORA article 19.4

75 DORA article 19.3

ANTICIPEZ VOTRE COMMUNICATION DE CRISE CYBER

Une décennie de communication de crise par des entités victimes de cyberattaque démontre à elle seule que l’improvisation en la matière n’est guère productive. Pour prendre le contrepied de ce constat, DORA impose rationalisation et transparence dans la gestion des crises cyber, en obligeant d’abord les entités financières à disposer d’une "fonction de gestion de crise"[76] en cas d’activation des plans de continuité ou de réponse à incident.

DORA impose en plus une organisation permettant la gestion coordonnée de la communication de crise pour l’entité financière impactée à l’égard de ses salariés, de ses clients et "contreparties", de ses prestataires ainsi que du public et des médias[77]. A ce titre, l’entité doit préparer et tester[78] son "plan de communication en situation de crise" et désigner "au moins une personne" chargée de la stratégie de communication à l’égard "du public et des médias"[79].

L’entité doit ensuite anticiper sa communication à l’égard de ses salariés et de ses partenaires contractuels, clients ou prestataires. DORA impose d’ailleurs de prévoir une communication interne spécifique à l’égard des salariés de l’entité en charge de la réponse et de la remédiation à incident de sécurité.

Enfin, la communication à l’égard des clients "et des contreparties" de l’entité doit porter "au minimum" sur les "incidents majeurs" ainsi que sur les "vulnérabilités majeures"[80], dont la communication / divulgation aux AES ne fait pourtant pas parties des obligations imposées aux entités financières.

76 DORA article 10.7

77 DORA article 17.3.d

78 DORA article 11.6.b

79 DORA article 14.3

80 DORA article 14.1

10. "CAPTURER LA BICHE DE CÉRYNIE" : RÉDIGEZ VOS AVENANTS CONTRACTUELS ET TENEZ VOTRE REGISTRE DES ACCORDS CONTRACTUELS

La biche sacrée de la déesse Artémis était rapide et insaisissable, rappelant la nécessité de l'agilité et de la précision lors de la rédaction des avenants contractuels et de la tenue d'un registre des contrats. Les institutions financières doivent être aussi adroites qu'Hercule en s'assurant que leurs contrats sont conformes au règlement DORA, et en restant alertes vis-à-vis du respect des exigences contractuelles par leurs prestataires.

GÉREZ LE RISQUE CONTRACTUEL AVEC VOS PRESTATAIRES SOUS-TRAITANTS

La terreur officielle de l’UE, ce sont les cyberattaques indirectes, dites "supply-chain attacks"[81], qui commencent par la compromission d’un prestataire pour aboutir à celle d’un ou plusieurs de ses clients, cibles finales effectivement visées.

Pour remédier à ce véritable fléau, DORA intègre les "prestataires tiers de service TIC"[82] dans la liste des entités régulées et en tire deux conséquences dans l’articulation de sa règlementation.

La première conséquence est d’imposer aux prestataires TIC des obligations de sécurisation technique à l’identique de celles imposées à leur clients entités financières. Ainsi, une entité financière qui sous-traite une prestation supportant une fonction critique ou importante devrait imposer à son prestataire des mesures techniques de redondance identiques à celles que DORA lui impose (voir chapitre 7).

La seconde conséquence, qui répond à l’impératif de documenter toute action de mise en conformité, est d’imposer un très lourd encadrement des relations contractuelles entre les entités financières et leurs prestataires TIC, et tout particulièrement ceux fournissant un service soutenant une fonction critique ou importante.

Il faut d’ailleurs noter le glissement sémantique imposé par DORA qui en élargit notoirement le champs

81 ou attaque de la chaine d’approvisionnement IT en français

82 DORA article 2.1u

d'application, dans la mesure où les orientations EBA de 2019 n'encadrait "que" les prestations d'externalisation, là où DORA régule désormais tous les "prestataires tiers de service de TIC" dont la liste est extrêmement détaillée[83] (éditeur de logiciel "on premises", services IaaS, PaaS, SaaS, etc.).

Nous ne traiterons pas ici des dispositions de DORA encadrant les obligations spécifiques qui s'imposeront à certains prestataires "critiques" pour l'UE[84], qui seront désignés et régulés directement par la Commission européenne.

ÉVALUEZ VOTRE RISQUE DE DÉPENDANCE ET DE CONCENTRATION

DORA impose aux entités financières de lister parmi leurs contrats de prestation ceux qui portent sur l'externalisation de tout ou partie d'une fonction critique ou importante[85]. Nous ne traiterons ici que de ces "accords contractuels" dont la mise en conformité nous semble prioritaire (voir chapitre 1.4).

Le premier critère mis en avant par DORA est celui du risque de dépendance de l'entité financière à l'égard de son prestataire, qui doit prendre en compte "[sa] nature, [son] ampleur, [sa] complexité et [son] importance"[86].

Le second critère d'appréciation obligatoire selon DORA est celui du "risque de concentration informatique"[87] par un prestataire gérant une fonction critique ou importante.

DORA précise à l'article 3.29, que le risque de concentration s'apprécie au regard de "l'exposition à des prestataires tiers critiques de services TIC individuels ou multiples et liés, créant un degré de dépendance à l'égard de ces prestataires, de sorte que l'indisponibilité, la défaillance ou tout autre type d'insuffisance de ces derniers peut potentiellement mettre en péril la capacité d'une entité financière à assurer des

83 Voir annexe III Final report du 10 janvier 2024 "On Draft Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554"

84 DORA articles 31, 41, 42 et 43 : "prestataires tiers critiques de services TIC"

85 DORA article 28

86 DORA article 28.1.b (i)

87 DORA articles 28.4.c et 29

fonctions critiques ou importantes, ou l’exposer à subir d’autres types d’effets préjudiciables, y compris des pertes importantes, ou mettre en péril la stabilité financière de l’UE dans son ensemble".

Outre ces deux critères de fond, DORA impose aux entités financières des opérations formelles de vérification, avant de contracter avec un prestataire[88] :

- d’évaluer "si les conditions de surveillance en matière de conclusion de contrats sont remplies";
- "d’identifier et d’évaluer tous les risques pertinents" relatif au contrat envisagé;
- de s’assurer, "tout au long des processus de sélection et d’évaluation, que les prestataires présentent les qualités requises";
- d’identifier et d’évaluer tout risque "de conflit d’intérêt" susceptible de naitre du fait du contrat à conclure.

Ceci rappelé, voyons les clauses que les contrats conclus, ou à conclure ("par écrit" précise DORA à l’article 30.1), devront obligatoirement contenir.

VÉRIFIEZ VOS CLAUSES CONTRACTUELLES OBLIGATOIRES

La liste résumée des impératifs d’analyse de risque "avant de conclure un accord contractuel" portant sur une fonction critique ou importante[89] donne le vertige :

- préciser le lieu géographique de traitement et de stockage des données;
- détailler ce qui relève de la protection des données en termes "de disponibilité, [d’] authenticité, [d’] intégrité et [de] confidentialité";
- décrire les "niveaux de service";
- définir le coût de "l’assistance en cas d’incident";
- détailler et tester les "plans d’urgence" et les "mesures de sécurité";
- détailler les clauses relatives à "[l’] accès, [la] récupération et [la] restitution des données"; etc.

88 DORA article 28.4

89 DORA article 30

INSISTEZ SUR LES DROITS D'ACCÈS, D'INSPECTION ET D'AUDIT DE VOS PRESTATAIRES

DORA insiste sur la nécessité pour les entités financières d'assurer "un suivi permanent des performances"[90] de chaque prestataire qui passe notamment par l'obligation de prévoir contractuellement des droits "d'accès, d'inspection et d'audit" dont "l'exercice effectif n'est pas entravé ou limité par d'autres accords contractuels". Les clauses d'audit - obligatoires donc - doivent contenir "des précisions sur la portée, les procédures à suivre et la fréquence de ces inspections et audits".

> **"**Les droits d'accès, d'inspection et d'audit des prestataires sont des exigences contractuelles clés**"**

DÉTAILLEZ LES CONDITIONS DE RÉSILIATION DE VOS CONTRAT DE SERVICE

Insistons sur les obligations contractuelles spécifiques prévues à l'article 30.3.f de DORA encadrant la résiliation d'un contrat de service portant sur une fonction critique ou importante. Le contrat doit préciser (i) les droits et les délais de préavis de résiliation, et (ii) l'existence d'une période de transition qui doit permettre à l'entité soit de "migrer" la prestation chez un autre prestataire, soit de réinternaliser la prestation concernée.

En outre, DORA prévoit quatre cas de résiliation obligatoire[91] d'un contrat de service TIC, par exemple dans l'hypothèse où "le suivi des risques liés aux prestataires... a révélé l'existence de circonstances susceptibles d'altérer l'exécution des fonctions prévues par l'accord contractuel".

90 DORA article 30.3.e

91 DORA article 28.7

RÉDIGEZ DES AVENANTS DE MISE EN CONFORMITÉ DORA !

Deux méthodes sont possibles pour les entités financières qui souhaiteraient pouvoir prouver leur conformité à DORA dès le 17 janvier 2025 : mettre à jour tous leurs contrats avec tous leurs prestataires (c'est-à-dire re-signer chaque contrat après sa mise à jour) ou opter pour la rédaction d'avenants. Le choix de l'avenant de mise en conformité DORA nous semble offrir deux avantages majeurs : (i) mettre à jour les contrats existants à moindre frais et dans des conditions matérielles et de délais (presque) compatibles avec le calendrier d'entrée en application de DORA et surtout (ii) rendre ces contrats facilement auditables, notamment par les AES. Ici encore, privilégier la rédaction d'avenants DORA pour les contrats portant sur les fonctions critiques ou importantes nous semble la politique contractuelle la plus pertinente et la plus conforme à l'esprit, si ce n'est à la lettre, de DORA.


10. "Capturer la biche de Cérynie" ...

Retour au sommaire

TENEZ À JOUR VOTRE REGISTRE D'INFORMATION DES ACCORDS CONTRACTUELS

Outre des obligations de rédaction, DORA impose la tenue d'un "registre d'information des accords contractuels"[92] conclus avec tous [c'est nous qui soulignons] les prestataires TIC. Si cette obligation n'est pas nouvelle, son champs est singulièrement élargi dans la mesure où les orientations EBA de 2019 imposaient 20 points obligatoires[93], là où DORA en impose désormais 93 pour les "fonctions critiques ou importantes"[94]. L'écart de mise en conformité à conduire est donc substantiel. Évidemment, ce registre devra identifier ceux des contrats qui portent sur des fonctions critiques ou importantes et les autres, "au niveau de l'entité et aux niveaux sous-consolidé et consolidé"[95].

A l'identique du registre des traitements imposé par le RGPD, DORA prévoit que le registre des contrats doit être tenu à disposition des AES.

> **"**Le registre tenu à jour et le reporting aux autorités sont à prévoir en permanence**"**

92 DORA article 28.3

93 EBA orientations relatives à l'externalisation 25 février 2019 points 54 et 55

94 Voir le "final report" de l'ITS détaillant la structure obligatoire du registre et les mentions qu'il doit contenir publié sur le site web des AES le 17 janvier 2024 https://www.eiopa.europa.eu/publications/set-rules-under-dora-ict-and-third-party-risk-management-and-incident-classification_en

95 DORA articles 28.2 et 28.3

INFORMEZ LES AES LORSQUE C'EST OBLIGATOIRE

DORA exige que les entités financières "communiquent au moins une fois par an le nombre de nouveaux accords relatifs à l'utilisation de services TIC, les catégories de prestataires [TIC], le type d'accords contractuels et les services et fonctions de TIC qui sont fournis"[96].

DORA impose également aux 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"[97].

96 *DORA article 28.3.al.3*

97 *DORA article 28.3.al.5*

Retour au sommaire

11. "TUER LES OISEAUX DU LAC STYMPHALE" : GÉREZ LES OUBLIS DE DORA

Ces créatures, nuisibles par leur nombre et leur nature destructrice, symbolisent les omissions des régulateurs qui peuvent s'accumuler et brouiller les pistes d'une mise en conformité. Comme Hercule utilisant des cymbales pour les chasser, les entités financières doivent adopter des stratégies innovantes pour anticiper et gérer les "oublis de DORA".

L’ÉPINEUX PROBLÈME DE LA DETTE TECHNIQUE

La brièveté de l’encadrement par DORA des obligations portant sur les "systèmes de TIC hérités"[98] est inversement proportionnelle avec la criticité du problème auquel sont confrontées les DSI des secteurs de la banque ou de l’assurance qui doivent assurer le fonctionnement et la maintenance d’applications écrites par exemple en COBOL[99] et dont certaines sont vieilles de 60 ans. Pourtant, ce n’est qu’une obligation "d’évaluation spécifique du risque" "au moins une (1) fois par an... et, dans tous les cas, avant et après la connexion de technologies, d’applications ou de systèmes" à laquelle DORA astreint les entités financières.

PENSEZ À VOTRE POLITIQUE DE MOTS DE PASSE

DORA n’évoque pas l’impératif de mise en place obligatoire d’une politique de mots de passe solides pour l’ensemble de ses collaborateurs, oubli auquel les DSI et les RSSI remédieront nécessairement en France, dans le respect des impératifs de la CNIL[100].

PRÉVOYEZ DES CHARTES ÉTHIQUES POUR TOUS LES COLLABORATEURS

Quoique DORA soit muette sur ce point, les entités financières n’oublieront pas d’adopter et d’imposer, au moins pour leurs utilisateurs à profit ADMIN, des "chartes éthiques" décrivant les droits et surtout les obligations qui s’imposent à leurs collaborateurs et dont le non-respect doit pouvoir faire l’objet de sanctions disciplinaires. Ces chartes sont aujourd’hui obligatoires pour permettre l’obtention de certification de cybersécurité, comme par exemple les normes ISO 27001 ou SecNumCloud v3.2.

98 une définition à l’article 3.3, l’article 8.7 et une unique mention dans le Considérant n°43

99 https://www.lemonde.fr/economie/article/2023/05/23/informatique-le-secteur-bancaire-manque-de-specialistes-du-cobol_6174417_3234.html

100 CNIL délibération n°2022-100 du 21 juillet 2022

L'IMPÉRATIF DE LA SÉCURITÉ PHYSIQUE

Autre chapitre qui surprend par son absence dans DORA (sauf dans la liste des tests de l'article 25.1): la sécurité physique. Cet impératif, nécessaire à la sécurité de tout réseau et de tout système d'information, est pourtant présent dans la quasi-totalité des référentiels cybersécurité (hygiène ANSSI, ISO 27001, HDS, etc.).

RAPPELEZ L'IMPÉRATIF DE LA SÉCURITÉ DES DÉVELOPPEMENTS

Autre grand absent, la sécurité des développements logiciels n'est même pas citée dans DORA, alors qu'on en trouve mention en toutes lettres à l'article 21.3 de NISv2. Cette absence est d'autant plus surprenante que l'on retrouve plusieurs critères du processus S-SDLC (Secure Software Development Life Cycle) dans la liste des tests de résilience opérationnelle de DORA[101] : tests de compatibilité, test de performance, etc. Il semblerait pourtant légitime pour une entité financière souhaitant prouver son respect de l'état de l'art, de demander des preuves de sécurisation de ses process de développement logiciel à ses prestataires, notamment lorsqu'ils lui fournissent une fonction critique ou importante.

101 DORA article 25.1

“De l'importance de la veille réglementaire”

LISEZ LES RTS ET LES ITS

Les oublis relativement nombreux de DORA, ne doivent pas cacher la réalité de cette règlementation : ce qui ne figure pas dans le texte du règlement fera probablement l’objet de correction et de détails dans les documents techniques produits par les AES. La lecture attentive des RTS et des ITS, déjà publiés pour certains le 17 janvier 2024, et l’implémentation effective de leurs éléments sera un impératif de tout projet raisonné de mise en conformité avec la règlementation DORA. A noter que 2 RTS sont prévus pour encadrer spécifiquement les "Fonctions Critiques ou Importantes".

Retour au sommaire

12. CONCLUSION : NE VOUS CONTENTEZ PAS DE "NETTOYER LES ÉCURIES D'AUGIAS"

Tel Hercule ayant détourné deux rivières pour nettoyer les écuries du roi Augias de leur saleté accumulée, les entités financières doivent apprécier, chaque année, l'ensemble de leurs risques liés aux TIC, en prenant les décisions appropriées afin de garantir la propreté de leur cadre de gestion des risques.

PLANIFIEZ VOTRE CYCLE DE REVUE DU CADRE DE GESTION DES RISQUES ET DE VOTRE CONFORMITÉ DORA

Il appartient à la direction de l’entité financière d’examiner "périodiquement la mise en œuvre de la politique de continuité [de ses] activités de TIC... et des plans de réponse et de rétablissement des TIC"[102]. Cette périodicité est au cœur de DORA, qui impose un chantier constant, par cycles au moins annuels, de mise à jour de l’analyse de la cybermenace, de l’organisation de l’entité financière et des moyens qu’elle met en œuvre pour y répondre.

Le principe de revue annuelle est imposé par l’article 6.5 de DORA : "Le cadre de gestion du risque [de TIC] est documenté et réexaminé au moins une fois par an... Il est amélioré en permanence sur la base des enseignements tirés de la mise en œuvre et du suivi...".

DORA impose de plus, et systématiquement, des révisions des plans, politiques et audits en cas de "survenance d’incidents majeurs"[103] qui méritent de ne pas attendre les revues habituellement planifiées en cas de "modification importante de l’infrastructure" (numérique) de l’entité[104].

Enfin, certaines obligations de DORA sont prévues de manière continue, à l’instar de l’identification des "sources de risque"[105].

102 DORA article 5.2.al.2.e

103 DORA article 6.5

104 DORA article 8.3

105 DORA article 8.2

Retour au sommaire

PILOTEZ UN PROJET TRANSVERSE QUI IMPLIQUE TOUS LES MÉTIERS DE VOTRE ENTITÉ FINANCIÈRE

Le nombre des priorités à prendre en compte pour qu'une entité financière puisse estimer son risque de non-conformité révèle déjà la pluralité des chantiers à lancer : des actions métiers et d'organisation permettant d'agir ensuite sur les chantiers techniques et juridiques. C'est une certitude : la DSI et le RSSI ne seront pas seuls à devoir gérer le projet de mise en conformité DORA de leur entité.

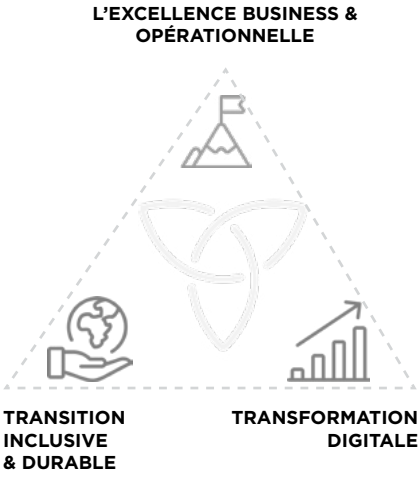
S'il faut encore emprunter à la mythologie grecque, le chantier de mise en conformité DORA s'apparente pour les entités financières au tonneau des Danaïdes. Mais là où les cinquante filles du Roi Danaos furent condamnées à travailler sans fin, les entités financières devront documenter leur effort continu vers une résilience opérationnelle effective.

La mise en conformité DORA est une obligation légale, qui sera contrôlée. Cette règlementation est l'occasion pour chaque entité financière de vérifier ce qui est critique et ce qui ne l'est pas, et de faire de leur cybersécurité une réalité, aujourd'hui nécessaire.

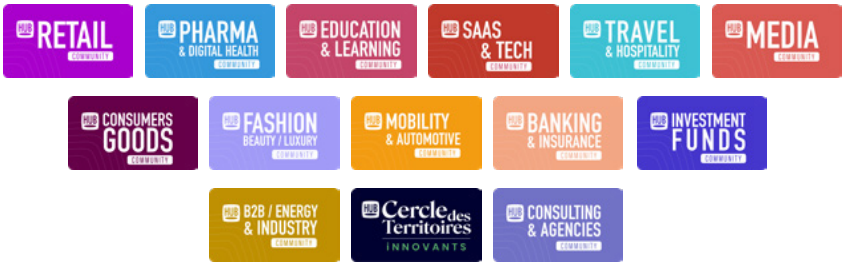
À PROPOS DU HUB INSTITUTE

Fondé en 2012 par Vincent Ducrey, Emmanuel Vivier et Perle Bagot, le HUB Institute, avec plus de 20 communautés professionnelles, est le **tiers de confiance du marché** sur les sujets de transformation digitale et durable des entreprises.

Notre mission : vous permettre via nos trois activités de **comprendre et d’anticiper** les tendances d’aujourd’hui et de demain, d’échanger avec les acteurs les plus innovants et **d’accélérer votre croissance et vos ambitions business.**



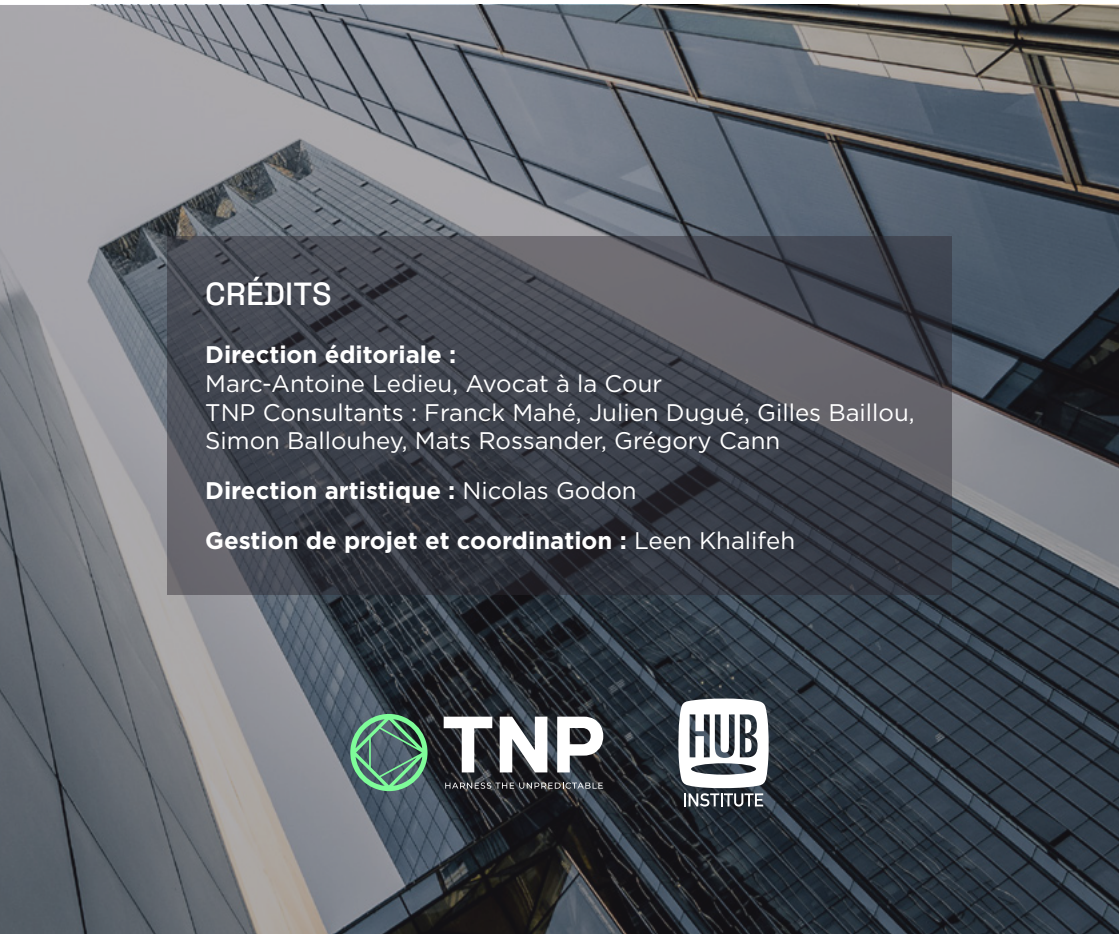
Communautés Sectorielles



Communautés Fonctionnelles

À PROPOS DE TNP CONSULTANTS

Créé en 2007, TNP Consultants est un cabinet de conseil européen spécialisé dans les transformations stratégiques, opérationnelles, digitales et réglementaires des entreprises. TNP intervient sur les dimensions de stratégie opérationnelle, systèmes d'information, métier et capital humain, dans les secteurs de la banque, de l'assurance, du transport, de l'énergie et de l'automobile et du secteur public. TNP a fait de l'accélération de la performance de ses clients son ADN. Ses équipes sont aujourd'hui présentes dans trois zones géographiques : Europe continentale (France, Luxembourg, Italie, Suisse, Allemagne, Monaco), Afrique (Maroc, Tunisie, Côte d'Ivoire), Asie et Moyen-Orient (Inde, Émirats Arabes Unis).



CRÉDITS

Direction éditoriale :
Marc-Antoine Ledieu, Avocat à la Cour
TNP Consultants : Franck Mahé, Julien Dugué, Gilles Baillou, Simon Ballouhey, Mats Rossander, Grégory Cann

Direction artistique : Nicolas Godon

Gestion de projet et coordination : Leen Khalifeh

TNP
HARNESS THE UNPREDICTABLE

HUB
INSTITUTE