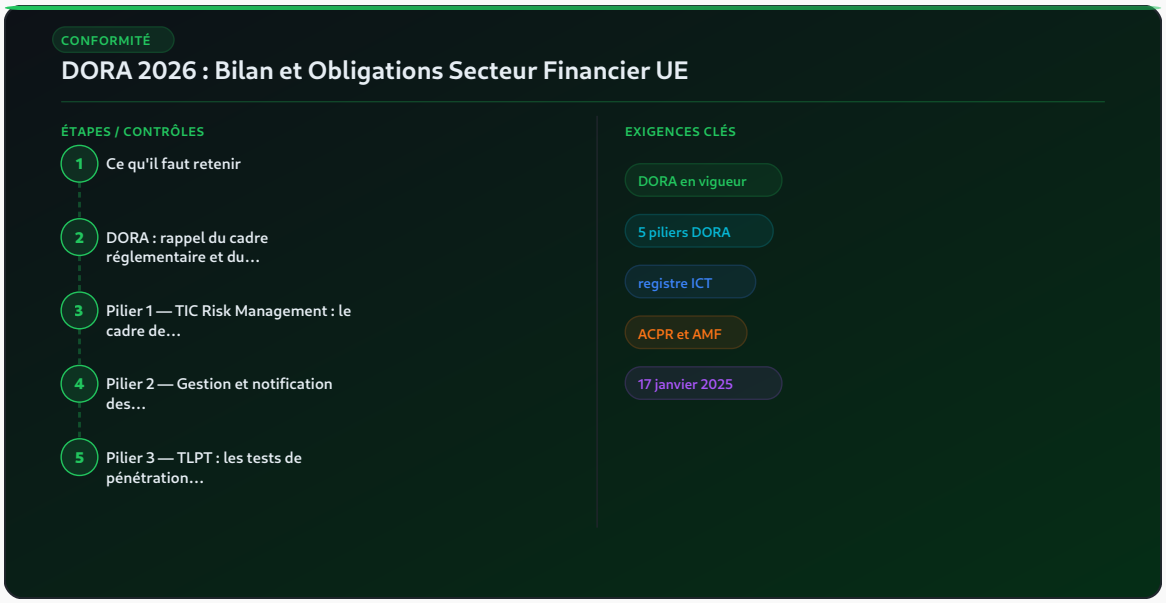
DORA 2026 : Bilan d'Application et Obligations du Secteur Financier

> Bilan d'application DORA 2026 pour le secteur financier — TLPT, gestion TIC tiers, registre ICT, incidents majeurs et rôle de l'ACPR et de l'AMF en France.

Le règlement DORA (Digital Operational Resilience Act), entré en vigueur le 17 janvier 2025, a achevé sa première année d'application dans le secteur financier européen avec des résultats contrastés mais globalement positifs. Les établissements financiers français — banques, assurances, sociétés de gestion, entreprises d'investissement, prestataires de services de paiement et contreparties centrales — ont dû absorber simultanément les cinq piliers de DORA tout en gérant leurs obligations prudentielles habituelles et les premiers contrôles de l'ACPR et de l'AMF désormais coordinateurs avec l'ANSSI dans le cadre NIS2. Ce bilan exhaustif de 2026 analyse l'état de conformité du secteur financier français à DORA, les points de conformité difficiles, les pratiques émergentes en matière de TLPT (Threat-Led Penetration Testing), la gestion du registre ICT et les défis spécifiques des PMF (Petites et Moyennes entités Financières) qui bénéficient d'un régime allégé mais qui peinent à en définir les contours pratiques avec leurs régulateurs sectoriels.

À RETENIR



Ce qu'il faut retenir

DORA en vigueur depuis le 17 janvier 2025 — premier bilan 2026 : conformité partielle, focus sur le registre ICT et les incidents.

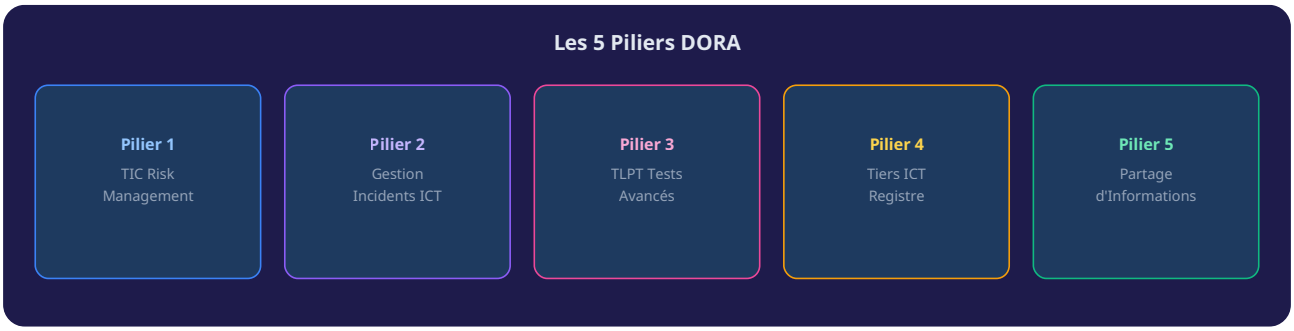
Les **5 piliers DORA** : risk management TIC, gestion des incidents, TLPT, gestion des tiers ICT et partage d'informations.

Le **TLPT** (Threat-Led Penetration Testing) est obligatoire pour les entités financières significatives selon des modalités définies par les AES.

Le **registre ICT** des tiers — obligation la plus complexe à opérationnaliser selon les retours de place.

ACPR et AMF assurent la supervision DORA en France avec des cycles de contrôle désormais rodés.

Les PMF bénéficient d'un régime allégé mais doivent identifier leur catégorie avec précision pour calibrer leurs obligations.



DORA : rappel du cadre réglementaire et du calendrier d'application

Le règlement DORA (Règlement UE 2022/2554 sur la résilience opérationnelle numérique du secteur financier) a été publié au Journal officiel de l'UE le 27 décembre 2022. Il est entré en application le **17 janvier 2025** après une période de transition de deux ans, pendant laquelle les autorités européennes de supervision (AES — ABE, AEMF et AEAPP) ont publié les normes techniques réglementaires (RTS) et d'exécution (ITS) précisant les modalités d'application.

> ⚡ **Retour terrain**
>
> Pour un opérateur d'importance vitale dans le secteur de l'eau, la mise en conformité LPM impliquait de qualifier des équipements de supervision SCADA datant de 2008 — non qualifiables dans leur version actuelle. La solution retenue a été une architecture de démilitarisée (DMZ) avec diode de données entre le SI IT et le SI OT, permettant de maintenir les équipements legacy tout en satisfaisant aux exigences de cloisonnement.

DORA s'applique à un périmètre très large d'entités financières : établissements de crédit, établissements de monnaie électronique, prestataires de services de paiement, entreprises d'investissement, fournisseurs de services sur crypto-actifs, dépositaires centraux de titres,

contreparties centrales, plateformes de négociation, gestionnaires de fonds alternatifs, sociétés de gestion d'OPCVM, prestataires de services de notation de données, et les prestataires de services ICT tiers critiques désignés par les AES.

En France, l'**ACPR (Autorité de Contrôle Prudentiel et de Résolution)** supervise DORA pour les établissements de crédit, les assurances et les établissements de paiement. L'**AMF (Autorité des Marchés Financiers)** supervise les entreprises d'investissement et les gestionnaires de fonds. Une coordination formelle entre ACPR, AMF et ANSSI a été mise en place pour articuler les contrôles DORA avec les obligations NIS2 lorsqu'une même entité relève des deux régimes — une articulation complexe qui a fait l'objet d'une note conjointe en 2025.

Pilier 1 — TIC Risk Management : le cadre de gestion des risques DORA

Le premier pilier de DORA impose aux entités financières de disposer d'un **cadre de gestion des risques TIC** robuste et documenté. Ce cadre doit couvrir l'ensemble des risques liés aux technologies de l'information et de la communication qui pourraient impacter la résilience opérationnelle numérique de l'entité, avec une stratégie de résilience numérique approuvée par l'organe de direction.

Le cadre de gestion des risques TIC doit notamment inclure : une politique de sécurité de l'information documentée, des procédures de gestion des incidents TIC, des plans de continuité des activités et de reprise après sinistre incluant les scénarios de défaillance majeure des systèmes TIC critiques, et un processus de gestion des changements dans les systèmes TIC. L'**organe de direction** est explicitement responsable de l'approbation et du suivi de ce cadre — une obligation de gouvernance similaire à NIS2 qui crée une responsabilité personnelle des membres du conseil d'administration et du comité de direction.

Une particularité DORA importante : la norme exige que les entités financières maintiennent un **inventaire exhaustif et actualisé de leurs actifs TIC** (matériels, logiciels, configurations, flux de données entre systèmes) et identifient les *fonctions critiques ou importantes (FCI)* qui, en cas

de perturbation, affecteraient significativement la continuité des services financiers. Cet inventaire est le point de départ de toutes les analyses de risques et des tests de résilience DORA.

Pilier 2 — Gestion et notification des incidents ICT

DORA impose un régime structuré de **classification et de notification des incidents ICT majeurs** qui présente des similitudes avec NIS2 mais s'en distingue sur plusieurs points importants. La classification des incidents repose sur des critères quantitatifs définis dans les RTS des AES : nombre de clients affectés, durée de la perturbation, pertes financières causées, et criticité des systèmes affectés.

Un **incident ICT majeur** au sens DORA doit être notifié simultanément à l'autorité compétente nationale (ACPR ou AMF) et, lorsque l'incident a un impact transfrontalier, à l'autorité compétente du pays d'accueil. Le délai de notification initiale est de **4 heures** après qualification de l'incident comme majeur pour la notification préliminaire, puis 24 heures pour la notification intermédiaire, et enfin 1 mois pour le rapport final — un régime plus contraignant que celui de NIS2 en termes de précision des informations exigées mais avec des délais initiaux légèrement plus longs.

Les établissements financiers sont également tenus de notifier les incidents aux **clients significatifs** affectés, dans un délai et selon des modalités définis dans les contrats et conformes aux exigences DORA. Cette obligation de communication client est une nouveauté importante par rapport aux régimes réglementaires antérieurs et impose de préparer des modèles de communication de crise adaptés à différents scénarios d'incidents ICT.

Pilier 3 — TLPT : les tests de pénétration guidés par la menace

Le **Threat-Led Penetration Testing (TLPT)** est l'une des innovations les plus structurantes de DORA. Ces tests avancés, inspirés du programme TIBER-EU de la Banque Centrale

Européenne, simulent des attaques réalistes basées sur des scénarios de menaces actuels ciblant spécifiquement le secteur financier. Le TLPT diffère fondamentalement des tests de pénétration classiques par sa durée (6-12 mois), sa sophistication (techniques APT réalistes), et sa gouvernance rigoureuse (supervision directe des régulateurs).

DORA rend le TLPT obligatoire pour les entités financières **significatives** désignées par les autorités compétentes sur la base de critères de taille, de systémicité et de criticité pour le système financier. En France, l'ACPR a commencé à désigner les entités soumises à TLPT en 2025, en commençant par les plus grandes banques et assurances de dimension systémique. Le cycle TLPT doit être renouvelé tous les **3 ans au minimum** pour les entités désignées.

La réalisation d'un TLPT DORA impose de faire appel à des équipes red team certifiées TIBER ou CBEST et à des fournisseurs de Threat Intelligence agréés, d'impliquer un auditeur indépendant pour superviser le test et valider les résultats, et de produire un rapport final présenté à l'organe de direction et à l'autorité compétente. Le coût d'un TLPT DORA complet, incluant les phases de Threat Intelligence, de red teaming et d'évaluation remédiation, est généralement compris entre 500 000 et 2 millions d'euros pour une grande entité financière — un investissement significatif qui nécessite une préparation minutieuse plusieurs mois avant le démarrage du test.

Un retour terrain : lors de l'accompagnement d'une banque de taille moyenne dans la préparation de son premier TLPT DORA, nous avons constaté que les 6 mois de préparation étaient aussi importants que le test lui-même. L'inventaire des systèmes critiques dans le périmètre de test, la définition des scénarios de menaces pertinents avec le fournisseur de Threat Intelligence, et la mise en place de la gouvernance interne du test (comité de pilotage, équipe bleue désignée, communication avec le régulateur) ont représenté 40 % du coût total.

Pilier 4 — Registre ICT des tiers : l'obligation la plus complexe

Le registre des tiers ICT est, selon les remontées de place françaises, **l'obligation DORA la plus difficile à opérationnaliser**. Il impose à chaque entité financière de maintenir un registre complet et actualisé de tous ses prestataires TIC, avec pour chaque prestataire un niveau de documentation proportionnel à sa criticité pour les fonctions importantes ou critiques de l'entité.

Le format du registre est défini par un ITS des AES qui précise les champs obligatoires : identification du prestataire, description du service fourni, classification du service (FCI ou non), pays d'établissement du prestataire et de traitement des données, sous-traitants ICT du prestataire (sous-chaîne d'approvisionnement), et évaluation de la concentration des risques ICT. Cette exigence de traçabilité sur plusieurs niveaux de la chaîne d'approvisionnement ICT est particulièrement complexe car de nombreux prestataires de premier rang sous-traitent eux-mêmes des composants critiques à des prestataires de second rang que l'entité financière ne contrôle pas directement.

Type de prestataire ICT	Criticité DORA	Niveau documentation registre
Prestataire ICT critique désigné AES	Critique systémique	Documentation complète + supervision AES directe
Prestataire supportant une FCI	Critique pour l'entité	Documentation renforcée + contrats conformes DORA
Prestataire supportant des fonctions non-FCI	Standard	Documentation de base + clauses contractuelles minimales

Clauses contractuelles DORA : révision des contrats ICT

DORA impose des **clauses contractuelles minimales obligatoires** dans tous les contrats avec des prestataires ICT tiers supportant des fonctions critiques ou importantes. Ces clauses doivent couvrir : la description précise des services fournis et les niveaux de service (SLA) pour la disponibilité et la performance, les droits d'audit de l'entité financière et de ses régulateurs sur le prestataire ICT, les obligations de notification d'incidents ICT par le prestataire à l'entité cliente, les exigences de sécurité des données et de localisation des données, et les clauses de résiliation et de stratégie de sortie avec délais et conditions de transfert.

La révision des contrats ICT existants pour intégrer les clauses DORA a représenté un travail colossal pour les grandes entités financières françaises entre 2023 et 2025. Les grands établissements de crédit avaient parfois plusieurs centaines de contrats ICT à réviser, avec des prestataires dont certains ont été récalcitrants à accepter les droits d'audit. L'**ABE (Autorité Bancaire Européenne)** a publié des orientations sur les négociations avec les prestataires ICT

qui donnent aux entités financières des arguments pour imposer les clauses DORA lors des renouvellements contractuels.

Un point d'opinion assumé sur les contrats DORA : les droits d'audit sur les grands prestataires cloud (AWS, Microsoft Azure, Google Cloud) restent une source de tension majeure. Ces hyperscalers proposent des programmes d'audit standardisés (partage de certifications ISO 27001, SOC 2, rapports d'audit mutualisés) qui ne correspondent pas toujours aux droits d'audit individualisés exigés par DORA. La Commission Européenne et les AES doivent clarifier ce point dans leurs orientations pour éviter une impasse contractuelle qui bloquerait l'adoption du cloud par le secteur financier.

Pilier 5 — Partage d'informations sur les cybermenaces

Le cinquième pilier de DORA encourage le **partage volontaire d'informations sur les cybermenaces** entre entités financières au sein de dispositifs de partage reconnus. Cette dimension coopérative reflète la conviction que la résilience du secteur financier est un bien commun qui bénéficie d'une approche collective plutôt que de silos compétitifs entre établissements concurrents.

En France, les mécanismes de partage d'informations pour le secteur financier incluent le **CERT Banque de France**, les groupes de travail de la Fédération Bancaire Française (FBF) sur la cybersécurité, et la participation aux plateformes européennes de partage d'informations comme FS-ISAC (Financial Services Information Sharing and Analysis Center). DORA clarifie le cadre juridique permettant ce partage d'informations sensibles sur les menaces entre entités concurrentes, en précisant que ce partage est conforme au droit de la concurrence lorsqu'il porte sur des informations de sécurité non-commerciales.

Régime allégé DORA pour les PMF : périmètre et conditions

DORA prévoit un **régime allégé (proportionné)** pour les petites et moyennes entités financières (PMF) définies selon des critères de taille combinant le bilan total, le nombre de clients et la complexité des activités. Ce régime allégé permet aux PMF de se dispenser de certaines obligations du pilier 1 (cadre TIC allégé), d'être exemptées du TLPT, et de disposer de délais adaptés pour la mise en conformité.

La définition des PMF au sens DORA est cependant plus complexe que les seuils simples de NIS2 : elle varie selon le type d'entité financière. Pour les établissements de crédit, les seuils ABE définissent des critères de taille de bilan et de business model. Pour les gestionnaires de fonds, les seuils AEMF prennent en compte les actifs sous gestion. Pour les assurances, les critères AEAPP s'appuient sur le volume de primes. Cette diversité de critères selon le type d'entité crée une complexité pratique que les entités à activités multiples doivent analyser entité par entité.

Un point de vigilance important pour les PMF : l'exemption du TLPT et le régime allégé du cadre TIC ne signifient pas absence de toute obligation. Les PMF restent soumises aux obligations de notification d'incidents ICT, aux exigences contractuelles minimales pour leurs prestataires ICT critiques, et aux obligations de maintien d'un registre ICT (simplifié). L'ACPR a précisé dans ses communications de 2025 que le régime allégé DORA ne doit pas être interprété comme une exemption générale mais comme une proportionnalité des exigences qui reste exigeante pour les entités même de taille modeste.

Supervision des prestataires ICT critiques par les AES

L'une des innovations les plus significatives de DORA est la **supervision directe des prestataires ICT tiers critiques par les AES**. Pour la première fois, des entités non financières — les grands prestataires cloud et les fournisseurs de services ICT systémiques pour le secteur financier — peuvent être soumis à une supervision directe de l'ABE, de l'AEMF ou de l'AEAPP.

La désignation des prestataires ICT critiques est réalisée annuellement par une commission de désignation conjointe des AES, sur la base de critères incluant le nombre d'entités financières clientes, la substituabilité du service, l'impact systémique d'une défaillance, et l'interdépendance avec les infrastructures financières critiques. Les premiers prestataires ICT critiques désignés en 2025 incluent plusieurs grands hyperscalers cloud et fournisseurs de services de clearing et règlement qui supportent des infrastructures financières critiques dans toute l'UE.

Les prestataires ICT critiques désignés sont soumis à des audits réguliers des AES, à des tests de résilience coordonnés, et peuvent se voir imposer des mesures correctives par les autorités. Cette supervision directe crée un nouveau type de relation réglementaire entre les autorités financières européennes et les prestataires technologiques, qui n'étaient jusqu'alors soumis qu'aux régulations sectorielles de leur pays d'établissement — un changement de paradigme majeur pour des acteurs comme AWS, Microsoft ou Google.

Bilan 2026 : les points durs de la conformité DORA en France

Le bilan de la première année complète d'application de DORA révèle plusieurs points durs communs à la majorité des établissements financiers français.

Point dur n°1 : le registre ICT des sous-traitants. La traçabilité sur plusieurs niveaux de la chaîne d'approvisionnement ICT reste incomplète pour la plupart des établissements. Les prestataires de premier rang ne fournissent pas systématiquement les informations sur leurs propres sous-traitants dans un format exploitable, et la mise à jour continue du registre est une charge opérationnelle significative sous-estimée lors de la préparation à DORA.

Point dur n°2 : les droits d'audit sur les hyperscalers cloud. La tension entre les droits d'audit individuels exigés par DORA et les programmes d'audit mutualisés proposés par AWS, Microsoft et Google n'a pas été résolue de manière satisfaisante pour tous les établissements. Certains ont accepté les programmes d'audit mutualisés comme suffisants au regard des guidelines ABE, d'autres maintiennent une position de non-conformité temporaire en attendant des clarifications réglementaires.

Point dur n°3 : la qualification des FCI (fonctions critiques ou importantes). La définition des fonctions critiques ou importantes qui déclenchent les obligations renforcées DORA est sujette à interprétation. Certains établissements ont adopté une approche conservatrice en qualifiant de nombreuses fonctions en FCI, créant une charge de conformité élevée, tandis que d'autres ont adopté une approche minimaliste qui pourrait être contestée lors des contrôles ACPR.

DORA et cloud : enjeux spécifiques pour le secteur financier

La conformité DORA impose des **exigences spécifiques pour l'utilisation du cloud** dans le secteur financier qui vont au-delà des guidelines précédentes de l'EBA sur l'externalisation cloud. La stratégie cloud des entités financières doit désormais intégrer explicitement les contraintes DORA : stratégie de sortie documentée et testée, clauses d'audit dans les contrats cloud, analyse de concentration des risques cloud (dépendance à un seul fournisseur), et localisation des données dans des juridictions conformes aux exigences réglementaires applicables.

La **stratégie de sortie** cloud est particulièrement complexe à élaborer car elle implique de documenter comment l'entité pourrait migrer ses applications critiques vers un autre prestataire ou vers une infrastructure on-premise dans un délai acceptable, sans interruption majeure des services financiers. Pour les entités ayant des architectures cloud-native avec des services propriétaires du fournisseur (services serverless spécifiques, bases de données propriétaires, services IA de l'hyperscaler), cette stratégie de sortie impose souvent de prévoir une réécriture significative des applications — un investissement que beaucoup d'établissements rechignent à réaliser de manière préventive.

La certification SecNumCloud de l'ANSSI constitue une réponse française aux enjeux de souveraineté numérique dans le cloud pour les données financières les plus sensibles, bien que son adoption reste limitée par le nombre encore restreint de prestataires qualifiés et les surcoûts associés par rapport aux hyperscalers internationaux.

Articulation DORA et NIS2 : le guide pratique pour les entités doubles

Les entités financières soumises simultanément à DORA et NIS2 — en pratique toutes les entités financières significatives car DORA est lex specialis pour le secteur financier mais certaines activités peuvent relever des deux régimes — bénéficient de clarifications importantes publiées en 2025 par la Commission Européenne.

DORA est considéré comme lex specialis par rapport à NIS2 pour les entités financières dans son champ d'application. Concrètement, une banque soumise à DORA n'a pas à déployer un programme NIS2 séparé pour ses activités bancaires : DORA est censé offrir un niveau de protection équivalent ou supérieur aux obligations NIS2. Cependant, si la banque détient des filiales opérant dans des secteurs non-financiers soumis à NIS2 (par exemple une filiale de services numériques), ces filiales restent soumises à NIS2 de manière autonome.

La coordination ACPR-AMF-ANSSI vise à éviter les doubles audits et les contrôles redondants pour les entités relevant des deux régimes. En pratique, les contrôles DORA réalisés par l'ACPR sont reconnus comme couvrant les exigences équivalentes NIS2, à condition que le programme de conformité DORA soit complet et documenté. Notre guide NIS2 Phase 2 détaille l'articulation des deux régimes du point de vue des entités concernées.

Tests de résilience opérationnelle numérique : au-delà du TLPT

DORA impose une approche structurée des **tests de résilience opérationnelle numérique** qui va bien au-delà du seul TLPT. Toutes les entités financières, y compris les PMF non soumises au TLPT, doivent réaliser régulièrement des tests de résilience adaptés à leur taille et à leur profil de risque.

Ces tests comprennent à minima des **tests de vulnérabilités et de pénétration** sur les systèmes supportant les FCI, des **tests de continuité des activités** validant les plans PCA/PRA cyber, des **exercices de crise** simulant des incidents ICT majeurs (ransomware, DDoS sur systèmes de paiement, défaillance de prestataire ICT critique), et des **tests de restauration** validant les

capacités réelles de reprise depuis les sauvegardes dans les délais RTO/RPO définis. Les résultats de ces tests doivent être documentés, présentés à l'organe de direction et aux autorités sur demande, et utilisés pour améliorer le cadre de gestion des risques TIC.

DORA 2026 : calendrier des prochaines obligations et standards

Si les obligations principales de DORA sont en vigueur depuis janvier 2025, plusieurs chantiers réglementaires restent ouverts en 2026 et méritent d'être suivis de près par les entités financières.

Les **RTS sur la sous-traitance des prestataires ICT critiques** finalisent les modalités de supervision directe par les AES, avec des exigences spécifiques pour les rapports des prestataires désignés. Les **orientations sur les tests de résilience avancés** pour les entités non soumises au TLPT précisent les méthodologies acceptables pour les tests alternatifs. Les **orientations sur la gestion des risques ICT concentrés** fourniront un cadre pour évaluer et gérer la dépendance systémique à un nombre restreint de prestataires ICT — le risque de concentration cloud notamment.

Le premier **cycle complet de supervision DORA** par les AES des prestataires ICT critiques désignés débutera en 2026-2027, avec des inspections sur site et des audits techniques qui permettront d'affiner les interprétations des exigences DORA dans le contexte des architectures réelles des prestataires systémiques. Pour rester informé des publications réglementaires DORA, le site de l'ABE sur DORA centralise toutes les normes techniques et orientations.

Notre article de bilan DORA est complété par nos analyses sur la certification SecNumCloud pour les besoins cloud souverains du secteur financier et sur les investigations forensiques cloud désormais nécessaires pour reconstituer les timelines d'incidents ICT majeurs dans les environnements cloud financiers.

FAQ — DORA 2026 Secteur Financier

Mon établissement est-il soumis au TLPT DORA ?

Le TLPT DORA s'applique aux entités financières significatives désignées par les autorités compétentes nationales sur la base de critères de taille, de systémicité et de criticité pour le système financier. En France, l'ACPR et l'AMF effectuent les désignations pour leurs secteurs respectifs. Si votre établissement n'a pas reçu de désignation formelle, il n'est pas soumis au TLPT obligatoire mais reste soumis à des tests de pénétration réguliers selon les orientations ABE sur les tests de résilience. La désignation peut intervenir à tout moment si l'établissement atteint les seuils ou change de profil de risque systémique.

Comment définir les fonctions critiques ou importantes (FCI) dans notre établissement ?

Les FCI sont les fonctions dont la défaillance ou la perturbation affecterait significativement la continuité des services financiers de l'établissement ou du système financier plus largement. La qualification FCI doit être réalisée en impliquant les métiers (pas seulement la DSI) et en analysant l'impact d'une interruption de chaque fonction sur les clients, les contreparties et la stabilité financière. Les orientations ABE fournissent des critères de qualification mais laissent une part de jugement à l'établissement. Il est recommandé d'adopter une approche légèrement conservatrice (inclure des fonctions borderline en FCI) pour éviter de se retrouver non-conforme si le régulateur considère qu'une fonction non-qualifiée en FCI aurait dû l'être.

Que faire si nos prestataires ICT refusent les droits d'audit DORA ?

Un prestataire ICT qui refuse les droits d'audit imposés par DORA expose l'entité financière à une non-conformité réglementaire. En pratique, la première étape est d'invoquer les orientations ABE sur les contrats cloud et l'externalisation qui donnent un cadre clair sur les droits minimaux d'audit. Pour les grands prestataires cloud, les programmes d'audit mutualisés (CSA STAR, SOC 2 Type II, ISO 27001) peuvent être acceptés comme alternative proportionnée si l'autorité compétente les reconnaît formellement. En dernier recours, un prestataire ICT qui maintient son refus doit être considéré comme un risque de concentration et son remplacement par un

prestataire conforme doit être planifié — DORA donne explicitement le droit à l'entité de résilier un contrat pour non-conformité aux exigences réglementaires.

DORA s'applique-t-il aux fintechs et aux néobanques ?

Oui, DORA s'applique aux fintechs et néobanques dès lors qu'elles sont agréées en tant qu'établissements de paiement, établissements de monnaie électronique ou établissements de crédit dans l'UE. Les fintechs agréées en tant qu'entreprises d'investissement ou prestataires de services sur crypto-actifs sont également dans le périmètre DORA. Le régime allégé pour les PMF peut s'appliquer aux fintechs de taille modeste, mais elles restent soumises aux obligations de notification d'incidents ICT et aux exigences contractuelles minimales pour leurs prestataires cloud et leurs API tierces.

Quelles sont les sanctions possibles en cas de non-conformité à DORA ?

DORA prévoit des sanctions administratives pouvant atteindre **1 % du chiffre d'affaires journalier moyen mondial** pour les entités financières non conformes, sur une durée maximale de 6 mois consécutifs. Pour les prestataires ICT critiques désignés, les sanctions peuvent atteindre 5 millions d'euros ou 1 % du chiffre d'affaires mondial annuel. Les autorités compétentes nationales ont également la possibilité de publier des avertissements publics, de suspendre ou de retirer les agréments dans les cas les plus graves. En France, l'ACPR et l'AMF ont confirmé que les premiers contrôles DORA seront prioritairement axés sur les obligations documentaires et le registre ICT, avant de passer à des sanctions financières pour les cas de non-conformité grave.

Concentration des risques ICT : le risque systémique cloud dans le secteur financier

L'un des risques systémiques les plus préoccupants identifiés dans le cadre de DORA est la **concentration des risques ICT** au niveau sectoriel : une grande partie du secteur financier

européen s'appuie sur un nombre très restreint de prestataires cloud et de fournisseurs de services ICT critiques. Une défaillance majeure d'un hyperscaler cloud affectant simultanément des dizaines d'établissements financiers clients représenterait un risque systémique pour la stabilité financière comparable à la défaillance d'une infrastructure de marché.

Les AES ont publié des orientations sur la gestion du risque de concentration ICT qui exigent que les entités financières analysent régulièrement leur exposition à ce risque, notamment la part de leurs FCI hébergées chez un seul prestataire cloud, la substituabilité de ce prestataire dans un délai acceptable, et les interdépendances entre prestataires (un prestataire ICT hébergé sur le cloud d'un autre prestataire ICT). Cette analyse de concentration doit alimenter la stratégie de diversification ICT de l'entité et ses plans de continuité d'activité.

Pour les entités financières françaises, la certification SecNumCloud constitue une réponse partielle à ce défi de concentration en favorisant l'adoption de prestataires cloud qualifiés par l'ANSSI, réduisant la dépendance aux hyperscalers américains pour les données et systèmes les plus sensibles. L'émergence de prestataires cloud européens qualifiés SecNumCloud (OVHcloud, Outscale/Dassault Systèmes, Bleu) offre des alternatives concrètes pour diversifier les risques de concentration tout en maintenant des niveaux de service compatibles avec les exigences opérationnelles du secteur financier.

Formation et sensibilisation DORA : les obligations pour les équipes et la direction

DORA impose des exigences de **formation et de sensibilisation** à tous les niveaux de l'organisation. L'organe de direction doit disposer des compétences suffisantes pour comprendre et superviser les risques TIC — une exigence qui se traduit par des formations spécifiques pour les membres des conseils d'administration et des comités de risque sur les enjeux de résilience opérationnelle numérique et les obligations DORA.

Les équipes opérationnelles impliquées dans la gestion des risques TIC, la gestion des incidents et le registre ICT doivent bénéficier de formations régulières sur les procédures DORA, les critères de classification des incidents, et les processus de notification réglementaire. Les équipes

IT chargées de la maintenance des systèmes supportant les FCI doivent intégrer les exigences DORA dans leurs processus de gestion des changements et de maintenance, pour éviter que des modifications mal contrôlées des systèmes critiques ne créent des risques de perturbation non anticipés.

Les établissements financiers ont investi significativement dans la formation DORA entre 2023 et 2025 dans le cadre de leurs programmes de préparation à l'application du règlement. En 2026, la priorité se déplace vers la **culture de la résilience** — intégrer les réflexes DORA dans les pratiques quotidiennes des équipes plutôt que de considérer DORA comme un projet de conformité externe. Cette transformation culturelle est le défi de long terme de DORA, au-delà de la mise en œuvre technique et documentaire des premières années d'application.

Intégration DORA dans le SMSI et les processus de gouvernance existants

Les établissements financiers qui avaient préalablement investi dans des systèmes de management de la sécurité de l'information (SMSI ISO 27001) et des processus de gestion des risques opérationnels (Bâle III pour les banques, Solvabilité II pour les assurances) disposent d'une base solide pour l'intégration de DORA. La résilience opérationnelle numérique n'est pas un concept nouveau dans le secteur financier — c'est l'extension et la formalisation de ce qui existait déjà sous des formes diverses.

La stratégie d'intégration optimale consiste à **enrichir le SMSI existant** avec les exigences spécifiques DORA plutôt que de créer un système de management parallèle : étendre la politique de sécurité de l'information pour couvrir explicitement la résilience opérationnelle numérique DORA, enrichir le processus de gestion des incidents pour intégrer la classification et la notification DORA, et compléter le registre des actifs TIC pour en faire le registre ICT DORA. Cette approche intégrée réduit la charge documentaire, évite les incohérences entre systèmes de management parallèles, et facilite les audits croisés ISO 27001 / DORA.

Les organisations soumises à la fois à DORA et au référentiel RGPD doivent également s'assurer de la cohérence entre les registres des traitements RGPD et le registre ICT DORA : les

prestataires ICT qui traitent des données personnelles pour le compte de l'établissement financier sont à la fois sous-traitants RGPD et prestataires ICT DORA, avec des obligations contractuelles distinctes dans les deux régimes qui doivent être harmonisées dans un contrat unique structuré.

Maturité cyber et DORA : grille d'évaluation pour les établissements financiers

Pour évaluer la maturité de leur programme de conformité DORA, les établissements financiers peuvent s'appuyer sur une grille d'évaluation structurée autour des cinq piliers. Cette grille distingue quatre niveaux de maturité : initial (conformité documentaire basique), défini (processus formalisés mais non testés), géré (processus testés régulièrement et améliorés) et optimisé (culture de la résilience intégrée et amélioration continue proactive).

La majorité des établissements financiers français se situe en 2026 entre les niveaux défini et géré sur la plupart des piliers DORA. Le pilier 3 (TLPT) représente le niveau de maturité le plus avancé pour les entités désignées qui ont complété leur premier cycle complet, tandis que le pilier 4 (registre ICT) présente le niveau de maturité le plus hétérogène avec des écarts importants entre les grands établissements systémiques qui disposent d'équipes dédiées à la gestion des fournisseurs ICT et les entités de taille intermédiaire qui n'ont pas encore industrialisé ce processus.

Pilier DORA	Maturité médiane FR 2026	Principal point dur
Pilier 1 — TIC Risk Management	Géré	Qualification FCI / inventaire actifs TIC complet
Pilier 2 — Incidents ICT	Géré	Délais de notification serrés, qualification incident majeur
Pilier 3 — TLPT	Optimisé (entités désignées)	Coût élevé, ressources TLPT rares en France
Pilier 4 — Registre ICT tiers	Défini	Sous-traitants niveau 2-3, droits d'audit cloud
Pilier 5 — Partage d'informations	Initial/Défini	Cadre juridique partage sensible, adoption des plateformes

La maturité DORA du secteur financier français en 2026 doit être analysée dans le contexte d'un secteur qui avait déjà un niveau de maturité cybersécurité supérieur à la moyenne des autres secteurs économiques, grâce aux exigences prudentielles préexistantes de l'ACPR et de l'AMF et aux investissements importants réalisés post-pandémie pour sécuriser les infrastructures de télétravail et les services numériques. DORA a néanmoins identifié des lacunes importantes — notamment dans la gestion de la chaîne d'approvisionnement ICT et les tests avancés de résilience — qui ne pouvaient pas être comblées sans un cadre réglementaire contraignant. Le bilan 2026 est globalement positif en termes de mobilisation du secteur, mais la conformité réelle aux exigences les plus opérationnelles (registre ICT complet, droits d'audit cloud effectifs, TLPT réalisés pour toutes les entités désignées) reste un travail en cours qui se prolongera jusqu'en 2027-2028 pour les établissements les plus complexes. Les ressources TIBER-EU disponibles sur le site de la Banque Centrale Européenne constituent la référence pour les tests TLPT avancés, complétant les orientations ABE spécifiques à DORA accessibles sur eba.europa.eu.

Pour les établissements financiers qui souhaitent approfondir leur compréhension des enjeux de résilience cloud dans le contexte DORA, notre analyse de la certification SecNumCloud 2026 et notre guide sur la forensique CloudTrail AWS constituent des ressources complémentaires pour sécuriser et auditer les environnements cloud sur lesquels reposent les systèmes financiers critiques. Notre analyse NIS2 Phase 2 apporte enfin un éclairage sur les synergies et différences entre DORA et NIS2 pour les entités soumises aux deux régimes simultanément — une situation commune dans les groupes financiers dont les filiales opèrent dans des secteurs couverts par NIS2 mais pas par DORA.

La trajectoire de maturité DORA pour les prochaines années s'orientera vers trois axes prioritaires selon les retours des superviseurs européens : premièrement, l'industrialisation du registre ICT avec des outils automatisés permettant la mise à jour en temps quasi-réel et la détection proactive des nouveaux sous-traitants critiques introduits par les prestataires de premier rang ; deuxièmement, le développement d'une véritable capacité de TLPT domestique en France avec davantage de prestataires certifiés TIBER capables de réaliser ces tests complexes à des coûts raisonnables pour les établissements de taille intermédiaire ; troisièmement, la normalisation des échanges d'informations sur les cybermenaces dans le secteur financier via des plateformes et des formats standardisés qui facilitent la contribution et la consommation d'intelligence sur les menaces sans surcharger les équipes sécurité des établissements contributeurs. Ces évolutions, combinées à la montée en régime des contrôles ACPR-AMF,

façonneront la conformité DORA du secteur financier français au cours des prochains exercices de supervision.

En matière de budget et de ressources pour la conformité DORA, les établissements financiers français ont consacré en moyenne entre 0,8 % et 1,5 % de leur budget IT annuel à la mise en conformité DORA en 2024-2025. Ce chiffre représente des investissements conséquents pour les grands groupes bancaires et des efforts significatifs en proportion de leurs ressources pour les établissements de taille intermédiaire. La majorité de ces investissements a porté sur : la mise à niveau des outils de gestion des risques TIC (GRC — Governance, Risk and Compliance), la révision des contrats ICT avec intégration des clauses DORA, la construction ou l'amélioration du registre ICT des tiers, et les programmes de formation des équipes et de la direction. Les investissements dans le TLPT et les tests de résilience avancés représentent une part moindre du budget global mais des coûts unitaires très élevés concentrés sur un nombre restreint d'entités désignées.

Pour les années 2026-2028, les priorités d'investissement DORA se déplacent vers l'automatisation et l'outillage : des solutions de gestion des risques ICT tiers (TPRM — Third Party Risk Management) intégrant les spécificités du registre DORA, des plateformes de gestion des incidents ICT avec workflow de notification réglementaire automatisé, et des outils de monitoring de la conformité contractuelle permettant de détecter automatiquement les contrats ICT arrivant à renouvellement qui nécessitent une mise à jour avec les clauses DORA. Cette industrialisation de la conformité DORA est la clé de la soutenabilité à long terme du programme de conformité pour les établissements financiers qui ne peuvent pas se permettre de mobiliser des équipes nombreuses de manière permanente sur des tâches de conformité manuelles et répétitives.

L'écosystème des prestataires spécialisés dans la conformité DORA s'est rapidement structuré en France depuis 2023. Les grands cabinets d'audit et de conseil (Deloitte, KPMG, PwC, EY, Mazars) ont développé des offres DORA complètes allant du diagnostic de conformité au déploiement du registre ICT et à l'accompagnement des TLPT. Des spécialistes plus ciblés (cabinets de cybersécurité, experts en gestion des risques TIC, fournisseurs de solutions GRC) complètent l'offre pour les besoins plus techniques ou plus spécialisés. Les établissements financiers de taille intermédiaire qui n'ont pas pu se permettre un accompagnement complet dès 2023 commencent à rattraper leur retard en 2026 en s'appuyant sur les guides publiés par les AES, les bonnes pratiques partagées au sein des associations professionnelles, et des

accompagnements ciblés sur les points de conformité les plus critiques comme le registre ICT et les procédures de notification d'incidents qui sont systématiquement vérifiés lors des contrôles ACPR et AMF dans le cadre de la supervision DORA.

Il convient aussi de noter que DORA a engendré une transformation positive dans la culture de la résilience opérationnelle des établissements financiers français : la résilience numérique est désormais traitée au même niveau d'attention que les risques de crédit et les risques de marché dans les comités de risque des conseils d'administration, avec des reportings réguliers incluant des indicateurs quantitatifs sur la disponibilité des systèmes critiques, le délai moyen de détection et de résolution des incidents ICT, et l'état d'avancement de la conformité aux cinq piliers. Cette élévation de la résilience numérique dans l'agenda des organes de gouvernance est sans doute la contribution la plus durable de DORA à la sécurité du secteur financier européen, au-delà des obligations documentaires et des contrôles réglementaires qui constituent l'aspect le plus visible mais pas nécessairement le plus transformateur du règlement.