AYI NEDJIMI Consultants

DORA 2026 : Premier Bilan et Contrôles ACPR - Guide Complet

Catégorie : Conformité Lecture : 14 min Publié le : 19/01/2026 Auteur : Ayi NEDJIMI

Guide complet DORA 2026 : premier bilan après un an d. Guide technique complet avec recommandations pratiques et outils pour les professionnels de.

DORA 2026 : Premier Bilan et Contrôles ACPR - Guide Complet constitue un enjeu majeur pour les professionnels de la sécurité informatique et les équipes techniques. Ce guide détaillé sur dora 2026 bilan conformite propose une méthodologie structurée, des outils éprouvés et des recommandations opérationnelles directement applicables. L'objectif est de fournir aux praticiens — consultants, ingénieurs sécurité, administrateurs systèmes — les connaissances et les techniques nécessaires pour aborder ce sujet avec rigueur. Chaque section s'appuie sur des retours d'expérience terrain et intègre les évolutions les plus récentes du domaine. Les recommandations présentées sont adaptées aux environnements d'entreprise et tiennent compte des contraintes opérationnelles réelles.

1 Introduction : DORA un an après

Le règlement qui a transformé la finance européenne

Le 17 janvier 2025 marquait l'entrée en application du **règlement** européen 2022/2554, plus connu sous l'acronyme DORA (Digital Operational Resilience Act). Un an après, le secteur financier européen a profondément évolué dans sa gestion des risques liés aux technologies de l'information et de la communication (TIC). Ce règlement, directement applicable dans tous les États membres sans transposition, a imposé un changement de référence majeur. Guide

complet DORA 2026 : premier bilan après un an d. Guide technique complet avec recommandations pratiques et outils pour les professionnels de. Ce guide couvre les aspects essentiels de dora 2026 bilan conformite : méthodologie structurée, outils recommandés et retours d'expérience opérationnels. Les professionnels y trouveront des recommandations directement applicables.

> DORA ne se contente pas d'exiger une conformité documentaire : il impose une véritable transformation opérationnelle. Les **entités** financières doivent désormais démontrer leur capacité à maintenir leurs fonctions critiques face à des perturbations TIC majeures, qu'il s'agisse de cyberattaques, de défaillances de prestataires ou de catastrophes naturelles affectant les infrastructures numériques.
>
> Ce guide dresse le bilan de cette première année d'application, analyse les retours des contrôles superviseurs et propose une feuille de route pour les organisations qui doivent encore renforcer leur conformité ou anticiper les évolutions réglementaires à venir.

Périmètre et entités concernées

DORA s'applique à un large spectre d'entités financières : établissements de crédit, entreprises d'investissement, établissements de paiement et de monnaie électronique, sociétés de gestion d'actifs, entreprises d'assurance et de réassurance, institutions de retraite professionnelle, agences de notation de crédit, et bien d'autres acteurs du secteur financier.

Fait notable, **le règlement** introduit également un cadre de surveillance directe pour les prestataires tiers critiques de services TIC (CTPP - Critical Third-Party Providers). Pour la première fois, des fournisseurs de cloud computing ou de services technologiques peuvent être soumis à une supervision européenne coordonnée s'ils sont désignés comme critiques pour le secteur financier.

En France, l'ACPR (Autorité de Contrôle Prudentiel et de Résolution) et l'AMF (Autorité des Marchés Financiers) assurent conjointement la supervision de l'application de DORA, avec des compétences réparties selon les types d'entités. Cette double supervision nécessite une coordination étroite entre les régulateurs et impose aux entités une veille réglementaire attentive.

22 000+
Entités financières concernées dans l'UE

5
Piliers de résilience opérationnelle numérique

17/01/25
Date d'entrée en application

Notre avis d'expert
La conformité réglementaire est un marathon, pas un sprint. Trop d'organisations traitent la certification comme un projet ponctuel plutôt qu'un processus continu d'amélioration. Sans appropriation par les équipes opérationnelles, le système de management reste un document mort.

Votre registre des traitements est-il à jour et reflète-t-il la réalité opérationnelle ?

2 Bilan de la première année d'application

Un démarrage contrasté selon les acteurs

Le premier constat après un an d'application de DORA est la grande hétérogénéité des niveaux de maturité entre les entités financières. Les grandes banques systémiques et les assureurs majeurs, disposant de ressources importantes et habitués aux exigences réglementaires strictes, ont généralement atteint un niveau de conformité satisfaisant sur les aspects fondamentaux du règlement.

En revanche, les structures de taille intermédiaire et les nouveaux acteurs (fintechs, insurtechs, néobanques) ont rencontré des difficultés significatives. Le principe de proportionnalité prévu par DORA, censé adapter les exigences à la taille et au profil de risque des entités, s'est révélé plus complexe à appliquer que prévu. Plusieurs entités ont sous-estimé les ressources nécessaires pour atteindre la conformité.

Les prestataires TIC critiques (CTPP) désignés par les autorités européennes de surveillance ont dû s'adapter à un cadre de supervision entièrement nouveau. Les premiers contrôles sur ces acteurs ont révélé des lacunes dans la documentation de leurs procédures de continuité d'activité et dans leur capacité à fournir les informations requises aux entités financières clientes.

Chronologie DORA : Du Règlement à la Supervision Active

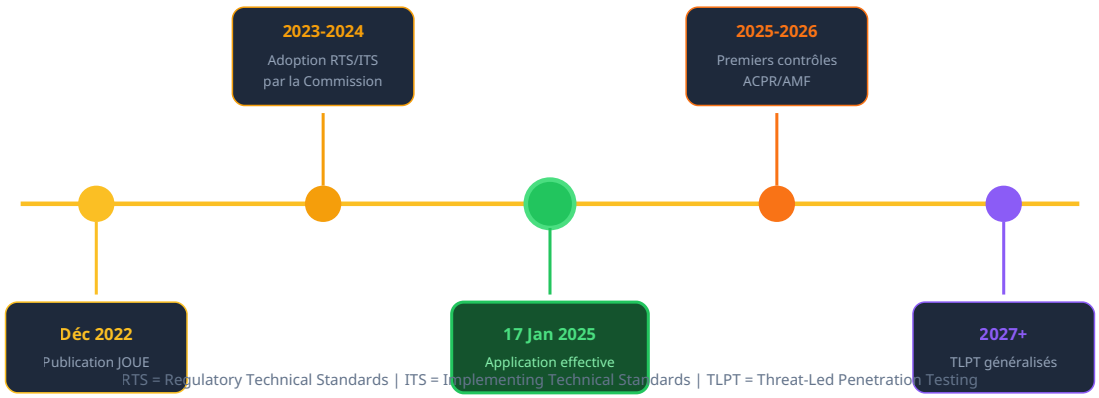

Figure 1 : Les jalons clés de DORA depuis sa publication jusqu'à la supervision renforcée

Statistiques clés des premiers contrôles

Les données agrégées des premières campagnes de contrôle révèlent des tendances préoccupantes. Environ 35% des entités contrôlées présentaient des insuffisances significatives dans leur cadre de gestion des risques TIC. Les principales lacunes concernaient la documentation des procédures, l'identification exhaustive des actifs TIC critiques et la formalisation des plans de réponse aux incidents.

Le registre des accords TIC, exigence centrale de DORA, s'est révélé particulièrement problématique. Plus de 40% des entités n'avaient pas un registre conforme aux exigences du règlement technique RTS 2024/XXX. Les difficultés portaient sur l'exhaustivité des informations relatives aux prestataires, la classification des fonctions sous-traitées et l'évaluation des risques de concentration.

Sur le volet des tests, la situation est contrastée. Si les tests de continuité d'activité sont généralement effectués, les tests de pénétration avancés (TLPT) restent insuffisamment déployés, même parmi les entités qui y seront soumises obligatoirement. Les régulateurs ont souligné l'importance d'anticiper ces exigences plutôt que d'attendre les échéances.

3 Les 5 piliers en pratique

DORA s'articule autour de cinq piliers fondamentaux qui structurent l'approche de résilience opérationnelle numérique. Chacun de ces piliers comporte des exigences spécifiques détaillées dans **le règlement** et précisées par les normes techniques réglementaires (RTS) adoptées par la Commission **européenne**. Pour approfondir, consultez ISO 27001:2022 - Guide Complet de Certification et Mise e....

Les 5 Piliers de la Résilience Opérationnelle DORA

Figure 2 : Structure des 5 piliers fondamentaux de DORA

Pilier 1 : Gestion des risques TIC

Le premier pilier impose aux entités financières d'établir un cadre complet de gestion des risques TIC. Ce cadre doit être approuvé par l'organe de direction, qui assume la responsabilité finale de la gestion des risques TIC. Les entités doivent notamment identifier et documenter tous leurs actifs TIC, établir une cartographie des risques, définir des politiques de sécurité de l'information et mettre en place des mesures de protection adaptées.

La gouvernance TIC exigée par DORA va au-delà des pratiques habituelles. L'organe de direction doit recevoir des rapports réguliers sur la situation des risques TIC, approuver la stratégie de résilience opérationnelle numérique et s'assurer de l'allocation de ressources suffisantes. Au moins un membre de l'organe de direction doit disposer de compétences TIC suffisantes.

Pilier 2 : Gestion des incidents TIC

DORA impose un processus structuré de gestion des incidents TIC comprenant la détection, la classification, le traitement et la notification. Les incidents majeurs doivent être notifiés à l'autorité compétente selon un calendrier précis : notification initiale dans les 4 heures suivant la classification comme incident majeur, rapport intermédiaire dans les 72 heures et rapport final dans le mois.

La classification des incidents repose sur des critères définis dans les RTS : nombre de clients affectés, durée de l'incident, étendue géographique, pertes financières, impact réputationnel et criticité des services touchés. Les entités doivent tenir un registre de tous les incidents TIC, majeurs ou non, et en tirer des enseignements pour améliorer leur résilience.

Pilier 3 : Tests de résilience opérationnelle

Toutes les entités financières doivent déployer un programme de tests de résilience opérationnelle numérique. Ce programme comprend des tests annuels (analyses de vulnérabilités, tests de performance, tests de continuité) et, pour les entités significatives, des tests de pénétration avancés (TLPT - Threat-Led Penetration Testing) au moins tous les trois ans. Les recommandations de CNIL constituent une reference essentielle.

Les TLPT constituent une innovation majeure de DORA. Ces tests, basés sur le cadre TIBER-EU, simulent des attaques réalistes par des équipes spécialisées (red teams) ciblant les fonctions critiques de l'entité. Les scénarios sont élaborés à partir de renseignements sur les menaces (threat intelligence) et doivent être validés par l'autorité compétente. Les recommandations de ENISA constituent une reference essentielle.

Cas concret
Clearview AI a été condamnée à des amendes cumulées de plus de 50 millions d'euros par plusieurs autorités européennes pour collecte massive de données biométriques sans consentement. Cette affaire a posé les jalons de la régulation de la reconnaissance faciale en Europe et a alimenté le débat sur l'AI Act.

4 Registre des accords TIC

Point de vigilance ACPR
Le registre des accords TIC est l'un des points les plus contrôlés lors des inspections. L'exhaustivité et la qualité des informations sont essentielles : identification des prestataires, fonctions sous-traitées, localisation des données, évaluation des risques et plans de sortie.

Structure et contenu du registre

L'article 28 de DORA impose aux entités financières de tenir un registre d'informations actualisé de tous leurs accords contractuels portant sur l'utilisation de services TIC fournis par des prestataires tiers. Ce registre doit permettre une vision complète de l'écosystème TIC externalisé et faciliter la supervision par les autorités compétentes.

Le RTS associé détaille les informations minimales à renseigner : identification du prestataire (raison sociale, LEI, pays d'établissement), description des services fournis, classification des fonctions (critiques/importantes ou non), localisation des données et des centres de traitement, clauses contractuelles clés (audit, résiliation, sous-traitance), et évaluation des risques associés.

Une attention particulière doit être portée à l'analyse des risques de concentration. DORA exige d'identifier les situations où plusieurs fonctions critiques dépendent d'un même prestataire ou d'un nombre limité de prestataires. Cette analyse doit également couvrir les risques liés à la sous-traitance en cascade par les prestataires directs.

Reporting aux autorités

Le registre doit être transmis aux autorités compétentes sur demande ou selon des périodicités définies. En France, l'ACPR a mis en place un portail dédié pour la collecte de ces informations. Le format de transmission suit le template standardisé européen, facilitant l'agrégation et l'analyse au niveau de l'Union.

Les autorités utilisent ces données pour identifier les prestataires susceptibles d'être désignés comme critiques (CTPP) et pour évaluer les risques systémiques liés à la concentration. Les entités doivent donc s'assurer de la cohérence et de l'exactitude des informations déclarées, sous peine de sanctions.

Catégorie	Informations requises	Fréquence MAJ
Identification prestataire	LEI, raison sociale, pays, groupe	À chaque changement
Services fournis	Description, fonctions supportées, criticité	Annuelle minimum
Localisation données	Pays stockage, traitement, support	À chaque changement
Sous-traitance	Chaîne complète, pays, fonctions	À chaque changement
Évaluation risques	Concentration, continuité, réversibilité	Annuelle

Comment démontrez-vous l'accountability exigée par le RGPD en cas de contrôle ?

5 Tests de résilience opérationnelle

Programme de tests annuels

DORA impose à toutes les entités financières de maintenir un programme de tests de résilience opérationnelle numérique. Ce programme doit être proportionné à la taille de l'entité, à son profil de risque et à la criticité de ses services. Il comprend obligatoirement des tests de base : analyses de vulnérabilités, évaluations de la sécurité des réseaux, tests de performance et de charge, tests de pénétration et tests de continuité d'activité.

Les tests doivent couvrir l'ensemble des systèmes et applications TIC supportant des fonctions critiques ou importantes. Les résultats doivent être documentés, analysés et donner lieu à des plans de remédiation avec des échéances définies. L'organe de direction doit être informé des résultats significatifs et valider les plans d'action.

Tests TLPT avancés

Les entités financières identifiées comme significatives par les autorités compétentes doivent réaliser des tests de pénétration avancés fondés sur la menace (TLPT) au moins tous les trois ans. Ces tests simulent des cyberattaques réalistes menées par des équipes de hackers éthiques (red teams) utilisant les mêmes techniques que des attaquants réels.

Le processus TLPT se déroule en plusieurs phases : définition du **périmètre** avec l'autorité compétente, élaboration de scénarios basés sur des renseignements de menace (threat intelligence), exécution des tests sur une période étendue, et restitution détaillée avec plan de remédiation. L'autorité compétente doit valider le prestataire de tests et les scénarios avant leur exécution. Pour approfondir, consultez PCI DSS 4.0.1 en 2026 : Retour d'Expérience et Guide.

Processus de Test TLPT (Threat-Led Penetration Testing)

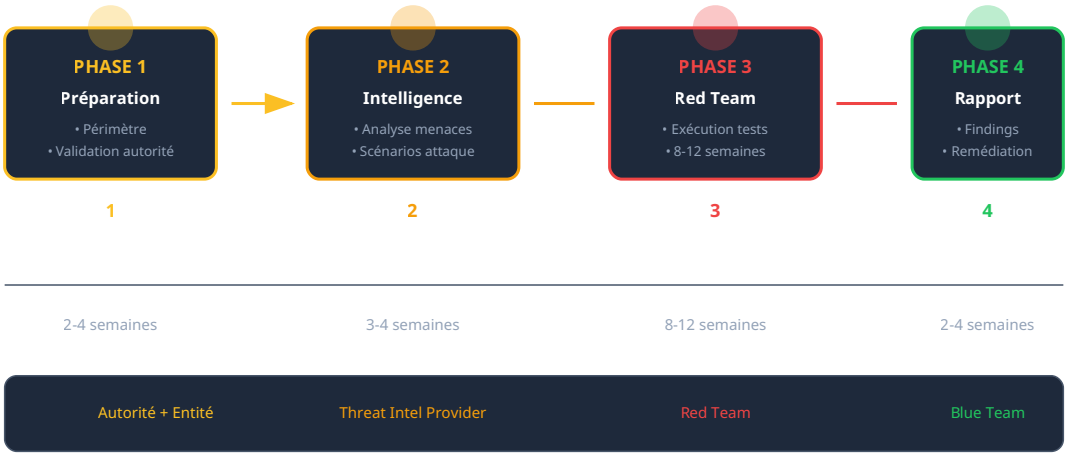

Figure 3 : Déroulement d'un test TLPT selon le framework TIBER-EU Pour approfondir, consultez SecNumCloud 2026 et Schéma EUCS : Guide Complet Qualification Cloud Souverain.

Reconnaissance mutuelle des tests

DORA introduit un mécanisme de reconnaissance mutuelle des tests TLPT entre États membres. Lorsqu'un groupe financier réalise un TLPT sur une infrastructure partagée, les autorités compétentes des différents pays peuvent convenir de reconnaître ce test pour les entités locales du groupe, évitant ainsi la multiplication des tests sur les mêmes systèmes.

Ce mécanisme facilite la conformité des groupes pan-européens tout en maintenant un niveau élevé d'exigence. Il nécessite une coordination étroite entre autorités et une documentation précise du **périmètre et** des conditions de réalisation des tests.

6 Gestion et notification des incidents

Processus de gestion des incidents TIC

DORA impose aux entités financières de configurer un processus complet de gestion des incidents TIC couvrant la détection, l'enregistrement, la classification, l'escalade, la résolution et la communication. Ce processus doit être formalisé dans une politique dédiée approuvée par l'organe de direction et régulièrement testée.

La détection précoce est essentielle. Les entités doivent déployer des capacités de surveillance permettant d'identifier rapidement les anomalies et les comportements suspects. Les sources incluent les systèmes de détection d'intrusion (IDS/IPS), les SIEM, les outils d'analyse comportementale (UEBA) et les remontées utilisateurs.

Classification des incidents majeurs

Un incident TIC est classé comme majeur s'il atteint certains seuils définis par les RTS. Ces seuils concernent notamment : le nombre de clients affectés (direct ou indirect), la durée de l'indisponibilité des services, l'étendue géographique de l'impact, les pertes financières estimées, l'impact sur les marchés financiers et la perte potentielle de données.

Délais de notification impératifs

- T+4h : Notification initiale après classification comme incident majeur
- T+72h : Rapport intermédiaire avec analyse préliminaire
- T+1 mois : Rapport final avec analyse des causes et mesures correctives

Template de notification

Les notifications aux autorités compétentes suivent un format standardisé défini par les ITS. La notification initiale doit contenir : l'identification de l'entité, la date et l'heure de détection, la nature de l'incident, les services affectés, une première estimation de l'impact et les mesures de confinement initiées.

Le rapport intermédiaire approfondit l'analyse avec les causes probables identifiées, l'étendue réelle de l'impact, les mesures de remédiation en cours et une estimation actualisée des délais de résolution. Le rapport final fournit l'analyse complète des causes racines, les mesures correctives mises en œuvre et les enseignements tirés pour prévenir la récurrence.

7 Contrôles ACPR : points de vigilance

Méthodologie de contrôle

L'ACPR a adapté sa méthodologie de contrôle pour intégrer les exigences DORA. Les inspections sur place combinent désormais l'analyse documentaire traditionnelle avec des tests techniques permettant de vérifier l'effectivité des dispositifs déclarés. Les équipes de contrôle incluent des spécialistes IT capables d'évaluer la pertinence des architectures et des mesures de sécurité.

Les contrôles permanents (sur pièces) ont également été renforcés avec des demandes périodiques de reportings standardisés : registre TIC, tableaux de bord des incidents, résultats des tests de résilience et indicateurs clés de risque. La cohérence entre ces différentes sources est systématiquement vérifiée.

Points de vigilance identifiés

Les premiers retours des contrôles ACPR ont mis en lumière plusieurs zones de faiblesse récurrentes. La gouvernance TIC reste souvent insuffisante : implication limitée de l'organe de direction, absence de compétences TIC au sein du conseil, reporting inadapté. Les entités doivent renforcer la culture cyber au plus haut niveau.

La cartographie des actifs TIC manque fréquemment d'exhaustivité. Les shadow IT, les applications métiers développées localement et les interconnexions avec les filiales échappent souvent à l'inventaire. Or, DORA exige une vision complète pour évaluer correctement les risques.

Les plans de continuité d'activité (PCA) et de reprise d'activité (PRA) présentent des lacunes récurrentes : scénarios insuffisamment variés, tests partiels ne couvrant pas les fonctions critiques, absence de test intégrant les prestataires clés. L'ACPR attend des exercices réalistes et complets.

Grille de Contrôle ACPR - Points de Vigilance DORA

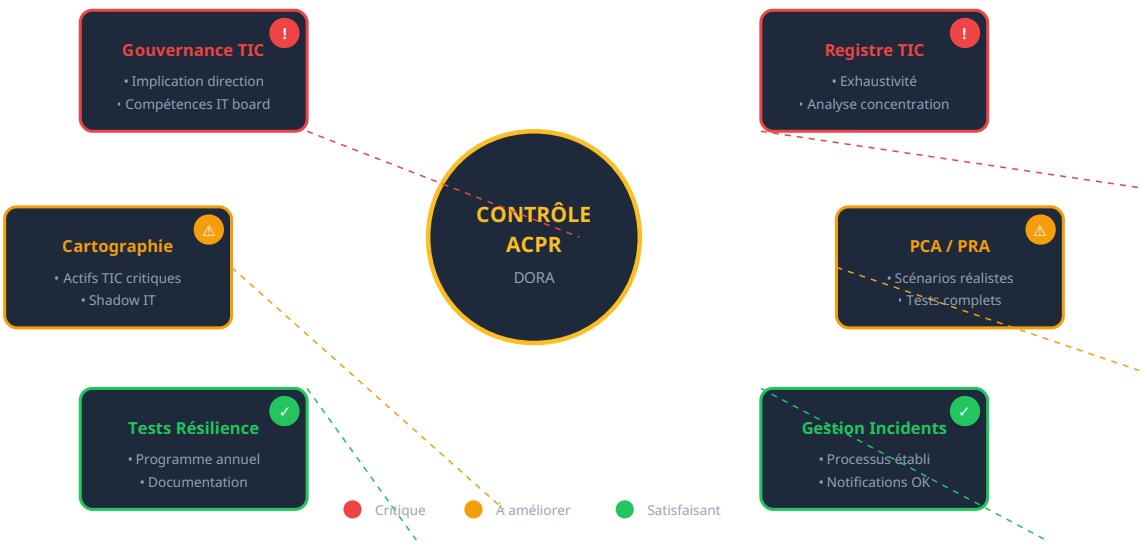

Figure 4 : Principaux points de vigilance relevés lors des contrôles ACPR sur DORA

8 Gestion des prestataires TIC tiers

Due diligence renforcée

DORA impose une due diligence approfondie avant de recourir à un prestataire TIC tiers pour des fonctions critiques ou importantes. Cette évaluation doit couvrir la capacité technique du prestataire, sa solidité financière, son organisation de la sécurité de l'information, ses certifications (ISO 27001, SOC 2), sa conformité réglementaire et sa réputation sur le marché.

L'analyse doit également porter sur la chaîne de sous-traitance. Le prestataire doit fournir des informations sur ses propres sous-traitants intervenant dans la prestation, leur localisation et les fonctions qu'ils assurent. L'entité financière doit pouvoir s'opposer à certains sous-traitants ou exiger des garanties supplémentaires.

Clauses contractuelles obligatoires

Les contrats avec les prestataires TIC tiers doivent inclure des clauses spécifiques prévues par DORA : droit d'audit de l'entité financière et des autorités de supervision, obligation de notification des incidents affectant le service, conditions de résiliation et d'assistance à la réversibilité, garanties de localisation des données et de protection des informations confidentielles. Pour approfondir, consultez Sécurité LLM Adversarial : Attaques, Défenses et Bonnes.

Pour les fonctions critiques ou importantes, des clauses supplémentaires sont requises : niveaux de service garantis (SLA) avec pénalités, plans de continuité d'activité du prestataire, tests de résilience conjoints, reporting périodique détaillé et mécanismes d'escalade en cas de défaillance.

Stratégies de sortie

DORA exige que les entités financières disposent de stratégies de sortie documentées pour chaque prestataire supportant des fonctions critiques. Ces stratégies doivent prévoir les conditions de migration vers un autre prestataire ou d'internalisation, les délais de préavis nécessaires, les formats de récupération des données et les ressources à mobiliser.

La testabilité des stratégies de sortie est un point d'attention des régulateurs. Les entités doivent pouvoir démontrer qu'elles ont les compétences et les ressources pour exécuter ces plans en cas de besoin, par exemple en maintenant une documentation technique à jour ou en conservant des compétences internes sur les systèmes externalisés.

9 Erreurs fréquentes et pièges à éviter

Erreur 1 : Approche purement documentaire
De nombreuses entités ont abordé DORA comme un exercice de conformité documentaire, produisant des politiques et procédures sans les implémenter effectivement. Les régulateurs testent l'opérationnalité des dispositifs, pas seulement leur existence sur papier. Les contrôles incluent des tests techniques et des mises en situation.

Erreur 2 : Sous-estimation du périmètre TIC
L'inventaire des actifs TIC se limite souvent aux systèmes centraux, omettant les applications métiers, les outils collaboratifs, les connexions avec les prestataires et le shadow IT. Un périmètre incomplet conduit à des angles morts dans la gestion des risques et à des non-conformités lors des contrôles.

Erreur 3 : Gouvernance TIC déconnectée
Le cadre de gouvernance TIC reste parfois une structure formelle sans lien réel avec les décisions opérationnelles. L'organe de direction reçoit des rapports mais ne les challenge pas. Les comités de risque TIC n'ont pas de pouvoir décisionnel effectif. DORA exige une gouvernance active et impliquée.

Erreur 4 : Tests insuffisamment réalistes
Les tests de continuité se limitent souvent à des exercices partiels sur des environnements de test, sans impliquer les prestataires clés ni simuler des scénarios de crise réels. DORA attend des tests complets incluant la chaîne de valeur et des scénarios variés (cyberattaque, défaillance prestataire, catastrophe).

Erreur 5 : Registre TIC incomplet
Le registre des accords TIC présente fréquemment des lacunes : prestataires non référencés, informations de localisation manquantes, analyse de concentration absente, évaluation des risques superficielle. Ce registre étant un outil central de supervision, son incomplétude expose à des sanctions.

10 Feuille de route 2026-2027

Priorités immédiates (S1 2026)

Les entités présentant des lacunes significatives doivent agir sans délai. Les priorités du premier semestre 2026 concernent la mise en conformité du registre TIC (exhaustivité, qualité des données, analyse de concentration), le renforcement de la gouvernance TIC (implication effective de l'organe de direction, reporting adapté) et la formalisation des stratégies de sortie pour les prestataires critiques.

Les entités doivent également s'assurer de la conformité de leurs contrats avec les prestataires TIC. Les clauses DORA obligatoires doivent être intégrées, par avenant si nécessaire. Cette mise à jour contractuelle peut prendre plusieurs mois de négociation avec certains grands prestataires.

Consolidation (S2 2026)

Le second semestre doit permettre de consolider les fondamentaux et d'améliorer la maturité opérationnelle. Les tests de résilience doivent être étendus pour couvrir l'ensemble des fonctions critiques et inclure les prestataires clés. Les processus de gestion des incidents doivent être testés et affinés. La formation et la sensibilisation des équipes doivent être renforcées.

C'est également la période pour anticiper les exigences à venir. Les entités susceptibles d'être soumises aux TLPT doivent engager les préparatifs : sélection des prestataires, définition du périmètre préliminaire, renforcement des capacités de détection (blue team) pour tirer pleinement parti des tests.

Excellence opérationnelle (2027+)

À partir de 2027, l'objectif est d'atteindre l'excellence opérationnelle. La résilience numérique doit être intégrée dans la culture de l'organisation, avec des processus matures et continuellement améliorés. Les premiers cycles TLPT seront achevés et leurs enseignements intégrés. Le partage d'informations sur les menaces (pilier 5) devra être effectif.

Les régulateurs européens prévoient également des évolutions du cadre réglementaire. Des guidelines complémentaires sont attendues, ainsi que des clarifications sur certains aspects techniques. Les entités doivent maintenir une veille active et une capacité d'adaptation pour intégrer ces évolutions.

Besoin d'accompagnement DORA ?

Nos experts vous accompagnent dans l'évaluation de votre conformité DORA, l'élaboration de votre feuille de route et la mise en œuvre opérationnelle des exigences du règlement.

Demander un diagnostic DORA
Pour approfondir ce sujet, consultez notre outil open-source iso27001-toolkit qui facilite l'accompagnement à la certification ISO 27001.

Questions frequentes

Comment ce sujet impacte-t-il la securite des organisations ?

Ce sujet a un impact significatif sur la securite des organisations car il touche aux fondamentaux de la protection des systemes d'information. Les entreprises doivent evaluer leur exposition, installer des mesures preventives adaptees et former leurs equipes pour faire face aux risques associes a cette problematique.

Quelles sont les bonnes pratiques recommandees par les experts ?

Pourquoi est-il important de se former sur ce sujet en 2026 ?

En 2026, la maitrise de ce sujet est devenue incontournable face a l'evolution constante des menaces et des exigences reglementaires. Les professionnels de la cybersecurite doivent maintenir leurs competences a jour pour proteger efficacement les actifs numeriques de leur organisation et repondre aux obligations de conformite.

Sources et références : CNIL · ANSSI

Conclusion

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr