

Conformité numérique dans l'UE

Guide pratique

Actions et preuves pour neuf textes européens

SCAI – Swiss Cyber AI | 8 octobre 2026 | www.swisscyberai.org

Un outil pour la sécurité, l'IT, le juridique, la protection des données, les achats et les métiers. Définir le périmètre, attribuer les responsabilités, combler les lacunes urgentes, tester les contrôles et conserver les preuves.

Utiliser ce guide en trois séances de travail

Séance	Travail à réaliser	Résultat attendu
1 Délimiter 60 minutes	Le juridique et les métiers examinent les textes et les questions de périmètre aux pages 2 et 3.	Une fiche de périmètre approuvée par entité ou service.
2 Attribuer 90 minutes	Les responsables identifient les lacunes avec les pages 4 à 16 et la revue fournisseurs en page 20.	Actions, responsables, échéances et preuves attendues.
3 Démontrer Une demi-journée	Simuler les notifications, restaurer un service et vérifier des preuves. Utiliser les pages 17 à 23.	Résultats des tests et plan de 90 jours financé.

Trouver la bonne rubrique

Pages	Outils de travail
2 à 6	Tableau des textes avec liens, périmètre, responsabilités et contrôles communs
7 à 16	NIS2 et listes de contrôle pratiques pour les neuf textes
17 à 19	Gestion des incidents et délais de notification
20 à 23	Revue fournisseurs, plan de 90 jours et fiches réutilisables
24	Échéances et sources officielles complémentaires

Mode d'emploi : Les références roses soulignées ouvrent l'article ou le paragraphe sur EUR-Lex ; les points sont indiqués dans le libellé. « Appui » relie une recommandation à son objectif juridique, sans rendre la méthode ou la cible obligatoire. Les citations sont de courts extraits officiels ; lire la disposition complète pour ses conditions.

Appliquer chaque obligation selon son périmètre, le rôle et sa date d'application. Ajouter les règles nationales et sectorielles. Responsables proposés, tests et plan de 90 jours sont des recommandations ; ce guide ne certifie pas la conformité.

Textes européens et liens officiels

Ouvrir le texte dans la dernière colonne. Sur EUR-Lex, vérifier la version consolidée actuelle, les modifications et les actes d'exécution applicables. Les pages suivantes expliquent leur mise en œuvre.

Texte	Quand l'examiner	Premier livrable	Texte officiel UE
RGPD	Traitement de données personnelles dans le champ territorial de l'article 3.	Registre des traitements et des flux de données.	Règlement 2016/679 Art. 3, 5, 24, 28, 30 à 35
NIS2	Secteur ou service couvert, seuils de taille et exceptions. Application selon le droit national.	Classification de l'entité et circuit local de notification.	Directive 2022/2555 Art. 2 à 4, 20, 21, 23, 26
DORA	Entités financières visées. Régime distinct pour les prestataires TIC critiques désignés.	Cadre TIC et registre fournisseurs.	Règlement 2022/2554 Art. 2, 5 à 16, 19, 24 à 30
Règlement IA	Fourniture ou déploiement d'IA dans le champ du texte. Les obligations dépendent du rôle et de la finalité.	Inventaire et classification des IA.	Règlement 2024/1689 Art. 2 à 6, 16, 26, 50, 53, 113
CRA	Matériels ou logiciels couverts mis à disposition sur le marché de l'UE.	Périmètre produit et procédure de notification des vulnérabilités.	Règlement 2024/2847 Art. 2, 13, 14, 32, 69, 71; annexe I
CER	Entités identifiées comme critiques selon le droit national.	Décision de désignation et plan de risques tous aléas.	Directive 2022/2557 Art. 6, 8, 12 à 15
Data Act	Données de produits connectés, services connexes, partage de données ou services de traitement.	Procédure d'accès aux données et sortie du cloud testée.	Règlement 2023/2854 Art. 1 à 5, 13, 23 à 31, 50
eIDAS	Identité, signatures, cachets électroniques et services de confiance ; obligations selon le rôle.	Politique de signature et validation du service de confiance.	Règlement 910/2014 Modifié par 2024/1183
DSA	Services intermédiaires proposés dans l'UE ; obligations selon le type et la taille du service.	Classification du service et procédure de signalement.	Règlement 2022/2065 Art. 2, 11 à 18, 19 à 32, 33

Lire le règlement IA avec le règlement (UE) 2026/1744, qui modifie le calendrier et certaines obligations. La consolidation eIDAS intègre l'identité numérique européenne. Pour NIS2 et CER, référencer aussi la transposition nationale.

Références juridiques [Modification du règlement IA 2026/1744](#) | [Modification eIDAS 2024/1183](#)

Déterminer les textes applicables

Documenter le périmètre par entité juridique et activité. Une qualification globale du groupe ne suffit pas. Un siège suisse ne détermine pas le statut des filiales européennes, des produits commercialisés dans l'UE ou des services proposés dans l'UE.

Questions dans cet ordre	À consigner	Voir
1 Quelle entité et quelle activité ?	Raison sociale, pays, établissement, service, produit, clients et lien avec l'UE. NIS2 Art. 26 · RGPD Art. 3 · DSA Art. 2(1)	Ouvrir une fiche en page 22.
2 Des données personnelles sont-elles traitées ?	Rôle de responsable du traitement ou sous-traitant, personnes concernées et analyse territoriale de l'article 3. RGPD Art. 3 · RGPD Art. 4(7) · RGPD Art. 4(8)	RGPD en page 9.
3 L'entité relève-t-elle d'un secteur couvert ?	Services réels, catégorie NIS2 de l'annexe I ou II, taille selon les règles UE, exceptions et droit national. NIS2 Art. 2 · NIS2 annexe I · NIS2 annexe II	NIS2 aux pages 7 et 8.
4 Est-ce une entité financière réglementée ?	Catégorie exacte de l'article 2, exclusions et éventuel régime simplifié. DORA Art. 2 · DORA Art. 16	DORA en page 10.
5 L'entité fournit-elle ou utilise-t-elle de l'IA ?	Finalité, rôle de fournisseur ou déployeur ; interdictions, haut risque, transparence et IA à usage général (GPAI). Règl. IA Art. 2 · Règl. IA Art. 5 · Règl. IA Art. 6	Règlement IA en page 11.
6 Des produits numériques sont-ils vendus ?	Rôle de fabricant, importateur ou distributeur, périmètre produit, exclusions et mise sur le marché UE. CRA Art. 2 · CRA Art. 3 · CRA Art. 32	CRA en page 12.
7 Existe-t-il une notification de désignation critique ?	Désignation, date de réception, service couvert et exclusions sectorielles. CER Art. 6(3) · CER Art. 8	CER en page 13.
8 Quels services de données ou en ligne existent ?	Produits connectés, cloud, services de confiance, hébergement utilisateur ou places de marché. Data Act Art. 1 · eIDAS Art. 2 · DSA Art. 3(g)	Pages 14 à 16.

Approuver une conclusion vérifiable

Retenir l'un des quatre statuts : applicable maintenant ; applicable à une date donnée ; non applicable avec motifs ; à clarifier avec réviseur et échéance. Joindre les faits et la disposition justifiant la conclusion.

Le contrat fournisseur constitue une source d'obligations distincte. Un client réglementé peut imposer des exigences contractuelles même si le fournisseur n'entre pas directement dans le champ du texte. Examiner l'articulation DORA/NIS2 pour l'entité financière et les obligations concernées.

Réexaminer le périmètre en cas de changement

- Nouveau pays, acquisition, service, produit, finalité IA, segment de clientèle ou notification d'une autorité.
- Changement important de taille, d'externalisation, de marque, de produit ou du texte juridique.

Références juridiques [NIS2 Art. 2 à 4](#) | [RGPD Art. 3](#) | [DORA Art. 1 et 2](#)

Attribuer les responsabilités et définir l'achèvement

La direction reste responsable des obligations que la loi lui attribue. Le CISO coordonne la sécurité ; métiers, protection des données, juridique et responsables produits assument leurs tâches. Remplacer les rôles ci-dessous par des noms.

Rôle	Responsabilité pratique	Preuve d'achèvement
Sponsor de direction	Approuver le périmètre, les priorités, les ressources et les décisions de risque majeures. Traiter les actions critiques en retard. Appui : NIS2 Art. 20(1) · DORA Art. 5(2)	Décisions datées, budget et suivi.
Juridique ou conformité	Confirmer les rôles, règles nationales, autorités et délais ; tenir le registre juridique. Appui : NIS2 Art. 2 · NIS2 Art. 23 · RGPD Art. 24(1)	Fiches de périmètre et de notification vérifiées.
CISO et opérations de sécurité	Coordonner les contrôles cyber, la détection, la réponse et la vérification. Consigner les lacunes de couverture. Appui : NIS2 Art. 21(1) · DORA Art. 5(2)(c)	Responsables des contrôles, tests et dossiers d'incident.
CIO et responsables de services	Gérer les actifs, accès, configurations, corrections et rétablissements de services. Appui : DORA Art. 8(1) · DORA Art. 9(4) · DORA Art. 12(1)	Exports de couverture et résultats de restauration.
Responsable données et DPO	Le responsable pilote le programme ; le DPO désigné conseille et contrôle en toute indépendance. Appui : RGPD Art. 24(1) · RGPD Art. 38 · RGPD Art. 39(1)	Registres, avis et demandes d'exercice des droits.
Responsable produit ou IA	Assumer le cycle de vie produit ou la finalité IA, les mises en service, la surveillance et le support. Appui : CRA Art. 13 · Règl. IA Art. 16 · Règl. IA Art. 26	Classification, autorisation de mise en service et historique.
Achats et responsable fournisseur	Évaluer les fournisseurs, obtenir les clauses requises, suivre les prestations et maintenir les plans de sortie. Appui : NIS2 Art. 21(2)(d) · DORA Art. 28	Dossier fournisseur approuvé et sortie testée.
Réviseur des contrôles	Vérifier des preuves, si possible indépendamment de l'opérateur du contrôle ; confirmer la clôture. Appui : NIS2 Art. 21(2)(f) · DORA Art. 6(6)	Constats, nouveaux tests et décisions de clôture.

Définir des critères d'achèvement stricts

- Le contrôle a un périmètre, un responsable nommé et un mode opératoire documentés.
- La mise en œuvre couvre la population visée ; les exclusions sont visibles et approuvées.
- Un test daté démontre le résultat attendu ; tout échec a une action et une échéance.
- Le lien vers la preuve fonctionne et précise l'entité, le système, la période et le réviseur.

Effectuer une brève revue mensuelle

Examiner les nouveaux périmètres, actions à risque élevé en retard, tests échoués et capacité de notification. Demander une décision précise à la direction pour financer une correction ou accepter un risque. Une revue globale au moins trimestrielle est recommandée.

Références juridiques [NIS2 Art. 20](#) | [DORA Art. 5](#) | [RGPD Art. 24 et 38](#)

Mettre en place le socle de sécurité commun

Réutiliser les contrôles NIST ou autres adaptés. Les mesures suivantes sont un point de départ pratique, pas une liste de certification UE. Définir fréquences et cibles selon le risque, puis appliquer les exigences légales ou contractuelles plus strictes.

Contrôle et action	Responsable proposé	Preuve à échantillonner
01 Inventorier services critiques, IT, cloud, OT, données et dépendances. Rapprocher la découverte du registre. Appui : NIS2 Art. 21(2)(i) · DORA Art. 8(1)	Responsables de services	Actifs non gérés et carte des dépendances.
02 Imposer une authentification forte et le moindre privilège. Séparer les comptes administrateurs ; maîtriser les accès d'urgence. Appui : NIS2 Art. 21(2)(i)-(j) · DORA Art. 9(4)(c)-(d)	Équipe identités	Tester la connexion, les privilèges et le retrait des accès au départ.
03 Prioriser les vulnérabilités selon exploitation, exposition et impact. Fixer une échéance aux exceptions. Appui : NIS2 Art. 21(2)(e) · DORA Art. 9(4)(f)	IT et OT	Suivre un constat urgent jusqu'à la correction et au nouveau test.
04 Appliquer des configurations sûres et protéger les terminaux. Inclure serveurs et appareils sans support dans les rapports de lacunes. Appui : DORA Art. 9(2)-(3) · NIS2 Art. 21(1)	Exploitation IT	Rapport de couverture et réponse à une détection testée.
05 Segmenter les systèmes critiques et protéger les accès distants. Tester l'accès fournisseur et l'isolement d'urgence. Appui : DORA Art. 9(4)(b) · NIS2 Art. 21(1)	Réseau et OT	Test des flux autorisés et exercice d'isolement approuvé.
06 Collecter les journaux utiles, surveiller les alertes et prévoir une réponse hors heures ouvrées. Appui : DORA Art. 10(1)-(3) · NIS2 Art. 21(2)(b)	Opérations de sécurité	Trace de la détection à la réponse ; escalade prise en charge.
07 Protéger les sauvegardes d'une compromission de la production. Restaurer un service métier complet. Appui : NIS2 Art. 21(2)(c) · DORA Art. 12(1)-(3)	Responsables de services	Durée réelle de restauration, intégrité des données et validation métier.
08 Évaluer fournisseurs critiques, concentration et sous-traitants ; convenir d'une assistance rapide en cas d'incident. Appui : NIS2 Art. 21(2)(d) · DORA Art. 28(4) · DORA Art. 30	Achats	Évaluation des risques, contrat et contact testé.
09 Protéger les données sensibles par les accès, le chiffrement et une conservation maîtrisée. Appui : RGPD Art. 5(1)(e)-(f) · RGPD Art. 32(1)(a) · NIS2 Art. 21(2)(h)	Responsables des données	Échantillon d'accès, récupération des clés et preuve de suppression.
10 Former personnel et direction ; exercer la gestion d'incident, la continuité et les notifications légales. Appui : NIS2 Art. 20(2) · NIS2 Art. 21(2)(g) · DORA Art. 13(6)	RH et CISO	Formation par rôle et actions d'exercice clôturées.

Prioriser sans attendre le programme complet

Escalader immédiatement les accès privilégiés exposés, failles exploitées, sauvegardes critiques manquantes et circuits de notification inutilisables. Prévoir une protection temporaire et une correction durable. Un plan approuvé ne réduit pas à lui seul l'exposition.

Références juridiques [NIS2 Art. 21](#) | [RGPD Art. 32](#) | [DORA Art. 6 à 14](#)

Relier contrôles, obligations et décisions

Réutiliser les preuves communes tout en conservant chaque exigence juridique et lacune restante. Un score de maturité ou un certificat est une preuve d'appui dans son périmètre, pas une conformité automatique.

Travail commun	Dispositions soutenues	Distinguer les exigences
Évaluation des risques	NIS2 Art. 21(2)(a) · DORA Art. 6(1) · RGPD Art. 35(1) · CER Art. 12 · Règl. IA Art. 9	Risques de service, atteintes aux personnes, résilience physique et risques IA ont des critères différents.
Accès et restauration	RGPD Art. 32(1)(b)-(c) · NIS2 Art. 21(2)(c) · DORA Art. 9 · DORA Art. 12	Vérifier les systèmes couverts, la reprise métier et la période des preuves.
Développement sécurisé	CRA Art. 13(1)-(2) · CRA annexe I · NIS2 Art. 21(2)(e) · Règl. IA Art. 9	Évaluer séparément la conformité produit et les obligations selon le rôle IA.
Revue fournisseurs	RGPD Art. 28(3) · NIS2 Art. 21(2)(d) · DORA Art. 28 · DORA Art. 30 · Data Act Art. 25	Les clauses de traitement, les contrats TIC financiers et les droits de changement diffèrent.
Gestion des incidents	RGPD Art. 33 · RGPD Art. 34 · NIS2 Art. 23 · DORA Art. 19 · CRA Art. 14 · CER Art. 15	Déclencheur, entité tenue de notifier, autorité, délai et contenu différent.

Rendre chaque décision de risque exécutable

Consigner scénario, service et personnes concernés, protections, impact plausible et traitement. Fixer responsable et échéance, puis un test démontrant la réduction du risque. Escalader ce qui ne peut être financé ou légalement accepté.

Limitier les exceptions dans le temps

Une exception exige périmètre, motif, mesure compensatoire, approbateur, échéance et test de clôture. L'acceptation du risque ne dispense pas d'une obligation légale. Le juridique vérifie la licéité de la solution temporaire.

Exemple de correspondance rigoureuse

Un test démontre la restauration de l'application A dans l'objectif convenu. Le relia aux obligations pertinentes de disponibilité et de restauration. Une dépendance fournisseur manquante ou un service d'identité non testé reste une lacune ; ne pas déclarer tout le texte satisfait.

Validation des changements

Avant tout nouveau service, fournisseur, usage IA ou lancement produit : revoir le périmètre et les risques, confirmer les notifications ou étapes de conformité, tester les contrôles et consigner l'accord métier. Recommencer si la finalité change.

Références juridiques [NIS2 Art. 21](#) | [RGPD Art. 25 et 35](#) | [CRA annexe I](#)

NIS2 périmètre et gouvernance

Déterminer le champ par entité et service. Appliquer la transposition nationale ; ne pas attendre un courrier du régulateur si la loi impose une autoévaluation ou un enregistrement.

Extrait du texte «*approuvent les mesures de gestion des risques en matière de cybersécurité*» [NIS2 Art. 20\(1\)](#)
L'approbation par la direction figure explicitement dans le texte UE ; la mettre en œuvre selon le droit national.

Étape	Action	Livrable requis
1 Qualifier l'activité	Rattacher les services réels aux annexes I ou II et aux catégories nationales : énergie, transports, santé, eau, infrastructures numériques, gestion de services TIC et certaines industries manufacturières. NIS2 Art. 2(1) · NIS2 annexe I · NIS2 annexe II	Motifs de classement du secteur et du service, avec disposition exacte.
2 Calculer la taille	Appliquer les règles UE de taille, y compris entreprises partenaires et liées pertinentes. Recueillir effectifs et données financières. Vérifier les exceptions pour les petites entités. NIS2 Art. 2(1)-(2)	Calcul et analyse des exceptions validés par le juridique.
3 Classer l'entité	Déterminer le statut essentiel ou important selon l'article 3 et le droit national. Vérifier désignations particulières et compétence transfrontière. NIS2 Art. 3(1)-(2) · NIS2 Art. 26	Classification et autorité compétente.
4 S'enregistrer si requis	Confirmer délais locaux, données d'enregistrement, accès au portail et notifications de changement. Nommer responsable et suppléant. NIS2 Art. 3(4) · NIS2 Art. 27(2)-(3)	Accusé de réception ou motif documenté d'absence d'obligation.
5 Mobiliser la direction	La direction approuve et supervise les mesures et suit la formation requise. Consigner décisions et ressources. NIS2 Art. 20(1)-(2)	Procès-verbaux, preuves de formation et responsables d'actions.
6 Préparer les notifications	Définir les critères d'importance et les délais. Le règlement 2024/2690 vise certains prestataires numériques. NIS2 Art. 23(3)-(4) · 2024/2690 Art. 3	Procédure locale, canal testé et exercice d'incident.

Questions pratiques de classification

- Exploitions-nous nous-mêmes un service couvert ou l'achetons-nous seulement ?
- L'activité manufacturière relève-t-elle d'une catégorie précisément visée ?
- Une exception de taille, une désignation critique ou un texte sectoriel modifie-t-il le résultat ?

Articulation : Pour les entités financières couvertes par DORA, examiner l'articulation sectorielle de l'article 4 NIS2. Conserver dans l'analyse le RGPD et les obligations relatives aux produits ou autres.

Références juridiques [NIS2 Art. 2 à 4 et 20](#) | [Règles d'exécution du secteur numérique](#)

NIS2 liste de contrôle opérationnelle

L'article 21 exige des mesures techniques, opérationnelles et organisationnelles proportionnées. Les dix domaines servent à vérifier l'exhaustivité ; les exigences nationales et les risques déterminent la mise en œuvre précise.

Extrait du texte «des politiques et des procédures pour évaluer l'efficacité des mesures» [NIS2 Art. 21\(2\)\(f\)](#)
Conserver les résultats des tests et les corrections, pas seulement les politiques.

Domaine de l'article 21	Action pratique	Preuve
Analyse des risques et politique de sécurité	Approuver une analyse des risques par service et une politique de sécurité utilisable. NIS2 Art. 21(2)(a)	Analyse à jour, approbation et plan de traitement.
Gestion des incidents	Définir triage, autorité de réponse, confinement et décisions de notification. NIS2 Art. 21(2)(b)	Procédure, exercice et dossier d'incident.
Continuité et gestion de crise	Fixer les objectifs de reprise ; protéger les sauvegardes et tester la restauration. NIS2 Art. 21(2)(c)	Résultats de restauration et exercice de crise.
Sécurité de la chaîne d'approvisionnement	Évaluer les fournisseurs directs ; traiter les vulnérabilités pertinentes et les pratiques sécurisées. NIS2 Art. 21(2)(d)	Registre fournisseurs, décisions et contrats.
Acquisition et développement	Intégrer la sécurité dans la conception, les changements, la maintenance et le traitement ou la divulgation des vulnérabilités. NIS2 Art. 21(2)(e)	Preuves de mise en service et suivi des vulnérabilités.
Évaluation de l'efficacité	Tester l'efficacité des contrôles sur tout le périmètre annoncé. NIS2 Art. 21(2)(f)	Échantillons, échecs et nouveaux tests.
Cyberhygiène et formation	Former utilisateurs et direction selon leurs rôles et les risques actuels. NIS2 Art. 21(2)(g)	Dossiers de formation et contrôles des acquis.
Cryptographie	Définir où et comment chiffrer ; gérer les clés et leur récupération. NIS2 Art. 21(2)(h)	Standard, responsable des clés et récupération testée.
Personnel, accès et actifs	Gérer arrivées, mobilités, départs, privilèges et responsabilité des actifs. NIS2 Art. 21(2)(i)	Revue des accès et rapprochement des actifs.
Authentification et communication	Appliquer, selon les besoins, MFA ou authentification continue et communications sécurisées. NIS2 Art. 21(2)(j)	Configuration, exceptions et test du canal d'urgence.

Trois résultats à démontrer le premier mois

- Au départ d'un salarié, les accès, y compris privilégiés et tiers, sont retirés dans le délai approuvé.
- Un service critique peut être restauré avec ses dépendances d'identité, de réseau et de fournisseurs.
- L'équipe incident accède au bon canal de l'autorité et prépare une alerte précoce dans les délais.

Le règlement 2024/2690 détaille les exigences pour certaines entités numériques. Sa liste n'est pas automatiquement obligatoire dans tous les secteurs NIS2.

Références juridiques [NIS2 Art. 21](#) | [Règlement 2024/2690](#)

RGPD liste de contrôle pratique

Évaluer séparément responsables du traitement et sous-traitants. Les données des salariés et contacts professionnels sont personnelles ; le B2B n'est pas une exemption générale. Le responsable doit rendre compte ; le DPO désigné conseille et contrôle.

Extrait du texte «est en mesure de démontrer que celui-ci est respecté» [RGPD Art. 5\(2\)](#)

Rendre facilement accessibles les preuves de chaque contrôle.

Actions et preuves

Action	Responsable proposé	Preuves à conserver
Identifier finalités, données, personnes, destinataires et conservation. Documenter les bases légales et les conditions des catégories particulières si nécessaire. RGPD Art. 5(1) · RGPD Art. 6 · RGPD Art. 9 · RGPD Art. 30	Métiers et protection des données	Registre, base légale et carte des flux.
Fournir une information claire et ne collecter que le nécessaire. Définir la conservation et une suppression effective. RGPD Art. 5(1)(c)-(e) · RGPD Art. 13 · RGPD Art. 14	Responsables des données	Notices publiées et exemple de suppression vérifié.
Conclure les clauses de l'article 28 avec les sous-traitants. Examiner sous-traitants ultérieurs, transferts internationaux et garanties. RGPD Art. 28(2)-(3) · RGPD Art. 44 · RGPD Art. 46	Juridique et achats	Clauses de traitement et analyse des transferts.
Mettre en place une sécurité adaptée au risque. Évaluer le besoin d'une AIPD et la réaliser avant un traitement à risque élevé. RGPD Art. 32(1) · RGPD Art. 35(1)	CISO et protection des données	Résultats des contrôles, AIPD et décisions de traitement.
Traiter les demandes de droits en sécurité. Suivre le délai d'un mois et toute prolongation licite, à expliquer pendant le premier mois. RGPD Art. 12(3) · RGPD Art. 12(6) · RGPD Art. 15	Opérations données	Vérification d'identité, réponse et suivi des délais.
Préparer décisions et communications de violation. Documenter toutes les violations, y compris les décisions de ne pas notifier. RGPD Art. 33(5) · RGPD Art. 34	Responsable incident et données	Registre des violations, analyse des risques et accusés.

Tests proposés et dispositions associées

- Suivre un dossier salarié ou client de la collecte à la suppression, y compris les copies des fournisseurs.
- Simuler une demande d'accès et une violation touchant la disponibilité comme la confidentialité.

Les tests appuient : [RGPD Art. 5\(2\)](#) · [RGPD Art. 12\(3\)](#) · [RGPD Art. 32\(1\)\(d\)](#)

Attention : Le consentement n'est pas la base par défaut de toute activité. Des données chiffrées peuvent rester personnelles. Une violation est possible sans exfiltration confirmée.

Références juridiques [RGPD Art. 5 à 6, 12, 28, 30 à 35](#)

DORA liste de contrôle pratique

DORA s'applique depuis le 17 janvier 2025 aux entités financières visées, sous réserve des exclusions et de la proportionnalité. Les fournisseurs TIC ordinaires répondent aux contrats clients ; les prestataires tiers TIC critiques désignés relèvent d'une supervision distincte.

Extrait du texte «définit, approuve, supervise et est responsable de la mise en œuvre» [DORA Art. 5\(2\)](#)
Consigner les décisions de direction et le suivi du cadre TIC.

Actions et preuves

Action	Responsable proposé	Preuves à conserver
Relier fonctions critiques ou importantes aux systèmes, données, personnes et fournisseurs. Identifier concentrations et points uniques de défaillance. DORA Art. 8(1) · DORA Art. 8(5) · DORA Art. 29(1)	Métiers et IT	Cartographie des fonctions et analyse des dépendances.
Maintenir le cadre de risque TIC approuvé et les dispositifs de continuité, de reprise et de communication. DORA Art. 5(2) · DORA Art. 6(1) · DORA Art. 11 · DORA Art. 14	Direction et risques	Cadre approuvé, revues et décisions de traitement.
Classer les incidents selon les critères applicables et préparer les notifications d'incidents majeurs. Distinguer prise de connaissance et classification. DORA Art. 18(1) · DORA Art. 19(1) · 2025/301 Art. 5	Responsable incident	Liste de classification et chronologie des notifications.
Exécuter un programme proportionné de tests de résilience. Déterminer si les tests avancés de pénétration fondés sur la menace s'appliquent. DORA Art. 24(1)-(2) · DORA Art. 26	CISO et risques	Plan de tests, constats, nouveaux tests et décision TLPT.
Tenir le registre prescrit des accords contractuels TIC. Couvrir diligence, concentration, sous-traitance et clauses obligatoires. DORA Art. 28(3)-(4) · DORA Art. 29 · DORA Art. 30	Achats et juridique	Registre, contrats et évaluations des prestataires.
Tester continuité et sortie des dépendances importantes. Confirmer exports utilisables, compétences de remplacement, capacité et délais réalistes. DORA Art. 11(6) · DORA Art. 28(8)	Responsables de services	Exercice de reprise ou sortie et acceptation métier.

Tests proposés et dispositions associées

- Simuler la perte du service d'identité commun à la production et à la reprise après sinistre.
- Préparer une notification d'incident majeur dans les limites de quatre et 24 heures de la page 18.

Les tests appuient : [DORA Art. 11\(6\)](#) · [DORA Art. 24\(1\)](#) · [2025/301 Art. 5](#)

Attention : Externaliser les notifications ou l'exploitation ne transfère pas la responsabilité de l'entité financière. Une liste générique de fournisseurs ne remplace pas le registre d'informations prescrit.

Références juridiques [DORA Art. 5 à 16, 19, 24 à 30](#) | [Délais de notification](#)

Règlement IA liste de contrôle pratique

Classer le système et sa finalité. Consigner le rôle de fournisseur, déployeur, importateur ou distributeur ; distinguer l'application de son modèle d'IA à usage général (GPAI). Réévaluer si l'usage ou le système change.

Extrait du texte «prennent des mesures pour favoriser le développement de la maîtrise de l'IA» [Règl. IA modifié Art. 4\(1\)](#)
Il s'agit de l'article 4, paragraphe 1, modifié ; adapter la maîtrise de l'IA aux usages et risques réels.

Actions et preuves

Action	Responsable proposé	Preuves à conserver
Inventorier usages IA, responsables, entrées, sorties, personnes concernées, outils connectés et fournisseurs. Rechercher les pratiques interdites avant utilisation. Règl. IA Art. 2(1) · Règl. IA Art. 3(3)-(4) · Règl. IA Art. 5 · Règl. IA modifié Art. 5(1a)	Métiers et juridique	Registre IA, finalité et contrôle des interdictions.
Évaluer les obligations de haut risque, transparence et GPAI. Consigner rôle, justification juridique et date d'application ; revoir modifications ou changement de marque. Règl. IA Art. 6 · Règl. IA Art. 25(1) · Règl. IA Art. 50 · Règl. IA Art. 53 · 2026/1744 Art. 1(40)	Gouvernance IA	Classification approuvée et déclencheurs de révision.
Appliquer les obligations actuelles d'information et de maîtrise de l'IA. Former aux usages et risques ; fournir les mentions requises sur l'interaction ou les contenus. Règl. IA modifié Art. 4(1) · Règl. IA Art. 50(1)-(4)	Métiers et RH	Mentions, supports de formation et participation.
Pour le haut risque concerné, prévoir documentation, qualité et conformité du fournisseur, ou supervision et suivi du déployeur. Règl. IA Art. 16 · Règl. IA Art. 17 · Règl. IA Art. 26 · Règl. IA Art. 43 · 2026/1744 Art. 1(40)	Produit ou métiers	Exigences et preuves selon le rôle.
Évaluer données personnelles et effets dommageables. Tester cas représentatifs, limites et intervention humaine effective. RGPD Art. 35(1) · Règl. IA Art. 9 · Règl. IA Art. 14 · Règl. IA Art. 27(1)	Données et métiers	AIPD si requise, tests et décision de mise en service.
Pour les agents, limiter droits sur les outils et accès aux données ; fixer limites d'action, approbations et arrêt testé. Appui : Règl. IA Art. 14(4)(d)-(e) · Règl. IA Art. 15(5) · RGPD Art. 32(1)	Ingénierie et CISO	Carte des droits, journaux d'actions et test d'arrêt.

Tests proposés et dispositions associées

- Demander au responsable d'expliquer finalité, rôle juridique et licéité du système.
- Tester une sortie erronée et une instruction non autorisée à un outil ; vérifier intervention et reprise.

Les tests appuient : [Règl. IA Art. 14](#) · [Règl. IA Art. 15](#) · [2026/1744 Art. 1\(40\)](#)

Attention : Les contrôles des agents sont des recommandations, pas une architecture imposée. La modification de 2026 change les dates du haut risque ; voir page 24. Les autres obligations applicables subsistent.

Références juridiques [Règl. IA](#) | [Modification de 2026](#)

Cyber Resilience Act liste pratique

Vérifier si le produit comportant des éléments numériques est couvert et le rôle de l'opérateur. Les notifications de l'article 14 s'appliquent depuis le 11 septembre 2026 ; la plupart des exigences dès le 11 décembre 2027.

Extrait du texte «être mis à disposition sur le marché avec une configuration de sécurité par défaut» [CRA annexe I partie I \(2\)\(b\)](#)

Appliquer les conditions de risque, de champ et l'exception B2B sur mesure prévues par la disposition complète.

Actions et preuves

Action	Responsable proposé	Preuves à conserver
Définir périmètre produit, traitement distant nécessaire, versions, mise sur le marché UE et exclusions. Choisir la procédure de conformité. CRA Art. 2 · CRA Art. 3(1)-(2) · CRA Art. 32	Produit et juridique	Périmètre, rôle et décision de conformité.
Évaluer les risques cyber du produit. Intégrer la sécurité dans la conception, les paramètres par défaut, les accès et les mises à jour. CRA Art. 13(1)-(3) · CRA annexe I partie I	Ingénierie	Analyse des menaces, exigences et tests de sécurité.
Suivre composants logiciels et vulnérabilités. Préparer une nomenclature logicielle lisible par machine et un canal de divulgation. CRA annexe I partie II (1), (5)-(6)	Sécurité produit	Inventaire des composants, SBOM et signalements reçus.
Financer le support et les mises à jour sûres sur le cycle de vie. Justifier la durée de support : en principe au moins cinq ans, sauf usage attendu plus court. CRA Art. 13(8) · CRA Art. 13(19) · CRA annexe I partie II (7)-(8)	Gestion produit	Décision de support, date de fin publiée et tests de mise à jour.
Préparer documentation technique, instructions, déclaration UE et marquage CE selon la procédure de conformité applicable. CRA Art. 13(12) · CRA Art. 28 · CRA Art. 30 · CRA Art. 31 · CRA Art. 32	Produit et qualité	Dossier de mise sur le marché et preuves de conformité.
Notifier dès maintenant les vulnérabilités exploitées et incidents graves concernés. Inclure les anciens produits visés par l'article 69. CRA Art. 14(1)-(4) · CRA Art. 69(3) · CRA Art. 71	Équipe réponse produit	Contact pour le délai de 24 h, classification et notifications.

Tests proposés et dispositions associées

- Pour un produit commercialisé, identifier versions touchées, composants, responsable du support et contact client.
- Simuler une vulnérabilité de l'évaluation à la notification, la diffusion du correctif et les instructions utilisateurs.

Les tests appuient : [CRA Art. 13\(2\)](#) · [CRA Art. 14](#) · [CRA annexe I partie II](#)

Attention : Un SaaS autonome n'est pas automatiquement un produit CRA. Un traitement distant nécessaire peut en faire partie. Le support doit refléter l'usage attendu ; cinq ans ne suffisent pas toujours.

Références juridiques [CRA Art. 13, 14, 32, 69 et 71](#)

Résilience des entités critiques liste pratique

CER vise la résilience des entités critiques désignées et des services essentiels face aux perturbations physiques et autres. Vérifier désignation et notification nationales. Les exclusions sectorielles comptent, notamment pour banques, infrastructures financières et numériques.

Extrait du texte «des mesures techniques, des mesures de sécurité et des mesures organisationnelles appropriées et proportionnées pour garantir leur résilience» [CER Art. 13\(1\)](#)

Relier les mesures à l'évaluation des risques de l'entité et au droit national.

Actions et preuves

Action	Responsable proposé	Preuves à conserver
Consigner notification de désignation, réception, service, autorité et obligations. Vérifier les exceptions sectorielles et nationales. CER Art. 6(3) · CER Art. 8	Juridique et continuité	Dossier de désignation et échéances applicables.
Évaluer les aléas naturels et humains : électricité, eau, accès, personnel, sabotage et dépendances transfrontières. CER Art. 12(1)-(2)	Continuité et installations	Analyse des risques tous aléas.
Protéger sites et activités de façon proportionnée. Définir accès, protections physiques et mesures concernant le personnel autorisées par la loi. CER Art. 13(1)(a)-(b), (e) · CER Art. 14	Installations et RH	Contrôles, accès autorisés et vérifications licites.
Planifier continuité, solutions de repli et reprise. Confirmer ressources, alternatives et niveaux minimaux de service viables. CER Art. 13(1)(c)-(d)	Responsable métier	Plan de résilience et dispositifs pour les dépendances.
Former le personnel et simuler une perturbation. Nommer un correspondant et préparer les notifications d'incidents importants. CER Art. 13(1)(f) · CER Art. 13(3) · CER Art. 15(1)	Responsable continuité	Exercice, fiche de contact et procédure de notification.
Suivre le calendrier à partir de la notification. Évaluation des risques sous neuf mois ; chapitre III applicable en principe après dix mois. CER Art. 6(3) · CER Art. 12(1)	Juridique et sponsor	Plan daté fondé sur la notification réelle.

Tests proposés et dispositions associées

- Simuler une coupure prolongée d'électricité ou d'eau, un site inaccessible et l'indisponibilité d'un fournisseur clé.
- Démontrer le service minimal maintenu, sa durée, les personnes et les ressources nécessaires.

Les tests appuient : [CER Art. 13\(1\)\(c\)-\(d\), \(f\)](#)

Attention : Un plan de reprise cyber ne couvre pas seul la résilience physique. Consigner séparément classifications NIS2/CER et obligations locales, même si les preuves sont partagées.

Références juridiques [CER Art. 6, 8 et 12 à 15](#)

Data Act liste de contrôle pratique

Identifier les rôles : fabricant de produits connectés, fournisseur de services connexes, utilisateur, détenteur ou destinataire de données, prestataire de traitement. Un client cloud doit aussi intégrer les règles de changement aux achats et au plan de sortie.

Extrait du texte «prennent les mesures prévues aux articles 25, 26, 27, 29 et 30» [Data Act Art. 23](#)

Lire l'obligation complète de changement, avec rôle, périmètre et exceptions.

Actions et preuves

Action	Responsable proposé	Preuves à conserver
Identifier données des produits et services connexes, métadonnées, accès et détenteur de chaque jeu de données. Data Act Art. 2(15)-(17) · Data Act Art. 3(1)	Responsables produit et données	Catalogue des données et carte des rôles.
Fournir les informations précontractuelles et l'accès utilisateur requis. Vérifier identité et habilitation sans procédures obstructives. Data Act Art. 3(2)-(3) · Data Act Art. 4(1)	Produit et exploitation	Informations, circuit de demande et échantillon fourni.
Traiter le partage admissible avec des tiers. Vérifier RGPD, secrets d'affaires, usages permis et protections nécessaires. Data Act Art. 4(6)-(9) · Data Act Art. 5 · Data Act Art. 6	Juridique et données	Décision de partage, garanties et conditions d'accès.
Vérifier clauses abusives et transparence des contrats de données. Faire examiner les demandes contraignantes d'organismes publics par le juridique. Data Act Art. 13 · Data Act Art. 14 · Data Act Art. 17	Juridique et achats	Revue contractuelle et analyse de la demande.
Pour les services cloud ou de traitement couverts, définir données exportables, interfaces, transition, assistance, frais et suppression. Data Act Art. 25 · Data Act Art. 27 · Data Act Art. 29 · Data Act Art. 30	Responsable de service	Contrat et plan de changement exécutable.
Tester l'export vers un autre environnement ; rapprocher les enregistrements et consigner les limites fonctionnelles ou d'interopérabilité. Appui : Data Act Art. 23(c)-(d) · Data Act Art. 30	IT et métiers	Test export/import et actions de sortie.

Tests proposés et dispositions associées

- Demander un jeu de données représentatif d'un produit connecté ; vérifier exhaustivité, format, métadonnées et autorisation.
- Lire les données cloud exportées avec un outil indépendant ; mesurer durée et effort réels.

Les tests appuient : [Data Act Art. 4\(1\)](#) · [Data Act Art. 23\(c\)](#) · [Data Act Art. 30](#)

Attention : Le Data Act ne donne pas accès à toutes les données d'entreprise et n'écarte pas le RGPD. La suppression des frais de changement n'élimine pas tous les frais de service ou de résiliation anticipée.

Références juridiques [Data Act Art. 3 à 5, 13, 23 à 31 et 50](#)

eIDAS et confiance numérique liste pratique

Distinguer l'entreprise utilisant signatures ou identité électroniques du prestataire de confiance réglementé. La liste vise d'abord l'entreprise utilisatrice ; prestataires et acteurs des portefeuilles ont des exigences supplémentaires selon leur rôle.

Extrait du texte «L'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite.» [eIDAS Art. 25\(2\)](#)

Vérifier séparément pouvoirs de signature et formalités nationales.

Actions et preuves

Action	Responsable proposé	Preuves à conserver
Lister transactions, pays, parties et formalités. Déterminer le niveau de signature ou cachet requis par processus. Appui : eIDAS Art. 2(3) · eIDAS Art. 25 · eIDAS Art. 35	Juridique et responsable processus	Politique reliant transactions et niveaux de signature.
Choisir et vérifier le service. Si le statut qualifié est requis, vérifier le service précis dans les listes de confiance officielles. eIDAS Art. 22(1) · eIDAS Art. 32(1)	Achats et juridique	Validation datée du statut du service.
Vérifier identité et pouvoir de signer. Protéger les moyens de signature ; prévoir délégation, révocation et départs. Appui : eIDAS Art. 26 · eIDAS Art. 32(1)	Identités et métiers	Preuve d'identité et pouvoir de signature.
Conserver fichier signé, validation, certificats, données temporelles et preuves pour les vérifications futures. Appui : eIDAS Art. 32(1) · eIDAS Art. 34	Responsable des archives	Dossier de validation et de conservation.
Tester la validation hors du portail fournisseur. Garantir la pérennité des preuves après fin du contrat ou défaillance du prestataire. Appui : eIDAS Art. 32 · eIDAS Art. 34	IT et archives	Validation indépendante et test d'export.
Pour les services d'identité ou de confiance, évaluer séparément conformité, supervision, incidents et obligations des portefeuilles EUDI. eIDAS Art. 5a · eIDAS Art. 19a · eIDAS Art. 20 · eIDAS Art. 24	Service et juridique	Plan de conformité et notification selon le rôle.

Tests proposés et dispositions associées

- Vérifier un document signé sans se limiter à une capture d'écran ou à un courriel d'approbation du fournisseur.
- Vérifier que le signataire avait le pouvoir d'effectuer la transaction au moment de signer.

Les tests appuient : [eIDAS Art. 32](#) · [eIDAS Art. 34](#)

Attention : Une signature électronique qualifiée a dans l'UE l'effet d'une signature manuscrite, mais ne prouve pas à elle seule le pouvoir de représenter l'entreprise ni le respect de toute formalité nationale. Un cachet électronique est distinct.

Références juridiques [eIDAS Art. 22, 25, 32 et 35](#) | [Listes de confiance UE](#)

Digital Services Act liste pratique

Classer chaque service : simple transport, cache, hébergement, plateforme, place de marché ou très grand service désigné. Un site d'entreprise publiant ses propres contenus n'est pas automatiquement une plateforme DSA.

Extrait du texte «Ces mécanismes sont faciles d'accès et d'utilisation» [DSA Art. 16\(1\)](#)

Tester le mécanisme de notification d'hébergement avec un signalement réaliste.

Actions et preuves

Action	Responsable proposé	Preuves à conserver
Documenter fonctions, destinataires UE et opérateur. Vérifier la portée exacte des exemptions liées à la taille. DSA Art. 2(1) · DSA Art. 3(g), (i) · DSA Art. 19(1) · DSA Art. 29	Produit et juridique	Classification du service et analyse des exemptions.
Publier contacts et conditions requis. Expliquer clairement restrictions de contenu et politiques de modération. DSA Art. 11(1) · DSA Art. 12(1) · DSA Art. 14(1)	Juridique et exploitation	Points de contact, conditions et preuve de publication.
Pour l'hébergement, permettre les signalements de contenus illicites. Examiner diligemment les cas, consigner les décisions et fournir les motifs requis. DSA Art. 16(1)-(6) · DSA Art. 17(1)-(3)	Confiance et sécurité	Signalement, analyse, décision et communication.
Pour les plateformes concernées, gérer les réclamations et examiner publicité, interfaces et protection des mineurs. DSA Art. 20(1) · DSA Art. 25 · DSA Art. 26 · DSA Art. 28	Produit et exploitation	Résultats des réclamations et vérifications de conception.
Pour les places de marché concernées, assurer la traçabilité des professionnels et la conformité dès la conception. DSA Art. 30(1)-(3) · DSA Art. 31	Responsable marketplace	Vérifications des professionnels et tests de publication des offres.
Suivre le nombre de destinataires et toute désignation. Si le service est désigné très grand, appliquer le régime supplémentaire de risques systémiques et d'audit. DSA Art. 24(2) · DSA Art. 33 · DSA Art. 34 · DSA Art. 37	Conformité	Calcul des utilisateurs, désignation et plan de contrôle.

Tests proposés et dispositions associées

- Soumettre un signalement réaliste de contenu illicite et le suivre jusqu'à une décision motivée.
- Tester une réclamation applicable et vérifier la correction d'une erreur antérieure.

Les tests appuient : [DSA Art. 16\(6\)](#) · [DSA Art. 20\(4\)](#)

Attention : Les exemptions des micro et petites entreprises suppriment certaines obligations, pas tout le règlement. L'article 18 vise certains soupçons d'infractions menaçant la vie ou la sécurité ; le DSA n'impose pas de délai cyber universel de 72 heures.

Références juridiques [DSA Art. 11 à 18, 19 à 32 et 33 à 42](#)

Gérer la première heure d'un incident

Lancer confinement et analyse juridique ensemble. Les délais ci-dessous sont des objectifs internes recommandés, pas des délais légaux. Ne pas attendre la cause racine pour notifier lorsque la loi l'exige.

Objectif	Action	Résultat
0 à 15 minutes	Nommer responsable incident et secrétaire. Protéger les personnes, activer les contacts et préserver les journaux. Consigner découverte et horaires connus en UTC. Appui : NIS2 Art. 21(2)(b) · DORA Art. 17(3)(a)	ID de dossier, chronologie et périmètre initial touché.
15 à 30 minutes	Confiner selon les procédures autorisées. En OT, associer si possible la sécurité ou le responsable du site avant une action perturbatrice. Identifier entités, services, produits et données touchés. Appui : DORA Art. 17(3)(b), (f) · NIS2 Art. 21(2)(b)	Décisions de confinement et impact métier.
Avant 30 minutes	Contacter juridique, données, métiers et produit selon le cas. Évaluer chaque déclencheur et consigner les heures de prise de connaissance ou de classification juridiques. Appui : RGPD Art. 33(1) · NIS2 Art. 23(3) · DORA Art. 18(1)	Décisions et échéances distinctes par notification.
Avant 60 minutes	Nommer déclarant et suppléant par circuit. Rédiger faits initiaux, inconnues et protections. Confirmer les informations clients et contractuelles. Appui : RGPD Art. 33(3)-(4) · NIS2 Art. 23(4) · DORA Art. 19(1)	Notifications initiales approuvées ou décision motivée de non-notification.

Une chronologie et des délais juridiques distincts

Consigner détection, prise de connaissance selon chaque texte, classification majeure/importante, décisions, envois et accusés. Un événement peut déclencher plusieurs lois pour différentes entités du groupe. Une notification ne satisfait pas automatiquement tous les régimes.

Contenu minimal du dossier d'incident

- ID ; entité juridique ; responsable et suppléant ; services, pays, données et versions concernés.
- Faits confirmés ; hypothèses ; impact sur l'activité et les personnes ; sources et horodatage de chaque mise à jour.
- Déclencheur par texte ; échéance exacte ; destinataire ; approbateur ; déclarant ; accusé ; prochaine mise à jour.
- Confinement, reprise, emplacement des preuves et protection des clients.

Avant la clôture

Vérifier tous les compléments et rapports finaux. Consigner cause, rétablissement des services et données, risque résiduel, actions, responsables et nouveaux tests. Conserver les motifs de non-notification et les réexaminer si les faits changent.

Références juridiques [RGPD Art. 33 et 34](#) | [NIS2 Art. 23](#) | [Règles de notification DORA](#)

Principaux délais de notification d'incident

Appliquer ces règles UE avec le circuit national, les seuils, l'autorité compétente et les normes techniques. Tous les délais sont des maxima ; l'obligation d'agir sans retard injustifié demeure.

Régime et déclencheur	Premier envoi	Suivi et destinataire
RGPD responsable du traitement Violation de données, sauf risque improbable pour les droits et libertés.	Sans retard injustifié, si possible sous 72 heures après en avoir pris connaissance. Motiver tout retard.	Autorité de protection des données compétente. Compléter progressivement sans retard supplémentaire injustifié. Documenter toutes les violations. RGPD Art. 33(1), (3)-(5)
RGPD sous-traitant et personnes concernées	Sous-traitant : informer le responsable sans retard injustifié. Responsable : informer les personnes sans retard injustifié en cas de risque élevé, sous réserve de l'article 34.	Ne pas accorder au sous-traitant un délai supposé de 72 heures. Suivre séparément les délais contractuels. RGPD Art. 33(2) · RGPD Art. 34(1)-(3)
NIS2 Incident important selon les critères applicables.	Alerte précoce sous 24 heures après connaissance d'un incident important ; notification sous 72 heures. Les deux sans retard injustifié.	CSIRT ou autorité compétente. Rapport final sous un mois après la notification ; rapport intermédiaire sur demande. NIS2 Art. 23(3) · NIS2 Art. 23(4)(a)-(d)
NIS2 incident en cours et services de confiance	Prestataires de confiance : notification des incidents concernés sous 24 heures au lieu de 72.	Si l'incident se poursuit à la date du rapport final, fournir un état d'avancement puis un rapport final sous un mois après son traitement. NIS2 Art. 23(4)(b), (e)
DORA Incident majeur lié aux TIC selon les critères applicables.	Dès que possible : sous quatre heures après classification majeure et au plus tard 24 heures après connaissance. Si classé après 24 heures, sous quatre heures après classification.	Autorité financière compétente. Rapport intermédiaire sous 72 heures après la notification initiale ; mise à jour à la reprise. Rapport final sous un mois après l'intermédiaire ou sa dernière mise à jour. DORA Art. 19(1) · 2025/301 Art. 5(1)-(4)

Configurer les délais avant l'exercice

Pour chaque entité, renseigner portail, autorité, seuils, formulaires, déclarant et suppléant en page 22. Tester l'accès sans envoyer de vraie notification.

DORA prévoit des règles et exceptions pour week-ends et jours fériés. Prévoir une couverture continue ; n'utiliser une prolongation qu'après vérification de l'éligibilité selon l'article 5 et des décisions de l'autorité.

Références juridiques [RGPD Art. 33 et 34](#) | [NIS2 Art. 23](#) | [DORA Règlement 2025/301 Art. 5](#)

Notifications produits et autres circuits

Ajouter ces circuits selon l'activité et le rôle juridique. Vérifier dates d'application et droit national ; ne pas appliquer un délai générique unique.

Régime et déclencheur	Délai et circuit pratique
CRA Vulnérabilité activement exploitée	Le fabricant notifie via la plateforme unique au CSIRT coordinateur et à l'ENISA. Alerte précoce sous 24 heures après connaissance ; notification de vulnérabilité sous 72 heures. Rapport final sous 14 jours après disponibilité d'une mesure corrective ou d'atténuation. CRA Art. 14(1)-(2)
CRA Incident grave touchant la sécurité du produit	Mêmes destinataires et plateforme. Alerte précoce sous 24 heures après connaissance ; notification sous 72 heures. Rapport final sous un mois après notification. Prévoir l'information des utilisateurs concernés selon l'article 14. CRA Art. 14(3)-(4), (8)
CER Perturbation importante ou potentiellement importante des services essentiels	Notifier l'autorité sans retard injustifié ; premier envoi sous 24 heures après connaissance, sauf impossibilité opérationnelle. Si pertinent, rapport détaillé sous un mois ; intégrer la règle nationale à la procédure locale. CER Art. 15(1)
Règlement IA Incident grave impliquant une IA à haut risque	Vérifier rôle et transition. Le fournisseur notifie immédiatement dès le lien causal ou sa probabilité raisonnable, au plus tard sous 15 jours après connaissance. Infraction de grande ampleur ou perturbation d'infrastructure critique de l'art. 3(49)(b) : immédiatement, sous deux jours. Décès : immédiatement si lien suspecté, sous dix jours. Autorité de surveillance du marché ou Bureau de l'IA selon l'art. 75 modifié. Règl. IA Art. 73(1)-(4) · Règl. IA Art. 26(5) · Règl. IA modifié Art. 75(1a)
eIDAS Atteinte à la sécurité ou perturbation d'un service de confiance	Prestataires non qualifiés : art. 19a, sans retard injustifié et sous 24 heures après connaissance. Qualifiés : art. 24(2)(fb), sans retard injustifié et sous 24 heures après l'incident. Informer l'organe de contrôle et les autres destinataires requis. Vérifier séparément NIS2 et RGPD ; il s'agit d'obligations de prestataires. eIDAS Art. 19a(1)(b) · eIDAS Art. 24(2)(fb)
DSA Soupçon d'infraction pénale visée	L'hébergeur informe rapidement l'autorité répressive ou judiciaire compétente selon l'article 18 lorsque le critère légal relatif à la vie ou à la sécurité est rempli. C'est distinct des notifications cyber. DSA Art. 18(1)-(2)

Règle opérationnelle : Consigner versions, support, utilisateurs concernés, protections et informations restant sensibles. Le juridique et le produit coordonnent communications réglementaires et clients. Ajouter notifications contractuelles, d'assurance et sectorielles à la même chronologie.

Références juridiques [CRA Art. 14](#) | [CER Art. 15](#) | [Règlement IA Art. 73](#) | [Modification IA](#) | [eIDAS](#) | [DSA Art. 18](#)

Unifier la validation des fournisseurs et achats

Valider à la sélection, au renouvellement et aux changements importants. Adapter l'effort à l'impact, aux données, aux accès et au rôle juridique, pas seulement au coût. Renforcer la revue d'un petit fournisseur ayant des accès privilégiés critiques.

Décision	Question au fournisseur ou responsable	Preuves à obtenir
Périmètre et impact	Quelle entité fournit le service ? Quelles fonctions, données et quels systèmes en dépendent ? Appui : DORA Art. 28(3)-(4) · RGPD Art. 28(1)	Description du service, lieux et carte des dépendances.
Accès et données	Qui administre ? Quels sous-traitants ou lieux traitent les données ? Comment maîtriser accès et suppression ? Appui : RGPD Art. 28(2)-(3) · RGPD Art. 44	Modèle d'accès, clauses de traitement et flux de données.
Sécurité et résilience	Que teste-t-on ? Quelles exclusions restent ? Le fournisseur peut-il rétablir le service selon nos besoins ? Appui : NIS2 Art. 21(2)(d) · DORA Art. 28(4)(c)-(d)	Rapport d'audit pertinent, constats ouverts et preuves de reprise.
Coopération en cas d'incident	Sous quel délai, par qui et avec quels faits serons-nous informés ? Une assistance hors horaires est-elle disponible ? Appui : RGPD Art. 28(3)(f) · DORA Art. 30(2)(f), (3)(b)	Obligations de notification négociées et contact testé.
Audit et changements	Pouvons-nous obtenir des preuves ? Quels changements, sous-traitants ou interruptions doivent être notifiés ? Appui : RGPD Art. 28(3)(h) · DORA Art. 30(2)(a), (3)	Clauses, droits de changement et matrice des responsabilités.
Sortie et portabilité	Peut-on exporter des données utilisables, transférer le service et confirmer la suppression ? Quels délais, coûts et dépendances restent ? Appui : DORA Art. 28(8) · Data Act Art. 25(2)	Plan de sortie, export test et conditions de résiliation.
Clauses propres à chaque texte	Y a-t-il traitement RGPD ? DORA s'applique-t-il au client ? Data Act, IA ou obligations produit sont-ils pertinents ? Appui : RGPD Art. 28(3) · DORA Art. 30(2)-(3) · Data Act Art. 25	Liste juridique complétée selon les conditions applicables.

Prendre une décision d'approbation explicite

Approuver, approuver sous conditions datées, ou refuser/suspendre. Joindre lacunes, mesures compensatoires, responsable métier et date de revue. Escalader toute exigence contractuelle obligatoire ou légale impossible à respecter.

Test d'acceptation

Choisir un fournisseur critique. Appeler son contact d'escalade, examiner le périmètre d'audit, exporter des données représentatives et identifier une solution viable de continuité ou sortie. Transformer les échecs en actions plutôt que classer le questionnaire.

Références juridiques [RGPD Art. 28](#) | [NIS2 Art. 21](#) | [DORA Art. 28 à 30](#) | [Data Act chapitre VI](#)

Réaliser les 90 premiers jours

Plan de mise en œuvre proposé. Toute échéance légale, tout incident actif ou toute exposition critique prime. Engager immédiatement les obligations en retard au lieu de les reporter à une phase ultérieure.

Quand	Lot de travail	Pilote responsable	Critères d'acceptation
Jours 1 à 10	Confirmer le périmètre des entités et activités. Identifier lois nationales, autorités et obligations de notification. Appui : NIS2 Art. 2 · RGPD Art. 3 · DORA Art. 2	Sponsor et juridique	Chaque entité prioritaire a un périmètre validé ou une question ouverte avec échéance.
Jours 1 à 15	Corriger les lacunes urgentes d'accès et d'exposition ; vérifier sauvegardes critiques et contacts incident. Appui : NIS2 Art. 21(2)(c), (i)-(j) · NIS2 Art. 23	CIO et CISO	Expositions critiques corrigées ou protégées ; circuit de notification utilisable.
Jours 11 à 30	Nommer les responsables des contrôles et des textes. Créer index de preuves et registre d'actions priorisé. Appui : NIS2 Art. 20(1) · DORA Art. 5(2)(c) · RGPD Art. 24(1)	Responsable programme	Chaque lacune prioritaire a un responsable, une échéance et un test de clôture.
Jours 16 à 45	Examiner fournisseurs critiques et flux de données personnelles. Classer les activités IA et produit. Appui : DORA Art. 28(4) · RGPD Art. 30 · Règl. IA Art. 6 · CRA Art. 2	Métiers et spécialistes	Contrats, classifications et lacunes opérationnelles consignés.
Jours 31 à 60	Déployer les contrôles prioritaires ; tester reprise, accès privilégiés et notifications. Appui : NIS2 Art. 21(2)(f) · DORA Art. 11(6)	Responsables de services	Résultats réels des tests ; corrections des échecs financées.
Jours 61 à 75	Retester les corrections. Échantillonner les preuves et vérifier les changements réglementaires nationaux. Appui : NIS2 Art. 21(2)(f) · DORA Art. 6(5)-(6)	Contrôle et juridique	Clôtures étayées par des preuves ; applicabilité à jour.
Jours 76 à 90	La direction examine risque résiduel, ressources et trimestre suivant. Appui : NIS2 Art. 20(1) · DORA Art. 5(2)(g)	Sponsor de direction	Décisions, budget, prochaines étapes et questions juridiques ouvertes explicites.

Règle de priorisation

Priorité 1 : violation légale en cours, notification imminente ou exposition opérationnelle critique. Priorité 2 : lacunes majeures touchant services importants ou personnes. Priorité 3 : améliorations après maîtrise des deux premières catégories. Reclasser si les faits changent.

Présenter les décisions plutôt que les volumes d'activité

Montrer ce qui peut échouer, l'obligation touchée, le responsable de la correction, sa date de test et la décision attendue. De nombreuses politiques ou formations ne prouvent pas à elles seules l'efficacité opérationnelle.

Fiches réutilisables de périmètre et d'autorités

Copier ces champs dans le registre existant. Créer une fiche par entité et activité, avec preuves et décision du réviseur. Les champs entre crochets sont à compléter par l'équipe.

Les fiches proposées appuient : [NIS2 Art. 2](#) · [NIS2 Art. 23\(4\)](#) · [RGPD Art. 33\(3\)](#)

Fiche de périmètre

Champ	À compléter
Fiche et objet	[ID de fiche] [Entité juridique] [Pays] [Activité ou produit]
Rôle métier et juridique	[Service et clients] [Lien UE] [Responsable du traitement/fournisseur/déploieur/autre rôle]
Base juridique	[Texte] [Article] [Lien de transposition nationale] [Version vérifiée]
Faits et conclusion	[Taille et secteur] [Exceptions] [Applicable maintenant / plus tard / non / à clarifier]
Dates d'application	[Début de l'obligation] [Délai d'enregistrement] [Réception de la désignation si pertinent]
Décision et réexamen	[Responsable] [Réviseur juridique] [Approbation] [Prochaine revue] [Déclencheur]

Fiche d'autorité et de notification

Champ	À compléter par circuit
Circuit et déclencheur	[Entité] [Texte] [Source du seuil] [Début et durée du délai]
Autorité	[Autorité ou CSIRT] [URL du portail officiel] [Téléphone de secours]
Personnes	[Déclarant et mobile] [Suppléant et mobile] [Approbateur et escalade]
Accès et envoi	[Gestionnaire du compte] [Authentification] [Modèle] [Emplacement des accusés]
Test	[Dernier test d'accès] [Résultat] [Question ouverte et responsable]

Avant de valider la fiche

- Le juridique a vérifié l'entité, le rôle, la règle nationale et la date d'application.
- Déclarant et suppléant accèdent au portail ; les contacts de secours sont disponibles hors ligne.
- Les identifiants sont dans un coffre approuvé, pas dans cette fiche.

Contrôle qualité : Si des faits manquent, conserver le statut « à clarifier ». Nommer responsable et échéance plutôt que présumer une exemption.

Fiches réutilisables d'actions et de preuves

Créer une action par lacune, liée à l'exigence et au contrôle. Conserver les preuves sensibles dans un espace contrôlé ; le registre les référence sans les dupliquer.

Champ de la fiche	Contenu à saisir
Exigence et lacune	[ID action] [Entité] [Texte et article] [Lacune précise et impact]
Action et responsabilité	[Action] [Responsable nommé] [Équipe de réalisation] [Priorité] [Échéance]
Traitement temporaire	[Mesure compensatoire] [Approbation] [Expiration] [Licéité vérifiée]
Test de clôture	[Population et méthode] [Résultat attendu] [Date du test] [Réviseur]
Preuve et statut	[Lien preuve] [Périmètre et période] [Résultat réel] [Ouvert / en cours / testé / clos]

Exemple rempli

Lacune : accès fournisseur privilégié à un service critique sans authentification forte. Action : imposer l'authentification approuvée et supprimer les comptes inutilisés. Responsable : service d'identité. Clôture : tester chaque accès et rapprocher les comptes actifs. Preuves : configuration datée, tests et exceptions approuvées. Relier à l'exigence précise, sans déclarer tout le texte satisfait.

Les fiches et cibles proposées appuient : [NIS2 Art. 21\(2\)\(f\)](#) · [DORA Art. 6\(5\)-\(6\)](#) · [RGPD Art. 24\(1\)](#)

Tableau de bord mensuel de direction

Indicateur	Cible proposée	Escalader si
Entités prioritaires au périmètre approuvé	100 % du périmètre prioritaire	Une activité réglementée reste non résolue ou en retard.
Actions de priorité 1 en retard	0	Une action reste en retard.
Services critiques réussissant les tests de reprise	100 % des tests programmés	Un service manque son objectif de reprise.
Accès critiques conformes au standard	100 % ou traitement temporaire approuvé	Un accès exposé manque de protections adaptées.
Circuits de notification avec accès testé et suppléant	100 % des circuits applicables	Un circuit requis est inutilisable.
Actions closes avec preuve vérifiée indépendamment	100 % des clôtures échantillonnées	Une clôture repose seulement sur une politique ou une affirmation.

Ces cibles sont des recommandations de gestion, pas des garanties juridiques. Définir dénominateurs, période et sources de preuves. Distinguer obligation, couverture du contrôle et résultat opérationnel.

Suivre les échéances et les modifications

Référence juridique : 8 octobre 2026. Vérifier modifications et transposition nationale avant une décision importante de périmètre ou de notification. Conserver version et date d'application dans le registre juridique.

Instrument	Date ou déclencheur	Action pratique
NIS2	Délai de transposition UE : 17 octobre 2024.	Vérifier droit national, enregistrement et notifications locales. NIS2 Art. 41(1)
DORA	Applicable depuis le 17 janvier 2025.	Appliquer dès maintenant le cadre et les normes techniques actuelles. DORA Art. 64
CRA	Notifications depuis le 11 septembre 2026 ; exigences principales le 11 décembre 2027.	Notifier selon l'article 14 ; planifier conformité produit et preuves du cycle de vie. CRA Art. 71 · CRA Art. 69(3)
Règlement IA	Application générale le 2 août 2026, avec exceptions échelonnées et modifiées.	Appliquer les obligations pertinentes de maîtrise, interdictions, GPAI et transparence. 2026/1744 Art. 1(40) · Règl. IA modifié Art. 4(1)
IA à haut risque	2 décembre 2027 pour les obligations concernées de l'annexe III ; 2 août 2028 pour l'annexe I.	Utiliser l'article 113 modifié et vérifier les transitions des systèmes existants. 2026/1744 Art. 1(40)
Transition IA	Certaines nouvelles interdictions et transition de marquage des systèmes existants : 2 décembre 2026.	Vérifier le champ exact des articles 5 et 50 après modification. Règl. IA modifié Art. 111(4) · 2026/1744 Art. 1(40)
Data Act	Application générale le 12 septembre 2025. L'article 3(1) vise les produits et services connexes mis sur le marché après le 12 septembre 2026.	Vérifier l'accès dès la conception des nouveaux produits. Data Act Art. 50
Data Act changement	Suppression des frais de changement dès le 12 janvier 2027.	Revoir les clauses de sortie et distinguer les autres frais autorisés. Data Act Art. 29(1)
CER et eIDAS	Les délais CER dépendent de la notification de désignation. Les obligations de portefeuille dépendent du rôle et des actes d'exécution.	Consigner déclencheurs et échéances réels ; éviter une date unique pour tout le groupe. CER Art. 6(3) · CER Art. 12(1) · eIDAS Art. 5a(1) · eIDAS Art. 5f

Sources officielles complémentaires

Références juridiques [Exécution NIS2 Règlement 2024/2690](#) | [Notification DORA Règlement 2025/301](#) | [Modification IA 2026/1744](#) | [Modification eIDAS 2024/1183](#)

RGPD et DSA sont déjà généralement applicables. Ajouter les règles nationales et sectorielles pertinentes. Les textes officiels font foi ; responsables proposés, tests et plan offrent une méthode pratique d'application des exigences identifiées.