Luxgap
DATA PRIVACY PARTNER

RÈGLEMENT (UE) 2022/2554

EN APPLICATION DEPUIS LE 17 JANVIER 2025

DORA — Digital Operational Resilience Act

Passer de la conformité « papier » à une **résilience opérationnelle mesurable**. Luxgap accompagne vos équipes pour réduire le risque ICT, répondre aux exigences de supervision, et industrialiser la gestion des incidents, tests et prestataires.

Julien Winkin – Julien.winkin@luxgap.com +352 621 583 116

Pourquoi DORA change la donne — vraiment

Le règlement DORA (Digital Operational Resilience Act) marque un tournant majeur dans la régulation du secteur financier européen. Pour la première fois, un texte impose des **exigences uniformes et contraignantes** sur la sécurité des réseaux et systèmes d'information supportant les processus métiers de l'ensemble des entités financières — et de leurs prestataires ICT.

Contrairement aux directives précédentes, DORA ne se contente pas de recommandations : il exige des **preuves tangibles** d'une résilience opérationnelle effective. La conformité « déclarative » ne suffit plus. Les superviseurs attendent désormais une résilience *prouvable*, fondée sur des artefacts, des processus opérés et des traces documentées.

Gestion des risques ICT

Cadre complet, politiques, inventaires, contrôles, BCP/DR et monitoring continu des risques technologiques

Notification des incidents

Incidents ICT majeurs + notification volontaire des cybermenaces significatives selon des templates harmonisés UE

Tests de résilience

Programme de tests adapté au risque incluant TLPT pour les entités significatives

Partage d'informations

Mécanismes contrôlés de partage de renseignements sur cybermenaces et vulnérabilités entre entités

Risque prestataires ICT

Cadre de supervision des prestataires critiques, registre, clauses contractuelles et stratégies de sortie

➡️ **Objectif DORA :** une résilience *evidence-based* — chaque exigence doit être adossée à des preuves concrètes, pas à de simples déclarations d'intention.

Qui est concerné ? Le champ d'application en pratique

DORA vise **la quasi-totalité de l'écosystème financier européen**. Son périmètre est volontairement large : il ne s'agit plus de réguler uniquement les grandes banques, mais d'assurer la résilience de l'ensemble de la chaîne de valeur financière, y compris les acteurs qui en dépendent technologiquement.

Entités financières directement soumises

- **Établissements de crédit** (banques commerciales, banques d'investissement)
- **Entreprises d'assurance et de réassurance**
- **Entreprises d'investissement** et sociétés de gestion d'actifs
- **Infrastructures de marché** (CCP, dépositaires centraux, plateformes de négociation)
- **Établissements de paiement** et établissements de monnaie électronique
- **Intermédiaires d'assurance** — y compris accessoire (référence explicite à l'art. 2(1) du règlement)
- **Fonds de pension professionnels**, agences de notation, administrateurs d'indices de référence
- **Prestataires de services sur crypto-actifs**

Prestataires ICT — indirectement mais fortement impactés

Même sans être directement régulés, vos fournisseurs ICT sont concernés **par ricochet** via les obligations que DORA impose aux entités financières :

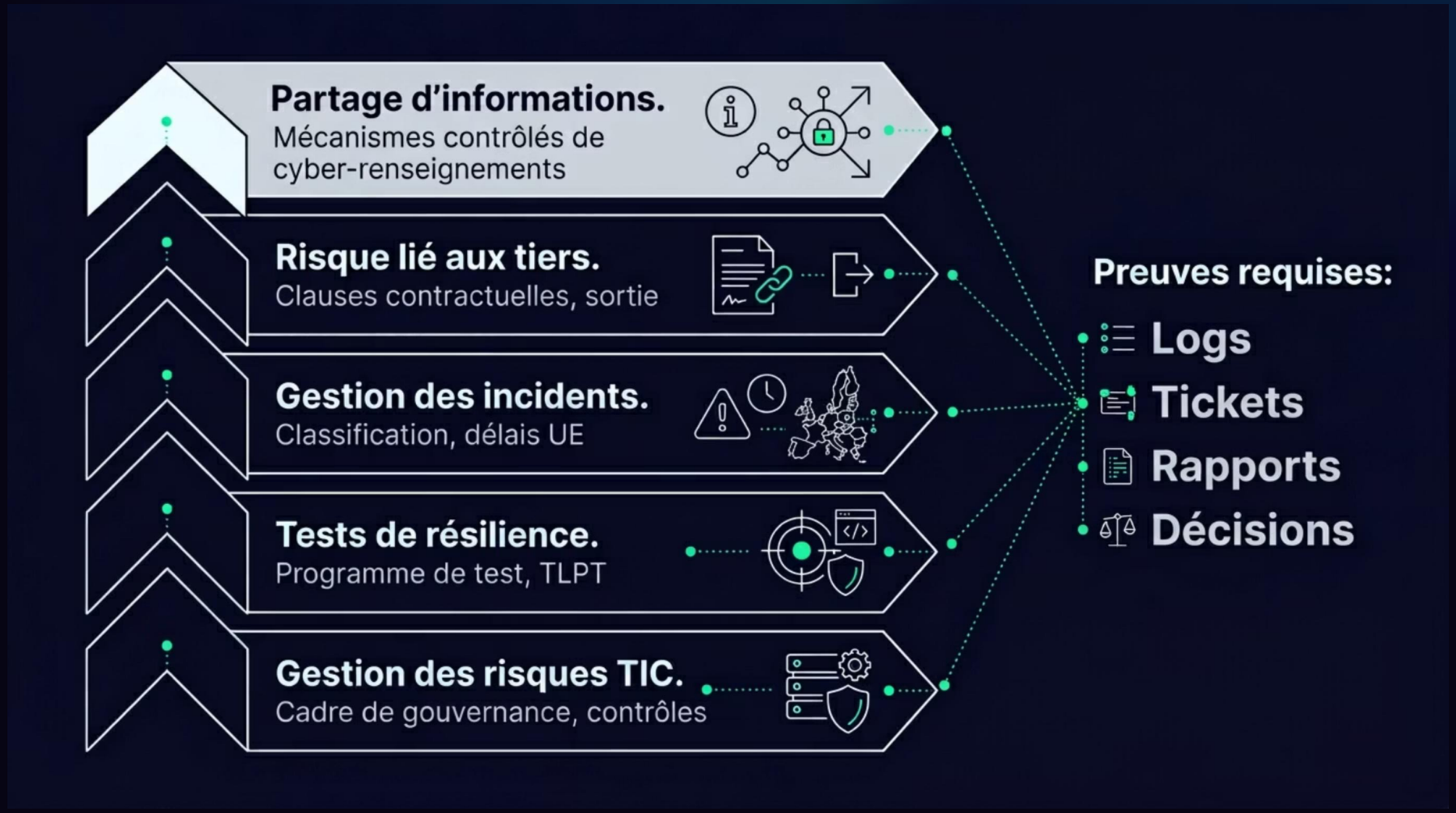
- **Cloud providers** (IaaS, PaaS, SaaS)
- **SOC / MSSP** (centres opérationnels de sécurité)
- **Éditeurs SaaS** critiques
- **MSP / infogérants**
- **Prestataires de données** et hébergeurs

Implications : obligations contractuelles renforcées, registre d'information, droit d'audit, exigences de localisation des données, et stratégie de sortie documentée.

VUE D'ENSEMBLE

Les 5 piliers DORA — et la « preuve » attendue

DORA s'articule autour de cinq piliers fondamentaux. Chacun d'entre eux ne se résume pas à une politique documentée : les superviseurs attendent des **artefacts concrets**, des **processus opérés en continu** et des **traces vérifiables** (logs, tickets, rapports de tests, décisions de comités, communications de crise).



➡️ **Chaque pilier = artefacts + processus opérés + traces.** La supervision européenne récompense la cohérence, la traçabilité et la capacité d'exécution — pas le volume de documentation.

Notre promesse Luxgap : DORA utile = Résilience + Pilotage

Chez Luxgap, nous considérons que la conformité DORA n'a de valeur que si elle **sert réellement votre résilience opérationnelle**. Nous ne livrons pas des classeurs — nous construisons des capacités mesurables, testées et auditables. Notre approche transforme chaque exigence réglementaire en un levier concret de réduction du risque et d'amélioration de la performance opérationnelle.

1

Réduire le downtime

Prévention proactive, détection rapide, réponse structurée et restauration accélérée. Chaque minute de disponibilité préservée protège votre chiffre d'affaires et la confiance de vos clients.

2

Accélérer la décision en crise

Rôles clairs, scénarios pré-établis, runbooks opérationnels et plans de communication prêts à l'emploi. En situation de crise, la vitesse de décision est votre premier bouclier.

3

Sécuriser l'externalisation ICT

Contrats conformes, registre d'information actualisé, droit d'audit effectif et stratégie de sortie testée. Vos prestataires deviennent des partenaires de résilience, pas des sources de risque.

4

Réussir les contrôles

Dossier « audit-ready » structuré, preuves cohérentes, traçabilité groupe. Vous abordez chaque inspection avec sérénité et démontrez votre maîtrise.

5

Industrialiser la démarche

Mesure continue, tests réguliers, amélioration itérative et formation des équipes. La conformité n'est pas un projet ponctuel — c'est une discipline pérenne.

PILIER 1

ICT Risk Management — Ce que DORA exige, concrètement

Le premier pilier de DORA constitue le socle de l'ensemble du dispositif. Il impose un cadre de gestion des risques ICT qualifié de **« sound, comprehensive and well-documented »** (solide, complet et bien documenté). Ce n'est pas un exercice théorique : les superviseurs attendent un cadre vivant, opéré au quotidien, et dont chaque composante est adossée à des preuves concrètes. Luxgap met en place — ou renforce — chaque brique de ce cadre.

Gouvernance ICT

Définition claire des rôles et responsabilités, création ou renforcement des comités dédiés (comité risque ICT, comité sécurité), mise en place du reporting vers l'organe de direction. L'art. 5 de DORA rend l'organe de direction **directement responsable** du cadre ICT risk management.

Inventaire ICT & classification

Cartographie exhaustive des actifs ICT (systèmes, applications, données, réseaux), classification des services et fonctions en **« critiques / importantes »**, identification des dépendances internes et externes — y compris la chaîne de sous-traitance.

Politiques & standards

Rédaction ou mise à jour des politiques couvrant : gestion des accès (IAM), chiffrement, gestion des vulnérabilités, journalisation (logs), gestion des changements (change management), sécurité des réseaux. Chaque politique est alignée sur les RTS de l'EBA.

BCP/DR — Continuité & reprise

Plans de continuité d'activité et de reprise après sinistre couvrant les fonctions critiques, objectifs de restauration définis (RTO/RPO), tests réguliers documentés, et mise à jour itérative après chaque exercice ou incident réel.

Monitoring & indicateurs

Mise en place d'indicateurs clés de risque (KRIs), d'alertes précoces, de tableaux de bord de suivi d'efficacité des contrôles. Le monitoring doit être **continu**, pas ponctuel — DORA exige une surveillance active des menaces et des vulnérabilités.

Sources : art. 6 du règlement DORA (cadre ICT) ; RTS cadre de gestion des risques ICT (EBA)

PILIER 1 — ZOOM

Le « DORA Evidence Pack » — Ce qui fait gagner en audit

L'un des changements les plus significatifs apportés par DORA est l'exigence de **preuves tangibles et traçables** pour chaque composante du cadre ICT. Les superviseurs ne se contentent plus de lire des politiques : ils vérifient leur application effective. Luxgap constitue pour vous un **DORA Evidence Pack** structuré, maintenable et directement exploitable en cas de contrôle.

01

Registre des actifs & cartographie

Inventaire exhaustif avec classification « critique / important » de chaque actif, service et fonction. Cartographie des interdépendances et identification des points de défaillance uniques (SPOF).

02

Catalogue des contrôles

Mapping tri-dimensionnel : exigences DORA ⟷ contrôles ⟷ preuves. Chaque exigence réglementaire est rattachée à un ou plusieurs contrôles opérationnels, eux-mêmes adossés à des preuves vérifiables.

03

Politique de continuité / reprise

Documentation BCP/DR complète incluant les résultats de tests, les écarts identifiés, les actions correctives engagées et les validations par la direction.

04

Tableaux de bord KRIs

Indicateurs clés de risque couvrant : vulnérabilités ouvertes, incidents en cours, disponibilité des systèmes critiques, conformité des contrôles. Suivi historique et tendances.

05

Plan de remédiation priorisé

Priorisation par criticité du risque, effort de mise en œuvre et dépendances. Suivi des jalons, responsables identifiés, et reporting de progression vers la direction.

Conseil Luxgap : Un dossier de preuves bien structuré réduit de 40 à 60 % le temps de préparation aux contrôles et élimine le stress des inspections de dernière minute.

PILIER 2

Testing & TLPT — Sortir du « pentest annuel »

DORA élève significativement le niveau d'exigence en matière de tests de résilience. Fini le pentest annuel « pour cocher la case » : le règlement impose un **programme de tests adapté au profil de risque** de chaque entité, couvrant l'ensemble du spectre — des scans de vulnérabilités aux exercices de crise en passant par les tests de reprise. Pour les entités les plus significatives, DORA peut imposer du **Threat-Led Penetration Testing (TLPT)**, aligné sur le cadre TIBER-EU.

Stratégie de tests

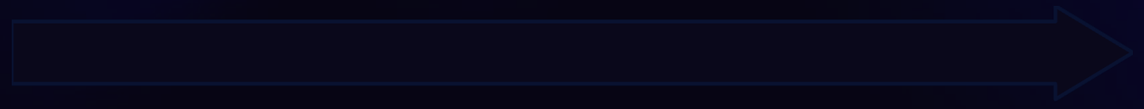
Conception d'un programme pluriannuel intégrant : scans de vulnérabilités (hebdomadaires), revues de configuration, tests d'intrusion (pentests), exercices de gestion de crise, tests de continuité et de reprise (DR tests). Chaque type de test est calibré sur la criticité des fonctions concernées.

Gouvernance des tests

Définition de l'indépendance des testeurs, du périmètre couvert, des critères d'acceptation des résultats, et des conditions de retest. La gouvernance garantit que les tests produisent des résultats exploitables et non biaisés.

Chaîne de remédiation

Tracking systématique des vulnérabilités identifiées, SLA de remédiation par criticité, validation des corrections et retest automatisé. Aucune faille ne reste sans suivi.



Préparation TLPT

Pour les entités éligibles : approche alignée TIBER-EU, constitution du dossier superviseur, sélection des prestataires de threat intelligence et de red team, gestion des exigences RTS spécifiques au TLPT.

Sources : art. 24-27 du règlement DORA ; RTS TLPT (référence TIBER-EU)

⚠ PILIER 3

Incident Management & Reporting — Classification et notification harmonisées

DORA standardise au niveau européen la classification des incidents ICT et les délais de notification aux autorités compétentes. Les RTS et ITS publiés en 2024-2025 définissent précisément les critères, seuils, templates et calendriers. La fenêtre de réaction est serrée : **4 heures après classification** pour la notification initiale, 72 heures pour le rapport intermédiaire, 1 mois pour le rapport final.

Délais réglementaires

1 **Détection → Classification**

Identification de l'incident et application des critères de classification « majeur / non-majeur » selon le RTS 2024/1772

2 **Notification initiale : 4h**

Après classification (et dans les 24h après détection). Transmission aux autorités compétentes via templates harmonisés ITS 2025/302

3 **Rapport intermédiaire : 72h**

Mise à jour de l'analyse, mesures prises, estimation de l'impact et premières actions correctives engagées

4 **Rapport final : 1 mois**

Analyse complète de l'incident, causes racines, impact définitif, leçons apprises et actions correctives

L'Incident Reporting Kit Luxgap

Nous livrons un kit opérationnel complet, directement exploitable par vos équipes SOC, IT, juridiques et communication :

Arbre de décision

Critères et seuils « majeur / non-majeur » formalisés, RACI de classification, escalade automatique vers les bons interlocuteurs

Playbooks opérationnels

Procédures SOC, IT, Legal et Communications — couvrant la notification interne, vers les autorités et vers les clients impactés

Templates préremplis

Formulaires harmonisés UE pré-complétés avec les données statiques de votre entité + procédure de collecte garantissant qualité et traçabilité

PILIER 3 — MODÈLE OPÉRATIONNEL

Notre modèle « 7 phases » — De l'obligation au processus incident actionnable

Luxgap ne se contente pas de documenter une procédure d'incident : nous transformons l'obligation DORA en un **processus opérationnel prêt à exécuter**, testé régulièrement et adossé à des preuves à chaque étape. Ce modèle couvre l'intégralité du cycle de vie d'un incident, de la préparation à l'amélioration continue.

1. Préparation & prévention

Scénarios de risque, veille menaces, hardening, formation des équipes, pré-positionnement des outils et des contacts

2. Détection & réponse immédiate

Alertes automatisées, triage initial, activation du RACI, notification initiale dans les délais réglementaires

3. Confinement, éradication & atténuation

Isolation des systèmes affectés, élimination de la menace, réduction de l'impact sur les fonctions critiques

4. Recovery & restauration

Restauration des services selon les objectifs RTO/RPO, vérification de l'intégrité des données, reprise progressive des opérations

5. Analyse post-incident & adaptation

Root cause analysis, timeline documentée, leçons apprises, rapport final aux autorités, ajustement des contrôles

6. Amélioration continue & mise à jour

Intégration des retours d'expérience, mise à jour des procédures, re-calibration des alertes, enrichissement des scénarios

➡️ **Le facteur différenciant :** à chaque phase, des **preuves** sont générées et conservées — tickets, timelines horodatées, décisions de comité, communications tracées. C'est cette discipline de traçabilité qui fait la différence en contrôle.

PILIER 4

Prestataires ICT — Le vrai sujet : registre, contrats & exit

Le pilier 4 de DORA est souvent celui qui génère le plus de travail opérationnel. Il ne s'agit plus simplement de « gérer les fournisseurs » : DORA exige une **maîtrise complète de la chaîne de sous-traitance ICT**, avec des obligations contractuelles précises, un registre d'information normalisé et des stratégies de sortie réellement testables. Les textes de niveau 2 (RTS et ITS) publiés en 2024-2025 détaillent chaque exigence.

RTS 2024/1773	ITS 2024/2956	RTS 2025/532
Politique sur les accords contractuels pour services ICT supportant des fonctions critiques ou importantes	Registre d'information standardisé sur les accords ICT — format, contenu et fréquence de mise à jour	Exigences spécifiques sur la sous-traitance ICT, y compris la chaîne de sous-traitants

Ce que Luxgap opère pour vous

1

Inventaire complet

Cartographie de tous les prestataires ICT, évaluation de la criticité, identification des dépendances — y compris la « chain of subcontractors » souvent négligée. Analyse du risque de concentration.

2

Remédiation contractuelle

Revue et mise en conformité des clauses : droit d'audit, accès aux données, localisation, notification d'incidents, SLA de performance et de sécurité, transferabilité, coopération avec les autorités.

3

Stratégie de sortie testable

Plan d'exit documenté pour chaque prestataire critique : réversibilité des données, continuité de service pendant la transition, alternatives identifiées, et test périodique de la faisabilité du plan.

FOCUS RÉGLEMENTAIRE

Oversight des prestataires critiques (CTPP) — Anticiper les contrôles

Les Autorités européennes de surveillance (ESAs : EBA, EIOPA, ESMA) ont le pouvoir de **désigner des prestataires ICT comme « critiques » (CTPP — Critical Third-Party Providers)**, les soumettant ainsi à un cadre de supervision directe. Cette désignation a des implications majeures — pas seulement pour le prestataire, mais pour **toutes les entités financières qui en dépendent**.

Implications pour votre organisation

Même si vous n'êtes pas un cloud provider, vos contrats et votre gouvernance doivent répondre à des exigences strictes :

Auditabilité & accès

Vos contrats doivent garantir que les autorités de supervision — et vous-même — pouvez auditer le prestataire, accéder à ses locaux, obtenir les informations nécessaires. Ce droit ne peut être limité par des clauses de confidentialité.

Concentration & dépendances

Vous devez identifier et maîtriser les risques de concentration : combien de fonctions critiques dépendent du même prestataire ? Existe-t-il des alternatives viables ? Le risque systémique est-il documenté ?

Exit crédible

La stratégie de sortie ne peut pas être un document théorique rangé dans un tiroir. Elle doit être **réaliste, testée et actualisée** — avec des délais de migration, des coûts estimés et des alternatives opérationnelles.

Ce que les superviseurs récompensent : cohérence + traçabilité

Les retours d'expérience des premières inspections montrent clairement ce qui distingue un programme DORA « solide » d'un programme fragile. Les superviseurs ne cherchent pas la perfection : ils cherchent la **cohérence**, la **traçabilité** et la **capacité d'exécution**. Voici les marqueurs concrets qui font la différence lors d'un contrôle.

Un registre ICT vivant

Prêt à être transmis aux autorités à tout moment, avec un **processus de mise à jour documenté** et des responsables identifiés. Pas un fichier Excel figé depuis 6 mois — un registre opérationnel alimenté en continu.

Des incidents classés de manière reproductible

Critères de classification appliqués de façon homogène, arbre de décision formalisé, et **reporting dans les délais** — 4h, 72h, 1 mois. La reproductibilité de la classification est un point clé d'audit.

Des tests planifiés, suivis et retestés

Programme de tests documenté, résultats tracés, **remédiation pilotée avec SLA**, et retest systématique des vulnérabilités corrigées. Le suivi de bout en bout est la preuve d'une démarche mature.

Des contrats alignés DORA

Pour toutes les fonctions critiques et importantes : clauses conformes aux RTS, droit d'audit effectif, notification d'incidents, SLA documentés, et **stratégie de sortie crédible**.

OFFRE LUXGAP

Modules « à la carte » — Résultat garanti, adossé aux preuves

Notre offre DORA est conçue pour s'adapter à votre niveau de maturité et à vos priorités. Chaque module est autonome et peut être activé indépendamment, tout en s'intégrant parfaitement dans une démarche globale. Du diagnostic initial à l'opération continue, nous couvrons l'intégralité du cycle de vie de votre programme DORA.

1. DORA QuickScan

Direction + IT + Risk + Legal

Cartographie de l'applicabilité, délimitation du périmètre, évaluation du niveau de maturité actuel, et identification des priorités. Livrable : rapport de positionnement avec recommandations d'action immédiate.

2. DORA Gap & Roadmap

Pilier par pilier

Gap analysis détaillée par rapport aux exigences DORA et RTS/ITS, définition de la cible, construction du plan de remédiation priorisé avec estimation de l'effort, des dépendances et du calendrier de mise en œuvre.

3. DORA Build

Implémentation & documentation

Construction opérationnelle : rédaction des politiques et procédures, mise en place du registre d'information, création du kit incident, conception du programme de tests, élaboration des clauses fournisseurs conformes.

4. DORA Run

Opération & amélioration continue

Pilotage opérationnel du programme : tableaux de bord de suivi, exercices réguliers, revues périodiques, mise à jour continue des preuves et de la documentation. La conformité devient une discipline pérenne.

💡 **Logique « amélioration continue » :** Chaque module alimente le suivant. Les preuves générées en phase Build sont maintenues en phase Run. Les retours d'exercices enrichissent les gaps identifiés. Votre programme DORA gagne en maturité à chaque cycle.

Livrables concrets — Ce que vous pourrez montrer demain en contrôle

Chaque livrable Luxgap est conçu pour être directement exploitable en situation de contrôle ou d'audit. Pas de documentation abstraite : des **artefacts opérationnels, structurés et maintenables** qui démontrent votre maîtrise de chaque pilier DORA.

ICT Risk Management Framework

Cadre complet incluant le mapping exigences ↔ contrôles ↔ preuves. Document vivant servant de référentiel pour l'ensemble du programme.

Inventaire actifs & fonctions critiques

Registre des actifs, services et fonctions ICT avec criticité, dépendances internes/externes et cartographie des risques associés.

Programme de tests

Planning pluriannuel, scénarios de test, rapports d'exécution, suivi des remédiations et retests. Gouvernance et critères d'acceptation formalisés.

Incident Reporting Kit

Arbre de classification, RACI, templates de notification (ITS), procédure de collecte des données et playbooks par type de partie prenante.

Registre prestataires (ITS)

Registre d'information conforme au format ITS 2024/2956, processus de maintien à jour documenté, et alertes sur les échéances contractuelles.

Politique contractuelle & plan d'exit

Modèles de clauses conformes pour fonctions critiques/importantes, plans de sortie testables par prestataire, et analyse du risque de concentration.

SERVICE CONTINU

DORA-as-a-Service — Ce qui rend l'offre utile au quotidien

La conformité DORA ne s'arrête pas au « Go Live ». Les exigences sont continues, les menaces évoluent, et les superviseurs attendent une **amélioration permanente**. Luxgap propose un accompagnement récurrent qui maintient votre programme DORA vivant, opérationnel et à jour — sans mobiliser vos équipes en permanence.

E-learning & sensibilisation

Programme de formation continu et traçable couvrant la sécurité ICT et la résilience opérationnelle. Modules adaptés par profil (direction, IT, métier, compliance). Chaque session est documentée pour constituer une preuve de formation lors des contrôles — conformément à l'exigence DORA de sensibilisation des collaborateurs.

Scans de vulnérabilités hebdomadaires

Scans automatisés sur l'ensemble du périmètre ICT, avec rapport de vulnérabilités classé par criticité. Suivi de la remédiation intégré : chaque vulnérabilité est trackée jusqu'à sa résolution. Historique complet disponible pour démontrer la discipline de correction.

Revue & mise à jour documentaire

Revue périodique de l'ensemble du corpus documentaire : politiques, standards, procédures, preuves. Mise à jour proactive en fonction des évolutions réglementaires (nouveaux RTS/ITS, guidelines ESAs) et des retours d'expérience internes.

Revues périodiques

Exercices réguliers (tests incidents, DR, crise), revue des plans de continuité, analyse des incidents survenus, et intégration des leçons apprises dans le programme. Chaque revue produit un PV documenté alimentant le DORA Evidence Pack.

Pourquoi Luxgap — Notre différenciation

Le marché du conseil en conformité réglementaire ne manque pas d'acteurs. Ce qui distingue Luxgap, c'est notre capacité à articuler **exigence juridique et réalité opérationnelle** — pour produire une conformité qui fonctionne en pratique, pas seulement sur le papier.

Double lecture : juridique + technique

Nous maîtrisons à la fois les obligations réglementaires (règlement DORA, RTS, ITS, guidelines ESAs) et leur traduction opérationnelle (contrôles, runbooks, preuves techniques). Cette double compétence évite le décalage fréquent entre ce que le texte exige et ce que les équipes IT implémentent.

Orientation supervision

Nous savons ce que les superviseurs cherchent lors d'un contrôle : **cohérence entre documentation et réalité**, traçabilité des décisions, et capacité d'exécution démontrée. Notre approche est calibrée pour maximiser votre performance en audit.

Approche pragmatique

Nous priorisons les risques réels et les fonctions critiques, sans « paperware » inutile. Chaque livrable a un usage opérationnel identifié. Nous refusons la documentation qui n'existe que pour elle-même.

Industrialisation pérenne

Formation continue des équipes, scans automatisés, maintenance documentaire récurrente — nous installons les mécanismes qui font vivre votre conformité dans la durée, sans dépendance excessive au conseil externe.

> « Ce qui compte en contrôle = cohérence, traçabilité, exécution. Luxgap construit des programmes DORA qui passent l'épreuve du réel — pas seulement celle du papier. »

PASSEZ À L'ACTION

Prochaine étape — Simple et efficace

DORA est en application depuis le **17 janvier 2025**. Chaque jour qui passe sans programme structuré augmente votre exposition réglementaire et opérationnelle. La bonne nouvelle : il est encore temps de construire un dispositif solide, à condition d'agir maintenant avec méthode.

1

Cadrage du périmètre

Identification des entités, des fonctions critiques et importantes, et des prestataires ICT concernés. Définition des frontières du programme et des parties prenantes clés.

2

QuickScan & priorisation

Évaluation rapide de votre maturité DORA, identification des écarts majeurs, et priorisation par criticité du risque, impact métier et effort de mise en œuvre.

3

Lancement des « must-have »

Démarrage immédiat sur les fondamentaux : registre d'information, kit incident, remédiation contractuelle, programme de tests et constitution des preuves.

17/01

Date d'application

DORA est pleinement applicable depuis janvier 2025

5

Piliers d'exigences

Couvrant risques, tests, incidents, prestataires et partage

4h

Délai de notification

Pour les incidents ICT majeurs après classification

Contactez Luxgap dès aujourd'hui pour planifier votre QuickScan et engager votre trajectoire vers une résilience opérationnelle mesurable, prouvable et durable.

Julien Winkin – Julien.winkin@luxgap.com +352 621 583 116