

Versa Sovereign SASE et conformité DORA

Répondre aux exigences de résilience opérationnelle du secteur financier de l'UE avec Versa Sovereign SASE

Le règlement sur la résilience opérationnelle numérique (DORA) établit des exigences contraignantes quant à la manière dont les entités financières de l'UE doivent gérer les risques liés aux technologies de l'information et de la communication (TIC), maintenir leur résilience opérationnelle et superviser leurs prestataires technologiques. Le respect de ces obligations nécessite une infrastructure prenant en charge des opérations sécurisées, la réponse aux incidents, les tests de résilience et l'auditabilité réglementaire sur l'ensemble de l'environnement TIC. Versa Sovereign SASE fournit une solution SASE complète, conçue spécifiquement pour les organisations réglementées, en maintenant les plans de données, de contrôle et de gestion au sein de la juridiction de l'UE, tout en prenant en charge des modèles de déploiement managés ou sur site. Pour les organisations soumises à DORA, Versa offre une voie directe vers la conformité, sans sacrifier les capacités de sécurité ni la flexibilité opérationnelle qu'exigent les infrastructures critiques modernes.

Le cadre DORA

Le règlement sur la résilience opérationnelle numérique (DORA) (Règlement (UE) 2022/2554), entré en vigueur le 17 janvier 2025, établit un cadre unifié pour la gestion des risques TIC et la résilience opérationnelle dans l'ensemble du secteur financier de l'UE, couvrant les entités financières ainsi que les prestataires tiers critiques de services TIC.

DORA regroupe des exigences sectorielles existantes au sein d'un règlement unique articulé autour de six domaines clés :

- Gestion des risques TIC : gouvernance, cadres de gestion des risques, visibilité des actifs, contrôles d'accès, détection des menaces, réponse aux incidents, sauvegarde et récupération, ainsi qu'amélioration continue
- Gestion et notification des incidents TIC : processus définis pour classer, gérer et notifier les incidents TIC majeurs aux autorités de contrôle
- Tests de résilience opérationnelle : tests réguliers des systèmes et processus TIC, y compris des tests de pénétration fondés sur la menace (TLPT - Threat-Led Penetration Testing) pour les entités importantes
- Gestion des risques liés aux prestataires tiers TIC : supervision des prestataires technologiques, incluant les exigences contractuelles, d'audit, de risque de concentration et de stratégie de sortie
- Partage d'informations : partage volontaire de renseignements sur les cybermenaces entre entités financières
- Supervision des prestataires TIC critiques : supervision au niveau de l'UE pour les prestataires désignés comme systémiquement critiques

Contrairement aux réglementations principalement axées sur la protection des données, DORA cible directement la résilience opérationnelle, exigeant des entités financières qu'elles démontrent des opérations TIC sécurisées, résilientes et auditables sur l'ensemble de leurs réseaux, systèmes et environnements technologiques tiers.

Versa Sovereign SASE

Dans ce contexte réglementaire, Versa Sovereign SASE propose une architecture conçue spécifiquement pour répondre à des exigences strictes en matière d'exploitation, de sécurité et de gouvernance, offrant des capacités complètes de réseau et de sécurité tout en maintenant les données, le contrôle et l'exploitation au sein de frontières souveraines.

En tant que modèle de déploiement de la plateforme VersaONE Universal SASE, cette solution répond à une limite majeure du SASE cloud traditionnel : même avec des points de présence locaux, l'inspection du trafic, les décisions de politique et la gestion de la plateforme peuvent continuer à dépendre d'une infrastructure située hors de la juridiction visée.

Versa Sovereign SASE aligne les trois plans de l'architecture SASE au sein d'un environnement d'exploitation souverain :

- **Plan de contrôle** : la validation d'identité, l'évaluation des politiques et les décisions de connexion s'effectuent au sein de l'environnement souverain désigné.
- **Plan de données** : l'inspection du trafic, la protection contre les menaces et le filtrage de contenu sont exécutés au niveau des points de présence locaux, sans détournement du trafic pour traitement hors juridiction.
- **Plan de gestion** : l'administration de la plateforme, la journalisation, la configuration et l'accès opérationnel restent gouvernés localement.

Dans l'UE, le service Sovereign SASE-as-a-Service de Versa est disponible avec l'ensemble des opérations, du traitement des données et du support régis par le droit de l'UE, indépendamment de l'infrastructure cloud mondiale de Versa. Pour les organisations exigeant un contrôle infrastructurel complet, Versa Sovereign SASE est également disponible en déploiement on-premise ou en cloud privé au sein de l'UE.

Correspondance entre les exigences DORA et Versa Sovereign SASE

Le tableau suivant illustre comment les capacités de Versa Sovereign SASE peuvent accompagner les clients dans la mise en œuvre des exigences DORA relatives à la résilience opérationnelle et à la gestion des risques TIC.

Exigence DORA	Capacité Versa Sovereign SASE	Résultat
Chapitre II – Gestion des risques TIC		
Art. 5 – Gouvernance et organisation	Tableau de bord de gestion avec RBAC et séparation des tâches ; gestion unifiée des politiques sur l'ensemble des fonctions de sécurité et de réseau	Soutient la responsabilité de la direction en matière de risques TIC grâce à des contrôles de gouvernance auditables et à des rôles opérationnels définis
Art. 5 – Gouvernance et organisation	Plateforme unifiée VersaONE intégrant NGFW, ZTNA, SWG, IPS, ATP ; journaux d'audit et tableaux de bord centralisés ; tous les plans fonctionnent au sein de frontières souveraines	Soutient la mise en œuvre d'une architecture centralisée de gestion des risques TIC avec une visibilité unifiée et l'application des politiques
Art. 7 – Systèmes, protocoles et outils TIC	SD-WAN sécurisé avec basculement automatique et résilience multi-chemins ; chiffrement Perfect Forward Secrecy et AES-256 ; passerelles géo-redondantes	Soutient une connectivité TIC résiliente et des communications sécurisées grâce à la redondance et à des contrôles cryptographiques modernes

Art. 8 – Identification	Découverte automatisée des équipements et empreintes numériques ; détection du Shadow IT via CASB ; visibilité applicative par DPI ; établissement de référence comportementale UEBA	Identifie et classe les actifs TIC, les dépendances cloud et les schémas d'accès anormaux, en appui à l'inventaire des actifs et des risques
Art. 9 – Protection et prévention	ZTNA avec évaluation continue de la posture ; MFA ; DLP avec modèles prédéfinis (PII, RGPD, PCI-DSS) ; pare-feu GenAI ; SWG ; plan de contrôle localisé avec décisions d'accès contenues au sein des frontières souveraines	Applique l'accès selon le principe du moindre privilège, une authentification forte et des contrôles de protection des données, avec des décisions de politique entièrement gouvernées au sein de l'environnement souverain
Art. 10 – Détection	UEBA avec détection d'anomalies pilotée par IA ; ATP avec multi-antivirus, IA/ML et bac à sable ; NG-IPS ; détection de tunnels DNS ; DEM pour les anomalies de performance ; le tout aligné sur MITRE ATT&CK	Fournit une détection continue et en temps réel des menaces et des anomalies TIC, avec une classification structurée alignée sur un cadre de menaces standardisé
Art. 11 – Réponse et récupération	Basculement automatique du SD-WAN ; passerelles géo-redondantes en haute disponibilité active-active ; actions de confinement ATP ; micro-segmentation pour limiter le rayon d'impact ; opérations de récupération gouvernées au sein du plan de gestion souverain	Soutient des workflows rapides de confinement, de réponse et de récupération au sein des frontières juridiques
Art. 12 – Procédures de sauvegarde et de récupération	Sauvegarde et restauration de la configuration ; journalisation et données de configuration localisées au sein du plan de gestion souverain	Soutient la récupération de l'état des politiques réseau et sécurité, les données de sauvegarde étant stockées au sein de la juridiction souveraine
Art. 13 – Apprentissage et évolution	Cartographie post-incident UEBA et ATP selon MITRE ATT&CK ; mise à jour continue des flux de renseignement sur les menaces ; rapports de sécurité et tableaux de bord centralisés	Permet un examen structuré post-incident et une amélioration continue des contrôles de risques TIC sur la base de renseignements actualisés sur les menaces
Art. 14 – Communication	Alertes et rapports centralisés ; intégration SIEM via IPFIX, Syslog et VMS	Fournit des données d'événements de sécurité opportunes et structurées, en appui aux processus de communication de crise internes et externes

Chapitre III – Gestion et notification des incidents TIC

Art. 17 – Processus de gestion des incidents	Alertes en temps réel UEBA et ATP avec classification automatisée ; journaux d'événements de sécurité NG-IPS et DNS ; diffusion SIEM via IPFIX, Syslog, NetFlow et PCAP ; tableaux de bord par module	Soutient l'alerte précoce, la journalisation structurée des incidents et des rôles de réponse définis, conformément aux exigences DORA en matière de processus de gestion des incidents
Art. 18 – Classification des incidents	DEM pour la quantification de l'impact opérationnel ; notation de gravité ATP et UEBA avec cartographie MITRE ATT&CK ; reporting par service	Fournit des données structurées de gravité et d'impact, en appui à la classification des incidents liés aux TIC selon les critères DORA
Art. 19 – Notification des incidents majeurs	Journalisation complète via IPFIX, Syslog, NetFlow et PCAP ; intégration SIEM via VMS ; l'ensemble des données de journalisation est stocké et traité au sein de la juridiction souveraine	Fournit une journalisation centralisée pour la collecte de preuves et les processus réglementaires de notification des incidents, tout en maintenant le traitement des journaux au sein de la juridiction souveraine

Chapitre IV – Tests de résilience opérationnelle numérique

Art. 24–25 – Tests de résilience opérationnelle numérique	Segmentation réseau ZTNA pour environnements de test contrôlés ; RBAC pour isoler les tests de la production ; cartographie MITRE ATT&CK pour le cadrage des tests ; données de référence ATP et IPS pour les évaluations de vulnérabilités	Permet des tests structurés de résilience et de vulnérabilité avec un rayon d’impact maîtrisé et un historique de configuration documenté pour l’analyse des écarts
Art. 26 – Tests de pénétration fondés sur la menace (TLPT)	Renseignement sur les menaces aligné sur MITRE ATT&CK pour le cadrage des tests ; micro-segmentation ZTNA pour des environnements de test isolés ; la télémétrie et les résultats TLPT restent au sein des frontières souveraines	Soutient les activités TLPT en permettant des environnements de test isolés et un traitement localisé de la télémétrie au sein de modèles de déploiement souverains

Chapitre V – Gestion des risques liés aux prestataires tiers TIC

Art. 28 – Gestion des risques liés aux prestataires tiers	Détection du Shadow IT via CASB ; surveillance de la posture SSPM et CSPM ; protection des données par API sur IaaS et SaaS ; Sovereign SASE-as-a-Service exploité au sein de la juridiction de l’UE	Identifie et surveille les dépendances TIC envers des tiers, tout en soutenant des dispositifs contractuels et opérationnels régis par l’UE pour les services critiques de réseau et de sécurité
Art. 29 – Risque de concentration TIC	Visibilité CASB, CSPM et SSPM sur l’ensemble du paysage des services cloud ; architecture Sovereign SASE fonctionnant indépendamment de l’infrastructure mondiale partagée de Versa	Offre une transparence opérationnelle, des options de déploiement souverain et une dépendance réduite à une infrastructure partagée à l’échelle mondiale
Art. 30 – Dispositions contractuelles clés	Sovereign SASE-as-a-Service avec exploitation régie par l’UE, traitement des données localisé et support ; RBAC et piste d’audit à l’appui des droits d’audit ; plan de contrôle/gestion local avec contrôles d’accès opérationnels vérifiables	Soutient les exigences contractuelles et de supervision de DORA grâce à une exploitation régie par l’UE, un traitement localisé, une journalisation d’audit et des contrôles d’accès opérationnels
Art. 31–44 – Supervision des prestataires TIC critiques	Sovereign SASE contracté via une entité juridique de l’UE avec exploitation localisée ; journalisation et piste d’audit à l’appui des demandes d’information réglementaires ; support et contacts opérationnels régis par l’UE	Fournit des preuves documentées du modèle d’exploitation, à l’appui des évaluations réglementaires et des missions de supervision

Chapitre VI – Partage d’informations

Art. 45 – Partage d’informations	Flux de renseignement sur les menaces (réputation de fichiers, DNS, ATP) ; diffusion SIEM via IPFIX, Syslog et VMS ; alignement MITRE ATT&CK pour un échange de menaces standardisé ; la télémétrie de menaces est conservée au sein de la juridiction souveraine	Permet la participation à des dispositifs sectoriels de partage des menaces tout en minimisant les transferts transfrontaliers de télémétrie
----------------------------------	---	--

Pourquoi les organisations soumises à DORA choisissent Versa

La conformité à DORA exige une infrastructure capable de démontrer le contrôle opérationnel, la résilience et l'auditabilité sur l'ensemble de la pile réseau et sécurité. En tant que premier fournisseur à avoir lancé le Sovereign SASE sur le marché, Versa propose un modèle de déploiement conçu spécifiquement pour les organisations réglementées ayant besoin d'indépendance opérationnelle et de contrôle souverain.

Principales raisons pour lesquelles les entités financières choisissent Versa Sovereign SASE pour leur conformité DORA :

- Souveraineté de bout en bout : les plans de données, de contrôle et de gestion restent au sein d'une infrastructure hébergée et contrôlée dans l'UE
- Capacités SASE complètes : ZTNA, NGFW, SWG, CASB, DLP, IPS, ATP et SD-WAN intégrés au sein d'environnements souverains
- Gouvernance auditable : la journalisation, le RBAC et l'intégration SIEM soutiennent le reporting réglementaire et la supervision des tiers
- Déploiement flexible : disponible en tant que service managé, en déploiement sur site, ou en cloud privé au sein de l'UE

Demandez une démonstration pour voir Versa Sovereign SASE en action.

Découvrez Versa Sovereign SASE.

À propos de Versa

Versa, un leader mondial du SASE, permet aux organisations de créer des réseaux auto-protecteurs qui simplifient et automatisent radicalement leur infrastructure réseau et sécurité. Propulsée par l'IA, la plateforme VersaONE Universal SASE offre des solutions convergentes SSE, SD-WAN et SD-LAN qui protègent les données et défendent contre les cybermenaces, tout en offrant une expérience numérique supérieure. Des milliers de clients dans le monde, avec des centaines de milliers de sites et des millions d'utilisateurs, font confiance à Versa pour leurs réseaux et leur sécurité critiques.