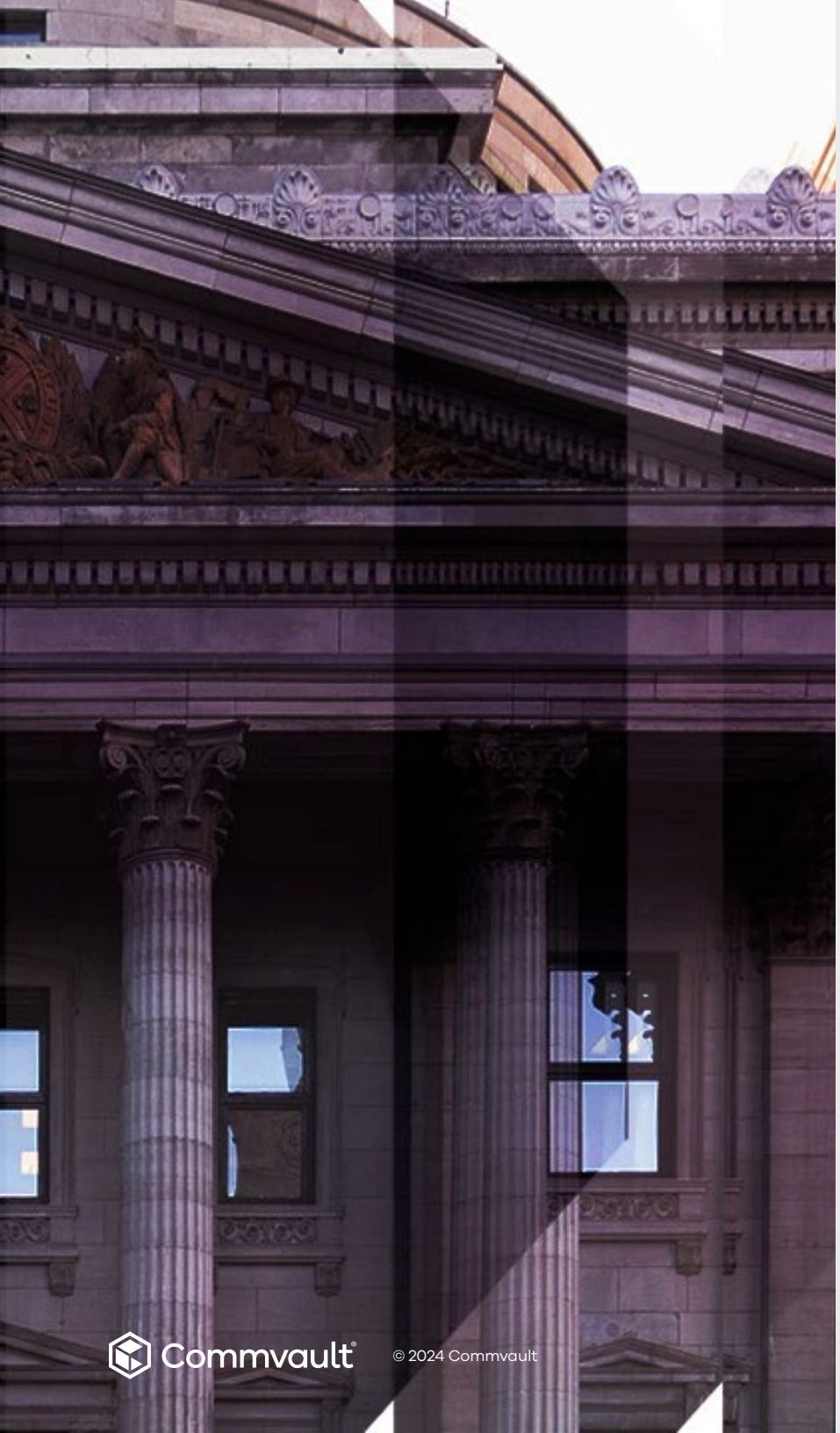
eBOOK

Maîtrise de DORA : Stratégies de Résilience opérationnelle numérique

Comment les solutions Commvault peuvent-elles vous aider à répondre aux exigences réglementaires.

Commvault®

CONTENU



Aperçu

À partir du 17 janvier 2025, les entités financières de l'Union européenne devront se conformer à la loi sur la Résilience opérationnelle numérique (Digital Operational Resilience Act, DORA), conçue pour améliorer la cyber-résilience dans l'ensemble du secteur. Elle concerne les banques, les compagnies d'assurance et les fournisseurs de services tiers dans le domaine des technologies de l'information et de la communication (TIC).

Heureusement, Commvault dispose de solutions pour aider votre organisation à compléter vos efforts en matière de conformité, parmi lesquelles :

- l'identification des actifs informationnels critiques, visant à réduire les risques et à minimiser l'impact de la perte de données,
- l'alerte précoce en cas d'activités suspectes, intégrée dans l'écosystème de sécurité existant,
- une plateforme de récupération sécurisée, à confiance zéro et en réseau isolé air gap pour la cyber-résilience, quelle que soit la charge de travail,
- la réduction de la complexité ainsi que du coût de la récupération propre et des essais de récupération,
- la portabilité des charges de travail transversales, du cloud et des hyperviseurs pour assouplir les charges de travail et les données entre les clouds ou les centres de données.

Il est essentiel que toutes les parties prenantes comprennent les principales dispositions et l'impact qu'elles auront sur l'écosystème financier. Examinons les cinq principaux piliers de la règlementation DORA et comment les solutions Commvault peuvent vous aider à vous y conformer.

01 Exigences en matière de gestion des risques

Le chapitre II (articles 5 à 16) de la règlementation DORA détaille les activités de contrôle et les autres procédures et politiques de sécurité que les institutions financières doivent mettre en place et maintenir pour soutenir un processus adéquat de la gestion des risques liés aux TIC. Ces politiques doivent couvrir l'ensemble du cycle de vie des actifs de données et des systèmes TIC, depuis le développement et le déploiement jusqu'à la maintenance et le déclassement. Les entités financières sont censées revoir et mettre à jour régulièrement leurs stratégies de gestion des risques afin de s'adapter aux menaces nouvelles et émergentes.

Cela signifie que vous devez :

- comprendre clairement les données que vous possédez et leur sensibilité, ainsi que vos actifs et l'impact potentiel d'un incident sur ces mêmes actifs,
- augmenter la visibilité au sein de votre réseau grâce à la surveillance continue de l'activité des utilisateurs,
- analyser les schémas d'activité des utilisateurs et évaluer les risques en exploitant les logs et rapports d'audit détaillés,
- détecter les anomalies dans le comportement des utilisateurs et repérer les risques de sécurité potentiels,
- définir des règles d'alerte personnalisées conformément aux politiques de sécurité établies et recevoir des notifications en temps réel.

Les solutions Commvault peuvent aider à répondre à ces exigences grâce à la découverte, la classification et la protection des données sensibles ; mettre en place une plateforme standardisée de cyber-récupération ; recevoir des alertes rapides en cas de menace ; détourner les attaques à l'aide d'une technologie de déception avancée ; et utiliser la détection des anomalies pour faciliter la réponse aux incidents.

Voici quelques exigences spécifiques de cette disposition et comment les solutions Commvault peuvent aider.

Provision	Commvault Solution
L'article 8 exige que les organisations identifient, classent et documentent toutes les fonctions liées aux TIC ; identifient les systèmes et les données critiques ; et documentent les fournisseurs tiers.	Commvault dispose de capacités uniques pour identifier et classer les données avec Commvault Cloud Risk Analysis. Les TIC sont ainsi dotées d'un processus automatisé qui leur permet de tenir à jour la documentation sur les données sensibles et critiques et d'agir rapidement. Threatwise permet la découverte d'actifs et le suivi des risques au niveau des TTP lorsque le piège est exploité.
En vertu de l'article 9, les organisations doivent protéger de manière adéquate les systèmes TIC, afin de s'assurer qu'ils sont sécurisés et qu'ils ne peuvent pas être corrompus ou que des données ne peuvent pas être divulguées. Elles sont tenues d'isoler les copies de données pour se protéger d'une cyberattaque en cryptant les données.	Commvault permet aux organisations de construire une plateforme de cyber-récupération sécurisée à confiance zéro avec un tableau de bord de la posture de sécurité, MFA, MPA, PAM, RBAC avec une sécurité granulaire. Cette plateforme unique et intégrée fournit des copies de sauvegarde sécurisées, cryptées et immuables, répondant aux meilleures normes de cryptage.
L'article 10 exige des organisations qu'elles disposent de moyens pour détecter rapidement les activités anormales.	Commvault Cloud® Threat Scan et Threatwise permettent aux institutions de détecter de manière proactive les anomalies dans leur environnement, y compris les fichiers malveillants ou corrompus, les modifications à grande échelle des données ou les comportements qui pourraient indiquer qu'un attaquant effectue une reconnaissance. Les alertes relatives à ces anomalies sont émises sur la plateforme Commvault ou par le biais d'intégrations dans les outils de sécurité et de reporting existants tels que SIEM, SOAR ou les logiciels de gestion des services d'assistance.
L'article 11 exige des organisations qu'elles disposent de politiques documentées en matière de TIC et de continuité d'activité, avec un processus d'intervention et de récupération. Un tel dispositif doit être testé.	Commvault Cloud offre des processus de récupération flexibles et automatisés, y compris la possibilité de récupérer vers une salle blanche avec une copie en réseau isolé air gap. La salle blanche automatisée permet de simplifier les tests de récupération avec un impact et un coût réduits.
L'article 12 décrit les politiques et procédures de sauvegarde ainsi que les méthodes de continuité des activités. Les organisations doivent définir des objectifs de délai de récupération en fonction des besoins de l'entreprise et de la criticité des systèmes concernés. Les organisations doivent être en mesure de récupérer les données dans un autre endroit. En ce qui concerne la cyber-récupération, les organisations doivent être en mesure de procéder à une récupération vers une salle blanche.	Commvault offre la possibilité d'une gestion flexible des politiques. Commvault prend en charge de multiples emplacements dans des centres de données et des fournisseurs de clouds privés / publics. Tout cela est géré avec la même plateforme. Commvault Threat Scan surveille les logiciels malveillants et assure une récupération propre. Commvault propose un service de Récupération en salle blanche, qui permet d'effectuer des tests de récupération de manière automatisée.

02 Signalement des incidents

L'un des éléments essentiels de la règlementation DORA consiste en l'obligation pour les entités financières de signaler rapidement les cyber-incidents importants à leurs autorités de régulation respectives. Le chapitre III (articles 17 à 23) stipule que les entités concernées doivent avoir les moyens de détecter, de suivre, de classer et de signaler rapidement les incidents liés aux TIC, ainsi que d'établir les responsabilités et les plans d'atténuation pour les différents scénarios d'incidents.

Cette disposition garantit un flux d'informations en temps opportun entre les institutions financières et les autorités de surveillance financière, ce qui est essentiel pour gérer les risques systémiques et renforcer la résilience globale du secteur financier. La loi précise les types d'incidents qui doivent être signalés, les délais de notification et les informations détaillées qui doivent être incluses dans les rapports.

Les organisations doivent :

- détecter rapidement les incidents liés aux TIC, en recevant des notifications instantanées sur le comportement suspect des utilisateurs, les accès non autorisés et les anomalies ;
- accélérer le processus de réponse aux incidents en automatisant les contre-mesures, telles que le blocage des utilisateurs et l'arrêt des processus ;
- conserver une trace complète des preuves afin d'enquêter sur la cause, l'impact et la portée de l'incident et d'éviter que des cas similaires ne se reproduisent à l'avenir;
- exporter les enregistrements des activités des utilisateurs dans un format de fichier inviolable afin de fournir des preuves solides de l'incident pour les activités judiciaires ;
- informer sur les incidents de sécurité, démontrer la conformité de la sécurité aux autorités compétentes en soumettant des rapports bien structurés et informatifs.

Commvault aide les organisations à se mettre en conformité grâce à des indicateurs d'alerte précoce utilisant une technologie de déception ; une salle blanche pour les capacités judiciaires ; la détection des anomalies et l'analyse des menaces pour faciliter la gestion des incidents ; et des rapports normalisés grâce à l'intégration des systèmes de gestion de la sécurité (SIEM) et de gestion des risques (SOAR).

Commvault®

Voici quelques exigences spécifiques de cette disposition et comment les solutions Commvault peuvent aider.

Provision	Commvault Solution
Les articles 17 à 23 détaillent les capacités de gestion, d'harmonisation et de notification des incidents liés aux TIC dont doivent disposer les organisations.	Commvault Cloud rationalise les processus de réponse aux incidents et de cyberveille grâce à des capacités d'intégration étendues de l'écosystème. Les intégrations avec les SIEM, XSOAR et les fournisseurs tiers facilitent efficacement l'analyse des corrélations et les mesures d'atténuation.
Les articles 17 à 23 exigent également que les organisations accélèrent le processus de réponse aux incidents en automatisant les contre-mesures.	Commvault Cloud aide à fournir des indicateurs d'alerte précoce aux équipes de sécurité et à répondre à l'exigence de réagir dans les délais spécifiés aux incidents importants, en utilisant la cyber-déception et la détection d'anomalies.
Les articles 17 à 23 exigent des organisations qu'elles informent les autorités des incidents en matière de sécurité et qu'elles démontrent aux autorités compétentes qu'elles se conforment aux règles de cybersécurité en soumettant des rapports bien structurés et informatifs.	Commvault Cloud fournit des rapports basés sur la configuration et les données collectées par la plateforme, y compris la posture de sécurité de la plateforme, la piste d'audit, la protection des charges de travail, les politiques utilisées, le temps de récupération estimé ainsi que d'autres éléments. En outre, ces données peuvent être utilisées pour alimenter des outils et des portails externes.

03 Test de résilience opérationnelle numérique

Le chapitre IV (articles 24 à 27) du règlement DORA stipule que les organisations financières doivent évaluer et tester leur préparation à la gestion des incidents liés aux TIC au moins une fois par an afin d'identifier et d'éliminer les lacunes en matière de résilience opérationnelle. Cela comprend une série d'activités de test, telles que des évaluations de la vulnérabilité, des tests de pénétration et des exercices basés sur des scénarios. Ces tests sont conçus non seulement pour identifier les vulnérabilités des systèmes et processus TIC, mais surtout pour évaluer l'efficacité des capacités de prévention, de détection, de réponse et de récupération de l'entité.

Les entités financières doivent :

- établir, maintenir et tester périodiquement des plans de continuité des activités TIC appropriés, surtout en ce qui concerne les fonctions critiques ou importantes externalisées ou sous-traitées dans le cadre d'accords avec des prestataires de services TIC tiers;
- tester au moins une fois par an les plans de continuité des activités TIC ainsi que les plans de réponse et de récupération des TIC en lien avec les systèmes TIC qui soutiennent toutes les fonctions;
- tester régulièrement les systèmes TIC afin d'évaluer leur résilience aux perturbations, sur la base du cadre de test du règlement DORA.

Commvault peut aider les organisations à répondre à ces dispositions avec Cleanroom Recovery, qui fournit des tests de récupération à un coût total de possession (TCO) réduit ainsi que des capacités de tests judiciaires, des preuves tangibles et des preuves de réussite via des rapports.

Voici quelques exigences spécifiques de cette disposition et comment les solutions Commvault peuvent aider.

Provision	Commvault Solution
Les articles 24 à 27 contiennent des exigences en matière de tests opérationnels réguliers de la résilience, notamment en ce qui concerne les performances, la compatibilité et la continuité des activités.	Commvault Cloud possède la capacité unique d'orchestrer des tests de cyber-récupération avec une salle blanche dans le cloud public ou sur site. Cela inclut une copie des données en réseau isolé air gap et de l'orchestration de la récupération sur un endroit propre. Les tests de cyber-récupération peuvent également être effectués dans un centre de données en utilisant un environnement de récupération isolé.

04 Gestion des risques des tiers

Reconnaissant la dépendance croissante à l'égard des fournisseurs de services TIC tiers, le chapitre V (articles 28 à 44) du règlement DORA énumère les règles et les exigences que les entités financières doivent respecter afin de garantir la coopération avec les fournisseurs de services TIC et de gérer correctement les risques liés aux tiers. Les entités financières doivent effectuer une vérification diligente avant de conclure des accords avec des prestataires de services.

Ces entités doivent :

- contrôler l'activité des fournisseurs de services tiers sur les terminaux de leur organisation afin de garantir la conformité avec les politiques et les normes établies;
- définir des autorisations d'accès granulaires pour les fournisseurs tiers afin qu'ils n'aient accès qu'aux ressources et aux données dont ils ont besoin ;
- renforcer la sécurité des connexions RDP et détecter rapidement l'accès non autorisé à des données sensibles ou toute autre activité potentiellement malveillante;
- configurer des alertes et des notifications personnalisées en direct sur les comportements suspects et les violations de sécurité des utilisateurs tiers;
- surveiller l'activité des fournisseurs tiers au sein de votre infrastructure TI à l'aide de journaux d'activité utilisateur détaillés ;
- gérer le risque lié aux tiers et ne pas être trop dépendant de ces derniers;
- fournir une stratégie de sortie technique, le cas échéant.

Commvault peut aider les entreprises à se conformer aux réglementations grâce à la portabilité des données entre les charges de travail transversales, les clouds et les hyperviseurs.

Voici quelques exigences spécifiques de cette disposition et comment les solutions Commvault peuvent aider.

Provision	Commvault Solution
L'article 28.8 décrit comment les organisations doivent gérer le risque lié aux tiers et ne pas avoir une dépendance excessive à l'égard de ces derniers. Elles doivent fournir une stratégie de sortie technique le cas échéant.	La portabilité « any-to-any » de Commvault permet une migration fluide des données et des applications vers et depuis des fournisseurs tiers, et peut être utilisée comme une stratégie de sortie ou une solution de migration des données.

05 Partage d'informations

Le chapitre VI (article 45) du règlement DORA encourage les institutions financières à échanger des informations et des renseignements sur les cybermenaces afin d'améliorer la résilience opérationnelle numérique de l'ensemble du secteur.

Ces institutions devraient :

- capturer les enregistrements détaillés de l'activité des utilisateurs et documenter les incidents de sécurité afin de les partager avec les organismes de réglementation et d'autres entités financières dans le cadre du signalement des incident et de la coopération;
- générer des journaux et des rapports complets pour démontrer le respect des exigences réglementaires en matière de cybersécurité;
- exporter les données dans un format de fichier protégé pour partager les preuves de cybersécurité.

Commvault est en mesure de contribuer à ces efforts grâce à :

- l'échange bidirectionnel de renseignements sur les menaces / d'indicateur de compromission (IOC) à l'aide d'API REST natives et d'intégrations de sécurité tierces, ce qui permet d'enrichir les renseignements et de classer les événements / de les mettre à jour en fonction des incidents;
- une communication cryptée et signée par un certificat sur les appels Syslog / WebHook / API, permettant la diffusion en continu des journaux de sécurité pour l'archivage centralisé des preuves et la collecte de données légales;
- les actions / reconfigurations initiées par l'homme et la machine sont entièrement enregistrées par le biais de pistes d'audit intégrées, ce qui permet l'enregistrement de preuves.

Voici quelques exigences spécifiques de cette disposition et comment les solutions Commvault peuvent aider.

Provision	Commvault Solution
L'article 45 exige des entités financières qu'elles consignent de manière détaillée les activités des utilisateurs et qu'elles documentent les incidents de sécurité. Elles doivent générer des journaux et des rapports complets pour démontrer qu'elles respectent les exigences réglementaires en matière de cybersécurité.	Les solutions Commvault permettent aux organisations d'identifier les données sensibles, les configurations non sécurisées ou dont la sécurisation n'est pas activée, et de les capturer dans des ensembles de documentation partageables. Toutes les activités des utilisateurs, y compris les comptes de service API dans l'interface CV, sont saisies. En outre, Threatwise peut informer les communautés de sécurité quant aux détails TTP de l'attaque réelle grâce à la technologie de la déception.
L'article 45 impose également aux organisations d'exporter des données dans un format de fichier protégé afin de partager les preuves de cybersécurité.	Les solutions Commvault permettent de partager des renseignements et des journaux sur les menaces sous différents formats, via plusieurs canaux cryptés et authentifiés tels que Syslog / Webhook / RestAPI, assurant ainsi la capacité de centraliser la collecte et la sécurisation de tous les attributs liés aux risques en utilisant les outils centralisés des clients.

Sanctions en cas de non-respect des règles

Le non-respect du règlement DORA peut entraîner des sanctions importantes, qui sont cruciales pour maintenir l'intégrité et l'efficacité de la loi.

Elles peuvent varier en fonction de la gravité et de la nature de l'infraction. Elles sont conçues pour être dissuasives et proportionnées à la solidité financière et à la taille de l'entité, ainsi qu'à l'ampleur des perturbations causées par le non-respect des règles.

En cas d'infraction mineure, les entités financières peuvent recevoir un avertissement ou un blâme. Toutefois, pour les manquements les plus graves, les sanctions peuvent inclure des sanctions pénales et / ou administratives. En cas de non-conformité répétée ou d'infractions particulièrement graves, les autorités réglementaires ont le pouvoir d'imposer des sanctions supplémentaires. Il peut s'agir du retrait de licences, de l'interdiction temporaire d'exercer certaines activités commerciales ou d'autres restrictions nécessaires à la protection du système financier.

Contactez notre équipe pour en savoir plus sur la façon dont les solutions Commvault peuvent aider votre organisation à se conformer aux dispositions du règlement DORA.

commvault.com | 01 73 13 00 23 | talktous@commvault.com

Commvault®