

# L'alliance de l'analyse technico-légale et de la finance

## Une réponse stratégique aux exigences de conformité de l'UE

Alors que l'Union européenne renforce la mise en œuvre de la Directive NIS 2 et du Règlement sur la résilience opérationnelle numérique (DORA), le secteur financier se trouve confronté à un changement majeur. Ces réglementations soulignent à quel point il est indispensable d'améliorer les performances réseau et la résilience opérationnelle et rappellent aux établissements les enjeux majeurs qu'implique la conformité. Si les performances sont essentielles, l'accent est clairement mis ici sur le respect de strictes obligations de conformité pour veiller à protéger les établissements financiers contre les conséquences d'un non-respect de la conformité, notamment des pénalités sévères.

### Éviter les écueils de la mise en conformité réglementaire

Dans le paysage en pleine évolution des réglementations financières, la Directive NIS 2 et le règlement DORA présentent une suite d'exigences de sécurité qui sortent du cadre traditionnel de la sécurité et des opérations. Pour respecter ces exigences, un survol rapide des activités du réseau ne suffit plus. Il faut une analyse approfondie des détails des transactions et des communications réseau. Ces défis englobent des aspects techniques (tels que la latence, les limitations de bande passante et la complexité de l'infrastructure) tout en s'étendant à d'autres domaines tels que la fiabilité, la disponibilité, et les mesures globales de cybersécurité essentielles pour protéger l'intégrité du réseau.

VIAVI Solutions permet aux établissements financiers de relever aisément les défis de la conformité en utilisant le potentiel inexploité de l'écoute du réseau et de l'analyse technico-légale, transformant ainsi les obstacles réglementaires en avantages stratégiques.

*La non-conformité avec la directive NIS 2 peut entraîner des pénalités sévères, notamment des amendes pouvant atteindre 10 millions d'euros ou 2 % du chiffre d'affaires annuel global pour les entités essentielles, et engager la responsabilité de la direction, ce qui souligne l'importance d'une surveillance diligente des opérations informatiques.*



### Défis en matière de conformité et VIAVI Solutions

#### Les trois principaux défis :

1. **Déclarations d'incidents conformes à DORA** : des déclarations d'incidents détaillées et établies dans les délais sont un incontournable de la conformité au règlement DORA.
2. **Gestion des risques ICT pour NIS 2** : identifier et gérer les risques ICT est crucial dans le cadre de la directive NIS 2.
3. **Gestion des risques tiers** : NIS 2 et DORA soulignent tous deux l'importance de la gestion des risques tiers.

#### Ce que nous pouvons faire pour vous :

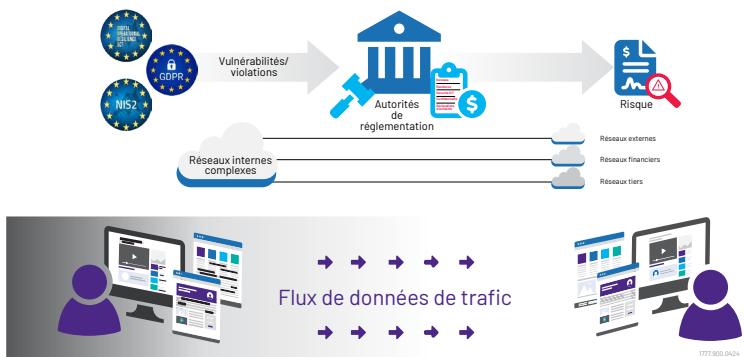
Grâce à la puissance de l'analyse technico-légale haute fidélité des réseaux, la plateforme Observer de VIAVI révolutionne les défis de conformité et de sécurité réseau auxquels sont confrontés les établissements financiers. Nos solutions combinent les données issues d'une multitude de sources (y compris IPFIX/NetFlow, Active Directory, Syslog, SNMP et les captures de paquets) pour créer une empreinte technico-légale complète. Cette approche complexe permet aux établissements d'identifier, d'analyser et de déclarer rapidement les incidents de conformité, largement avant le délai strict de 72 heures imposé par DORA. Elle permet également de répondre aux obligations de gestion proactive des risques et de conformité réglementaire de la directive NIS 2.

En offrant une visibilité sans pareil sur les flux de données du trafic réseau et les interactions tierces, VIAVI assure la conformité complète aux normes de sécurité en corrigeant efficacement les vulnérabilités et les risques dissimulés au sein des réseaux.

- **Empreintes technico-légales** : les capacités technico-légales haute fidélité, renforcées par la conservation des paquets capturés par Observer GigaStor, permettent une analyse rétrospective des transactions réseau, offrant ainsi une visibilité inégalée.

- Enregistrements de flux enrichis :** la plateforme Observer de VIAVI est unique par sa capacité à faire fusionner des données structurées et non structurées, ce qui crée un « super-enregistrement » de chaque conversation réseau et s'affranchit des limitations qui caractérisent les enregistrements classiques des flux.

- Sources de données intégrées :** Observer Apex décompose les silos de données et intègre l'analyse technico-légale des paquets et des données de flux pour produire des informations exploitables, ce qui rationalise les opérations affectées aux équipes SecOps et NetOps.



## Combler les lacunes avec VIAVI

Grâce à sa capacité à traiter les flux des données de trafic, VIAVI fournit des informations précieuses sur la manière dont chaque élément du réseau reçoit, classe et gère les paquets. Ce qui distingue VIAVI, c'est sa capacité unique à ingérer les flux de données de trafic de manière rapide et complète, depuis tout fournisseur, à grande échelle et avec précision. Les entreprises peuvent ainsi mieux comprendre les flux de données au sein du réseau et identifier, puis hiérarchiser, les lacunes potentielles en matière de conformité.

Envisageons les cas d'utilisation suivants :

Pour remédier aux attaques par rançongiciel, il est crucial de pouvoir sauvegarder et restaurer efficacement les opérations. C'est un domaine dans lequel VIAVI excelle en permettant aux organisations de découvrir la couverture des services et des serveurs qui constituent une application. En mappant les connexions des flux de données, les organisations peuvent évaluer l'efficacité du processus de restauration en veillant à ce que les fonctionnalités critiques soient rétablies à un niveau satisfaisant.

## Étapes suivantes dans la résolution du puzzle de la conformité : préparation à la conformité

La préparation en vue d'assurer la conformité aux règlements DORA et NIS 2 intègre une série d'actions « sans regret », parmi lesquelles l'analyse des lacunes dans les pratiques de gestion des risques ICT, l'amélioration de la détection des menaces et des rapports d'incidents, et la clarification des systèmes critiques afin de tester la résilience. En outre, il peut être demandé aux établissements financiers d'améliorer leurs capacités de gestion des incidents et d'éviter les écueils des risques tiers, le tout dans une fenêtre de deux ans pour DORA et les ajustements stratégiques exigés pour la conformité à la directive NIS 2.

Alors que les règlements NIS 2 et DORA s'imposent, il n'est pas envisageable de se pencher *a posteriori* sur les questions de conformité. VIAVI occupe une position unique pour assister les établissements financiers dans leur parcours réglementaire. En utilisant le réseau comme source de vérité, nous vous permettons de respecter efficacement les exigences de conformité. Notre expertise en matière d'analyse et d'approche technico-légale du réseau transforme la manière dont vous abordez la conformité en prenant en charge les questions cruciales telles que les déclarations d'incidents, la gestion des risques ICT et l'évaluation des risques tiers. Faites appel à VIAVI dès aujourd'hui pour renforcer votre posture de conformité et pour veiller à ce que vos opérations restent résilientes et en avance sur les courbes réglementaires.

*La finalisation du Règlement européen sur la résilience opérationnelle numérique (DORA) est un développement réglementaire important pour les sociétés de services financiers.*

Source : What can we expect from the Digital Operational Resilience Act | Deloitte Pays-Bas