Forensics Meets Finance

A Strategic Response to EU Compliance Requirements

With the European Union setting forth the NIS 2 Directive and the Digital Operational Resilience Act (DORA), the financial sector is on the brink of a significant shift. These regulations underscore the vital need for enhanced network performance and operational resilience, reminding institutions of the hefty stakes involved in compliance. While performance is key, the focus here pivots squarely to meeting stringent compliance mandates, ensuring that financial institutions are safeguarded against the repercussions of non-adherence, including severe penalties.

Navigating through the Challenges of Regulatory Compliance

In the evolving landscape of financial regulations, the NIS 2 Directive and DORA present a suite of compliance requirements that challenge traditional security and operational frameworks. Addressing these mandates requires more than just a cursory glance at network activities; it demands a deep dive into the intricate details of network transactions and communications. These challenges encompass technical aspects—such as latency, bandwidth limitations, and infrastructure complexity—and broader concerns including reliability, uptime, and overarching cybersecurity measures essential for protecting network integrity.

VIAVI Solutions empowers financial institutions to navigate key compliance challenges easily by leveraging the untapped potential of network listening and forensic analysis, turning regulatory hurdles into strategic advantages.

Non-compliance with NIS 2 directives can lead to severe penalties, including fines up to 10 million EUR or 2% of global annual turnover for essential entities, and management liability, highlighting the paramount importance of diligent oversight in IT operations.

Compliance Challenges and VIAVI Solutions

Top Three Challenges:

1. **Incident Reporting under DORA:** Timely and detailed incident reporting is a cornerstone of DORA compliance.
2. **ICT Risk Management for NIS 2:** Identifying and managing ICT risks is vital under NIS 2.
3. **Third-Party Risk Management:** Both NIS 2 and DORA emphasize the importance of managing third-party risks.

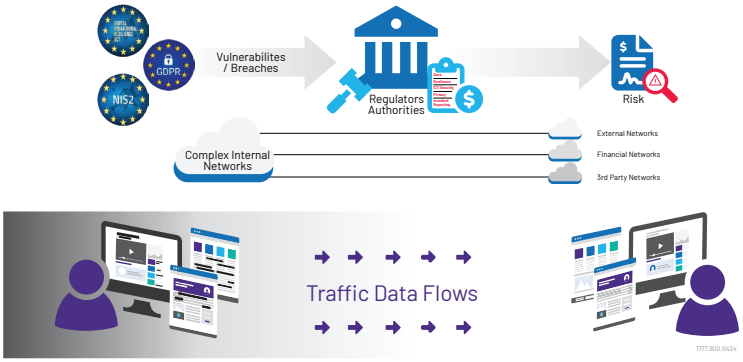
How We Help:

The VIAVI Observer platform revolutionizes compliance and network security challenges for financial institutions by harnessing the power of high-fidelity network forensics. Our solutions combine data from a myriad of sources—including IPFIX/NetFlow, Active Directory, Syslog, SNMP, and packet captures—to craft a comprehensive forensic footprint. This intricate approach empowers institutions to promptly identify, analyze, and report compliance incidents, significantly ahead of the stringent 72-hour deadline mandated by DORA, while also addressing the proactive risk management and regulatory compliance demands of NIS 2.

By offering unparalleled visibility into network traffic data flows and third-party interactions, VIAVI ensures comprehensive compliance with security standards, effectively mitigating vulnerabilities and hidden risks within networks.

- **Forensic Footprints:** Full-fidelity forensic capabilities, enhanced by packet retention from Observer GigaStor, allow for retroactive analysis of network transactions, granting unmatched visibility.

- **Enriched Flow Records:** The VIAVI Observer platform stands alone in its ability to merge structured and unstructured data, creating a 'super-record' for every network conversation, surpassing traditional flow record limitations.
- **Integrated Data Sources:** Breaking down data silos, Observer Apex integrates packet and flow data forensics into actionable insights, streamlining operations across SecOps and NetOps teams.



VIAVI configures and consumes traffic data flows to provide the comprehensive view needed for compliance.

Bridging the Gap with VIAVI

Capable of consuming traffic data flows, VIAVI provides invaluable insights into how each element of the network receives, classifies, and acts upon packets. What sets VIAVI apart is its unique ability to ingest traffic data flows rapidly and comprehensively from any vendor, at scale and with precision. This allows organizations to gain a clearer understanding of data flows within the network to quickly identify and prioritize potential compliance gaps.

Consider the following use case:

In the context of mitigating ransomware attacks, a vital aspect is the ability to perform backup and restoration operations effectively. Here, VIAVI excels by enabling organizations to discover the coverage of services and servers constituting an application. By mapping out the data flow connections, organizations can gauge the effectiveness of a restoration process, ensuring that critical functionalities are reinstated to a satisfactory level.

Next Steps in Solving the Compliance Puzzle – Compliance Readiness

Preparing for DORA and NIS 2 compliance encapsulates a series of "no regret" actions, including conducting a gap analysis of ICT risk management practices, enhancing threat detection and incident reporting, and clarifying critical assets for resilience testing. Additionally, financial institutions may be required to improve their incident management capabilities, and navigate third-party risk management, all within a two-year window for DORA and the strategic adjustments needed for NIS 2 compliance.

In the era of NIS 2 and DORA, compliance cannot be an afterthought. VIAVI stands uniquely positioned to assist financial institutions in navigating these regulatory waters. By leveraging the network as a source of truth, we enable you to meet mandatory compliance requirements effectively. Our expertise in network forensics and analysis transforms the way you approach compliance, addressing critical areas such as incident reporting, ICT risk management, and third-party risk assessment. Engage with VIAVI now to fortify your compliance posture and ensure your operations remain resilient and ahead of regulatory curves.

The finalization of the EU's Digital Operational Resilience Act (DORA) is a significant regulatory development for financial services (FS) firms expected later this year.

Source: What can we expect from the Digital Operational Resilience Act | Deloitte Netherlands

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact