

Navigating NIS2 compliance with the Zerto Cyber Resilience Vault



The NIS2 Directive marks a significant evolution in Europe’s approach to cybersecurity, introducing stricter standards for operational resilience, incident response, and risk management across critical sectors. For organizations affected by NIS2, achieving compliance means adopting advanced cybersecurity practices and tools that mitigate risk, minimize downtime, and enable service continuity.

The Zerto Cyber Resilience Vault is uniquely designed to help organizations not only meet the requirements of NIS2 but also build a proactive, future-proof resilience strategy. By aligning with key articles of the directive, Zerto, a Hewlett Packard Enterprise company, simplifies compliance while delivering industry-leading recovery speed, scalability, and flexibility.

NIS2 compliance: Key requirements addressed by Zerto

The NIS2 Directive lays out specific obligations that organizations must meet to ensure resilience against evolving cyber threats. Here’s how Zerto aligns with critical NIS2 articles.

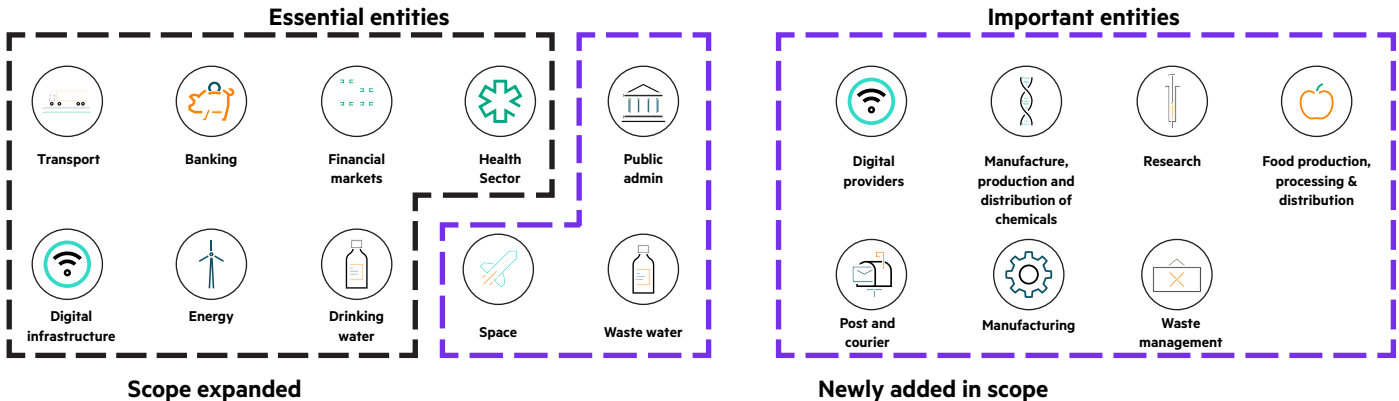


Figure 1. Essential and Important entities defined by NIS2¹

¹ "How to prepare for the NIS2 Directive?" EY.com

Article 21: Cybersecurity risk management measures

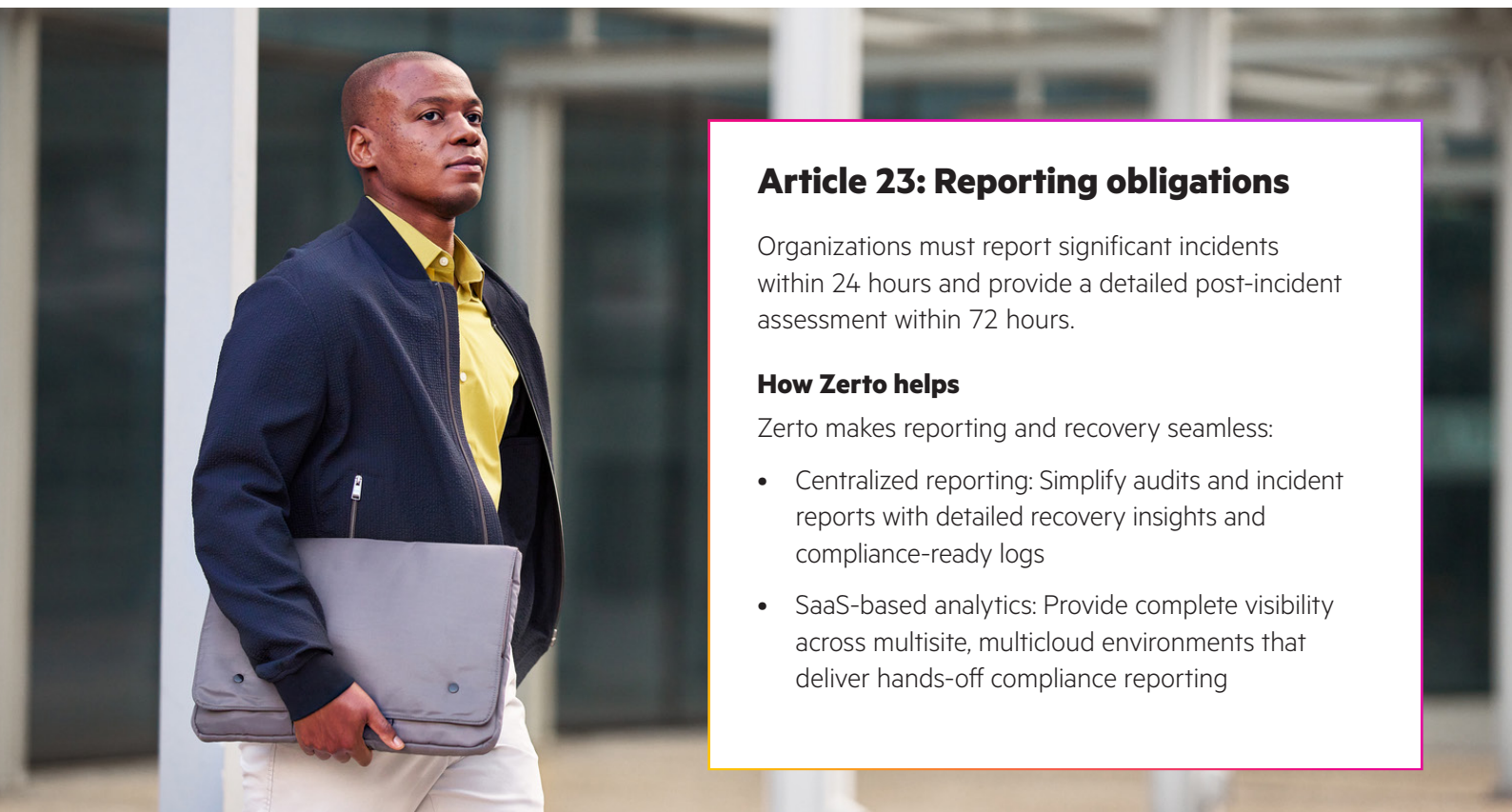
NIS2 mandates organizations to implement measures that reduce risks, promote resilience, and enable rapid recovery. These include:

- Incident detection and response
- Business continuity
- Secure backup and recovery practices

How Zerto helps:

The Zerto Cyber Resilience Vault provides advanced capabilities that directly align with Article 21:

- Continuous data protection (CDP): Helps minimize data loss with near-real-time replication. This enables rapid recovery of critical workloads without compromising business continuity
- Real-time encryption detection: Leverages algorithmic intelligence to swiftly alert users to encryption anomalies indicative of ransomware initiation
- Air-gapped recovery: Provides secure and isolated, immutable storage, which means that recovery data cannot be altered by ransomware or accidental deletion
- Non-disruptive testing: Validates your recovery strategy without interrupting business operations, giving your organization confidence in its resilience



Article 23: Reporting obligations

Organizations must report significant incidents within 24 hours and provide a detailed post-incident assessment within 72 hours.

How Zerto helps

Zerto makes reporting and recovery seamless:

- Centralized reporting: Simplify audits and incident reports with detailed recovery insights and compliance-ready logs
- SaaS-based analytics: Provide complete visibility across multisite, multcloud environments that deliver hands-off compliance reporting



Why Zerto is the right choice for NIS2 compliance

Achieving NIS2 compliance requires more than a checklist—it demands a comprehensive strategy that prioritizes resilience, flexibility, and speed. The Zerto Cyber Resilience Vault delivers on all fronts, providing organizations with:

1. First-rate recovery capabilities
 - a. Near-instant failover and failback to achieve minimal disruption to services
 - b. Continuous data protection mitigates the risk of data loss
2. Seamless testing and reporting
 - a. Conducts frequent recovery tests without downtime
 - b. Generates compliance-ready reports to streamline audits
3. Ransomware resilience
 - a. Isolates and recovers clean backups in the event of an attack, enabling compliance with NIS2's service continuity requirements



Take control of your cyber resilience

Align your organization with NIS2 requirements while building a stronger, more adaptable resilience strategy. Discover how the Zerto Cyber Resilience Vault can simplify compliance and elevate your recovery capabilities.

Learn more at

[HPE.com/zerto-cyber-resilience-vault](https://hpe.com/zerto-cyber-resilience-vault)

Visit [HPE.com](https://hpe.com)



Chat now (sales)

 **Hewlett Packard
Enterprise**

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a00143451ENW