DATASHEET

Radar® Compliance

NIS2 Directive Reporting Obligations

Compliance Solutions for Essential and Important Entities

The NIS2 Directive aims to enhance cybersecurity across the EU by establishing baseline security measures and reporting obligations for essential and important entities. It requires risk management measures, including incident response, supply chain security, and corporate accountability with management oversight and training.

Under NIS2, reporting timelines for cyber incidents have been shortened significantly with requirements to report incidents to their Computer Security Incident Response Team (CSIRT) within 24 hours and regulatory notification within 72 hours. This shorter timeframe pressures organizations to streamline detection and response processes to meet these deadlines and avoid potential penalties.

NIS2 Requirements

The NIS2 Directive introduces significant requirements to bolster cybersecurity across the EU. Firstly, organizations must establish **comprehensive cybersecurity frameworks** encompassing risk assessments, security policies, and procedures for evaluating their effectiveness.

A key aspect is developing robust **incident response capabilities**, including processes for the prompt reporting of significant incidents within specified timelines (e.g., 24-hour early warning) to CSIRTs or competent authorities, along with detailed incident notifications and final reports.

Furthermore, NIS2 mandates s**tronger supply chain security**, requiring entities to implement security measures

tailored to the vulnerabilities of their direct suppliers and to assess the overall security posture of their supply chain. These measures aim to minimize cyber risks and ensure business continuity in the face of cyber incidents.

What Constitutes a Significant Incident?

- Severe Operational Disruption: Incidents that cause or are capable of causing severe operational disruption of services or financial loss for the entity.
- Material or Non-Material Damage: Incidents that affect or are capable of affecting other natural or legal persons by causing considerable material or non-material damage.

Organizations need consistent risk assessment criteria to clearly define “significant events” under NIS2, ensuring accurate and timely reporting and reducing ambiguity.

Reporting Obligations and Timelines

Conducting risk assessment within the initial 24-72 hour reporting timeline of NIS2 is difficult because risk assessments are typically comprehensive processes that require the careful inspection of vulnerabilities and potential impacts. A sudden, unexpected incident

necessitates immediate action, pressuring incident response teams to act quickly to maintain organizational compliance and to avoid potential fines.

Similarly, incident response within this timeframe faces challenges in quickly determining the significance of an event. IR teams must rapidly assess if the incident meets the criteria for "severe operational disruption" or "considerable damage." Response notification obligations include:

- An **early warning within 24 hours** of becoming aware, indicating potential malicious causes or cross-border impact.
- An **incident notification within 72 hours**, updating the early warning and providing an initial assessment of severity, impact, and indicators of compromise.
- Further requirements include an **intermediate report upon request from their CSIRT, a final report within one month**, and progress reports for ongoing incidents.
- Additionally, entities must notify service recipients of significant incidents likely to affect them and any available remedies **without undue delay.** Trust service providers have a stricter **24-hour notification requirement** for significant incidents affecting their services.

Streamline NIS2 Reporting with Radar® Compliance

A significant hurdle in NIS2 compliance is the **ambiguity surrounding the definition of "significant impact"** and the need to establish **consistent incident reporting processes without a clearly defined risk matrix**.

Radar® Compliance addresses this by offering a **consistent and documented solution for risk assessment. Its configurable rules and assessment engine** allow organizations to **define their cybersecurity notification triggers and obligations** based on their specific business context and definition of material harm.

By automating the assessment of incidents against **predetermined criteria within a risk matrix in a consistent and standardized manner**, Radar® Compliance helps **define and assess events with "significant impact"** clearly and consistently. The solution's ability to document incident response provides regulator-friendly **audit trails and documented evidence** of this consistent assessment and decision-making process.

Radar® Compliance **streamlines communication and reporting** ahead of notification timelines by providing a **configurable workflow solution**. This helps operationalize security, risk, and cyber requirements with their associated internal and external notification obligations, **shortening the time spent reaching a notification decision**.

Preparing for Compliance

By understanding these key requirements and the associated challenges, essential and important entities can effectively prepare for compliance with the NIS2 Directive.

Radar® Compliance provides a **flexible and configurable solution** to help organizations establish **consistent, documented, and efficient processes** for managing cyber event notifications, directly addressing the challenges of **tight deadlines, defining significant impact, establishing reporting processes, ensuring comprehensive reporting, and demonstrating corporate responsibility** under the NIS2 Directive.

Simplify compliance with NIS2 reporting requirements with Radar® Compliance.

Schedule a Demo of Radar® Compliance ›

RadarFirst

Learn more at radarfirst.com

RadarFirst offers enterprise risk solutions to automate intelligent decisions for state, federal, international, and industry-specific regulations. Our patented assessment technology enables organizations to act quickly to determine obligations with evolving legal, contractual, and regulatory requirements. With RadarFirst, organizations can confidently navigate complex privacy and compliance reporting with consistent, documented decision-making.