SHOOSMITHS

NIS2 is here – What data centre providers & customers need to know about Europe's new cybersecurity regime

12 November 2024

The new Network and Information Systems Directive (NIS2) came into effect on 18 October 2024 and with it comes an overhaul of the way in which cybersecurity risk management is regulated in Europe.

Given that cloud-based architecture is now considered the industry-norm, data centres have become the custodians of the vast majority of our digital economy and form a core aspect of any critical infrastructure or service.

Unsurprisingly then, NIS2 represents a sea change for both data centres providers and their supply chain, from new incident reporting obligations, significant audit and oversight measures, and a substantial expansion in enforcement powers.

Sanctions for non-compliance under NIS2 are substantial, with fining powers of up to €10m or 2% of worldwide turnover and (in some cases) sanctions against management and the C-suite. Above all, NIS2 emphasises a proactive approach to cybersecurity and operational resiliency.

This article, part of our NIS2 series, provides a high-level overview of what you need to know for your sector and what steps you need to take now. For a more in-depth insight into NIS2 and its requirements, see our article here.

What does this mean for data centre providers?

NIS2 imposes obligations on a broader range of entities, depending on whether they are identified as being 'essential' or 'important'.

Given their absolutely essential role in the European economy, data centres and related providers are categorised under NIS2 as 'essential' and, therefore, subject to NIS2's most stringent security measures. Data centres and related providers, which include content delivery network providers, DNS providers, TLD name registries, as well as operators of internet exchanges and points of presence (PoPs), all fall under the broad digital infrastructure category regulated under NIS2.

Incidents, such as ransomware attacks and DDoS attacks perpetrated against data centre providers have become increasingly prevalent in recent years, with the majority of data centre providers experiencing such attacks on an almost daily basis (see, for example, the massive DDoS attack thwarted by OVHcloud this July).

The critical nature of data centres makes them high-profile targets, with the European Union Agency for Cybersecurity (ENISA) reporting a doubling of disruptive digital attacks in the EU (much of which has been attributed to state-backed groups) in its recent Threat Landscape report, and which further emphasises the need for strengthened cybersecurity measures in data centres.

Not just digital attacks but physical threats

Aside from digital attacks against Europe's digital infrastructure, the data centre sector represents a prime example of where NIS2 converges with its counterpart, the EU's Critical Entities Resilience Directive (CERD), which also entered into force on 18 October 2024.

The CERD covers similar content to NIS2 as it applies to resilience but is far broader in scope, applying to any type of threat an organisation may face. For example, while NIS2 requires a regulated entity to ensure its information systems are hardened against cybersecurity threats, vulnerabilities, and outages, the CERD extends this to all forms of threat, including physical factors such as natural disasters.

In this context, outages such as those impacting Google Cloud's data centres in July 2022 and April 2023 (caused by cooling system failures and a water leak), as well as Microsoft Azure's outage in July 2023 (caused by severe weather severing fibre connections between two EU data centres), all fall within the scope of CERD and, likely, NIS2.

These examples highlight not only the ongoing challenges data centres face in Europe and the necessity for continuous investment in cybersecurity to safeguard critical infrastructure, but also the intrinsic overlap with threats of a non-information security nature that nevertheless result in material service disruptions or critical outages.

In some cases, Member States are introducing measures under the CERD in parallel with NIS2, while in others, CERD requirements will be laid down on a standalone basis. It will, therefore, be important for organisations to understand the specific domestic variations of NIS2 and CERD that apply to them in their respective home countries.

However, what is clear is that for the data centre sector, an outage caused by a physical threat will most likely have implications for incident reporting and management obligations under NIS2.

Enhanced audit

One critical aspect of NIS2 that could materially change the way in which data centre providers approach their information security management, governance, and assurance practices is the introduction of enhanced audits.

NIS2 introduces enhanced audit and inspection measures, with each EU Member State regulator conducting regular (and in some cases unannounced) inspections and audits of a company's information security management frameworks and cybersecurity posture. Member State regulators will, naturally, take a cost-benefit approach when considering how to implement their new audit powers, including the frequency of such audits. However, given the criticality of the data centre sector, it is likely that regulator-conducted inspections and audits will become more commonplace.

One further notable point on audit is NIS2's concept of a cost recovery mechanism. This means that where a regulator finds compliance gaps, not only will the organisation face corrective action plans (with daily fines for non-conformity), but it will also be expected to pay for the regulator's audit. For those unfamiliar with audit, certification, and assurance within the sector, I can tell you that this can amount to quite a hefty bill.

Incident management

NIS2 represents a significant cultural change in the way organisations approach incident management, and for the personnel who will need to be involved in that process.

One of the most significant aspects of NIS2 is the emphasis on breach reporting, which requires affected entities to promptly report any cybersecurity incidents to the relevant authority without undue delay and no later than 24 hours after detection of the incident, with more detailed reporting at additional intervals.

For data centre providers, the incident management obligations have been laid down directly by the European Commission and represent a shift in the way incidents are both classified and reported. You can read more about the details in our dedicated article here, but the key reporting thresholds specifically for data centres include:

- Complete unavailability of **any** data centre service.
- SLA non-compliance for **more than one hour** or due to suspected malicious action.
- Compromise of data integrity, confidentiality, or authenticity, or compromised physical access.

This is in addition to the general categories of incidents (many of which will also be novel to organisations) that apply to the broader category of digital providers.

For data centre providers, this means that under NIS2:

- A regulated entity's information security team will need to be sufficiently resourced to ensure they can notify incidents within a 24-hour window.
- Information security teams will need to develop new processes for how they identify and classify incidents.
- Wider departments (particularly legal, compliance, and risk functions) will need to be introduced into the incident management process at an earlier stage to consider any impact to the company associated with notification. The presence of significant financial sanctions makes this a key priority.
- Members of the entity's legal, compliance, and risk departments will need to be upskilled on aspects of incident classification, containment, and mitigation to contribute effectively to this assessment.

Registration

With NIS2 comes a new mandatory registration requirement. A regulated entity will be required to register with its competent authority and provide key details about where the organisation provides its services, its IP ranges, and (where applicable) the identity and contact information of its designated representative.

Providers and suppliers located outside Europe and with no legal presence will need to appoint a local representative.

We have ISO 27001 – do we need to do anything?

In short – yes.

Most data centre providers already adhere to internationally recognised standards such as ISO 27001 (information security), ISO 22301 (business continuity), and SOC 2 (service organisation controls) as part of their approach to information security management. However, these frameworks alone are unlikely to fully meet the stringent and specific requirements of NIS2, which is fundamentally different in its scope.

In particular:

- **Scope of Application**: ISO certifications and frameworks like SOC 2 typically focus on specific domains—such as information security or operational controls—within the organisation. NIS2, by contrast, takes a more holistic approach. It applies to the entire ecosystem of a data centre provider, encompassing IT systems, operational technology (OT), supply chain risks, and even physical infrastructure.
- **Mandatory Incident Reporting**: As outlined above, NIS2 introduces incident classification and reporting timelines that are significantly more detailed and prescriptive than those under ISO 27001 or SOC 2 frameworks.
- **Regulator Oversight and Enforcement**: ISO certifications are fundamentally voluntary, whereas NIS2 imposes mandatory regulator-led oversight, including regular audits and inspections. In light of the significant financial penalties for non-compliance, existing certifications, while indicative of strong internal governance, do not prepare organisations for the rigorous external scrutiny required under NIS2.

That said, existing ISO certifications remain valuable components of a compliance programme. They can serve as a foundational framework for meeting NIS2 requirements, enabling organisations to implement targeted enhancements rather than a complete overhaul of their systems and processes.

Is there any other legislation to worry about?

Those reading about NIS2 for the first time may understandably think that this is it.

However, for the data centre sector, organisations will also need to contend with the Critical Entities Resilience Directive (CERD) and the EU's Cyber Resilience Act (CRA).

The CRA introduces cybersecurity requirements for any products with digital elements (e.g., IoT products and devices). Similar to the NIS List, it also introduces categories of "critical products" – those deemed most critical to core infrastructure or whose compromise has the potential to cause significant harm. Notable examples include:

- Network management, configuration, and traffic monitoring systems;
- Physical network interfaces;
- Firewalls and intrusion detection systems;
- Routers, modems, and switches;

- Microcontrollers and microprocessors;
- Hypervisors;
- Integrated circuits; and,
- Automation and control systems.

Products falling into any of the above categories will be subject to enhanced oversight mechanisms, including rigorous authorisation, testing, and certification requirements that must be met before they can be sold in Europe.

Many of these products are key components of data centres, meaning the CRA will play a significant role in shaping vendor management practices. Additionally, support infrastructure – such as HVAC/cooling systems, fire suppression equipment, UPS (uninterruptible power supplies), and physical access security – will also come under increased scrutiny.

I'm a data centre customer – what do I need to know?

Whether you operate your own privately managed data centre infrastructure, lease hosting services from a data centre operator, or are a cloud-first organisation relying on your provider's native data centre facilities, NIS2 and its implications for the data centre sector will likely impact you in some way.

For customers operating critical infrastructure or providing critical services – and to whom NIS2 may already apply – it is important to understand the overlaps and differences between a data centre provider's obligations and your own obligations under NIS2. In many cases, you may be able to rely on (or utilise) much of the data centre provider's resources and materials within your own NIS2 compliance programme.

For customers not directly affected by NIS2, these measures should be welcomed as they aim to enhance the overall resilience and security of Europe's data centre sector.

What about the UK

This article focuses on the EU's enhanced cybersecurity regime, which will not apply in the UK.

However, it is clear that the UK is in the process of introducing its own NIS2/CERD-equivalent legislation in the form of the new Cybersecurity and Resilience Bill.

In addition, on 12 September, the UK government added data centres to the UK's 'Critical National Infrastructure' (CNI) list – a notable change, as data centres had not previously been considered critical infrastructure in the UK. This new status aligns the UK's treatment of data centres with other essential services, such as emergency services, finance, healthcare, energy, and water supplies.

It is, therefore, anticipated that the addition of data centres to the CNI list coupled with the incoming reforms, will likely place UK cyber regulation of data centres on a par with that under NIS2/CERD in the not-too-distant future.

For specific guidance on the steps the UK is undertaking in this space, please contact a member of the Resiliency team.

What you need to do now

1. Familiarise yourself with the key requirements of NIS2 – you can read our more in-depth article here as a starting point.
2. Where you provide multiple digital services (e.g., operate a data centre and offer content delivery services) conduct a scoping assessment to ensure each service potentially regulated under NIS2 is identified.
3. Undertake a scoping assessment to assess which aspects of your core infrastructure fall within the scope of NIS2.
4. Keep track of the specific NIS2 implementation timeline for your home country – very few Member States were able to implement national implementing laws before the 17 October deadline.
5. Determine and complete registration requirements – for entities with a broad reach across Europe this may be a complicated assessment, potentially requiring multiple registrations.
6. Conduct a gap analysis between NIS2 measures (specifically those required in your home country), against your current cybersecurity posture and implement a rectification and improvement plan.
7. As a digital provider, understand the overlap between your obligations under NIS2 (specifically those laid down by the European Commission) and those of your customer-base across Europe (which may differ!).
8. Review and update existing incident management handling processes – you can read more about some of the changes to incident classification here.
9. Start your vendor management process **now**, given the significant time it often takes to cascade compliance throughout the supply chain.
10. Start repapering now, including your customer facing contracts as well as the various information your NIS2-regulated customer base will seek to evidence compliance with their own NIS2 obligations.

For further information on NIS2 or assistance with the above activities, please engage with our Resiliency team.

Disclaimer