

Cybersecurity

# Everything you need to know about the NIS2 Directive

Overview guide

LRQA





# Contents

**3**      What is the NIS2 Directive?

---

**5**      Who needs to comply with NIS2?

---

**6**      How can LRQA help

---

**8**      Addressing new requirements

---

**9**      Why LRQA?

---





# What is the NIS2 Directive?

**The Network and Information Security (NIS) Directive was an EU-led initiative which aimed to achieve a common level of cybersecurity across member states, targeting organisations across many sectors deemed critical to the economy.**

While it increased cybersecurity capabilities, implementation proved challenging, leading to fragmentation across the market. To address growing threats from digitalisation and cyber-attacks, the commission proposed replacing the NIS Directive with NIS2, which strengthens security requirements, addresses supply chain security, streamlines reporting, and introduces more stringent supervisory and enforcement measures, including harmonised sanctions across the EU. NIS2 broadens the range of entities falling under its scope, encompassing numerous organisations that were not required to comply with the original NIS Directive.





# What is the NIS2 Directive?

## Timeline

The legislation entered into force on 16 January 2023, and member states had until 17 October 2024 to transpose its measures into national law. Non-compliance will result in significant fines. In the UK, businesses could be fined up to £17 million; in the EU, 'essential' entities face penalties of up to €10 million, or 2% of their global turnover.

## How will NIS2 take shape in the UK?

The UK government has officially confirmed its intentions to update the NIS regulations. Despite the recent alignment between the UK and EU, statements suggest variations in the regulatory approach to safeguarding the cybersecurity of Critical National Infrastructure.

## Changes in incident reporting

The UK and EU are revising their incident reporting requirements to ensure that organisations report more incidents.

Under the EU's NIS2 Directive, organisations must report 'significant' incidents to their relevant authority, national Computer Security Incident Response Team (CSIRT), and in some instances, their customers. Incidents are considered 'significant' if they have caused or could cause severe operational disruption of the service, financial losses, or if they have affected or could cause considerable losses to others.

Organisations will be required to provide an 'early warning' within 24 hours of becoming aware of an incident, with a whole 'incident notification' required within 72 hours and a 'final report' to be submitted no later than one month after the incident notification.

In the UK, the definition of incidents is being expanded to include those that do not directly affect the continuity of the service but pose a significant risk to the affected entities and the services they provide. A final legal definition is yet to be determined, but the 72-hour reporting deadline is expected to remain unchanged. Relevant regulatory bodies within the sectors will still be responsible for setting regulations.



# Who needs to comply with NIS2?

[Previous](#)

[Next](#)



**NIS2 applies to all companies, suppliers and organisations that deliver essential or important services for the European economy and society. The existing NIS scope will significantly expand in the EU, with organisations in several new sectors deemed ‘essential’.**

## Examples of ‘essential entities’ include:

- Space
- Wastewater
- Public administration
- Managed service providers
- Data centre service providers
- Trust service providers
- Content delivery networks
- Public electronic communications networks and services.

## Examples of ‘important entities’ include:

- Postal services
- Chemical production and processing
- Food
- Manufacturing of key products, such as medical devices
- Digital providers (e.g., search engines, social media).

Companies classed as ‘important entities’ will also need to comply with the regulations; however, they will be subject to less regulatory oversight than those classified as ‘essential.’

In the UK, the government will have more power to bring additional sectors into the scope of NIS2 and will also be able to designate certain suppliers as ‘critical’, meaning they, too, would fall under the remit of the NIS2 regulations.

Under the old NIS Directive, EU member states were responsible for determining which entities would qualify as operators of ‘essential’ services; the new NIS2 Directive sees the introduction of a size-cap rule meaning all medium-sized and large entities operating within the specified sectors, or providing services covered by the Directive, will fall within the scope of NIS2. However, it is important to note that for some sectors (such as public electronic communication), regulations will apply regardless of size. Member states will also have the ability to designate organisations as ‘essential’ or ‘important’ entities, even if they fall under the size-cap rule.





# How can LRQA help?

Our deep experience in assurance, combined with award-winning cybersecurity services, enables us to deliver bespoke insights and protection against the unique threats facing your business. Keeping you one step ahead of cyber risks, today, tomorrow and beyond.

As your assurance partner, we are relentless in helping you respond to this new era of risk. We provide assessment, advisory and inspection services against the world's leading standards, schemes and recognised best practices, complemented by a connected portfolio of advanced cybersecurity services delivered by our experts.






## How can LRQA help?

# A standards-based approach to NIS2

The NIS2 requirements advise organisations to consider compliance with international standards, this is reflected by technical guidance issued by the European Union Agency for Cybersecurity (ENISA). For many organisations that need to comply with NIS2, obtaining ISO 27001 certification is a crucial initial step. This certification can serve as a foundation that can be further enhanced through compliance with other complementary extensions and standards such as CSA STAR, ISO 22301, ISO 27017, and ISO 27018.

According to Article 24 of the NIS2 Directive, member states also have the option to require certification of ICT products, services, and processes for essential or important entities under European cybersecurity schemes. Depending on your business category, certification against specific standards such as ISO 27001 and CSA STAR may become mandatory. It is therefore crucial to understand how each member state applies the Directive, as there might be variations across different territories.

**LRQA provide a range of assessment and training services against the world's leading standards and schemes - supporting your journey to NIS2 compliance.** 

### ISO 27001

ISO 27001 is the international management system standard that defines the requirements for an Information Security Management System (ISMS). The standard provides a best practice framework to identify, analyse and implement controls to manage and mitigate risks – reducing the likelihood of an information security breach.

[Find out more →](#)

### ISO 27017

ISO 27017 is a code of practice outlining additional information security controls, specifically for cloud service providers and their customers.

[Find out more →](#)

### ISO 27018

ISO 27018 is part of the ISO 27000 family of standards and is the code of practice for the protection of personally identifiable information (PII) in public clouds acting as PII processors.

[Find out more →](#)

### ISO 22301

ISO 22301 is the international standard for business continuity management. Certification demonstrates best practice around planning for, responding and recovering from unforeseeable events.

[Find out more →](#)

### CSA STAR

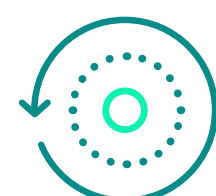
CSA STAR certification is a rigorous third-party audit programme for assessing the security level of cloud service providers to measure the functional level of cloud services.

[Find out more →](#)










# Addressing new requirements

Unlike its predecessor, NIS2 aims to standardise frameworks for easier adoption and harmonisation while introducing more robust cybersecurity measures.

Our experts bring innovative solutions to this complex and ever-evolving marketplace. As a world leader in cybersecurity, we provide threat-led services that span technical assurance, consulting and managed detection and response offerings. We devise and implement end-to-end cybersecurity strategies to manage and combat cyber risks across organisations.



These new measures include the following. Hover over to discover how our range of solutions can help you meet the requirements.

<p><b>Solution</b> </p> <p>Our cybersecurity experts provide risk analysis consultancy services can deliver risk models to ISO27005 and NIST 800-38.</p>	<p><b>Solution</b> </p> <p>We offer proactive testing of incident management plans and provide a quick reactive service.</p>	<p><b>Solution</b> </p> <p>Our CISO (Chief Information Security Officer) specialists provide business continuity and crisis management services both at a strategic and operational level.</p>	<p><b>Solution</b> </p> <p>Our CISO service offering provides you with the highest level of security.</p>	<p><b>Solution</b> </p> <p>Our CISO services and GRC (Governance, Risk Management and Compliance) experts specialise in establishing and maintaining policies and procedures.</p>
<p><b>Solution</b> </p> <p>Our GRC team specialises in a comprehensive range of cybersecurity training.</p>	<p><b>Solution</b> </p> <p>Our GRC team help you set and maintain JML (joining, moving, leaving) processes to optimise HR security.</p>	<p><b>Solution</b> </p> <p>Our specialists can help you implement effective and secure access control measures to protect your communications and emergency communications.</p>	<p><b>Solution</b> </p> <p>Discover our supplier &amp; third-party risk management package.</p> <p><a href="#">Find out more →</a></p>	



# Why LRQA?

[Previous](#)

[Next](#)



## We're everywhere you are

We're everywhere you are. With more than 300 highly qualified auditors and 250 dedicated cybersecurity specialists worldwide, we can provide a local service with a globally consistent dedication to excellence. Our people are technical experts with in-depth knowledge of information and cybersecurity risks, challenges, standards, regulations, and frameworks.



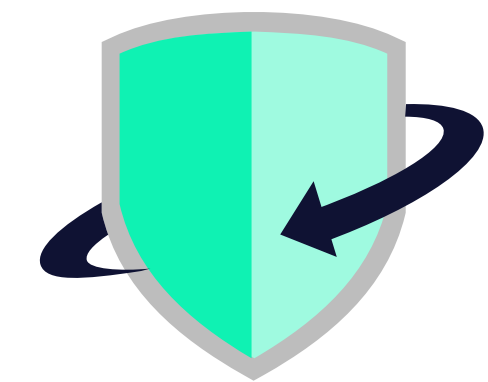
## Flexible delivery

In most cases, our training and certification services can be delivered on-site or remotely using safe and secure technology. If you opt for our remote delivery methods, you'll receive the same high-quality service with several added benefits, including flexibility, fast delivery, and access to global expertise.



## History of firsts

We were the first to receive UKAS accreditation to deliver certification services for a range of standards across the globe. We continue to be instrumental in developing a variety of specific standards and frameworks across different sectors.



## Total assurance

We've led the way in shaping our industry and continue to expand our services and expertise by collaborating with clients, acquiring businesses and forming new partnerships. The result is a unique and connected portfolio of services that can help you assure your assets and management systems, ensure complete cyber resilience and product integrity, navigate the energy transition, and source responsibly.





**About LRQA:**

LRQA is the leading global assurance partner, bringing together decades of unrivalled expertise in assessment, advisory, inspection and cybersecurity services.

Our solutions-based partnerships are supported by data-driven insights that help our clients solve their biggest business challenges. Operating in more than 150 countries with a team of more than 5,000 people, LRQA’s award-winning compliance, supply chain, cybersecurity and ESG specialists help more than 61,000 clients across almost every sector to anticipate, mitigate and manage risk wherever they operate.

In everything we do, we are committed to shaping a better future for our people, our clients, our communities and our planet.

**Get in touch**

Visit [www.lrqa.com](http://www.lrqa.com) for more information or email [cybersolutions@lrqa.com](mailto:cybersolutions@lrqa.com)



LRQA  
1 Trinity Park  
Bickenhill Lane  
Birmingham  
B37 7ES  
United Kingdom