fieldfisher

Reforms to the UK NIS Regulations: Following Europe's Lead?

September 2023

Reforms to the UK NIS Regulations: Following Europe’s lead?

The framework under the NIS 1 Directive for ensuring the resilience of critical infrastructure has been firmly in the spotlight of late, with wide-ranging reforms planned in both the EU and in the UK.

In this article, we take a brief look at the history of the NIS regime, review the changes proposed by the UK Government and compare these to the reforms underway in the EU

Background

The EU adopted the *Directive (EU) 2016/1148* (**NIS 1 Directive**) in 2016 in response to the growing threat of cyber attacks against critical infrastructure assets. The purpose of the NIS 1 Directive was to achieve a high common level of security for network and information systems within the EU, in turn supporting the proper functioning of economic markets and society more generally. For more information on the NIS 1 Directive, please see our previous briefing note here.

In December 2020, the European Commission announced that it would revise and repeal the NIS 1 Directive to address concerns regarding fragmentation in the regulatory framework across Member States and to raise the overall level of cybersecurity resilience across the EU. These revisions were passed in January 2023 in the form of *Directive (EU) 2022/2555* (**NIS 2 Directive**), which expands the scope and application of the NIS 1 Directive. Member States have until October 2024 to transpose the NIS 2 Directive into national law. For more information on the NIS 2 Directive, please see our previous briefing note here.

Meanwhile, in the UK, the NIS 1 Directive was implemented into national law in the form of the *Network and Information Systems Regulations 2018 (SI 2018/506)* (**UK NIS Regulations**). Since its adoption, the UK Government has conducted several reviews of the regulatory framework, with the UK NIS Regulations being updated in December 2020 in response to one such review. The UK Government has now foreshadowed more extensive reforms following a second review in 2022.

Proposed changes to the UK NIS Regulations

In January 2022, the UK Government sought public consultation on planned reforms to the UK NIS Regulations. Following the consultation period, the Government released a response in November 2022 which provides a good picture of the changes it intends to make (**Proposed NIS Reforms**). The changes address a number of concerns raised in previous reviews and reflect views collected during the public consultation period.

Regulation of managed services providers

The prevalence of managed services providers (**MSPs**) has increased since the UK NIS Regulations came into force in 2018. MSPs are companies that remotely manage aspects of their customers' IT systems. Because MSPs often have access to the IT systems of a large number of customers, they are an attractive target for cybersecurity attacks. As a result, the Proposed NIS Reforms will expand the concept of relevant digital service providers (**RDSPs**), a type of entity regulated by the UK NIS Regulations, to include MSPs.

The Proposed NIS Reforms will capture providers of managed services which have all of the following characteristics:

- the service is provided by one business to another;
- the service is related to the provision of IT services (such as systems, infrastructure, networks and/or security);
- the service relies on the use of network and information systems (whether of the provider, their customers or third parties); and
- the service provides regular and ongoing management support, active administration and/or monitoring of IT systems, IT infrastructure, IT

network, and/or their security.

Additionally, the UK Government has indicated that an MSP which exhibits the above characteristics would only be subject to the Proposed NIS Reforms if it meets certain risk-based criteria – i.e. the MSP either (i) has privileged access or connectivity to a customer's data, IT infrastructure, IT networks and/or IT systems, or (ii) performs essential or sensitive functions, such as the processing and/or storage of confidential or business-critical data. The UK Government is not currently proposing to include these criteria in the revised legislation but has indicated it will work closely with the regulator (the Information Commissioner) on how to apply these criteria in its application of the regulations.

The UK Government also provided the following examples of the types of managed services that would be in scope if they meet the above characteristics:

- IT outsourcing services (ITO)
- private wide area network (WAN) managed services
- private local area network (LAN) managed services
- service integration and management (SIAM)
- application modernisation
- application management
- managed security operations centre (SOC)
- security monitoring (SIEM)
- incident response
- threat and vulnerability management (TVM)

Small and micro RDSPs

Small and micro enterprises (i.e. those with less than 50 employees and an annual turnover and/or balance sheet of less than €10m) are excluded from the definition of RDSPs under the UK NIS Regulations, meaning they are not subject to the associated obligations. However, concerns were raised about a small number of critical providers that fall within the scope of this exclusion. The Proposed NIS Reforms will therefore retain the exclusion but allow the Information Commissioner to specify that certain small and micro RDSPs which are systemically critical to the UK's critical services or national security will be subject to the UK NIS Regulations.

Two-tier supervisory regime

The UK Government has indicated it will move to a two-tier supervisory regime for RDSPs as part of the Proposed NIS Reforms. This would involve the most critical RDSPs being subject to a new proactive supervisory regime, with the existing, reactive supervisory regime applying for other RDSPs. In response to feedback regarding the difficulty of implementing appropriate criteria for these two tiers, the government is planning to implement the supervisory regime via non-legislative mechanisms to the extent possible (with the Information Commissioner to take a risk-based approach and providing guidance on which entities will be considered most critical).

Delegated powers to update regulations

In order to respond more quickly and effectively to developments in technology and the cybersecurity threat landscape, the Proposed NIS Reforms would grant the UK Government powers to amend aspects of the UK NIS Regulations without passing an Act of Parliament.

The first of these powers would allow certain sections of the UK NIS Regulations (including sections related to the national framework, operators of essential services, digital services, enforcement and penalties) to be updated by secondary legislation, provided the updates are necessary and limited to matters covered by the existing NIS regime.

The second power would allow the UK Government to change the existing sectors and sub-sectors that are subject to the UK NIS Regulations (including to add new sectors and sub-sectors). The UK Government is not proposing to make any such changes for the time being, but has indicated that potential areas of expansion include:

- electric vehicles
- data centres
- batteries
- energy management and demand response services (e.g. electric chargepoint operators)
- organisations providing aggregation services in the energy sector
- manufacturing
- construction
- education
- waste water
- heat pumps

The UK Government's exercise of these new powers would allow it to respond to evolving risks and new threats more rapidly and would be subject to public consultation and potentially impact assessments. However, any changes made using these powers would not be subject to parliamentary scrutiny (as is currently the case).

New power to regulate critical sectoral dependencies

The Proposed NIS Reforms would grant the UK Government the power to designate critical suppliers (to be called 'critical dependencies') on which existing essential services depend. Critical dependencies would become subject to the same obligations that apply to operators of essential services under the UK NIS Regulations.

To qualify as a critical dependency:

- an organisation must supply a service that at least one operator of an essential service identifies as being dependent on to provide its essential service;
- provision of the service must rely on network and information systems; and
- an incident affecting the supply of the service is likely to have significant disruptive effects on the provision of the essential service.

Competent authorities would be tasked with assessing whether these criteria have been met on a discretionary basis by undertaking consultations and risk assessments within their sector. Competent authorities would then nominate potential critical dependencies to a government minister who would decide whether or not to designate the entity as such.

Additional incident reporting duties

The UK Government is concerned about the limited number of cybersecurity incidents being reported under the UK NIS Regulations. The Proposed NIS Reforms would therefore expand the requirement to report cybersecurity incidents beyond those which affect continuity of service. Operators of essential services and RDSPs would instead need to report any security incidents that have a significant impact on the security of network and information systems which underpin an essential service (regardless of whether the incident affected continuity of service). Competent authorities would provide guidance on the specific thresholds for this reporting within their sectors.

Full cost recovery for NIS functions

Competent authorities cannot currently recover the costs that they incur performing enforcement functions under the UK NIS Regulations from regulated organisations. These costs are instead borne by taxpayers. The Proposed NIS Reforms would allow competent authorities to recover the full costs of performing their NIS enforcement functions from regulated organisations, with competent authorities having responsibility for establishing and communicating how these cost recovery mechanisms would operate.

In addition, the UK Government intends to grant competent authorities greater flexibility in how they recover their costs for regulated organisations. It appears that under the Proposed NIS Reforms, competent authorities would potentially have the ability to both:

- recover costs on an estimated/projected basis, through monthly, quarterly or annual fees for all organisations regulated by the relevant competent authority; and
- recover exact costs on a historic, as occurred, basis via invoices to specific organisations (e.g. for an audit or investigation of the organisation).

We will need to wait for the UK Government to release draft legislation to fully understand the scope of the flexibility being afforded to competent authorities. It will then be up to individual competent authorities (within the scope of the increased flexibility), to decide on the mechanisms they will implement to recover costs from the organisations they regulate. The UK Government recognised the need for these mechanisms to be proportionate and transparent, indicating that competent authorities would need to seek input from regulated organisations and provide more robust guidance on how their chosen mechanisms will operate (including making fees publicly available),

Comparison of UK and EU reforms

Although the UK Government's Proposed NIS Reforms would expand the current UK NIS Regulations, the changes are not as expansive as those contained in the EU's NIS 2 Directive. The UK Government has acknowledged this divergence, indicating that its Proposed NIS Reforms are designed for the UK economy and to maximise the benefits to the UK. However, the inconsistent approach will still pose a challenge for organisations that will be regulated by both regimes and have different obligations under each.

The table below highlights some of the key similarities and differences between the current UK NIS Regulations, the UK's Proposed NIS Reforms (assuming these are enacted consistently with the UK Government's current indications) and the EU's NIS 2 Directive.

Conclusion

Organisations that operate in wide variety of sectors need to be alive to the reforms taking place in both the UK and Europe. From a UK perspective, organisations that are engaged in providing managed services are likely to become subject to the UK NIS regime for the first time. MSPs should therefore consider whether they will be captured and start putting plans in place to enable compliance with the UK NIS Regulations. In addition, organisations that provide services in the EU and fall within the expanded list of sectors and subsectors set out in the EU NIS 2 Directive need to start considering the requirements that will apply to them.

The UK Government has indicated that the Proposed NIS Reforms will be implemented as soon has parliamentary time allows. However, based on the current parliamentary schedule for the remainder of this year, we think it's more likely that draft legislation for the Proposed NIS Reforms will be released in the new year. For businesses based or operating in the EU, the NIS 2 Directive was passed in January 2023 and must be transposed into national law by individual Member States by October 2024.

Continue reading for a practical and digestible comparison of key aspects of the regulatory regimes.

Comparison of UK and EU reforms

Issue	Current UK NIS Regulations	Proposed UK NIS Reforms	EU NIS 2 Directive
Entities regulated	🟩⬜⬜⬜ **Operators of essential services (OESs)** – entities that provide a service which (i) is essential for the maintenance of critical societal or economic activities in certain subsectors (within broader sectors); (ii) relies on network and information systems; and (iii) satisfies a sector-specific threshold requirement or is designated by the relevant competent authority. **Sectors** – Energy, transport, health, water and digital infrastructure. These sectors are broken down into subsectors. Schedule 2 to the UK NIS Regulations then sets out the thresholds for when entities operating in each subsector will be considered OESs. **Relevant digital service providers (RDSPs)** – organisations that provide an online marketplace, online search engine or cloud computing service. Small and micro businesses are exempt.	🟨🟨⬜⬜ **OESs and sectors** – No changes are proposed to the definition of OES or the regulated sectors/subsectors under the current UK NIS Regulations. However, the Government would have new powers to change sectors and subsectors without passing an Act of Parliament. **RDSPs** – The definition of RDSPs would be expanded to include MSPs. The Information Commissioner would also have the power to designate specific small and micro businesses as RDSPs if they are systemically critical to the UK's critical services or national security. **Critical RDSPs** – Criteria to be defined (as far as possible) by the Information Commissioner adopting a risk-based approach. **Critical dependencies** – Designated by a government minister following nomination by a competent authority based on the following criteria: ● the organisation supplies a service that at least one OES is dependent on to provide its essential service; ● provision of the service relies on network and information systems; and ● an incident affecting supply of the service is likely to significantly disruptive the essential service.	🟥🟥🟥🟥 **Regulated entities** – entities which (i) provide their services or carry out their activities in the EU; (ii) have more than 50 employees and an annual turnover and/or balance sheet exceeding €10m; and (iii) operate in certain subsectors (within broader sectors). **Sectors** – In addition to the sectors from the current UK NIS Regulations, banking, financial market infrastructures, ICT service management (including MSPs), public administration, space, postal, waste, chemicals, food, manufacturing, digital providers (including social networking platforms) and research. Some of these sectors are new and some new subsectors have also been added. In addition, there have been changes to the types of entities that will be captured by particular sectors and subsectors. For instance, the digital infrastructure sector has been expanded to include providers of trust services, public electronic communications networks (PECNs) and publicly available electronic communications services (PECS). PECNs and PECSs are currently subject to security requirements under articles 40 and 41 of the European Electronic Communications Code. However, these articles will be repealed when the NIS 2 Directive commences in October 2024 and PECNs and PECSs are brought within its scope. Likewise, electronic trust service providers are subject to existing security and notification requirements under the eIDAS Regulation. **Essential and important entities** – Regulated entities are divided into essential entities and important entities based on the extent to which they are critical to their sector or the type of service they provide, as well as their size. The correct designation of an entity can be difficult to determine (and in some instances the applicable criteria will defined by individual Member States).

Issue	Current UK NIS Regulations	Proposed UK NIS Reforms	EU NIS 2 Directive
Cybersecurity risk management obligations	🟨🟨⬜⬜ **OESs** – Required to take: • technical and organisational measures to manage risks to the security of the network and information systems that their essential services rely on (to ensure a level of security appropriate to the risk, with regard to the state of the art); and • measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used to provide their essential services in order to ensure service continuity. **RDSPs** – Required to: • identify and take appropriate and proportionate measures to manage risks to the security of the network and information systems they rely on to provide services (the measures must ensure a level of security appropriate to the risk, considering the state of the art; prevent and minimise the impact of cybersecurity incidents to ensure service continuity; and take a number of other considerations into account).	🟧🟧🟧⬜ **Little or no changes to** requirements under the **current UK NIS Regulations**, except that: • critical RDSPs will be subject to a new proactive supervisory regime requiring them to more actively demonstrate compliance with NIS obligations (in addition to the existing reactive supervisory regime); and • critical dependencies will need to comply with the obligations applicable to OESs.	🟥🟥🟥🟥 **Essential and important entities** must take appropriate and proportionate technical, operational and organisational measures to: • manage security risks to networks and information systems used for their services; and • prevent or minimise the impact of incidents on service recipients and other services. The measures must: • ensure a level of security appropriate to the risk and take into account the state of the art, cost of implementation, the likelihood and severity of incidents and the entity's size and degree of risk exposure; and • be based on an all-hazards approach and include certain things (e.g. supply chain security and policies on risk analysis, cybersecurity and encryption). **Management bodies** of essential and important entities must: • approve the measures and oversee their implementation (and can be held liable for infringements); and • undergo cybersecurity risk-management training and encourage such training for employees.

Issue	Current UK NIS Regulations	Proposed UK NIS Reforms	EU NIS 2 Directive
Cybersecurity incident reporting obligations	🟨🟨⬜⬜ **OESs** – must notify a competent authority without undue delay and no later than 72 hours after becoming aware of any incident that has a significant impact on the continuity their essential services (having regard to the duration of the incident and the number of users and geographical area affected). The notification must contain certain information about the incident. **RDSPs** – must notify the ICO without undue delay and no later than 72 hours after becoming aware of any incident having a substantial impact on provision of their services (provided they have access to information to assess whether the impact is substantial and having regard to guidance from the ICO, the duration of the incident, the number of users and geographical area affected, the extent of disruption and the impact on economic and societal activities). The notification must contain certain information about the incident. **Incident** means any event that has an actual adverse effect on the security of network and information systems.	🟧🟧🟧⬜ **Incident reporting obligations would be expanded** for both OESs and RDSPs to include any incidents that have an impact on the security of network and information systems underpinning the provision of an essential service, regardless of whether the incident affected the continuity of that service.	🟥🟥🟥🟥 **Essential and important entities** must, upon experiencing an incident having a significant impact on the provision of their services, give the relevant computer security incident response team (CSIRT) or competent authority: ● within 24 hours after first becoming aware of the incident – an early warning notification containing basic information about the incident (e.g. whether it is suspected to have been caused unlawfully or maliciously and/or is likely to have a cross-border impact); ● within 72 hours after first becoming aware of the incident – an incident notification containing updates on the early warning and an initial assessment of the incident; ● on request of the CSIRT or competent authority – an intermediate report with relevant updates; and ● within one month of the incident notification – a final, detailed report. Where relevant, essential and important entities must also notify the recipients of services adversely affected by an incident. **Incident** means any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by (or accessible via) network and information systems. An incident will be **significant** if it has: ● caused (or is capable of causing) severe operational disruption of the service or financial losses for the relevant entity; or ● affected (or is capable of affecting) other entities or people by causing considerable material or non-material losses.

Issue	Current UK NIS Regulations	Proposed UK NIS Reforms	EU NIS 2 Directive
Penalties	🟨🟨🟨⬜ • Cap of £17m for a material contravention which has or could have created a significant risk to (or significant impact on or in relation to) service provision by the OES or RDSP. • Cap of £8,500,000 for a material contravention which does not meet the above criteria. • Cap of £1m non-material contraventions.	🟨🟨🟨⬜ **No changes are proposed to penalties** under the current UK NIS Regulations. However, the Government would have a new power to change penalties without passing an Act of Parliament.	🟥🟥🟥🟥 • Cap of the higher of €10m or 2% of total worldwide turnover for essential entities • Cap of the higher of €7m or 1.4% of total worldwide turnover for important entities • For essential entities, new powers to temporarily suspend an authorisation for the relevant services or temporarily ban any person at CEO or legal representative level from discharging their managerial responsibilities

Contacts

James Walsh
Partner, Technology
+44 330 460 7083
james.walsh@fieldfisher.com

Nikhil Shah
Director, Technology
+44 330 460 6346
nikhil.shah@fieldfisher.com

Tom Gilbert
Associate, Technology
+44 330 460 6279
tom.gilbert@fieldfisher.com