Transposition Note for the Network and Information Systems Regulation 2018

Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union ("the Directive"

These Regulations do not go beyond what is necessary to implement the EU regulation.

ARTICLE	UK LEGISLATION	RESPONSIBILITY
Chapter I – General provisions		
Art. 1 – Subject matter and scope *1. This Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market.*	No specific transposition necessary	Secretary of State
2. To that end, this Directive: *(a) lays down obligations for all Member States to adopt a national strategy on the security of network and information systems;* *(b) creates a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them;* *(c) creates a computer security incident response teams network ('CSIRTs network') in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation;* *(d) establishes security and notification requirements for operators of essential services and for digital service providers;* *(e) lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.*	No specific transposition necessary	

3. The security and notification requirements provided for in this Directive shall not apply to undertakings which are subject to the requirements of Articles 13a and 13b of Directive 2002/21/EC, or to trust service providers which are subject to the requirements of Article 19 of Regulation (EU) No 910/2014.	No specific transposition necessary	
4. This Directive applies without prejudice to Council Directive 2008/114/EC (1) and Directives 2011/93/EU (2) and 2013/40/EU (3) of the European Parliament and of the Council.	No specific transposition necessary	
5. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where such exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of such exchange. Such exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of operators of essential services and digital service providers.	Regulation 6 - which sets out the scope of information sharing by Competent Authorities, the SPOC and the CSIRT	
6. This Directive is without prejudice to the actions taken by Member States to safeguard their essential State functions, in particular to safeguard national security, including actions protecting information the disclosure of which Member States consider contrary to the essential interests of their security, and to maintain law and order, in particular to allow for the investigation, detection and prosecution of criminal offences.	Regulation 1(5)	

7. Where a sector-specific Union legal act requires operators of essential services or digital service providers either to ensure the security of their network and information systems or to notify incidents, provided that such requirements are at least equivalent in effect to the obligations laid down in this Directive, those provisions of that sector-specific Union legal act shall apply.	No specific transposition necessary. For the banking sector and the financial market infrastructures sector, we have not applied these Regulations where Article 1(7) applies.	
Art. 2 – Processing of personal data *1. Processing of personal data pursuant to this Directive shall be carried out in accordance with Directive 95/46/EC.*	No specific transposition necessary	Competent Authorities
2. Processing of personal data by Union institutions and bodies pursuant to this Directive shall be carried out in accordance with Regulation (EC) No 45/2001.	No specific transposition necessary	
Art. 3 – Minimum harmonisation *Without prejudice to Article 16(10) and to their obligations under Union law, Member States may adopt or maintain provisions with a view to achieving a higher level of security of network and information systems.*	Regulations as a whole.	Secretary of State
Art. 4 – Definitions *For the purposes of this Directive, the following definitions apply:* *(1) 'network and information system' means:* *(a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC;* *(b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or* *(c) digital data stored, processed, retrieved or transmitted by elements*	Regulation 1(2)	Secretary of State

covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;		
(2) 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;	Regulation 1(3)(g)	
(3) 'national strategy on the security of network and information systems' means a framework providing strategic objectives and priorities on the security of network and information systems at national level;	Regulation 2 - which establishes the UK's national strategy	
(4) 'operator of essential services' means a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2);	Regulation 8(1)	
(5) 'digital service' means a service within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (1) which is of a type listed in Annex III;	Regulation 1(2)	
(6) 'digital service provider' means any legal person that provides a digital service;	Regulation 1(2)	

(7) 'incident' means any event having an actual adverse effect on the security of network and information systems;	Regulation 1(2)	
(8) 'incident handling' means all procedures supporting the detection, analysis and containment of an incident and the response thereto;	No specific transposition necessary. Given effect through Regulation 11 - which sets out the duty to notify incidents	
(9) 'risk' means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems;	Regulation 1(2)	
(10) 'representative' means any natural or legal person established in the Union explicitly designated to act on behalf of a digital service provider not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the digital service provider with regard to the obligations of that digital service provider under this Directive;	No specific transposition necessary. See also regulation 1(3)(e).	
(11) 'standard' means a standard within the meaning of point (1) of Article 2 of Regulation (EU) No 1025/2012;	No specific transposition necessary.	
(12) 'specification' means a technical specification within the meaning of point (4) of Article 2 of Regulation (EU) No 1025/2012;	No specific transposition necessary.	

(13) 'internet exchange point (IXP)' means a network facility which enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;	Schedule 2, paragraph 10(5)(c)	
(14) 'domain name system (DNS)' means a hierarchical distributed naming system in a network which refers queries for domain names;	Schedule 2, paragraph 10(5)(a)	
(15) 'DNS service provider' means an entity which provides DNS services on the internet;	Schedule 2, paragraph 10(5)(b)	
(16) 'top-level domain name registry' means an entity which administers and operates the registration of internet domain names under a specific top-level domain (TLD);	Schedule 2, paragraph 10(5)(d)	
(17) 'online marketplace' means a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council (1) to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace;	Regulation 1(2)	

(18) 'online search engine' means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found;	Regulation 1(2)	
(19) 'cloud computing service' means a digital service that enables access to a scalable and elastic pool of shareable computing resources.	Regulation 1(2)	
Art. 5 – Identification of operators of essential services *1. By 9 November 2018, for each sector and subsector referred to in Annex II, Member States shall identify the operators of essential services with an establishment on their territory.*	Regulation 8 - which concerns the identification of operators of essential services and Schedule 2 - which sets out the list of essential services and the thresholds that will apply.	Secretary of State and Competent Authorities
2. The criteria for the identification of the operators of essential services, as referred to in point (4) of Article 4, shall be as follows: *(a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;* *(b) the provision of that service depends on network and information systems; and* *(c) an incident would have significant disruptive effects on the provision of that service.*	Regulation 8 - which concerns the identification of operators of essential services and Schedule 2 - which sets out the list of essential services and the thresholds that will apply.	
3. For the purposes of paragraph 1, each Member State shall establish a list of the services referred to in point (a) of paragraph 2.	Regulation 8 and Schedule 2 - which sets out the list of essential services and the thresholds that will apply.	

4. For the purposes of paragraph 1, where an entity provides a service as referred to in point (a) of paragraph 2 in two or more Member States, those Member States shall engage in consultation with each other. That consultation shall take place before a decision on identification is taken.	Regulation 8(7) and Regulation 3 - which sets out the role and responsibilities of competent authorities.	
5. Member States shall, on a regular basis, and at least every two years after 9 May 2018, review and, where appropriate, update the list of identified operators of essential services.	Regulation 8 - which concerns the identification of operators of essential services.	
6. The role of the Cooperation Group shall be, in accordance with the tasks referred to in Article 11, to support Member States in taking a consistent approach in the process of identification of operators of essential services.	Not required to be legislated for.	

7. For the purpose of the review referred to in Article 23 and by 9 November 2018, and every two years thereafter, Member States shall submit to the Commission the information necessary to enable the Commission to assess the implementation of this Directive, in particular the consistency of Member States' approaches to the identification of operators of essential services. That information shall include at least: *(a) national measures allowing for the identification of operators of essential services;* *(b) the list of services referred to in paragraph 3;* *(c) the number of operators of essential services identified for each sector referred to in Annex II and an indication of their importance in relation to that sector;* *(d) thresholds, where they exist, to determine the relevant supply level by reference to the number of users relying on that service as referred to in point (a) of Article 6(1) or to the importance of that particular operator of essential services as referred to in point (f) of Article 6(1).* *In order to contribute to the provision of comparable information, the Commission, taking the utmost account of the opinion of ENISA, may adopt appropriate technical guidelines on parameters for the information referred to in this paragraph.*	Regulation 4 - which specifies the role and responsibility of the SPOC (for article 7(c)). Otherwise, no specific transposition necessary.	SPOC and Secretary of State

Art. 6 – Significant disruptive effect *1. When determining the significance of a disruptive effect as referred to in point (c) of Article 5(2), Member States shall take into account at least the following cross-sectoral factors:* *(a) the number of users relying on the service provided by the entity concerned;* *(b) the dependency of other sectors referred to in Annex II on the service provided by that entity;* *(c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety;* *(d) the market share of that entity;* *(e) the geographic spread with regard to the area that could be affected by an incident;* *(f) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.*	Regulation 8 - which identifies operators of essential services and Schedule 2 - which sets out the list of essential services and the thresholds that will apply.	Secretary of State and Competent Authorities
2. In order to determine whether an incident would have a significant disruptive effect, Member States shall also, where appropriate, take into account sector-specific factors.	Regulation 8 - which identifies operators of essential services and Schedule 2 - which sets out the list of essential services and the thresholds that will apply.	
Chapter II – National frameworks on the security of network and information systems		

Art. 7 – National strategy on the security of network and information systems *1. Each Member State shall adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems and covering at least the sectors referred to in Annex II and the services referred to in Annex III. The national strategy on the security of network and information systems shall address, in particular, the following issues:* *(a) the objectives and priorities of the national strategy on the security of network and information systems;* *(b) a governance framework to achieve the objectives and priorities of the national strategy on the security of network and information systems, including roles and responsibilities of the government bodies and the other relevant actors;* *(c) the identification of measures relating to preparedness, response and recovery, including cooperation between the public and private sectors;* *(d) an indication of the education, awareness-raising and training programmes relating to the national strategy on the security of network and information systems;* *(e) an indication of the research and development plans relating to the national strategy on the security of network and information systems;* *(f) a risk assessment plan to identify risks;* *(g) a list of the various actors involved in the implementation of the national strategy on the security of network and information systems.*	Regulation 2 - which establishes the UK's national strategy	Secretary of State
2. Member States may request the assistance of ENISA in developing national strategies on the security of network and information systems.	Not required to be legislated for.	

3. Member States shall communicate their national strategies on the security of network and information systems to the Commission within three months from their adoption. In so doing, Member States may exclude elements of the strategy which relate to national security.	Regulation 2 - which establishes the UK's national strategy	
Art. 8 – National competent authorities and single point of contact *1. Each Member State shall designate one or more national competent authorities on the security of network and information systems ('competent authority'), covering at least the sectors referred to in Annex II and the services referred to in Annex III. Member States may assign this role to an existing authority or authorities.*	Regulation 3 - which sets out the role and responsibilities of competent authorities.	Secretary of State and Competent Authorities (except for Article 8(3))
2. The competent authorities shall monitor the application of this Directive at national level.	Regulation 3 - which sets out the role and responsibilities of competent authorities	
3. Each Member State shall designate a national single point of contact on the security of network and information systems ('single point of contact'). Member States may assign this role to an existing authority. Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact.	Regulation 4 - which specifies the role and responsibility of the SPOC	Secretary of State and the SPOC
4. The single point of contact shall exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the Cooperation Group referred to in Article 11 and the CSIRTs network referred to in Article 12.	Regulation 4 - which specifies the role and responsibility of the SPOC	

5. Member States shall ensure that the competent authorities and the single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure effective, efficient and secure cooperation of the designated representatives in the Cooperation Group.	Regulations 16(3)(a) and 21	
6. The competent authorities and single point of contact shall, whenever appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities and national data protection authorities.	Regulation 3(3) and Regulation 4(2)	
7. Each Member State shall notify to the Commission without delay the designation of the competent authority and single point of contact, their tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent authority and single point of contact. The Commission shall publish the list of designated single points of contacts.	Not required to be legislated for.	
Art. 9 – Computer security incident response teams (CSIRTs) *1. Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in point (1) of Annex I, covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well-defined process. A CSIRT may be established within a competent authority.*	Regulation 5 - which sets out the roles and responsibilities of the CSIRT	Secretary of State and CSIRT

2. Member States shall ensure that the CSIRTs have adequate resources to effectively carry out their tasks as set out in point (2) of Annex I. *Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network referred to in Article 12.*	Not required to be legislated for.	
3. Member States shall ensure that their CSIRTs have access to an appropriate, secure, and resilient communication and information infrastructure at national level.	Not required to be legislated for.	
4. Member States shall inform the Commission about the remit, as well as the main elements of the incident-handling process, of their CSIRTs.	Not required to be legislated for.	
5. Member States may request the assistance of ENISA in developing national CSIRTs.	Not required to be legislated for.	
Art. 10 – Cooperation at national level *1. Where they are separate, the competent authority, the single point of contact and the CSIRT of the same Member State shall cooperate with regard to the fulfilment of the obligations laid down in this Directive.*	Regulation 3 - which sets out the role and responsibilities of competent authorities, Regulation 4 - which specifies the role and responsibility of the SPOC, Regulation 5 - which sets out the roles and responsibilities of the CSIRT	Competent Authorities, CSIRT and SPOC
2. Member States shall ensure that either the competent authorities or the CSIRTs receive incident notifications submitted pursuant to this Directive. Where a Member State decides that CSIRTs shall not receive notifications, the CSIRTs shall, to the extent necessary to fulfil their tasks, be granted access to data on incidents notified by operators of essential services, pursuant to Article 14(3) and (5), or by digital service providers, pursuant to Article 16(3) and (6).	Regulation 11 - which sets out the duty to notify incidents	

3. Member States shall ensure that the competent authorities or the CSIRTs inform the single points of contact about incident notifications submitted pursuant to this Directive. *By 9 August 2018, and every year thereafter, the single point of contact shall submit a summary report to the Cooperation Group on the notifications received, including the number of notifications and the nature of notified incidents, and the actions taken in accordance with Article 14(3) and (5) and Article 16(3) and (6).*	Regulation 11 - which sets out the duty to notify incidents and Regulation 4 - which specifies the role and responsibility of the SPOC	
Chapter III – Cooperation		
Art. 11 – Cooperation Group *1. In order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence, and with a view to achieving a high common level of security of network and information systems in the Union, a Cooperation Group is hereby established.* *The Cooperation Group shall carry out its tasks on the basis of biennial work programmes as referred to in the second subparagraph of paragraph 3.*	Not required to be legislated for.	N/A

2. The Cooperation Group shall be composed of representatives of the Member States, the Commission and ENISA. *Where appropriate, the Cooperation Group may invite representatives of the relevant stakeholders to participate in its work.* *The Commission shall provide the secretariat.*	Not required to be legislated for.	

3. The Cooperation Group shall have the following tasks: *(a) providing strategic guidance for the activities of the CSIRTs network established under Article 12;* *(b) exchanging best practice on the exchange of information related to incident notification as referred to in Article 14(3) and (5) and Article 16(3) and (6);* *(c) exchanging best practice between Member States and, in collaboration with ENISA, assisting Member States in building capacity to ensure the security of network and information systems;* *(d) discussing capabilities and preparedness of the Member States, and, on a voluntary basis, evaluating national strategies on the security of network and information systems and the effectiveness of CSIRTs, and identifying best practice;* *(e) exchanging information and best practice on awareness-raising and training;* *(f) exchanging information and best practice on research and development relating to the security of network and information systems;* *(g) where relevant, exchanging experiences on matters concerning the security of network and information systems with relevant Union institutions, bodies, offices and agencies;* *(h) discussing the standards and specifications referred to in Article 19 with representatives from the relevant European standardisation organisations;* *(i) collecting best practice information on risks and incidents;* *(j) examining, on an annual basis, the summary reports referred to in the second subparagraph of Article 10(3);* *(k) discussing the work undertaken with regard to exercises relating to the security of network and information systems, education programmes and training, including the work done by ENISA;* *(l) with ENISA's assistance, exchanging best practice with regard to the identification of operators of essential services by the Member States, including in relation to cross-border dependencies,*	Not required to be legislated for.	

regarding risks and incidents; *(m) discussing modalities for reporting notifications of incidents as referred to in Articles 14 and 16.* *By 9 February 2018 and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks, which shall be consistent with the objectives of this Directive.*		

4. For the purpose of the review referred to in Article 23 and by 9 August 2018, and every year and a half thereafter, the Cooperation Group shall prepare a report assessing the experience gained with the strategic cooperation pursued under this Article.	Not required to be legislated for.	
5. The Commission shall adopt implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2). *For the purposes of the first subparagraph, the Commission shall submit the first draft implementing act to the committee referred to in Article 22(1) by 9 February 2017.*	Not required to be legislated for.	
Art. 12 – CSIRTs network *1. In order to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation, a network of the national CSIRTs is hereby established.*	Not required to be legislated for.	CSIRT
2. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT-EU. The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively support the cooperation among the CSIRTs.	Not required to be legislated for.	

3. The CSIRTs network shall have the following tasks: *(a) exchanging information on CSIRTs' services, operations and cooperation capabilities;* *(b) at the request of a representative of a CSIRT from a Member State potentially affected by an incident, exchanging and discussing non-commercially sensitive information related to that incident and associated risks; however, any Member State's CSIRT may refuse to contribute to that discussion if there is a risk of prejudice to the investigation of the incident;* *(c) exchanging and making available on a voluntary basis non-confidential information concerning individual incidents;* *(d) at the request of a representative of a Member State's CSIRT, discussing and, where possible, identifying a coordinated response to an incident that has been identified within the jurisdiction of that same Member State;* *(e) providing Member States with support in addressing cross-border incidents on the basis of their voluntary mutual assistance;* *(f) discussing, exploring and identifying further forms of operational cooperation, including in relation to:* *(i) categories of risks and incidents;* *(ii) early warnings;* *(iii) mutual assistance;* *(iv) principles and modalities for coordination, when Member States respond to cross-border risks and incidents;* *(g) informing the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (f), and requesting guidance in that regard;* *(h) discussing lessons learnt from exercises relating to the security of network and information systems, including from those organised by ENISA;* *(i) at the request of an individual CSIRT, discussing the capabilities and preparedness of that CSIRT;*	Regulation 5 - which sets out the role and duties of the CSIRT	

(j) issuing guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation.		
4. For the purpose of the review referred to in Article 23 and by 9 August 2018, and every year and a half thereafter, the CSIRTs network shall produce a report assessing the experience gained with the operational cooperation, including conclusions and recommendations, pursued under this Article. That report	Not required to be legislated for.	

shall also be submitted to the Cooperation Group.		
5. The CSIRTs network shall lay down its own rules of procedure.	Not required to be legislated for.	
Art. 13 – International cooperation *The Union may conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group. Such agreements shall take into account the need to ensure adequate protection of data.*	Not required to be legislated for.	
Chapter IV – Security of the network and information systems of operators of essential services		
Art. 14 – Security requirements and incident notification *1. Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.*	Regulation 10 - which sets out the security duties for operators of essential services For the banking sector and financial markets infrastructure sector Article 1(7) applies.	Secretary of State and Competent Authorities

2. Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.	Regulation 10 - which sets out the security duties for operators of essential services For the banking sector and financial markets infrastructure sector Article 1(7) applies.	
3. Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.	Regulation 11 - which sets out the duty to notify incidents	
4. In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account: *(a) the number of users affected by the disruption of the essential service;* *(b) the duration of the incident;* *(c) the geographical spread with regard to the area affected by the incident.*	Regulation 11 - which sets out the duty to notify incidents	

5. On the basis of the information provided in the notification by the operator of essential services, the competent authority or the CSIRT shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State. In so doing, the competent authority or the CSIRT shall, in accordance with Union law or national legislation that complies with Union law, preserve the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in its notification. *Where the circumstances allow, the competent authority or the CSIRT shall provide the notifying operator of essential services with relevant information regarding the follow-up of its notification, such as information that could support the effective incident handling.* *At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications as referred to in the first subparagraph to single points of contact of other affected Member States.*	Regulation 11 - which sets out the duty to notify incidents	
6. After consulting the notifying operator of essential services, the competent authority or the CSIRT may inform the public about individual incidents, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident.	Regulation 11 - which sets out the duty to notify incidents	
7. Competent authorities acting together within the Cooperation Group may develop and adopt guidelines concerning the circumstances in which operators of essential services are required to notify incidents, including on the parameters to determine the significance of the impact of an incident as referred to in paragraph 4.	Not required to be legislated for.	

Art. 15 – Implementation and enforcement *1. Member States shall ensure that the competent authorities have the necessary powers and means to assess the compliance of operators of essential services with their obligations under Article 14 and the effects thereof on the security of network and information systems.*	Regulation 15 - power to issue Information notices, Regulation 16 - power to inspect and Regulation 17 - power to enforce For the banking sector and financial markets infrastructure sector Article 1(7) applies.	Secretary of State and Competent Authorities
2. Member States shall ensure that the competent authorities have the powers and means to require operators of essential services to provide: *(a) the information necessary to assess the security of their network and information systems, including documented security policies;* *(b) evidence of the effective implementation of security policies, such as the results of a security audit carried out by the competent authority or a qualified auditor and, in the latter case, to make the results thereof, including the underlying evidence, available to the competent authority.* *When requesting such information or evidence, the competent authority shall state the purpose of the request and specify what information is required.*	Regulation 15 - power to issue Information notices, Regulation 16 - power to inspect and Regulation 17 - power to enforce For the banking sector and financial markets infrastructure sector Article 1(7) applies.	
3. Following the assessment of information or results of security audits referred to in paragraph 2, the competent authority may issue binding instructions to the operators of essential services to remedy the deficiencies identified.	Regulation 16 - power to inspect and Regulation 17 - power to enforce For the banking sector and financial markets infrastructure sector Article 1(7) applies.	
4. The competent authority shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches.	Regulation 3 - which sets out the role and responsibilities of competent authorities	

Chapter V – Security of the network and information systems of digital service providers		
Art. 16 – Security requirements and incident notification *1. Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements:* *(a) the security of systems and facilities;* *(b) incident handling;* *(c) business continuity management;* *(d) monitoring, auditing and testing;* *(e) compliance with international standards.*	Regulation 12 - which sets out the requirements for digital service providers	Secretary of State and Competent Authorities
2. Member States shall ensure that digital service providers take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services referred to in Annex III that are offered within the Union, with a view to ensuring the continuity of those services.	Regulation 12 - which sets out the requirements for digital service providers	
3. Member States shall ensure that digital service providers notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union. Notifications shall include information to enable the competent authority or the CSIRT to determine the significance of any cross-border impact. Notification shall not make the notifying party subject to increased	Regulation 12 - which sets out the requirements for digital service providers	

liability.		
4. In order to determine whether the impact of an incident is substantial, the following parameters in particular shall be taken into account: *(a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services;* *(b) the duration of the incident;* *(c) the geographical spread with regard to the area affected by the incident;* *(d) the extent of the disruption of the functioning of the service;* *(e) the extent of the impact on economic and societal activities.* *The obligation to notify an incident shall only apply where the digital service provider has access to the information needed to assess the impact of an incident against the parameters referred to in the first subparagraph.*	Regulation 12 - which sets out the requirements for digital service providers	
5. Where an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator.	Regulation 12 - which sets out the requirements for digital service providers	

6. Where appropriate, and in particular if the incident referred to in paragraph 3 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law, or national legislation that complies with Union law, preserve the digital service provider's security and commercial interests as well as the confidentiality of the information provided.	Regulation 12 - which sets out the requirements for digital service providers and Regulation 13 - which allows cooperation between Member States	
7. After consulting the digital service provider concerned, the competent authority or the CSIRT and, where appropriate, the authorities or the CSIRTs of other Member States concerned may inform the public about individual incidents or require the digital service provider to do so, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest.	Regulation 12 - which sets out the requirements for digital service providers	
8. The Commission shall adopt implementing acts in order to specify further the elements referred to in paragraph 1 and the parameters listed in paragraph 4 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2) by 9 August 2017.	Not required to be legislated for.	
9. The Commission may adopt implementing acts laying down the formats and procedures applicable to notification requirements. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2).	Not required to be legislated for.	

10. Without prejudice to Article 1(6), Member States shall not impose any further security or notification requirements on digital service providers.	Not required to be legislated for.	
11. Chapter V shall not apply to micro- and small enterprises as defined in Commission Recommendation 2003/361/EC.	Regulation 1 - which sets out the definitions, interpretation and applications used in the Regulations.	
Art. 17 – Implementation and enforcement *1. Member States shall ensure that the competent authorities take action, if necessary, through ex post supervisory measures, when provided with evidence that a digital service provider does not meet the requirements laid down in Article 16. Such evidence may be submitted by a competent authority of another Member State where the service is provided.*	Regulation 17 - power to enforce	Competent Authorities
2. For the purposes of paragraph 1, the competent authorities shall have the necessary powers and means to require digital service providers to: *(a) provide the information necessary to assess the security of their network and information systems, including documented security policies;* *(b) remedy any failure to meet the requirements laid down in Article 16.*	Regulation 15 - power to issue Information notices Regulation 16 - power to inspect Regulation 17 - power to enforce	
3. If a digital service provider has its main establishment or a representative in a Member State, but its network and information systems are located in one or more other Member States, the competent authority of the Member State of the main establishment or of the representative and the competent authorities of those other Member States shall cooperate and assist each other as necessary. Such assistance and cooperation may cover information exchanges between the competent authorities concerned and requests to	Regulation 13 - which allows cooperation between Member States	

take the supervisory measures referred to in paragraph 2.		
Art. 18 – Jurisdiction and territoriality *1. For the purposes of this Directive, a digital service provider shall be deemed to be under the jurisdiction of the Member State in which it has its main establishment. A digital service provider shall be deemed to have its main establishment in a Member State when it has its head office in that Member State.*	Given effect in definition of a "relevant digital service provider" in regulation 1(3)(e)	N/A
2. A digital service provider that is not established in the Union, but offers services referred to in Annex III within the Union, shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. The digital service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established.	Given effect in definition of a "relevant digital service provider" in regulation 1(3)(e)	
3. The designation of a representative by the digital service provider shall be without prejudice to legal actions which could be initiated against the digital service provider itself.	Not required to be legislated for.	
Chapter VI – Standardisation and voluntary notification		

Art. 19 - Standardisation *1. In order to promote convergent implementation of Article 14(1) and (2) and Article 16(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.*	Not required to be legislated for. Incorporated into Guidance by Competent Authorities	Competent Authorities
2. ENISA, in collaboration with Member States, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered.	Not required to be legislated for.	
Art. 20 – Voluntary notification *1. Without prejudice to Article 3, entities which have not been identified as operators of essential services and are not digital service providers may notify, on a voluntary basis, incidents having a significant impact on the continuity of the services which they provide.*	Not required to be legislated for.	N/A
2. When processing notifications, Member States shall act in accordance with the procedure set out in Article 14. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary notifications shall only be processed where such processing does not constitute a disproportionate or undue burden on Member States concerned.	Not required to be legislated for.	
Voluntary notification shall not result in the imposition upon the notifying entity of any obligations to which it would not have been subject had it not given that notification.	Not required to be legislated for.	

Chapter VII – Final provisions		
Art. 21 – Penalties *Member States shall lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall, by 9 May 2018, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.*	Regulation 18 - which sets out the penalty regime For the banking sector and financial markets infrastructure sector Article 1(7) applies.	Secretary of State and Competent Authorities
Art. 22 – Committee procedure *1. The Commission shall be assisted by the Network and Information Systems Security Committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.*	Not required to be legislated for.	N/A
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	Not required to be legislated for.	
Art. 23 – Review *1. By 9 May 2019, the Commission shall submit a report to the European Parliament and to Council, assessing the consistency of the approach taken by Member States in the identification of the operators of essential services.*	Not required to be legislated for.	N/A

2. The Commission shall periodically review the functioning of this Directive and report to the European Parliament and to the Council. For this purpose and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. In its review, the Commission shall also assess the lists contained in Annexes II and III, and the consistency in the identification of operators of essential services and services in the sectors referred to in Annex II. The first report shall be submitted by 9 May 2021.	Not required to be legislated for.	
Art. 24 – Transitional measures *1. Without prejudice to Article 25 and with a view to providing Member States with additional possibilities for appropriate cooperation during the period of transposition, the Cooperation Group and the CSIRTs network shall begin to perform the tasks set out in Articles 11(3) and 12(3) respectively by 9 February 2017.*	Not required to be legislated for.	Secretary of State
2. For the period from 9 February 2017 to 9 November 2018, and for the purposes of supporting Member States in taking a consistent approach in the process of identification of operators of essential services, the Cooperation Group shall discuss the process, substance and type of national measures allowing for the identification of operators of essential services within a specific sector in accordance with the criteria set out in Articles 5 and 6. The Cooperation Group shall also discuss, at the request of a Member State, specific draft national measures of that Member State, allowing for the identification of operators of essential services within a specific sector in accordance with the criteria set out in Articles 5 and 6.	Not required to be legislated for.	

3. By 9 February 2017 and for the purposes of this Article, Member States shall ensure appropriate representation in the Cooperation Group and the CSIRTs network.	Not required to be legislated for.	
Art. 25 – Transposition *1. Member States shall adopt and publish, by 9 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof.* *They shall apply those measures from 10 May 2018.* *When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.*	The whole Regulations and the Explanatory Note	Secretary of State
2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.	Not required to be legislated for.	
Art. 26 – Entry into force *This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.*	Not required to be legislated for.	N/A
Art. 27 – Addressees *This Directive is addressed to the Member States.*	Not required to be legislated for.	N/A

Annex I

TITLE	UK LEGISLATION	RESPONSIBILITY
Requirements and Tasks of Security Incident Response Teams	Regulation 5 - which sets out the roles and responsibilities of the CSIRT	CSIRT

Annex II

Sector	Subsector	Type of entity	Legislative implementation
Energy	Electricity	Electricity undertakings as defined in point (35) of Article 2 of Directive 2009/72/EC of the European Parliament and of the Council, which carry out the function of 'supply' as defined in point (19) of Article 2 of that Directive Distribution system operators as defined in point (6) of Article 2 of Directive 2009/72/EC Transmission system operators as defined in point (4) of Article 2 of Directive 2009/72/EC	Schedule 2 - the electricity subsector
	Oil	Operators of oil transmission pipelines Operators of oil production, refining and treatment facilities, storage and transmission	Schedule 2 - the oil subsector

	Gas	Supply undertakings as defined in point (8) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council Distribution system operators as defined in point (6) of Article 2 of Directive 2009/73/EC Transmission system operators as defined in point (4) of Article 2 of Directive 2009/73/EC Storage system operators as defined in point (10) of Article 2 of Directive 2009/73/EC LNG system operators as defined in point (12) of Article 2 of Directive 2009/73/EC Natural gas undertakings as defined in point (1) of Article 2 of Directive 2009/73/EC Operators of natural gas refining and treatment facilities	Schedule 2 - the gas subsector
Transport	Air transport	Air carriers as defined in point (4) of Article 3 of Regulation (EC) No 300/2008 of the European Parliament and of the Council Airport managing bodies as defined in point (2) of Article 2 of Directive 2009/12/EC of the European Parliament and of the Council, airports as defined in point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council, and entities operating ancillary installations contained within airports Traffic management control	Schedule 2 - the air transport subsector

		operators providing air traffic control (ATC) services as defined in point (1) of Article 2 of Regulation (EC) No 549/2004 of the European Parliament and of the Council	
	Rail transport	Infrastructure managers as defined in point (2) of Article 3 of Directive 2012/34/EU of the European Parliament and of the Council Railway undertakings as defined in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities as defined in point (12) of Article 3 of Directive 2012/34/EU	Schedule 2 - the rail transport subsector

	Water transport	Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council, not including the individual vessels operated by those companies Managing bodies of ports as defined in point (1) of Article 3 of Directive 2005/65/EC of the European Parliament and of the Council, including their port facilities as defined in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports Operators of vessel traffic services as defined in point (o) of Article 3 of Directive 2002/59/EC of the European Parliament and of the Council	Schedule 2 - the water transport subsector
	Road transport	Road authorities as defined in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 responsible for traffic management control Operators of Intelligent Transport Systems as defined in point (1) of Article 4 of Directive 2010/40/EU of the European Parliament and of the Council	Schedule 2 - the road transport subsector
Banking	-	Credit institutions as defined in point (1) of Article 4 of Regulation (EU) No 575/2013 of the European Parliament and of the Council	Article 1(7) of the NIS Directive

Financial market infrastructures	-	Operators of trading venues as defined in point (24) of Article 4 of Directive 2014/65/EU of the European Parliament and of the Council Central counterparties (CCPs) as defined in point (1) of Article 2 of Regulation (EU) No 648/2012 of the European Parliament and of the Council	Article 1(7) of the NIS Directive
Health sector	Health care settings (including hospitals and private clinics)	Healthcare providers as defined in point (g) of Article 3 of Directive 2011/24/EU of the European Parliament and of the Council	Schedule 2 - the healthcare subsector
Drinking water supply and distribution	-	Suppliers and distributors of water intended for human consumption as defined in point (1)(a) of Article 2 of Council Directive 98/83/EC but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential services	Schedule 2 - the drinking water supply and distribution subsector
Digital infrastructure	-	IXPs DNS service providers TLD name registries	Schedule 2 - the digital infrastructure subsector

Annex III

TITLE	**UK LEGISLATION**	**RESPONSIBILITY**
Types of Digital Services for the purposes of Point (5) of Article 4	Regulation 12 (1)	Secretary of State and Competent Authorities