Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by RDSPs for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact

Article 2

Security elements

1 Security of systems and facilities referred to in **[**F1regulation 12(2)(c)(i) of the NIS Regulations**]** means the security of network and information systems and of their physical environment and shall include the following elements:

a the systematic management of network and information systems, which means a mapping of information systems and the establishment of a set of appropriate policies on managing information security, including risk analysis, human resources, security of operations, security architecture, secure data and system life cycle management and where applicable, encryption and its management;

b physical and environmental security, which means the availability of a set of measures to protect the security of **[**F2RDSPs**]'** network and information systems from damage using an all-hazards risk-based approach, addressing for instance system failure, human error, malicious action or natural phenomena;

c the security of supplies, which means the establishment and maintenance of appropriate policies in order to ensure the accessibility and where applicable the traceability of critical supplies used in the provision of the services;

d the access controls to network and information systems, which means the availability of a set of measures to ensure that the physical and logical access to network and information systems, including administrative security of network and information systems, is authorised and restricted based on business and security requirements.

2 With regard to incident handling referred to in **[**F3regulation 12(2)(c)(ii) of the NIS Regulations**]**, the measures taken by the **[**F4RDSP**]** shall include:

a detection processes and procedures maintained and tested to ensure timely and adequate awareness of anomalous events;

b processes and policies on reporting incidents and identifying weaknesses and vulnerabilities in their information systems;

c a response in accordance with established procedures and reporting the results of the measure taken;

d an assessment of the incident's severity, documenting knowledge from incident analysis and collection of relevant information which may serve as evidence and support a continuous improvement process.

3 Business continuity management referred to in **[**F5regulation 12(2)(c)(iii) of the NIS Regulations**]** means the capability of an organisation to maintain or as appropriate restore the delivery of services at acceptable predefined levels following a disruptive incident and shall include:

a the establishment and the use of contingency plans based on a business impact analysis for ensuring the continuity of the services provided by **[**F2RDSPs**]** which shall be assessed and tested on a regular basis for example, through exercises;

b disaster recovery capabilities which shall be assessed and tested on a regular basis for example, through exercises.

4 The monitoring, auditing and testing referred to in **[**F6regulation 12(2)(c)(iv) of the NIS Regulations**]** shall include the establishment and maintenance of policies on:

a the conducting of a planned sequence of observations or measurements to assess whether network and information systems are operating as intended;

b inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, and efficiency and effectiveness targets are being met;

c a process intended to reveal flaws in the security mechanisms of a network and information system that protect data and maintain functionality as intended. Such process shall include technical processes and personnel involved in the operation flow.

5 International standards referred to in **[**F7regulation 12(2)(c)(v) of the NIS Regulations**]** mean standards that are adopted by an international standardisation body as referred to in point (a) of Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council(1). **[**F8United Kingdom, European and internationally accepted standards and specifications relevant to the security of network and information systems may also be used.**]**

6 **[**F2RDSPs**]** shall ensure that they have adequate documentation available to enable the competent authority to verify compliance with the security elements set out in paragraphs 1, 2, 3, 4 and 5.

Textual Amendments

F1 Words in Art. 2(1) substituted (20.1.2021) by The Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019 (S.I. 2019/653), reg. 1(2), **Sch. para. 14(5)(a)**; 2020 c. 1, Sch. 5 para. 1(1)

F2 Word in Regulation substituted (20.1.2021) by The Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019 (S.I. 2019/653), **Sch. para. 14(3)**; 2020 c. 1, Sch. 5 para. 1(1)

F3 Words in Art. 2(2) substituted (20.1.2021) by The Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019 (S.I. 2019/653), reg. 1(2), **Sch. para. 14(5)(b)**; 2020 c. 1, Sch. 5 para. 1(1)

F4 Word in Regulation substituted (20.1.2021) by The Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019 (S.I. 2019/653), **Sch. para. 14(2)**; 2020 c. 1, Sch. 5 para. 1(1)

F5 Words in Art. 2(3) substituted (20.1.2021) by The Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019 (S.I. 2019/653), reg. 1(2), **Sch. para. 14(5)(c)**; 2020 c. 1, Sch. 5 para. 1(1)

F6 Words in Art. 2(4) substituted (20.1.2021) by The Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019 (S.I. 2019/653), reg. 1(2), **Sch. para. 14(5)(d)**; 2020 c. 1, Sch. 5 para. 1(1)

F7 Words in Art. 2(5) substituted (20.1.2021) by The Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019 (S.I. 2019/653), reg. 1(2), **Sch. para. 14(5)(e)**; 2020 c. 1, Sch. 5 para. 1(1)

F8 Words in Art. 2(5) substituted (12.1.2022) by The Network and Information Systems (EU Exit) (Amendment) Regulations 2021 (S.I. 2021/1461), regs. 1, **4(2)**

(**1**) Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).