Regulation on the security and integrity of electronic communications networks and services

The security and integrity of electronic communications networks and services was introduced in the Electronic Communications Law (Law no. 5/2004, of 10 February, in its current version) through Law no. 51/2011, of 13 September, in transposition of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002, on a common regulatory framework for electronic communications networks and services, as amended by Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009, where the following specific competences were, among others, then entrusted to the National Communications Authority (ANACOM):

a) Approve technical measures of implementation and set additional requirements to be fulfilled by companies providing public communications networks or publicly available electronic communications services in the field of security and integrity, for the purposes of article 54-A and as provided for in paragraph 1 of article 54-C and article 54-D of the Electronic Communications Law;

b) Approve measures that define the circumstances, format and procedures applicable to reporting requirements for security breaches or loss of network integrity that have a significant impact on the operation of networks and services by companies providing public communications networks or accessible electronic communications services to the public, pursuant to the provisions of article 54-B and paragraph 2 of article 54-C of the Electronic Communications Law;

c) Determine the conditions under which companies providing public communications networks or publicly available electronic communications services shall disclose to the public information on security breaches or loss of integrity with a significant impact on the operation of networks and services under point *b)* of article 54-E of the Electronic Communications Law;

d) Determine the obligations by companies providing public communications networks or publicly available electronic communications services to perform security audits of networks and services and to send their report, as well as the requirements to be met by audits and applicable requirements to the auditing entities, in accordance with paragraphs 1 and 2 of article 54-F of the Electronic Communications Law.

By ANACOM decision on 12 December 2013, amended on 8 January 2014, ANACOM fulfilled the conditions applicable to the obligations of notification and public disclosure of security

breaches or integrity losses with a significant impact on the operation of networks and, on 12 June 2014, a reporting centre was set up, with a permanent operation, to receive notifications.

Based on the experience gained not only through the activity of the reporting centre, but also through national and international cooperation in this field, this Authority has the duty to exercise the above-mentioned competences through the adoption of a regulation on the security and integrity of networks and services.

As regards, in particular, the notification and public disclosure obligations, the Authority also has the duty to incorporate in this regulation the corresponding legislation the measures already implemented under the decision of 12 December 2013, the execution of which is understood to have come in an effective and consensual manner, without prejudice to some necessary adjustments in the face of the experience gathered in the activity of the reporting centre. In this way and for the sake of transparency and legal certainty, a duly articulated set of conditions applicable to the security and integrity of networks and services has been consolidated in a single tool.

In this context and by decision on 4 August 2016, ANACOM approved the initiation of the procedure for the preparation of a regulation on the security and integrity of networks and services, as well as the publication of its announcement in accordance with paragraph 1 of article 98 of the Code of Administrative Procedure.

By the end of the deadline, 18 contributions were received, which were analysed and weighted in the preparation of a first draft of a regulation on the security and integrity of networks and services, which, by decision on 29 December 2016, was approved and submitted to a regulatory procedure and a general consultation procedure, in accordance with article 10 of the Statutes of ANACOM, approved by Decree-Law no. 39/2015, of 16 March, and in articles 98 et seq. of the Code of Administrative Procedure and for the purposes set forth in article 8, and in particular in paragraph 4 of article 54-C of the Electronic Communications Law.

After publication of this first project in the 2nd series of the *Diário da República*, on 10 January 2017, and after an extension of the deadline by 15 working days, the public consultation took place until 14 March 2017, and 17 contributions were received in due course.

In view of the contributions received and considering the significant nature of the changes introduced, on the basis of the public consultation report, ANACOM decided to draw up a second draft of the regulation on the security and integrity of networks and services, which, by decision of 6 July 2018, was approved and submitted to a new regulatory procedure and general consultation procedure.

After publication of this second project in the 2nd series of the *Diário da República*, on 22 August 2018, the public consultation took place until 3 October 2018, and 14 contributions were duly

received, which were considered in the approval of this Regulation, containing its respective assessment of the report that supports ANACOM's options and which is published on the website of this Authority, together with the full contributions received.

In regulating the obligations of companies with regard to the security and integrity of networks and services, consideration was given both to the costs incurred by companies in meeting their obligations, against the benefits arising therefrom, which include not only the protection of the interests of citizens, and in particular the users of networks and services, support for the continued provision of relevant services to society and citizens, guaranteeing access to emergency services and, in general, promoting the development of the internal market by improving the reliability of networks and services, as well as those resulting from the prevention of security incidents and the prevention or minimisation of their impact.

To that end, the conclusions of the 2010 study on the assessment and characterisation of security in public communications networks and the 2012 assessment of the security and integrity of national electronic communications networks and services, both developed by ANACOM, as well as the information and experience gathered by this Authority since 2014, through its reporting centre, in the processing of notifications received, in the monitoring of security breaches or losses of integrity in question and in the context of its aggregated analysis, and participation in the Group of Experts of the article 13-A coordinated by ENISA (European Network and Information Security Agency).

Following the forest fires that occurred in 2017, ANACOM published a report of a working group that it coordinated and which was constituted by public and private entities, namely the Portuguese Business Communications Association (ACIST), the National Civil Protection Authority (ANPC), the Association of Operators of Electronic Communications (APRITEL), the Directorate General of Energy and Geology (DGEG), the Energy Services Regulatory Authority (ERSE), the Telecommunications Institute (IT) and companies from the electronic communications, transport and energy sectors.

This report, presented publicly in a session promoted by ANACOM on 29 May 2018, entitled "*Report of the Working Group on Forest Fires - Measures of Protection and Resilience of Electronic Communications Infrastructures"*, available on ANACOM's institutional website, included 27 measures that will significantly reduce the impact of forest fires on electronic communications networks and services and, consequently, its users, and whose implementation is, where applicable, duly articulated with the provisions of this regulation.

Thus, in the exercise of the attributions and powers conferred on ANACOM in point *m)* of paragraph 1 and point *e)* of paragraph 2, both of article 8, in point *a)* of paragraph 2 of article 9 and in article 10, all of the Statutes of ANACOM, as well as in articles 2-A and 54-A to 54-D, in point *b)* of article 54-E, in paragraphs 1 and 2 of article 54-F and in article 54-G of the Electronic

Communications Law, and in the pursuit and compliance with the objectives set out in point *c)* of paragraph 1 and point *f)* of paragraph. 4, both of article 5 of the same law, the Board of Directors of ANACOM, in the exercise of the powers conferred on it by point *b)* of paragraph 1 of article 26 of the Statutes, approved, by decision on 14 March 2019, the following regulation:

Regulation on the security and integrity of electronic communications networks and services

TITLE I

General Provisions

Article 1

Object

This regulation establishes:

a) The technical measures of implementation and additional requirements to be complied with by companies providing public communications networks or publicly available electronic communications services in the field of security and integrity for the purposes of article 54-A, and in the terms set forth in paragraph 1 of article 54-C and article 54-D of the Electronic Communications Law (Law no. 5/2004, of 10 February, in its current version) and under the terms of the Title II of this regulation;

b) The circumstances, format and procedures applicable to the reporting requirements for security breaches or loss of network integrity that have a significant impact on the operation of networks and services by companies providing public communications networks or publicly available electronic communications services, pursuant to article 54-B and paragraph 2 of article 54-C of the Electronic Communications Law and in accordance with Chapter I of Title III of this regulation;

c) The conditions under which companies providing public communications networks or publicly available electronic communications services shall disclose to the public security breaches or loss of integrity with a significant impact on the operation of networks and services under point *b)* of article 54-E of the Electronic Communications Law and in the terms provided for in Chapter II of Title III of this regulation;

d) Obligations to perform security audits of networks and services by companies providing public communications networks or publicly available electronic communications services and to send their report, as well as the requirements to be met by the audits and the requirements applicable to the auditing entities, in accordance with the provisions of paragraphs 1 and 2 of article 54-F of the Electronic Communications Law and in accordance with Title IV of this regulation.

Article 2

Definitions

1 - For the purposes of this regulation, the following definitions shall apply:

a) «Assets» means transmission or information systems, equipment and other physical and logical resources which make up or support a public communications network and its accesses, including interconnections, a publicly available electronic communications service or a related service and related facilities;

b) «Auditor» means the entity responsible for conducting an audit on the security of networks and services under paragraphs 1 and 2 of article 54-F of the Electronic Communications Law and in accordance with article 28 of this regulation;

c) «Audit» means the audit on the security of networks and services to be carried out by companies, in accordance with paragraphs 1 and 2 of article 54-F of the Electronic Communications Law and in accordance with Title IV;

d) «Main management and operation centre» means a centre which, by default or in an alternative mode, has the task of ensuring the management and operation of networks and services and of assets, including the identification and resolution of security incidents;

e) «Relevant clients» means the entities identified in accordance with paragraph 3 of this article;

f) «Employees» means employees or agents of companies;

g) «Key employees» means employees who perform tasks in the management and operation of the security and integrity of electronic communications networks and services, including at least:

i) The security officer, as provided for in article 14;

ii) The deputy of the security officer, if any, in accordance with article 14;

iii) Employees who act as a permanent point of contact, in accordance with article 15;

iv) Employees who are part of the security incidents response team, as provided for in article 16;

h) «Companies» means undertakings providing public communications networks or publicly available electronic communications services, as defined in the Electronic Communications Law;

i) «Security incident» means an event with a real adverse effect on the security of networks and services, including a breach of security or loss of integrity;

j) «Sophistication level 1» refers to the basic level, which includes the basic security measures, as provided for in article 7 and the Annex;

k) «Sophistication level 2» refers to the level of industry standard, including security measures based on appropriate national, European and international standards, specifications and recommendations, including review of their implementation, taking into account technical or organisational changes in companies or security incidents, in accordance with article 7 and the Annex;

l) «Sophistication level 3» means the state-of-the-art level, which includes advanced security measures, continuous monitoring and structural review of their implementation taking into account technical or organisational changes in companies, security incidents, tests or exercises, with a view to proactively improving the implementation of security measures, as provided for in article 7 and the Annex;

m) «Security officer» means an employee of the company responsible for the management of the security of networks and services and their representation in the performance of their duties under this regulation, in particular in accordance with article 14;

n) «Network and service security» means the ability of electronic communications networks or services to withstand, with a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of such networks and services, stored, transmitted or processed data or associated services offered or accessible through such networks or services;

o) «Relevant services» means services relevant to society and citizens provided by relevant clients, as provided for in paragraph 4 of this article;

p) «Security breach or loss of integrity with significant impact» means a breach of security or loss of integrity with the expected impact under article 21.

2 - For the purposes of this regulation, the following abbreviations and acronyms shall apply:

a) «ANACOM», the National Communications Authority (ANACOM);

b) «ANPC», the National Civil Protection Authority;

c) «CNCS», the National Cybersecurity Centre;

d) «CNPD», the National Data Protection Commission;

e) «EMGFA», the General Staff of the Armed Forces;

f) «ENISA», the European Network and Information Security Agency;

g) «GNS», the National Security Office;

h) «ICNF», the Institute for Nature Conservation and Forestry, I.P.;

i) «IPMA», the Portuguese Institute of the Sea and Atmosphere, I.P.;

j) «LCE», the Electronic Communications Law;

k) «PSAP», the Public Safety Answering Point(112 Service Centres);

l) «RNSI», the National Internal Security Network;

m) «SIRESP", the Integrated System of Emergency and Security Networks of Portugal;

n) «SRPCBA», the Regional Service of Civil Protection and Firemen of the Azores.

3 - For the purposes of point *e)* of paragraph 1, the following are considered as relevant clients:

a) The entities responsible for the management, operation and maintenance of SIRESP, regarding the operation of this system;

b) The Ministry of Internal Administration, regarding the operation of the RNSI;

c) The SRPCBA, regarding the operation of the integrated telecommunications network of emergency of the Autonomous Region of the Azores;

d) The EMGFA, regarding the operation of information systems and information and communication technologies necessary for the exercise of command and control in the Armed Forces;

e) The GNS, regarding the operation of the CNCS;

f) The operators of essential services identified under the terms of Law no. 46/2018 of 13 August, which establishes the legal regime for the security of cyberspace, in relation to the provision of essential services;

g) The owners or operators of critical infrastructures designated under Decree-Law no. 62/2011, of 9 May, and in other applicable legislation, regarding the operation of critical infrastructures.

4 - For the purposes of point *o)* of paragraph 1, the relevant services shall be those services which, in the terms of the requests from relevant clients, these are identified in the contracts concluded with the companies for essential network and service offers to ensure continuity of delivery of those relevant services.

Article 3

Scope

1 - In fulfilling their obligations regarding the security and integrity of networks and services provided for in the law and in this regulation, companies shall adopt the measures in an appropriate manner:

a) In normal operating conditions;

b) In extraordinary situations, including, but not limited to, the following situations:

i) Security incident;

ii) Network breakdown, emergency or force majeure, in the terms provided for in paragraph 1 of article 49 of the LCE;

iii) Exemptions provided for in points *a)*, *b)* and *c)* of paragraph 3 of article 3 of Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015, establishing measures concerning access to the Open Internet and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) 531/2012 on roaming on public mobile communications networks in the European Union;

iv) Serious accident or catastrophe, in accordance with the legal and regulatory provisions applicable to civil protection;

v) State of emergency, state of siege or state of war, in accordance with the applicable legal and regulatory provisions;

vi) Activation of an emergency plan for civil protection or plan in the context of emergency civil planning of the communications sector, under the terms provided in the applicable legal and regulatory provisions;

vii) Serious threat to internal security, including terrorist attacks, in accordance with the applicable legal and regulatory provisions on internal security.

2 - Companies shall comply with their obligations regarding the security and integrity of networks and services provided for in the law and in this regulation in a manner appropriate to changing climatic conditions and the risks of natural disasters or other extreme events including storms, landslides, floods, high winds, forest fires, earthquakes and tsunamis, among other things, as regards the choice of sites, equipment, materials and accommodation infrastructures and protection and preservation procedures.

3 - For the purposes of the previous paragraph, companies must take into account:

a) The information issued by the competent national, European or international authorities;

b) The National Strategy for Adaptation to Climate Change 2020, approved by the Resolution of the Council of Ministers 56/2015 of 30 July.

4 - Companies shall comply with their obligations regarding the security and integrity of networks and services provided for in the law and in this regulation in accordance with the provisions concerning the security of nationally classified matters and within the international organisations of which Portugal is a part.

5 - Companies must ensure that all assets which, regardless of their ownership, support the operation of their networks or their services, including terminal equipment to the extent that they are under their management, are subject to compliance with their security and integrity of the networks and services provided for in the law and in this regulation.

6 - Under the principle of good administration, ANACOM uses the information transmitted by the companies within the scope of this regulation to carry out its duties in the area of emergency planning of civil protection and emergency civil planning in the communications sector.

Article 4

Cooperation and sharing of information

1 - Companies should cooperate with ANACOM in the scope of the performance of its duties and the exercise of its competences in the matters of network and services security.

2 - Companies shall cooperate with each other in the fulfilment of their obligations regarding the security of networks and services, including in particular in the following situations:

a) Occurrence of one or more security incidents, especially in cases of common root cause;

b) Common risks, threats or vulnerabilities or that may potentiate a cascade effect;

c) Dependence or interdependence between networks or services, including, inter alia, access to and interconnection of networks, co-location of assets and sharing of infrastructure or other resources;

d) Common supplies of goods or services by third parties.

3 - For the purposes of the previous paragraph, ANACOM shares with companies the list of their permanent contact points, maintained under the provisions of article 15.

4 - For the purposes of this article, companies shall also cooperate, as appropriate, by carrying out joint actions, entering into agreements on mutual assistance or the sharing of information or knowledge.

Article 5

Electronic means

1 - All communications addressed to ANACOM within the scope of this regulation, as well as the sending of information, must be carried out by electronic means, under terms to be determined by ANACOM, in accordance with the provisions of the law and without prejudice to access to its services.

2 - ANACOM maintains and manages information on security and integrity in a secure information system, in accordance with the provisions concerning the security of classified information at the national level and within the framework of international organisations of which Portugal is a part.

TITLE II

Obligations of companies on security and integrity

CHAPTER I

General provisions

Article 6

Obligations of companies

1 - Pursuant to article 54-A of the LCE and in accordance with the provisions of this regulation:

a) Companies should take appropriate technical and organisational measures to prevent, manage and reduce risks of the security of networks and services, in particular by preventing or minimising the impact of security incidents on interconnected networks at national and international levels, and to users, and should be suitable to existing risks taking into account the state of the art;

b) Companies providing public communications networks shall take appropriate measures to ensure the integrity of their networks and ensure the continuity of the provision of the services they support.

2 - The technical and organisational measures and the additional requirements adopted by companies to comply with the provisions of the law and this regulation should:

a) Be in accordance with the decisions of the European Commission adopted in accordance with the procedure laid down in article 13-A of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002, on a common regulatory framework for electronic communications networks and services, as currently drafted;

b) Be based, in the absence of the decisions provided for in the previous paragraph, on existing national, European and international standards, specifications and recommendations on the subject, namely:

i) NP ISO/IEC 27001:2013 (*Information Technology - Security Techniques - Information Security Management Systems - Requirements*) and its revisions;

ii) ISO/IEC 27001:2013 (*Information technology - Security techniques - Information security management systems - Requirements*) and its revisions;

iii) ISO/IEC 27002:2013 (*Information technology - Security techniques - Code of practice for information security controls*) and its revisions;

iv) ISO/IEC 27011:2016 or Recommendation ITU-T X.1051 (04/2016*)* (*Information technology - Security techniques - Code of practice for ISO/IEC 27002 for telecommunications organisations)* and its revisions*;*

v) Recommendation ITU-T X.1053 (11/2017) (*Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organisations*) and its revisions;

vi) ISO/IEC 27005:2018 (*Information technology - Security techniques - Information security risk management*) and its revisions;

vii) Recommendation ITU-T X.1055 (11/2008) (*Risk management and risk profile for telecommunication organisations*) and its revisions;

viii) Recommendation ITU-T X.1056 (01/2009) *(Security incident management guidelines for telecommunications organisations)* and its revisions;

ix) Recommendation ITU-T X.1057 (05/2011) (*Asset management guidelines in telecommunication organisations*) and its revisions;

x) ISO 22301:2012 (*Societal security - Business continuity management systems - Requirements*) and its revisions;

xi) Other appropriate national, European or international standard, specification or recommendation;

c) Take into account the technical documents published by ENISA as a result of the work carried out at the level of the implementation of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for networks and electronic communications services, in its current drafting.

3 - The technical and organisational measures and the additional requirements adopted by the companies to comply with the provisions of the law and this regulation should also take into consideration:

a) The recommendations made by ANACOM, in particular with regard to the implementation of the security measures provided for in this regulation;

b) The technical instructions applicable to the construction or extension of suitable infrastructures, the use of suitable infrastructures and the installation of electronic communications network equipment and systems in suitable infrastructures, established under the provisions of Decree-Law no. 123/2009, of 21 May, in its current version.

4 - Companies shall ensure that the technical and organisational measures and additional requirements adopted to comply with the provisions of the law and this regulation are kept up to date.

Article 7

Technical measures of implementation and additional requirements

1 - For the purposes of the provisions of the previous article and under the terms of paragraph 1 of article 54-C and article 54-D of the LCE, companies shall, in particular, adopt all security measures included in sophistication levels 1 and 2 for the pursuit of each of the 25 security objectives listed in the Annex.

2 - Exemption from the provisions of the preceding paragraph, the cases in which, based on the results of a risk assessment for the security of networks and services carried out by the companies, include:

a) An adequate pursuit of a security objective does not require, on an exceptional basis and with prior authorisation from ANACOM following a reasoned request submitted for that purpose, compliance with one or several security measures provided for in sophistication level 2;

b) An adequate pursuit of a security objective requires compliance with one or more of the security measures provided for in sophistication level 3.

3 - For the purposes of point *a)* of the preceding paragraph, applications must be accompanied by the following elements:

a) Indication of security objective;

b) Indication of the security measure;

c) The risk assessment on which the application is based, and which ensures, by other measures, that the security objective in question is adequately achieved.

4 - Exemptions from the prior authorisation provided for in point *a)* of paragraph 2 shall be those companies which, in all their offers, have a number of subscribers or less than 1,000 accesses and whose offers are not essential to ensure the continuity of the provision of a relevant service without prejudice to the necessary risk assessment for the security of networks and services in accordance with the same paragraph 2.

5 - For the purposes of the provisions of the previous article, the security measures to be adopted by companies must include at least the following specific measures, as provided for in Chapter II of this Title:

a) Classification of assets and inventory of assets, under the terms set forth, respectively, in articles 8 and 9;

b) Review of risk assessments in accordance with article 10;

c) Procedures for controlling the exceptional management of Internet access traffic, in accordance with article 11;

d) Exercises, in accordance with article 12;

e) Information to relevant clients, in accordance with article 13;

f) Security officer, as provided for in article 14;

g) Point of permanent contact, in the terms provided for in article 15;

h) Security incident response team, as provided for in article 16;

i) Security Plan, in accordance with article 17;

j) Specific duties of communication to ANACOM, in the terms foreseen in article 18;

k) Annual security report as provided for in article 19.

CHAPTER II

Specific measures

Article 8

Asset Classification

1 - Companies shall classify assets in a class from A to C as provided for in this article.

2 - An asset shall be classified in class A if, as a result of disruption to its operation, the number of subscribers or accesses affected may be equal to or greater than 100,000 or the geographical area affected may, in accordance with paragraph 3 of this article, be equal to or greater than 2,000 km^2 or, where applicable, cover the entire territory of an island of the Autonomous Region of the Azores or of the Autonomous Region of Madeira.

3 - For the purposes of the previous paragraph, the criterion for the affected geographical area should only be applied if the criterion on the number of subscribers or accesses affected is inapplicable or, in this case, reasonably impossible to determine or estimate.

4 - The following assets shall also be classified in class A:

a) The main management and operation centre of a company which, in all its offers, has a total number of subscribers or accesses equal to or greater than 100,000;

b) The main management and operating centre of a company which includes at least one class A asset;

c) The assets on which the supply of networks and services depends on and which are essential to ensure the continuity of the provision of relevant services, and as such, are identified in the scope of the contract entered into with the relevant client concerned;

d) The assets that provide for international interconnection, interconnection between the Autonomous Regions, interconnection between the Continent and an Autonomous Region or interconnection between islands in the Autonomous Region of the Azores or in the Autonomous Region of Madeira, including submarine cable station, satellite station or transboundary terrestrial system;

e) The assets that have been identified under civil emergency planning in the communications sector or a civil protection contingency plan, under the terms set forth respectively in Decree-Law no. 73/2012 of 26 March and in point *e)* of paragraph 2 of of article 2-A of the LCE.

5 - An asset shall be classified in class B if, as a result of disruption to its operation, it causes or is likely to have a serious negative impact on the security of networks and services, except when, under the terms of the preceding paragraphs, it shall be classified in class A.

6 - An asset shall be classified in class C whenever it is not to be classified in either class A or B.

Article 9

Asset inventory

1 - Companies must prepare and maintain an inventory of all assets classified in classes A or B, signed by the security officer.

2 - For each asset, the following information should be included in the asset inventory:

a) Unique identifier;

b) Designation;

c) Classification, under the provisions of article 8;

d) The geographical coordinates of its location;

e) The identification of entities that own or manage the sites;

f) Characterisation including:

i) Supported functionalities and services;

ii) Rationale for classification under article 8, including a description of the potential impact of a disruption of its operation;

iii) Identification as single point of failure;

iv) Supplies of critical third parties for their operation, including management, operation, security and energy services;

v) Autonomy in case of power failure;

vi) In case of interconnection, indication of type (international interconnection, interconnection between Autonomous Regions, interconnection between the Mainland and an Autonomous Region or interconnection between islands in the Autonomous Region of the Azores or in the Autonomous Region of Madeira) and identification of interconnected companies;

g) Security measures, controls and records adopted, including redundancy, robustness and resiliency measures in the case of an asset identified as a single point of failure under the provisions of sub-point *iii)* of the preceding paragraph;

h) Recording of security breaches or loss of integrity with significant impact;

i) Record of changes made, including the results of integration and system tests performed and asset restoration plans.

3 - Companies must complete the asset inventory within 60 business days of the start date of the activity.

4 - Companies whose offers are supported by at least one class A asset shall communicate to ANACOM the list of assets in the inventory which, for each asset, contain the information in points *a)* to *d)* and sub-point *ii)* of point *f),* all from paragraph 2 of this article:

a) In its initial version, within 60 working days from the date of commencement of business or, if later, from the date from which companies support their offers in an asset classifiable in class A;

b) In an updated version, together with the annual security report.

Article 10

Review of risk assessments

Companies shall review risk assessments taking into account, in particular:

a) Security breaches or loss of integrity with significant impact or any other extraordinary situation referred to in point *b)* of paragraph 1 in article 3 occurred in the previous two years;

b) Information on threats, vulnerabilities and risks, including risks arising from changing weather conditions and risks of natural or other extreme events, issued by competent national, European or international authorities, including ANPC, IPMA, ICNF and ENISA, as well as information published annually or communicated to companies by ANACOM.

Article 11

Procedures for Control of Exceptional Management of Internet Access Traffic

1 - The adoption of measures for the management of Internet access traffic by companies should comply with Regulation (EU) 2015/2120 of the European Parliament and of the Council of the 25th November 2015.

2 - Companies should record information relevant to the control of exceptional Internet traffic management measures, which, for each measure adopted, includes, inter alia, the following elements:

a) The exception on which it is based, as provided for in points *a)*, *b) or c)* of paragraph 3 in article 3 of Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015, duly documented;

b) The nature of the measure, including blocking, slowing down, alteration, restriction, degradation or otherwise;

c) The object of the measure, in particular the contents, applications or services and ports or IP addresses covered;

d) The duration, including the start and end dates and time period of the measure.

3 - Companies should adopt and maintain a system for continuously monitoring Internet access traffic for detection of:

a) Risks to the security and integrity of the network, the services provided through it and the terminal equipment of end users;

b) Impending network congestion.

Article 12

Exercises

1 - Companies should develop and implement an exercise programme for a maximum period of two years to assess the security of networks and services and the adequacy of the security plan with a view to improving the technical and organisational measures taken, if applicable:

a) Assets classified in classes A or B;

b) Access to emergency services;

c) Support for the continuity of the provision of relevant services.

2 - Companies should promote, as appropriate, the participation of other companies or third parties in the implementation of the exercise programme.

3 - Companies must participate in the joint exercises that ANACOM, under the terms to be determined, deems necessary.

Article 13

Information to relevant clients

Following security incidents with an impact on the provision of networks and services that are essential to ensure the continuity of the provision of relevant services and identified as such under the contract concluded with the relevant client concerned, companies shall communicate to them the measures adopted or to be adopted which have an impact on the provision of relevant services in question.

Article 14

Security officer

1 - Companies shall designate a security officer, who, among the other duties provided for in this regulation, shall be responsible for:

a) Management of security policy;

b) Management of all the measures adopted in the area of network and service security under the provisions of the law and of this regulation.

2 - Companies may appoint an assistant to the security officer, who is responsible for carrying out the duties of the security officer in case of absence or impediment.

3 - Companies which are not established in the European Union or the European Economic Area and whose offers are supported by at least one class A insurable asset, shall ensure that employees designated for the functions provided for in this article are domiciled in a Member State of the European Union or the European Economic Area.

Article 15

Permanent point of contact

1 - Companies should establish a permanent point of contact function, which should ensure the ability to initiate and receive an operational and technical level of information flow between the company and ANACOM, namely guaranteeing:

a) The effectiveness of response to security incidents having an impact at or above the sector level, including support for the continuity of the provision of relevant services, and involving the participation of several companies;

b) The articulation between ANACOM and the company to obtain operational or technical information, following notification of a breach of security or loss of integrity with significant impact submitted by that or another company;

c) The construction and updating of situational information integrated in the context of a security breach or loss of integrity with significant impact or activation of civil protection emergency plan or plan within the scope of civil emergency planning of the communications sector;

d) The operationalisation of the procedures established under an emergency plan for civil protection or emergency civil planning in the communications sector;

e) The processing of ANACOM determinations in the sense of informing the public of security breaches or losses of integrity occurring in their networks and services, pursuant to the provisions of paragraph 3 of article 23;

f) The receipt of binding instructions issued under the provisions of paragraph 1 of article 54-G of the LCE;

g) The articulation between ANACOM and the security incident response team.

2 - Companies must also ensure that the permanent contact point function is equipped with the necessary means to develop cooperation and information-sharing actions between companies, in accordance with article 4.

3 - Companies should ensure the permanent point of contact function:

a) On a continuous basis (24 hours a day and seven days a week), when their offers are supported by at least one asset classifiable as class A;

b) In a continuous availability (24 hours a day and seven days a week) limited to periods of activation, initiated and terminated by ANACOM communication, in all other cases.

4 - Companies must ensure that permanent contact point has a main and alternative means of contact for communication with ANACOM under normal operating conditions, extraordinary situations referred to in sub-points *i), ii)* and *iii)* of point *b)* of paragraph 1 in article 3 and, as appropriate and in accordance with the applicable legal and regulatory provisions, in the situations referred to in other sub-points.

Article 16

Security incident response team

1 - Companies whose offers are supported by at least one asset classifiable as class A must have a security incident response team, with the resources and knowledge to prepare effectively for risks, threats and vulnerabilities and the response to security incidents affecting assets classified in classes A or B.

2 - Companies must complete the constitution of the team provided for in the previous paragraph within a period of six months from the date from which they bear their offers in an asset classifiable as class A.

3 - The team referred to in this article shall integrate the information security incident response system, in accordance with the terms to be determined pursuant to point *d)* of paragraph 2 in article 2-A of the LCE.

Article 17

Security plan

1 - Companies must develop and maintain a security plan, duly documented and signed by the security officer, which contains:

a) The security policy;

b) A description of all measures taken to ensure the security of networks and services under the provisions of the law and this regulation including, where applicable and on a case-by-case basis, the references to the measures and levels of sophistication in which they fall within, as provided for in the Annex;

c) The recording and analysis of major security incidents occurring over the past five years, including all security breaches or loss of integrity with significant impact;

d) The list of key contributors, including an indication of their role.

2 - Companies must complete the preparation of the security plan within six months from the date of commencement of their activity.

3 - Companies must also instruct the security plan with proof that the security officer, the assistant to the security officer, if existant, and the employees who perform the permanent contact function are duly mandated, under the terms legally established, to represent the company in the exercise of the functions entrusted to it, in the terms established in the law and in this regulation.

Article 18

Specific duties on communication to ANACOM

1 - Companies must notify ANACOM, within 20 working days of the start of their activity:

a) The security policy, in the terms foreseen in the previous article;

b) The information on the employees assigned to the functions of security officer and, as the case may be, of the assistant to the security officer, as provided for in article 14;

c) The information relating to the permanent contact point, as provided for in article 15.

2 - For the purposes of point *b)* of the preceding paragraph, companies shall communicate to ANACOM the following information regarding each employee:

a) Name;

b) Phone number(s);

c) E-mail address.

3 - For the purposes of point *c)* of paragraph 1, companies must communicate to ANACOM the following elements:

a) Telephone number;

b) Mobile phone number;

c) E-mail address;

d) Alternative contacts;

e) Geographical address of the place where the function is secured;

f) When applicable, contact elements for the activation of the permanent contact point function, as provided for in point *b)* of paragraph 3 in article 15, including telephone number, mobile number and e-mail address.

4 - Before the expiration of the period provided for in paragraph 1 of this article and in case of necessity, companies shall ensure that the contacts provided in the scope of the prior notice of commencement of activity, pursuant to the provisions of article 21 of the LCE, shall provisionally carry out the function provided for in article 15 of this regulation.

5 - Companies shall notify ANACOM, prior to its implementation, of any change to the information provided under this article.

Article 19

Annual security report

1 - Companies shall draw up an annual security report which, in a complete but succinct manner and for the calendar year to which it relates, contains the following elements:

a) Summary description of the main activities carried out in the area of network and service security, with a special focus on the assets classified in classes A or B and in the implementation of the exercise programme;

b) Quarterly statistics of all non-notified security incidents, including number and type of incidents;

c) Aggregate analysis of security incidents with the greatest impact, including all security breaches or loss of integrity with significant impact, and their average recovery time;

d) Recommendations of activities, including joint exercises, of measures or of cooperative practices that promote the improvement of the security of networks and services;

e) Issues identified and lessons learned following security incidents;

f) Any other relevant information.

2 - The companies must present the annual security report to ANACOM, signed by the security officer:

a) Regarding the first annual security report:

i) Until the last working day of January of the calendar year following the first calendar year of activity, when the activity started within the first half of the year;

ii) Until the last working day of January of the second calendar year following the first calendar year of activity, when the activity started in the second half of the year;

b) For the other annual security reports, until the last working day of January of the calendar year following the one they report.

3 - For the purposes of sub-point *ii)* of point *a)* of the preceding paragraph, the annual security report shall cover the whole period between the activity start date and the end of the previous calendar year.

4 - For the purposes of point *b)* of paragraph 1, ANACOM may define a common taxonomy of types of security incidents to be used by the companies, as well as the format in which the information should be presented.

TITLE III

Obligations of notification and information to the public

CHAPTER I

Notification obligations

Article 20

Scope of notification obligations

1 - For the purposes of article 54-B of the LCE, companies are required to notify ANACOM of breaches of security or loss of integrity that have a significant impact on the operation of the networks and services they offer, under the terms of this Chapter I.

2 - Compliance with the notification obligations provided for in this Chapter I shall be without prejudice to, or replace, in particular:

a) Compliance by companies with their obligations to notify security incidents to the competent authorities, in particular the ANPC, the Public Prosecution Office, the CNCS, the CNPD and the regional, local and sectoral authorities, as provided for in the provisions of the legal and regulatory requirements, including in the context of civil emergency planning in the communications, civil protection and internal security sectors;

b) Communications by companies to other companies involved in the security incidents in question, to the extent necessary to comply with the provisions of article 4 and paragraph 15 of article 22.

3 - For the purposes of point *a)* of the preceding paragraph, within the scope of its attributions and competences, in particular in matters of civil emergency planning in the communications and civil protection sector, ANACOM may, in collaboration with the competent authorities, make recommendations to companies on the link between the notification procedures in question.

Article 21

Circumstances

1 - For the purposes of the previous article, all breaches of security or loss of integrity that cause a serious disturbance to the operation of networks and services, with a significant impact on the continuity of such operation, according to the circumstances and rules provided for in the following paragraphs.

2 - For the purposes of the previous paragraphs, companies must notify ANACOM of:

a) Any breach of security or loss of integrity whose impact is included in one of the following levels:

Duration, and	**Number of subscribers or accesses affected (or, in accordance with point *e)* of paragraph 3 of this article, geographical area affected)**
≥ 30 minutes	no. of subscribers or accesses affected ≥ 500,000 (or, in accordance point *e)* of with paragraph 3 of this article, geographical area affected ≥3,000 km^2)
≥ 1 hour	500,000 > no. of subscribers or accesses affected ≥ 100,000 (or, in accordance with point *e)* of paragraph 3 of this article, 3,000 km^2 > affected geographical area ≥ 2,000 km^2)
≥ 2 hours	100,000 > no. of subscribers or accesses affected ≥ 30,000 (or, in accordance with point *e)* of paragraph 3 of this article, 2,000 km^2 > affected geographical area ≥ 1,500 km^2)
≥ 4 hours	30,000 > no. of subscribers or accesses affected ≥ 10,000

	(or, in accordance with point *e)* of paragraph 3 of this article, 1,500 km^2 > affected geographical area ≥ 1,000 km^2)
≥ 6 hours	10,000 > no. of subscribers or accesses affected ≥ 5,000 (or, in accordance point *e)* of with paragraph 3 of this article, 1,000 km^2 > affected geographical area ≥ 500 km^2)
≥ 8 hours	5,000 > no. of subscribers or accesses affected ≥ 1,000 (or, in accordance point *e)* of with paragraph 3 of this article, 500 km^2 > affected geographical area ≥ 100 km^2)

b) Any breach of security or loss of integrity affecting the delivery to PSAP, directly or indirectly, of calls to the European single emergency number 112 as well as calls to the national emergency number 115 for a period equal to or greater than 15 minutes;

c) Any breach of security or loss of recurring integrity, whenever the cumulative impact of its occurrences in a period of four weeks fulfils one of the conditions set forth in the preceding paragraphs;

d) Any breach of security or loss of integrity occurring on a date when the normal and continuous operation of the networks and services, as provided for in paragraph 4 of this article, is particularly relevant, provided that:

i) It lasts for one hour or more;

ii) It affects a number of subscribers or access points equal to or greater than 1,000 or, in accordance with point *e)* of paragraph 3 of this article, a geographical area equal to or greater than 100 km^2;

e) Any breach of security or loss of integrity affecting the operation of all networks and services offered by a company throughout the territory of an island of the Autonomous Regions of the Azores or Madeira, provided that it lasts for a period of 30 minutes or more, regardless of the number of subscribers or accesses affected and the geographical area affected;

f) Any breach of security or loss of integrity detected by the companies or communicated to them by their clients which has an impact on the functioning of the networks and services which are essential to ensure the continuity of the provision of the relevant services and which are identified as such within the contract concluded with its relevant clients, provided that it has a duration of 30 minutes or more;

g) Any breach of security or loss of integrity whose accumulated impact on a group of companies that meet the conditions set forth in paragraph 2 of article 3 of Law no. 19/2012, of 8 May, in its current version, meets one of the conditions set out in point *a)* and, in the part referring to this point, in point *c)*, both of this paragraph 2.

3 - For the purposes of the previous paragraph:

a) The impact of a breach of security or loss of integrity shall be measured by reference to all networks and all services of a company that are affected by it;

b) The number of subscribers or accesses affected by a security breach or loss of integrity corresponds to the sum of the number of subscribers or accesses that are affected by it in the various networks and services;

c) The number of subscribers of a service that is supported in another service is only counted when the support service is not affected;

d) The number of subscribers or accesses affected corresponds to the number of subscribers or accesses that are covered by the breach of security or loss of integrity or, if it is impossible to determine, an estimate based on the statistical elements held by the company;

e) The criterion for the affected geographical area should only be applied if the criterion on the number of subscribers or affected accesses is inapplicable or, in this case, reasonably impossible to determine or estimate.

4 - For the purposes of point *d)* of paragraph 2 and without prejudice to the identification by ANACOM of other dates, duly notified to the companies at least five working days in advance, the relevant dates shall be the following:

a) National election days (legislative, presidential, European or local elections);

b) National referendum days;

c) National exercise day of electronic communications networks or services, pursuant to point *c)* of article 54-D of the LCE and paragraph 3 of article 12 of this regulation;

d) Regional election days, as regards security breaches or loss of integrity in the region concerned.

Article 22

Format and Procedures

1 - For each breach of security or loss of integrity that should be subject to notification under the provisions of the previous article, companies must submit to ANACOM:

a) An initial notification pursuant to paragraphs 4 and 5 of this article;

b) A final notification pursuant to paragraphs 8 and 9 of this article;

c) Whenever a notice of termination of a breach of security or loss of integrity with significant impact is required in accordance with paragraph 6 of this article, and in the terms of paragraphs 6 and 7 of this article.

2 - In the circumstance provided for in point *c)* of paragraph 2 of the previous article, companies should only submit to ANACOM a final notification in accordance with the terms of paragraphs 8 and 9 of this article, with due adaptations.

3 - In the circumstance provided for in point *g)* of paragraph 2 of the previous article, a single series of notifications may be addressed to ANACOM, in accordance with paragraph 1 of this article, provided that:

a) They cover the full impact of the breach of security or loss of integrity;

b) They are presented on behalf of all companies.

4 - The initial notification should be sent as soon as possible and as long as the company can conclude that there is or there will be a significant impact within one hour after verification of the circumstance provided for in the previous article, which in the specific case determined the obligation to notify, without prejudice to compliance with this deadline, the company must prioritise the mitigation and resolution of breach of security or loss of integrity, beginning, when applicable, by reestablishing the provision of essential networks and services to ensure the continuity of the provision of relevant services.

5 - The notification provided for in the previous paragraph shall include the following information:

a) Name, telephone number and e-mail address of a representative of the company, for the purpose of possible contact by ANACOM;

b) Date and time of commencement or, if it is not possible to determine, the detection of breach of security or loss of integrity;

c) Date and time when the breach of security or loss of integrity assumed significant impact;

d) Date and time when the breach of security or loss of integrity has lost its significant impact or, if it continues, the estimated time limit for its loss;

e) Brief description of the breach of security or loss of integrity, including indication of the root cause category and, as far as possible, its details;

f) Possible estimate of its impact in terms of:

i) Affected networks and services;

ii) Access to emergency services;

iii) Number of subscribers or accesses affected;

iv) Relevant affected clients, when applicable;

v) Geographical area affected, in km^2;

g) Observations.

6 - After the loss of the significant impact of the breach of security or of loss of integrity, and where it has not already been communicated in the initial notification, companies must submit to ANACOM, as soon as possible, within a maximum period of two hours after its occurrence, a notification on the end of the security breach, or loss of integrity with significant impact.

7 - The notification referred to in the preceding paragraph shall include the following information:

a) Update of the information transmitted in the initial notification;

b) Brief description of the measures taken to resolve breach of security or loss of integrity;

c) Indication of the councils where there were subscribers, accesses or geographical area affected;

d) Description of the impact situation at the time of significant impact, including:

i) Networks and services still affected;

ii) Number of subscribers or accesses still affected;

iii) Relevant clients still affected, when applicable;

iv) Geographical area still affected, in km^2;

v) Councils where there are still subscribers, accesses or geographical area affected;

vi) Estimated times for full recovery of subscribers, accesses, relevant clients or geographical area still affected.

8 - The final notification must be signed by the security officer and sent within 20 working days from the time the breach of security or loss of integrity ceases to have a significant impact.

9 - The notification provided for in the previous paragraph shall include the following information:

a) Unique identifier of the breach of security or loss of integrity attributed by ANACOM upon initial notification;

b) Date and time when the breach of security or loss of integrity assumed significant impact;

c) Date and time when the breach of security or loss of integrity lost its significant impact;

d) The date and time of the commencement or, if it is not possible to determine, the detection of the breach of security or loss of integrity and the date and time of its end if they are different from the dates and times transmitted respectively under points *b)* and *c)*;

e) Impact of breach of security or loss of integrity in terms of:

- *i)* Networks (including national and international interconnections) and their infrastructures (including systems), indicating, in the case of assets classified in classes A or B, their unique identifier, and affected services;
- *ii)* Access to emergency services by the single European emergency number 112 (including access by the national emergency number 115);
- *iii)* Number of subscribers or accesses affected, by network and service;
- *iv)* Relevant affected clients, when applicable;
- *v)* Percentage of the number of subscribers or accesses affected in relation to total subscribers or accesses, by network and service;
- *vi)* Geographical area affected, in km^2;
- *vii)* Parishes and respective councils where there were affected subscribers, accesses or geographical area;

f) Description of the breach of security or loss of integrity, with indication of the root cause category and the respective detail;

g) Indication of measures taken to mitigate breach of security or loss of integrity;

h) Indication of the measures taken to resolve the breach of security or loss of integrity, including, in case of security breaches or loss of integrity with partial restoration times, chronology and detail of restoration steps;

i) Indication of measures taken and/or planned to prevent or minimise the occurrence of similar security breaches or similar integrity losses in the future (in the context of planning and/or operation, contingency plan, interconnection agreements, services and other relevant areas) and the date on which they have been or will be made effective;

j) Where applicable, information made available to the public regarding breach of security or loss of integrity, including any updates thereto, as well as the date and time of such communications;

k) Description of the residual impact situation at the date of the final notification, namely:

i) Networks and services still affected;

ii) Number of subscribers or accesses still affected;

iii) Relevant clients still affected, when applicable;

iv) Geographical area still affected, in km^2;

v) Parishes and their respective councils where there are still subscribers, accesses or geographical area affected;

vi) Estimated times for full recovery of subscribers, accesses, relevant clients or geographical area still affected;

l) Where applicable, indication of the presentation of a complaint to the Public Prosecution Office;

m) Other relevant information;

n) Observations.

10 - In cases where there is a residual situation of the impact existing at the date of the final notification, described under the provisions of point *k)* of the preceding paragraph, companies shall notify ANACOM, as soon as possible, on the total recovery of that residual situation.

11 - For the purposes of paragraphs 5, 7 and 9, security breaches or losses of integrity may have the following categories of root causes:

a) Accident or natural phenomenon;

b) Human error;

c) Malicious attack;

d) Maintenance or failure of hardware or software;

e) Failure to provide goods or services by a third party.

12 - The information included in the notifications provided for in this article in relation to the number of subscribers or accesses shall, whenever possible, comply with the definitions established in the framework of the obligations to provide periodic information to ANACOM.

13 - The notifications provided for in this article shall be made by the following means:

a) By electronic means, under the terms to be determined by ANACOM under the provisions of paragraph 1 of article 5;

b) In addition, and in respect of the initial notification and the notification of termination of breach of security or loss of integrity with significant impact, by telephone through the number to be indicated by ANACOM.

14 - Any change to the contacts provided for in the previous paragraph shall be communicated to the companies and published on the institutional website of ANACOM, at least 20 working days in advance.

15 - Companies whose networks or services are affected in their operation by the same security breach or loss of integrity shall cooperate with each other for the correct detection and evaluation of the impact of that breach of security or loss of integrity and, in the case provided for in point *g)* of paragraph 2 of the previous article, for the respective notification.

16 - In order to comply fully with the provisions of this Chapter, companies shall implement all means and procedures necessary for the detection, impact assessment and notification of security breaches or loss of integrity that meet the circumstances set forth in the preceding article.

CHAPTER II

Obligations of information to the public

Article 23

Conditions

1 - For the purposes of point *b)* of article 54-E of the LCE, companies shall inform the public of any breach of security or loss of integrity whose impact on the operation of their networks and services falls within one of the following levels:

Duration, and	**Number of subscribers or accesses affected (or, in accordance with point *e)* of paragraph 2 of this article, geographical area affected)**
≥ 30 minutes	no. of subscribers or accesses affected ≥ 500,000 (or, in accordance with point *e)* of paragraph 3 of this article, geographical area affected ≥ 3,000 km^2)
≥ 1 hour	500,000 > no. of subscribers or accesses affected ≥ 100,000 (or, in accordance with point *e)* of paragraph 3 of this article, 3,000 km^2 > geographical area affected ≥ 2,000 km^2)
≥ 2 hours	100,000 > no. of subscribers or accesses affected ≥ 30,000 (or, in accordance with point *e)* of paragraph 3 of this article, 2,000 km^2 > geographical area affected ≥ 1,500 km^2)
≥ 4 hours	30,000 > no. of subscribers or accesses affected ≥ 10,000 (or, in accordance with point *e)* of paragraph 3 of this article, 1,500 km^2 > geographical area affected ≥ 1,000 km^2)

2 - For the purposes of the previous paragraph:

a) The impact of a breach of security or loss of integrity shall be measured by reference to all networks and all services of a company that are affected by it;

b) The number of subscribers or accesses affected by a security breach or loss of integrity corresponds to the sum of the number of subscribers or accesses that are affected by it in the various networks and services;

c) The number of subscribers of a service that is supported in another service is only counted when the support service is not affected;

d) The number of subscribers or accesses affected corresponds to the number of subscribers or accesses that are covered by the breach of security or loss of integrity or, if it is impossible to determine, an estimate based on the statistical elements held by the company;

e) The criterion for the geographical area affected should only be applied if the criterion on the number of subscribers or affected accesses is inapplicable or, in this case, reasonably impossible to determine or estimate.

3 - The provisions of this article are without prejudice to the fact that, in circumstances not provided for in paragraph 1 and whenever ANACOM also considers it in the public interest and so determines, pursuant to point *b)* of article 54-E of the LCE, that companies should inform the public of security breaches or loss of integrity occurring on their networks and services.

Article 24

Content, means and deadlines for disclosure

1 - In informing the public of security breaches or loss of integrity referred to in the preceding article, companies shall:

a) Ensure that the content of the information is clear, accessible and as accurate as possible and includes, together with other elements considered relevant:

i) Indication of affected networks and services;

ii) Indication of the zone or zones which, as a result of the breaches of security or the loss of integrity occurred, are affected, broken down at municipality level, if possible, graphically on a map of Portugal;

iii) The expected resolution period or, when applicable, the date of resolution;

b) Provide the information at least in the respective Internet sites that they use in their relationship with the users, through a hyperlink immediately visible and identifiable on the first page of the site, without the use of the lift bar;

c) Make available the information as soon as possible, within a maximum of four hours after the initial notification to ANACOM;

d) Ensure that the information made available is kept up-to-date, in particular whenever there is a significant change and after the end of the breach of security or loss of integrity;

e) Keep the information available through the Internet accessible to the public, in the same locations referred to in point *b)*, during the period of 20 working days from the date of the end of the breach of security or loss of integrity.

2 - Companies must communicate to ANACOM, as soon as they start their activity, the URLs of the Internet pages on which, for the purposes of the provisions of point *b)* of the previous paragraph, they will disclose to the public the security breaches or integrity losses that occurred in their networks and services, as well as any subsequent amendment thereto at least five working days in advance of their implementation.

3 - ANACOM may, if it deems it appropriate and with a view to facilitating public access to information on security breaches or loss of integrity, in particular on its institutional website, disclose the URLs provided for in the previous paragraph.

4 - In order to comply fully with the provisions of this Chapter II, companies shall implement all means and procedures necessary for the detection, impact assessment and disclosure of security breaches or loss of integrity that meet the circumstances set forth in the previous article.

TITLE IV

Audits of network and service security

CHAPTER I

General provisions

Article 25

Duty to conduct an audit

For the purposes of paragraphs 1 and 2 of article 54-F of the LCE, companies whose offers are supported by at least one asset classified as Class A shall ensure, through independent auditors and at its own expense, the realisation of security audits to its networks and services, under the terms of this Title IV.

Article 26

Scope

Companies shall ensure that audits fall within a cycle of continuous improvement and enable an appropriate sample of the assets classified in classes A or B and taking into account the existing situation in the company to comply with applicable legal and regulatory standards.

Article 27

Reference documents and standards

Companies shall ensure that audits are based on existing national, European and international standards, specifications or recommendations on the subject, in particular:

a) ISO/IEC 17021-1:2015 (*Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements*) and its revisions;

b) ISO/IEC TS 17021-5:2014 *(Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 5: Competence requirements for auditing and certification of asset management systems)* and its revisions;

c) ISO/IEC TS 17021-6:2014 *(Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 6: Competence requirements for auditing and certification of business continuity management systems)* and its revisions;

d) ISO/IEC 27006:2015 (*Information technology - Security techniques – Requirements for bodies providing audit and certification of information security management systems*) and its revisions;

e) ISO/IEC 27007:2017 *(Information technology - Security techniques – Guidelines for information security management systems auditing)* and its revisions*;*

f) ISO 19011:2018 (*Guidelines for auditing management systems*) and its revisions;

g) Other appropriate national, European or international standard, specification or recommendation.

Article 28

Auditors

1 - Companies shall ensure that auditors and all employees involved in audits comply with the following requirements:

a) Technical competence, in particular in accordance with the standards, specifications and recommendations applicable under the provisions of the previous article;

b) Relevant experience in the electronic communications sector, in particular in the planning, operation or security of networks and services;

c) Appropriate accreditation issued by the competent authorities for access to classified material, whenever necessary and in the terms legally established.

2 - Companies should ensure that auditors are not their suppliers for other services, other than conducting independent and external audits, and that they submit statements of non-conflict of interest on their behalf and on behalf of all employees involved, in accordance with applicable legislation.

3 - Companies must, excluding duly substantiated exceptions, ensure rotation in the choice of auditors, so that the same auditor does not perform more than two consecutive audits.

Article 29

Duty of collaboration

1 - Companies shall provide the auditors with all the collaboration and assistance required to carry out audits under the terms of this Title IV, in particular:

a) Collaboration in preparing and conducting audits;

b) Collaboration in the preparation of audit reports;

c) Providing access to all requested evidence including the security plan, annual security reports and, where applicable, the audit report and the plan for correcting non-conformities of the last audit performed;

d) Providing access to the necessary means, in particular for conducting tests;

e) Providing access to sites;

f) Providing access to relevant suppliers at the level of network and service security;

g) Providing access to key employees.

2 - Companies must ensure direct access by ANACOM to the auditors and to the suppliers and collaborators provided for, respectively, in points *f)* and *g)* of the previous paragraph, as well as their availability for holding meetings with ANACOM and for the provision of clarifications requested by the Authority.

3 - Companies must safeguard the direct access to auditors and suppliers provided for in point *f)* of paragraph 1, by ANACOM, in the contracts concluded with them.

CHAPTER II

Audit Procedures

Article 30

Phases

Companies shall ensure that audits are carried out in a phased and sequenced manner, including the pre-audit phase, the audit phase and the post-audit phase, as provided for in this Chapter II.

Article 31

Pre-audit phase

1 - Companies must, together with the auditors, prepare and submit to ANACOM an audit proposal containing the following elements:

a) Identification of the auditors and all their employees involved in each phase of the audit;

b) Proof or declarations that prove compliance with the requirements of article 28;

c) Audit programme, duly substantiated, including the following elements:

i) Expected date for the start of the audit phase;

ii) Estimated duration of the audit phase;

iii) Indication of the assets covered by the sample, with reference to their unique identifiers;

iv) Activities planned.

2 - Companies must submit to ANACOM the audit proposal, signed by the security officer:

a) In the case of the first audit, within six months from the date from which the company supports its offers in an asset classifiable in class A;

b) In the case of subsequent audits, within two years from the date of submission of the audit proposal on which the previous audit was based or, where appropriate, within six months of the date on which the company undertakes its offers on an asset classifiable as class A.

3 - ANACOM is responsible for accepting the audit proposal and may, for this purpose, request the company and the auditor to provide the necessary clarifications and request from the company the supply of existing deficiencies.

Article 32

Audit phase

1 - The companies must start the audit phase within a maximum of 60 working days from the date of acceptance by ANACOM of the audit proposal.

2 - Companies must communicate, at least 20 working days in advance, the dates and locations where the activities of the audit phase will take place, so that ANACOM can, if it wishes and at least five days in advance with regard to the date of commencement of the activities, appoint a collaborator, duly accredited under the terms set forth in point *c)* of paragraph 1 of article 28, to attend them.

3 - The companies must ensure that the auditor draws up an audit report which, in accordance with the audit proposal accepted by ANACOM, includes the following elements:

a) List of non-conformities of the existing situation in the company;

b) Description and duration of the activities carried out.

4 - Companies should:

a) Ensure, in the contracts signed with the auditors, that the audit report is sent simultaneously by the auditors to the company and to ANACOM, within 20 working days of the completion of the audit phase;

b) Send to ANACOM a copy of the audit report, signed by the security officer within five working days of receiving it.

5 - ANACOM is responsible for accepting the audit report and may, for this purpose, request the company and the auditor to provide the necessary clarifications and to request to the company the supply of existing deficiencies.

Article 33

Post-audit phase

1 - Companies must prepare and send to ANACOM a plan for the correction of non-conformities contained in the audit report, signed by the security officer, within 40 working days of the date of acceptance by ANACOM of the audit report.

2 - The plan for the correction of non-conformities must contain:

a) Identification of all non-conformities and observations contained in the audit report, including any conclusions and recommendations;

b) For each non-conformity:

i) An analysis of its causes;

ii) Indication of corrective measures and deadlines.

3 - The companies must ensure that each of the measures included in the plan for the correction of non-conformities referred to in sub-point *ii)* of point *b)* of the previous paragraph is executed as soon as possible or within the maximum period that ANACOM, if it so wishes, determines.

TITLE V

Final and transitional provisions

Article 34

Penalty system

The infractions of this regulation are penalised in accordance with points *ee), ff), or gg)* of paragraph 2 or in points *u), v), x)* or *z)* of paragraph 3 of article 113 of the LCE.

Article 35

Entry into force and transitional provisions

1 - This regulation shall enter into force on the day following the date of its publication in *Diário da República*, without prejudice to the provisions of the following paragraphs.

2 - Without prejudice to compliance with the provisions of articles 54-A to 54-G of the LCE, companies with activity at the date of entry into force of this regulation shall:

a) Within 40 working days of entry into force of this regulation:

i) Approve the security policy, communicating it to ANACOM, within the same period, in the terms set forth in point *a)* of paragraph 1 of article 18, and begin to prepare the security plan, in accordance with the terms of article 17;

ii) Establish the function of the security officer, in accordance with the provisions of article 14, communicating to ANACOM, within the same period, the elements provided for in point *b)* of paragraph 1 and in paragraph 2 of article 18;

b) Within 60 working days of the date of entry into force of this regulation, classify the assets provided for in points *a)*, *b)* and *d)* of paragraph 4 of article 8;

c) Within 80 working days of the date of entry into force of this regulation, establish the function of permanent contact point, in accordance with the terms of article 15, communicating to ANACOM, within the same period, the elements provided for in point *c)* of paragraph 1 and in paragraph 3 of article 18;

d) Within one year of entry into force of this regulation:

i) If applicable, adopt the procedures for controlling the exceptional management of Internet access traffic, in accordance with the terms of article 11;

ii) Complete the asset classification and asset inventory, in accordance with articles 8 and 9 respectively, and send the initial version of the list provided for in paragraph 4 of article 9;

iii) Adopt all security measures included in sophistication level 1 and applicable in accordance with Title II and the Annex to this regulation, without prejudice to paragraphs 3 and 5 of this article;

e) Within eighteen months of the date of entry into force of this regulation and, where applicable, establish the security incident response team, in accordance with article 16;

f) Within two years of the entry into force of this regulation:

i) Adopt all other security measures applicable in accordance with Title II and the Annex to this regulation, without prejudice to paragraphs 3 and 5 of this article;

ii) Complete the drafting of the security plan in accordance with article 17.

3 - Without prejudice to compliance with the provisions of articles 54-A to 54-G of the LCE, companies with activity at the date of entry into force of this regulation shall also:

a) Draw up the first annual security report in accordance with article 19 to be reported for the first calendar year following the calendar year of the date of entry into force of this regulation;

b) Draw up and implement the first exercise programme as provided for in article 12 in the second calendar year following the calendar year of the date of entry into force of this regulation;

c) If they are subject to the obligation of carrying out an audit, in accordance with the provisions of article 25, submit to ANACOM the first audit proposal, as provided for in article 31, within a period of two years from the date of entry force of this regulation.

4 - Without prejudice to compliance with articles 54-A to 54-G of the LCE, companies which commence their activity after the date of entry into force of this regulation shall comply with the provisions of paragraphs 2 and 3 of this article, within the periods laid down therein, or, where appropriate, within the periods laid down in the articles mentioned.

5 - The provisions of article 13 and Title III shall enter into force within one year of the date of entry into force of this regulation.

6 - Until the determination by ANACOM of the specific electronic means for each communication and for each transmission of information, for the purposes of the provisions of paragraph 1 of article 5, these will be made by delivery to the services or by mail delivery.

7 - In the case of energy service providers and taking account of sectoral interdependence, the entry into force of the provisions on the priority restoration of the provision of networks and services, as provided for in paragraph 4 of article 22 and in point *b)* of the Security Objective

no.19 of the Annex depends on the entry into force of conditions for cooperation and priority treatment of companies within the framework of the legal and regulatory provisions applicable in the energy sector.

Article 36

Monitoring committee

1 - In order to monitor the application of this regulation, a committee is set up with the following tasks:

a) Promotion of harmonisation of measures;

b) Promotion of cooperation;

c) Evaluation of emerging risks;

d) Sharing of information and knowledge;

e) Analysis of challenges for the security of networks and services.

2 - The monitoring committee is composed of:

a) A representative of ANACOM;

b) Those responsible for the security of companies whose offers are supported by at least one class A asset, or their representative;

c) When appointed, two representatives of companies that do not support their offers in assets classified under class A.

3 - The designation of the representatives provided for in point *c)* of the preceding paragraph is made at a stakeholder meeting convened by ANACOM, for a renewable term of three years.

4 - The monitoring committee is coordinated by the representative of ANACOM and ordinarily meets at least twice a year and, extraordinarily, on the initiative of ANACOM.

5 - Other entities invited by ANACOM may attend meetings of the monitoring committee when discussion and analysis of specific matters so warrants.

6 - The technical and logistical support for the functioning of the monitoring committee will be provided by ANACOM.

Article 37

Revoking rule

ANACOM's decision of 12 December 2013 is revoked by the end of one year from the date of entry into force of this regulation.

ANNEX

Objectives and security measures

(referred to in paragraph 1 of article 7)

1 - **Security policy**

Establish and maintain an adequate network and service security policy.

Sophistication levels	**Security measures**
1 (Basic)	a) Define, approve and maintain a high-level security policy covering the security of networks and services. b) Publish and communicate the security policy to key employees.
2 (Industry standard)	c) Define, approve and maintain a detailed security policy regarding assets classified in classes A or B and critical business processes. d) Publish and communicate to all employees the security policy and how it affects their work. e) Review the security policy following changes or security incidents.
3 (State of the art)	f) Review the security policy on a regular basis, taking into account in particular previous security incidents, test and exercise results and security incidents affecting other similar companies in the sector.

2 - **Governance and risk management**

Establish and maintain an appropriate governance and risk management framework to identify, prevent, manage and reduce risks to network and service security.

Sophistication levels	Security measures
1 (Basic)	a) Draw up a list of the main risks to the security of networks and services, taking into account the threats to which the assets classified in classes A or B may be subject. b) Inform key employees of the main risks and how they are mitigated.
2 (Industry standard)	c) Establish a risk management methodology and tools at the level of industry standards, including existing national, European and international standards, specifications and recommendations on the subject. d) Ensure that key employees use risk management methodology and tools. e) Review risk assessments following changes or security incidents. f) Ensure that residual risks are accepted by management.
3 (State of the art)	g) Review the methodology and risk management tools periodically, taking into account, in particular, previous security changes and incidents.

3 - **Roles and responsibilities in the field of security**

Establish and maintain an appropriate structure of roles and responsibilities in the area of network and service security.

Sophistication levels	Security measures
1 (Basic)	a) Assign employees to roles and responsibilities in the area of network and service security. b) Ensure that employees performing duties in the field of network and service security are reachable in case of security incidents.

2 (Industry standard)	c) Appoint employees to the functions in the field of network and service security. d) Inform employees of the functions in the field of security of networks and services existing in the company and when they should be contacted.
3 (State of the art)	e) Regularly review the structure of roles and responsibilities in the area of network and service security, taking into account, in particular, previous security changes and incidents.

4 - **Security in contracts with third parties**

Establish and maintain a security policy for contracts with third parties to ensure that third-party dependencies do not adversely affect the security of networks and services.

Sophistication levels	**Security measures**
1 (Basic)	a) Include security requirements in contracts with third parties.
2 (Industry standard)	b) Define, approve and maintain a security policy for contracts with third parties. c) Ensure that all services and all supplies of goods by third parties comply with the security policy for contracts with third parties. d) Review the security policy for contracts with third parties as a result of changes or security incidents. e) Mitigate the residual risks that third parties do not address.
3 (State of the art)	f) Record security incidents related to or caused by third parties. g) Regularly review security policy for contracts with third parties, taking into account, in particular, previous security changes and incidents.

5 - **Verification of credentials and references**

Ensure an adequate verification of credentials and references of the employees involved, to the extent necessary for their functions and responsibilities.

Sophistication levels	**Security measures**
1 (Basic)	a) Verify the professional references of employees.
2 (Industry standard)	b) Verify the credentials and references of employees, to the extent necessary and in the terms allowed by law. c) Define, approve and maintain a credentials and references verification policy and procedures.
3 (State of the art)	d) Regularly review the policy and procedures for verifying credentials and references, taking into account, in particular, previous security changes and incidents.

6 - **Security knowledge, education and training**

Ensure that staff have sufficient knowledge and receive regular education and training on network and service security.

Sophistication levels	**Security measures**
1 (Basic)	a) Provide education, training and relevant materials to key employees on issues related to network and service security.
2 (Industry standard)	b) Implement an education and training programme, ensuring that key employees have sufficient and up-to-date network security knowledge and services.

	c) Organise training sessions and raise awareness in employees on the topics of network security and services of importance to the company.
3 (State of the art)	d) Periodically review the education and training programme, taking into account in particular the previous security changes and incidents. e) Test and evaluate the knowledge of employees on network security and services.

7 - **Change of employees**

Establish and maintain an appropriate procedure for managing employee changes or changing roles and responsibilities.

Sophistication levels	**Security measures**
1 (Basic)	a) After a change in employees, cancel rights, cards, equipment and other access resources, in case they are no longer necessary or allowed. b) Inform new employees of the policies and procedures in force.and provide them with training on the same.
2 (Industry standard)	c) Define, approve and maintain a policy and procedures regarding employee changes, taking into account the timely cancellation of rights, cards and access equipment. d) Define, approve and maintain a policy and procedures on the education and training of employees in their new roles and responsibilities.
3 (State of the art)	e) Periodically check that policies and procedures are effective. f) Review policies and procedures, taking into account, in particular, previous security changes and incidents.

8 - **Processing of violations**

Establish and maintain a disciplinary procedure for employees in case of violation of network and service security policies or establish a more comprehensive procedure that includes security incidents caused by violations of network and service security policies by employees.

Sophistication levels	**Security measures**
1 (Basic)	a) Hold employees accountable for security incidents caused by violations of policies, especially in the scope of the employment contract and in the terms allowed by law.
2 (Industry standard)	b) Establish procedures for dealing with violations of policies committed by employees.
3 (State of the art)	c) Periodically review the disciplinary procedure taking into account, in particular, previous amendments and security incidents.

9 - **Physical and environmental security**

Establish and maintain adequate physical and environmental security of assets.

Sophistication levels	**Security measures**
1 (Basic)	a) Prevent unauthorised physical access to assets and create environmental controls to protect against unauthorised access, theft, fire and flood. b) Define, approve and maintain procedures for the protection and preservation of assets in a manner appropriate to the evolution of climatic conditions and the risks of natural disasters or other extreme events, including storms, landslides, floods, high winds, forest fires, earthquakes and tsunamis.
2 (Industry standard)	c) Define, approve and maintain a policy on physical security measures and environmental controls.

	d) Implement physical and environmental controls at the level of the industry standard, including existing national, European and international standards, specifications and recommendations on the subject.
3 (State of the art)	e) Periodically assess the effectiveness of physical and environmental controls. f) Review policy on physical security measures and environmental controls, taking into account, in particular, previous security changes and incidents.

10 - **Security of supplies**

Establish and maintain adequate security of supplies (including, but not limited to, accommodation infrastructure, leased lines, electricity and fuel).

Sophistication levels	**Security measures**
1 (Basic)	a) Ensuring the security of supplies.
2 (Industry standard)	b) Define, approve and maintain a security policy for critical supplies. c) Implement security measures at the level of the industry standard, including existing national, European and international standards, specifications and recommendations in order to ensure continuity of supplies.
3 (State of the art)	d) Implement state-of-the-art security measures to ensure continuity of supplies. e) Regularly review security policy and measures to ensure continuity of supplies taking into account, in particular, previous security changes and incidents.

11 - **Asset access control**

Establish and maintain appropriate physical and logical access controls to assets.

Sophistication levels	Security measures
1 (Basic)	a) Have unique identifiers for users and systems, which must be authenticated before accessing services or systems. b) Implement mechanisms to control access to assets, in order to allow only authorised use.
2 (Industry standard)	c) Define, approve and maintain a policy and procedures for controlling access to assets, covering, in particular, the functions, rights, responsibilities and procedures for assigning and cancelling access rights. d) Select appropriate authentication mechanisms depending on the type and level of access. e) Monitor access to assets and have an exception approval procedure and improper access registration.
3 (State of the art)	f) Evaluate the effectiveness of access control policy and procedures and implement cross-checks of access control mechanisms. g) Review the access control policy, procedures and mechanisms.

12 - **Asset integrity**

Establish and maintain the integrity of the assets and protect them against viruses, malicious code and other malicious software that alter or may change their security and functionality.

Sophistication levels	Security measures
1 (Basic)	a) Ensure that the software of assets is not tampered with or altered, in particular by means of introductory controls and firewalls.

	b) Ensure that critical security information (including, but not limited to, passwords, shared secrets, and private keys) is not disclosed or tampered with. c) Check for malicious software in the assets.
2 (Industry standard)	d) Implementing industry-standard security measures, including existing national, European and international standards, specifications and recommendations, providing an in-depth defence against tampering and change of assets.
3 (State of the art)	e) Implement state-of-the-art controls to protect the integrity of assets. f) Review the effectiveness of security measures to protect the integrity of assets.

13 - **Operational procedures**

Establish and maintain procedures for the operation of assets classified in classes A or B by employees.

Sophistication levels	**Security measures**
1 (Basic)	a) Establish procedures and define and allocate the responsabilities for the operation of assets classified in classes A or B.
2 (Industry standard)	b) Define, approve and maintain an asset operation policy that ensures that the assets classified in classes A or B are operated and managed according to predefined procedures.
3 (State of the art)	c) Review the policy and operating procedures for assets classified in classes A or B, taking into account, in particular, changes and security incidents.

14 - **Management of changes**

Establish procedures for managing changes to assets classified in classes A or B in order to minimise the likelihood of security incidents.

Sophistication levels	Security measures
1 (Basic)	a) Establish and define procedures to introduce changes to assets classified in classes A or B.
2 (Industry standard)	b) Define, approve and maintain a policy and procedures for the management of changes to ensure that changes to assets classified in classes A or B are always performed according to a predefined procedure. c) Document the procedures for the management of changes and record, for each change, the steps of the procedure followed.
3 (State of the art)	d) Regularly review procedures for the management of changes, taking into account, in particular, previous changes and security incidents.

15 - **Asset management**

Establish and maintain asset management and configuration control procedures in order to manage the availability and configuration of assets classified in classes A or B.

Sophistication levels	Security measures
1 (Basic)	a) Manage assets classified in classes A or B and their configurations.
2 (Industry standard)	b) Define, approve and maintain a policy and procedures for asset management and configuration control.

3 (State of the art)	c) Regularly review the asset management and configuration control policy and procedures, taking into account, in particular, previous security changes and incidents.

16 - **Security incident management procedures**

Establish and maintain procedures for managing security incidents and forwarding to the appropriate employees.

Sophistication levels	**Security measures**
1 (Basic)	a) Ensure the availability and preparation of employees for the management and processing of security incidents. b) Record and typify all security incidents.
2 (Industry standard)	c) Define, approve and maintain a security incidents management policy and procedures.
3 (State of the art)	d) Investigate the most significant security incidents and prepare final reports of security incidents, including an indication of the measures taken and recommendations to mitigate the future occurrence of security incidents of the same type. e) Review security incident management policy and procedures, taking into account, in particular, previous security incidents.

17 - **Detection capability of security incidents**

Establish and maintain a security incident detection capability to ensure a timely, effective and orderly response to security incidents.

Sophistication levels	**Security measures**
1 (Basic)	a) Implement processes or systems for the detection of security incidents.

2 (Industry standard)	b) Implement processes or systems and procedures at industry-standard level, including existing national, European and international standards, specifications and recommendations on the subject, for the detection of security incidents. c) Implement processes or systems and procedures for recording and forwarding security incidents as quickly as possible to employees with appropriate roles.
3 (State of the art)	d) Regularly review the processes or systems and procedures for the detection of security incidents, taking particular account of previous security changes and incidents.

18 - **Notification and reporting of security incidents**

Establish and maintain adequate procedures for reporting and communicating security incidents, taking into account the provisions of the law.

Sophistication levels	**Security measures**
1 (Basic)	a) Notify and report security incidents, in progress or finalised, to authorities, third parties, customers and the public, as applicable or necessary.
2 (Industry standard)	b) Define, approve and maintain a policy and procedures for the notification and reporting of security incidents.
3 (State of the art)	c) Evaluate notifications and reports of security incidents. d) Review the policy and procedures for communicating and reporting on security incidents, taking into account, in particular, previous security changes and incidents.

19 - **Continuity strategy and contingency plans**

Establish and maintain contingency plans and a strategy for the continued operation of networks and services.

Sophistication levels	**Security measures**
1 (Basic)	a) Implement a strategy for the continued operation of networks and services, taking into account, in particular, the extraordinary situations provided for in point *b)* of paragraph 1 in article 3. b) Establish procedures for the priority restoration of the provision of networks and services through which relevant clients provide their relevant services, in particular in the extraordinary situations provided for in point *b)* of paragraph 1 in article 3.
2 (Industry standard)	c) Define, approve and maintain contingency plans for the assets classified in classes A or B, taking into account, in particular, the extraordinary situations provided for in point *b)* of paragraph 1 in article 3. d) Monitor the activation and execution of the contingency plans and record the recovery times with indication of conformity or non-compliance with the plans.
3 (State of the art)	e) Periodically review the strategy for the continued operation of networks and services. f) Review the contingency plans, taking into account, in particular, previous security changes and incidents.

20 - **Disaster Recovery Capabilities**

Establish and maintain appropriate disaster recovery capabilities for the restoration of networks and services in the event of major disasters and other extreme events, taking into account in particular the evolution of climatic conditions and the extraordinary situations referred to in point *b)* of paragraph 1 in article 3.

Sophistication levels	Security measures
1 (Basic)	a) Define plans and measures for the recovery and restoration of networks and services in the event of disasters, taking into account, in particular, the special situations referred to in point *b)* of paragraph 1 in article 3.
2 (Industry standard)	b) Define, approve and maintain a policy and procedures for the allocation with disaster recovery capabilities, taking into account, in particular, the special situations referred to in point *b)* of paragraph 1 in article 3. c) Provide disaster recovery capabilities at industry standard level, including existing national, European and international standards, specifications and recommendations, or ensure that they are available through third parties, taking into account, namely, the extraordinary situations provided for in point *b)* of paragraph 1 in article 3.
3 (State of the art)	d) Provide state-of-the-art disaster recovery capabilities in order to mitigate the impact of disasters, taking into account, in particular, the special situations referred to in point *b)* of paragraph 1 in article 3. e) Regularly review disaster recovery capabilities, taking into account in particular changes, previous security incidents, test and exercise results, and the extraordinary situations provided for in point *b)* of paragraph 1 in article 3.

21 - **Monitoring and event tracking policies**

Establish and maintain systems and functions for monitoring and recording events related to assets classified in classes A or B.

Sophistication levels	Security measures
1 (Basic)	a) Implement procedures for monitoring and recording events related to assets classified in classes A or B.

2 (Industry standard)	b) Define, approve and maintain a policy and procedures for monitoring and recording events related to assets classified in classes A or B. c) Implement mechanisms to monitor assets classified in classes A or B. d) Implement mechanisms for the collection and storage of records of events related to assets classified in classes A or B.
3 (State of the art)	e) Implement mechanisms for the automatic collection and analysis of records of events related to assets classified in classes A or B. f) Review the policy, procedures and mechanisms for monitoring and recording events relating to assets classified in classes A or B, taking into account, in particular, previous changes and security incidents.

22 - **Contingency Plan Exercises**

Establish and maintain policies for testing and exercising contingency and redundancy plans, whenever necessary in collaboration with third parties.

Sophistication levels	**Security measures**
1 (Basic)	a) Conduct and test contingency and redundancy plans to ensure that systems and processes work and that employees are prepared in case of high-impact security incidents.
2 (Industry standard)	b) Elaborate and implement a regular exercise programme to test contingency and redundancy plans, using realistic and variable scenarios over time. c) Ensure that the issues identified, and the lessons learned as a result of the exercises, are handled by responsible staff and

	that the relevant systems and processes are updated accordingly.
3 (State of the art)	d) Review the exercise programme, taking into account, in particular, previous changes and security incidents. e) Involve vendors and other third parties in the exercises, namely other companies, business partners or clients.

23 - **Asset Testing**

Establish and maintain policies to test assets, particularly in connection with new assets.

Sophistication levels	**Security measures**
1 (Basic)	a) Test assets before they are used or linked to the assets in operation.
2 (Industry standard)	b) Define, approve and maintain a policy and procedures for testing assets. c) Implement automatic testing tools.
3 (State of the art)	d) Review the policy, procedures and tools for testing assets, taking into account, in particular, previous security changes and incidents.

24 - **Security Assessments**

Establish and maintain an appropriate policy for conducting security assessments of the network services.

Sophistication levels	**Security measures**
1 (Basic)	a) Ensure that the assets classified in classes A or B are regularly subject to security assessments of the networks and

	services, including verifications and tests, in particular in the case of introduction of new assets and following changes.
2 (Industry standard)	b) Define, approve and maintain a policy and procedures for network and service security assessments.
3 (State of the art)	c) Assess the effectiveness of the policy and procedures for network and service security assessments. d) Review the policy and procedures for network and service security assessments, taking into account, in particular, previous changes and security incidents.

25 - **Compliance monitoring**

Establish and maintain a policy on monitoring compliance with legal and regulatory requirements.

Sophistication levels	**Security measures**
1 (Basic)	a) Monitor compliance with legal and regulatory requirements.
2 (Industry standard)	b) Define, approve and maintain a policy and procedures for monitoring and auditing compliance.
3 (State of the art)	c) Assess the policy and procedures for monitoring and auditing compliance. d) Review the policy and procedures for monitoring and auditing of compliance, taking into account, in particular, previous changes and security incidents.