SAND5G

https://sand5g-project.eu/

NIS-2 Directive Regulatory Compliance and Incident Reporting for 5G Operators

Dedicated Courses from National Authorities

D3.1: Security training, knowledge and capacity building report

This project has received funding from the DIGITAL EUROPE (DIGITAL) programme under Grant Agreement No 101127979

1

NIS-2 Introduction

From NIS-1 to NIS-2 Directive
Why change?

The Commission assessed the implementation of the NIS Directive 1:

- The scope of the NIS Directive 1 was too limited in terms of the areas it covered.
- The NIS Directive 1 was not sufficiently clear on issues related to the scope and Member States' competence in matters of jurisdiction.
- There was wide discretion for Member States in setting requirements regarding security measures and incident reporting.
- Ineffective supervision and enforcement regime.
- Differences in the level of financial – human resources between Member States / different levels of maturity.
- Member States do not systematically exchange information with each other.

NIS-2 Directive builds on the requirements and provisions of the original NIS1, and additionally:

- Extends the scope of cybersecurity rules to new sectors and entities.
- Introduces additional obligations regarding the notification of cybersecurity incidents, including strict deadlines and multiple stages within which the competent CSIRT must be informed.
- Specifies and strengthens the minimum horizontal cybersecurity risk management measures.
- Provides for various types of supervision and controls.
- Further improves the resilience and incident response capabilities of public and private entities, competent authorities and the EU as a whole.

Three Main Pillars of NIS2

MEMBER STATE RESPONSIBILITIES

National Authorities

National Strategies

CVD Frameworks

Crisis Management Frameworks

RISK MANAGEMENT

Accountability for top management for non compliance

Essential and important companies are required to take security measures

Companies are required to notify incidents within a given time frame

COMPANY RESPONSIBILITIES

CO-OPERATION AND INFO EXCHANGE

Cooperation Group

CSIRTs Network

CyCLONe

CVD and European Vulnerability registry

Peer-reviews

Biennial ENISA cybersecurity report

2

NIS-2 Scope

➢ Critical sectors: Annex I & Annex II

The NIS2 scope is covered by two annexes. The Directive applies to both public and private entities referred to in Annex I or II.

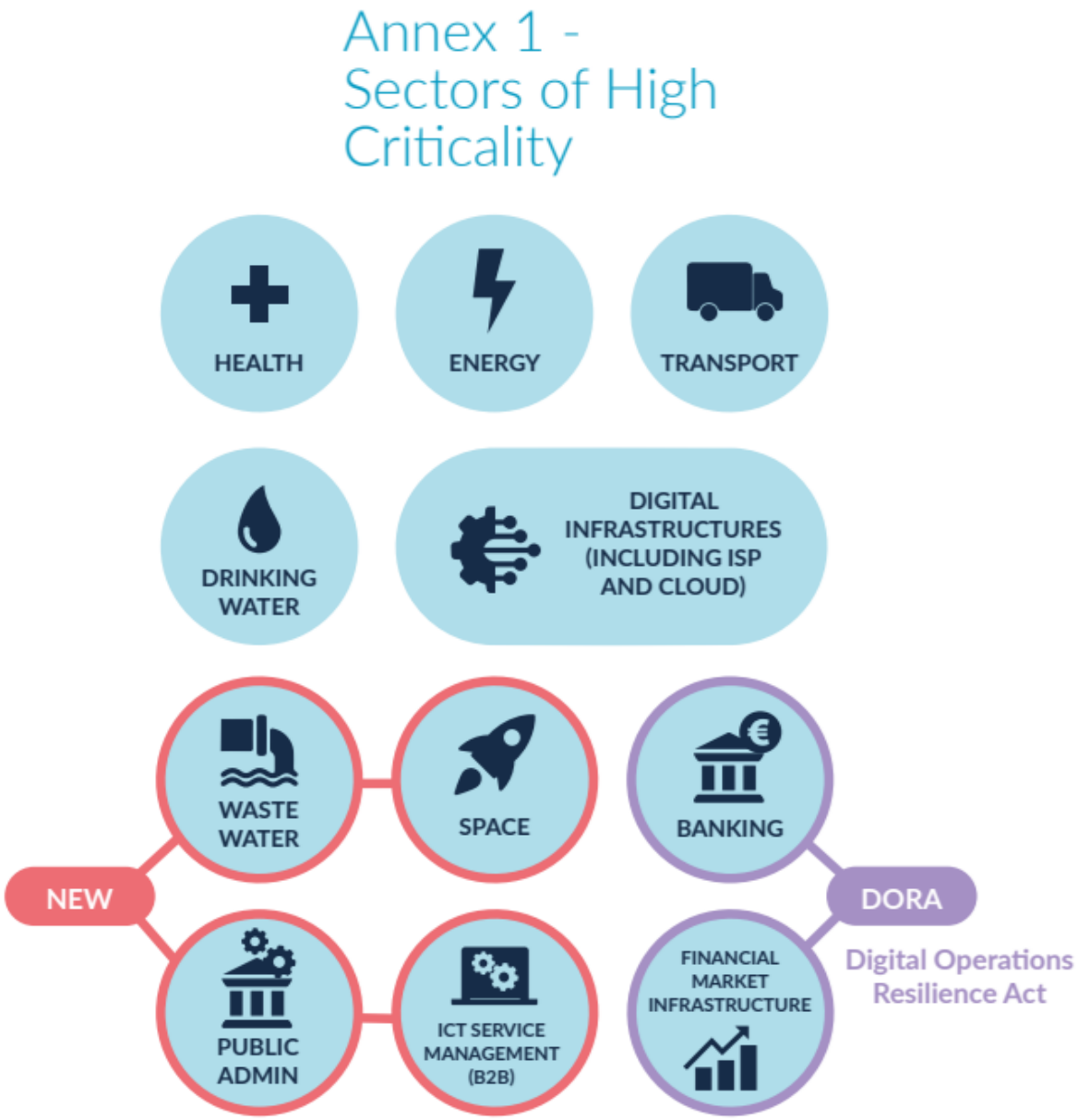
Annex I lists the sectors of high criticality, which can be either an Essential or an Important entity depending on the total annual revenue and size of the organization.

Annex II provides the other critical sectors set out by the EU, which will only fall into the Important Entity category.

➢ Entities in scope: essential and important entities

NIS2 also divides the entities that fall within the scope into two categories: ‘essential’ and ‘important’. The main differentiation is that a disruption of services in the essential group would be expected to have serious consequences for the country’s society as a whole.

The NIS-2 scope: Annex 1 & Annex 2



Annex I: Sectors of high criticality		LARGE ENTITIES (>= 250 employees or more than 50 million revenue)	MEDIUM ENTITIES (50-249 employees or more than 10million revenue)	SMALL & MICRO ENTITIES
1	ENERGY	ESSENTIAL	IMPORTANT	NOT IN SCOPE
2	TRANSPORT	ESSENTIAL	IMPORTANT	NOT IN SCOPE
		ESSENTIAL	IMPORTANT	NOT IN SCOPE
3	BANKING	ESSENTIAL	IMPORTANT	NOT IN SCOPE
4	FINANCIAL MARKET INFRASTRUCTURE	ESSENTIAL	IMPORTANT	NOT IN SCOPE
5	HEALTH	ESSENTIAL	IMPORTANT	NOT IN SCOPE
		ESSENTIAL	IMPORTANT	NOT IN SCOPE
6	DRINKING WATER	ESSENTIAL	IMPORTANT	NOT IN SCOPE
7	WASTE WATER	ESSENTIAL	IMPORTANT	NOT IN SCOPE

Annex I: Sectors of high criticality

DIGITAL INFRASTRUCTURE	LARGE ENTITIES (>= 250 employees or more than 50 million revenue)	MEDIUM ENTITIES (50-249 employees or more than 10million revenue)	SMALL & MICRO ENTITIES
Qualified trust service providers	ESSENTIAL	ESSENTIAL	ESSENTIAL
DNS service providers (excluding root name servers)	ESSENTIAL	ESSENTIAL	ESSENTIAL
TLD name registries	ESSENTIAL	ESSENTIAL	ESSENTIAL
Providers of public electronic communications networks	ESSENTIAL	ESSENTIAL	IMPORTANT
Non-qualified trust service providers	ESSENTIAL	IMPORTANT	IMPORTANT
Internet exchange point providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
Cloud computing service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
Data centre service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
Content delivery network providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE

Annex I: Sectors of high criticality		LARGE ENTITIES (>= 250 employees or more than 50 million revenue)	MEDIUM ENTITIES (50-249 employees or more than 10million revenue)	SMALL & MICRO ENTITIES
9	ICT-SERVICE MANAGEMENT (B2B)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
10	PUBLIC ADMINISTRATION ENTITIES	ESSENTIAL	ESSENTIAL	ESSENTIAL
		IMPORTANT	IMPORTANT	IMPORTANT
11	SPACE	ESSENTIAL	IMPORTANT	NOT IN SCOPE

Annex II: other critical sectors

		LARGE ENTITIES (>= 250 employees or more than 50 million revenue)	MEDIUM ENTITIES (50-249 employees or more than 10 million revenue)	SMALL & MICRO ENTITIES
1	POSTAL AND COURIER SERVICES	IMPORTANT	IMPORTANT	NOT IN SCOPE
2	WASTE MANAGEMENT	IMPORTANT	IMPORTANT	NOT IN SCOPE
3	CHEMICALS	IMPORTANT	IMPORTANT	NOT IN SCOPE
4	FOOD	IMPORTANT	IMPORTANT	NOT IN SCOPE
5	MANUFACTURING	IMPORTANT	IMPORTANT	NOT IN SCOPE

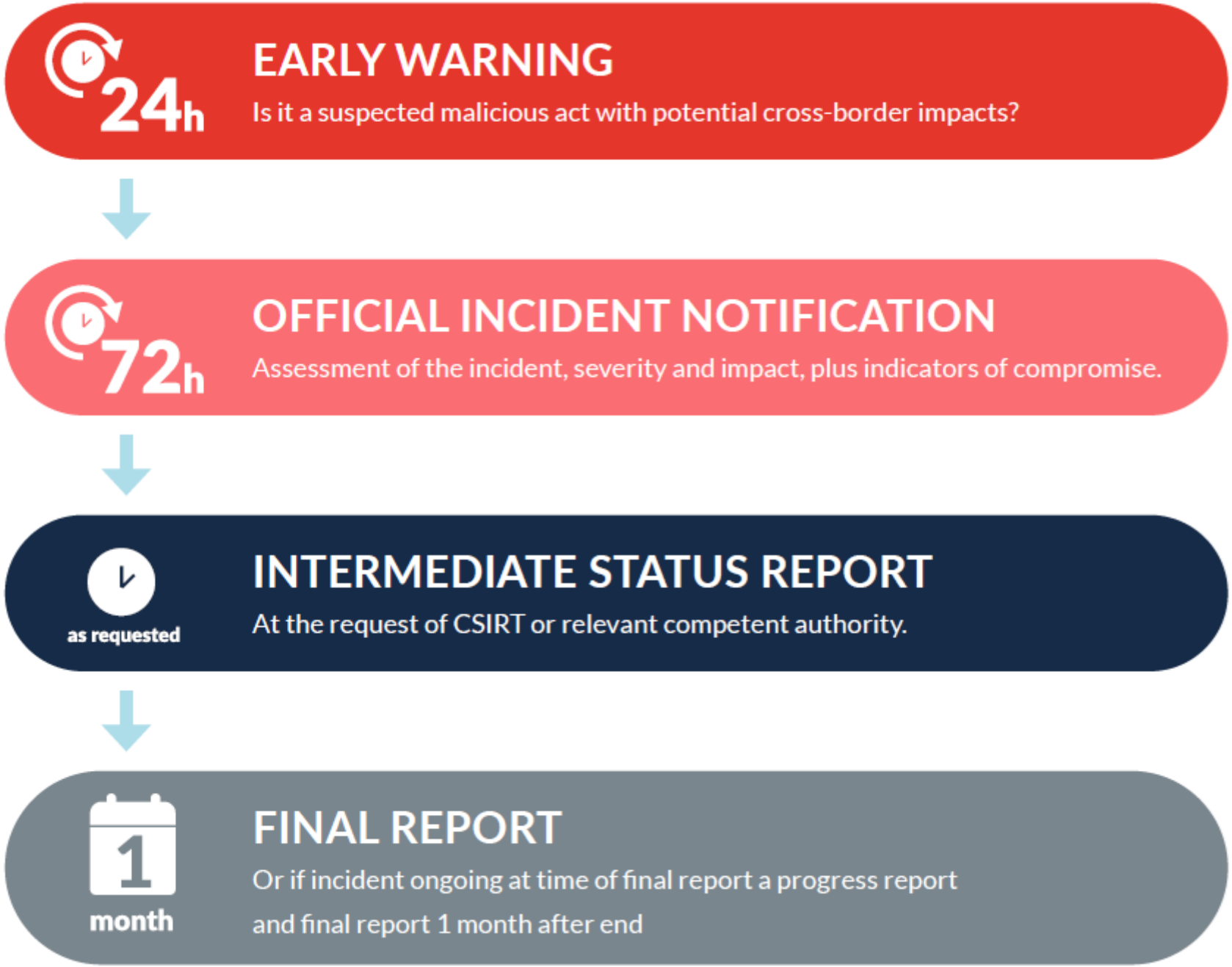
Annex II: other critical sectors		LARGE ENTITIES (>= 250 employees or more than 50 million revenue)	MEDIUM ENTITIES (50-249 employees or more than 10 million revenue)	SMALL & MICRO ENTITIES
6	DIGITAL PROVIDERS	IMPORTANT	IMPORTANT	NOT IN SCOPE
7	RESEARCH	IMPORTANT	IMPORTANT	NOT IN SCOPE
8	ENTITIES PROVIDING DOMAIN NAME REGISTRATION SERVICES	All sizes, but only subject to Article 3(3) and Article 28		

3

NIS-2 Incident notification

Incident Notification

- NIS2 imposes notification obligations in phases, for incidents which have a ‘significant impact’ on the provision of their services. These notifications must be made to the relevant competent authority or CSIRT (Computer Security Incident Response Team).
- Where appropriate, entities shall notify the recipients of their services of significant incidents.
- When in the public interest, the CSIRT or relevant competent authority may inform the public about the significant incident or may require the entity to do so.


24h
EARLY WARNING
Is it a suspected malicious act with potential cross-border impacts?
72h
OFFICIAL INCIDENT NOTIFICATION
Assessment of the incident, severity and impact, plus indicators of compromise.
as requested
INTERMEDIATE STATUS REPORT
At the request of CSIRT or relevant competent authority.
1
month
FINAL REPORT
Or if incident ongoing at time of final report a progress report
and final report 1 month after end

4

NIS-2 Cybersecurity Risk Management Measures

Cybersecurity Risk Management Measures

- Essential and Important entities must take appropriate and proportional technical, operational and organisational measures to manage the risks posed to the systems which underpin their services, and prevent or minimise the impact of incidents on their and other services.

- Such measures shall be based on an all-hazards approach that aims to protect the network and information systems and the physical environment of those systems from incidents.

NIS-2 mandatory security measures:

1. Risk analysis & information system security
2. Incident handling
3. Business continuity measures (back-ups, disaster recovery, crisis management)
4. Supply Chain Security
5. Security in system acquisition, development and maintenance, including vulnerability handling and disclosure
6. Policies and procedures to assess the effectiveness of cybersecurity risk management measures
7. Basic computer hygiene and trainings
8. Policies on appropriate use of cryptography and encryption
9. Human resources security, access control policies and asset management
10. Use of multi-factor, secured voice/video/text comm & secured emergency communication

Cybersecurity Risk Management Measures

All measures must be:

- Proportionate to risk, size, cost, and impact & severity of incidents
- Take into account the state-of-the-art, and where applicable relevant European and international standards

EU can:

- Carry out risk assessments of critical ICT services, systems or supply chains
- Impose certification obligations (delegated acts)
- Adopt implementing acts laying down technical requirements

5

Essential and Important Entities - Supervision

ESSENTIAL ENTITIES	IMPORTANT ENTITIES
✓ Ex Ante & Ex Post Supervision	✓ Ex Post Supervision
✓ On-site inspections and off-site supervision	✓ On-site inspections and off-site ex post supervision
✓ Regular & Targeted Security Audits	✓ Targeted Security Audits
✓ Security Scans	✓ Security Scans
✓ Information Requests	✓ Information Requests
✓ Requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned.	✓ Requests for information necessary to assess, ex post, the cybersecurity risk-management measures adopted by the entity concerned.
✓ Ad hoc audits, for example after a significant incident	✗

6

NIS-2 Enforcement and penalties

NIS2 provides national authorities with a minimum list of enforcement powers for non-compliance, including:

A	Issue **warnings** for non-compliance
B	Issue **binding instructions**
C	Order to **cease conduct** that is non-compliant
D	Order to **bring risk management measures** or reporting obligations in compliance to a specific manner and within a specified period
E	Order to **inform the natural or legal person(s)** to whom they provide services or activities which are potentially affected by a significant cyber threat
F	Order to **implement the recommendations** provided as a result of a security audit within a reasonable deadline
G	**Designate a monitoring officer** with well-defined tasks over a determined period of time to oversee the compliance
H	Order to **make public** aspects of non-compliance
I	Impose administrative **fines**
J	An essential entities **certification or authorisation concerning the service can be suspended**, if deadline for taking action is not met
K	And those responsible for discharging managerial responsibilities at chief executive officer or legal representative level can be temporarily **prohibited from exercising managerial functions** (applicable to essential entities only, not important entities).

Enforcement and penalties

NIS2 makes provision to impose administrative fines for infringements.

A maximum of **at least 10,000,000 EUR or up to 2% of the total worldwide annual turnover** of the undertaking to which the **ESSENTIAL ENTITY** belongs in the preceding financial year, whichever is higher.

A maximum of **at least 7,000,000 EUR or 1,4% of the total worldwide annual turnover** of the undertaking to which the **IMPORTANT ENTITY** belongs in the preceding financial year, whichever is higher.

7

NIS-2 Management Responsibilities

Management Responsibilities

Senior management have ultimate responsibility for cybersecurity risk management in essential and important entities. Failure by management to comply with NIS2 requirements could result in serious consequences, including liability, temporary bans and administrative fines as provided for in the implementing national legislation.

Management bodies of essential and important entities must:

Approve the adequacy of the cybersecurity risk management measures taken by the entity;

Supervise the implementation of the risk management measures;

Follow training in order to gain sufficient knowledge and skills to identify risks and assess cybersecurity risk management practices and their impact on the services provided by the entity

Offer similar training to their employees on a regular basis;

Be accountable for the non-compliance

Thanks for your participation

Questions and answers

1. What is the main difference between essential and important entities in NIS-2 Directive? (choose one answer)

☐ a. Important entities are large entities (in terms of size or revenue), whereas essential entities are medium-sized entities

☐ b. A disruption of services in an important entity would be expected to have serious consequences for the country's society as a whole

☐ c. A disruption of services in an essential entity would be expected to have serious consequences for the country's society as a whole

☐ d. There is no difference between essential and important entities

Correct answer: c

2. What is true about the Energy sector in NIS-2 Directive? (choose one answer)

☐ a. Energy sector is listed in Annex I (sectors of high criticality)

☐ b. Energy sector is listed in Annex II (other critical sectors)

☐ c. Energy sector is a new sector that wasn't in the scope of the NIS-1 Directive

☐ d. Energy sector is not in the scope of NIS-2 Directive

Correct answer: a

3. What is true about the Banking sector in NIS-2 Directive? (choose one answer)

☐ a. Banking sector is listed in Annex II (other critical sectors)

☐ b. Apart from NIS-2 Directive, the banking sector also complies with DORA Regulation (lex specialis)

☐ c. Banking sector is a new sector that wasn't in the scope of the NIS-1 Directive

☐ d. Banking sector is not in the scope of NIS-2 Directive

Correct answer: b

4. What is true about essential and important entities in Annex I and II of the NIS-2 Directive? (choose one answer)

☐ a. Essential entities are large entities of Annex I

☐ b. In Annex II, all medium entities are essential entities

☐ c. All entities of Annex I are important entities

☐ d. Essential and important entities are equally allocated in Annex I and II

Correct answer: a

5. In which sector and Annex of the NIS-2 Directive does a 5G provider of public electronic communications networks belong? (choose one anwser)

☐ a. In the ICT Service Management sector of Annex I

☐ b. In the Digital Providers sector of Annex II

☐ c. In the Digital Infrastructure sector of Annex I

☐ d. In the 5G sector of Annex I

Correct answer: c

6. A 5G provider of public electronic communications networks has become aware of a significant incident. What is he legally obliged to do? (choose one answer)

☐ a. The provider submits an early warning to the CSIRT or, where applicable, the competent authority, within 24 hours

☐ b. The provider waits for 3 days to see how the incident progresses and communicates with the CSIRT

☐ c. The provider isn't legally obliged to notify anyone

☐ d. The provider notifies ENISA within 72 hours

Correct answer: a

7. Which of the following is a mandatory security measure for entities in the scope of the NIS-2 Directive? (choose one answer)

☐ a. Use of multi-factor authentication

☐ b. Use of a next-generation firewall

☐ c. NIS-2 Directive lists a catalogue of non-binding technical guidelines, not mandatory security measures

☐ d. Use of CCTV cameras

Correct answer: a

8. Which is true about accountability for non-compliance with the NIS-2 Directive? (choose one answer)

☐ a. The CISOs of essential and important entities are accountable for the non-compliance

☐ b. The senior management of essential and important entities are accountable for the non-compliance

☐ c. There are no accountability issues regulated in the NIS-2 Directive

☐ d. Network administrators are responsible for approving the adequacy of the cybersecurity risk management measures taken by the entity

Correct answer: b

9. Which is true about the enforcement powers of NIS-2 Directive for national authorities? (choose one answer)

☐ a. National authorities can impose administrative fines

☐ b. National authorities can issue binding instructions

☐ c. National authorities can issue warnings for non-compliance

☐ d. All the above

Correct answer: d

10. Which is true about the supervision of essential and important entities in the scope of NIS-2 Directive? (choose one answer)

☐ a. There is only ex-post supervision for important entities

☐ b. There is only ex-ante supervision for essential entities

☐ c. On-site inspection isn't referred to in NIS-2 Directive

☐ d. Ad hoc audits can be conducted in important entities after a significant incident

Correct answer: a