Paloma LLaneza

NIS2 and eIDAS2: How to audit Trust Services in 2025

certeidas

CA Day - Berlin 27/10/2022

NIS2 Directive

eIDAS2 Regulation

- **Moving target**
- **References to NIS2**

certeidas

Press release | 13 May 2022 | Brussels

Commission welcomes political agreement on new rules on cybersecurity of network and information systems

Page contents

The Commission welcomes the political agreement reached today between the European Parliament and EU Member States on the **Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)** proposed by the Commission in December 2020.

The existing rules on the security of network and information systems (NIS Directive), have been the first piece of EU-wide legislation on cybersecurity and paved the way for a significant change in mind-set, institutional and regulatory approach to cybersecurity in many Member States. In spite of their notable achievements and positive impact, they had to be updated because of the increasing degree of digitalisation and

eIDAS2 security requirements

certeidas

eIDAS2 cybersecurity requirements

Standardization

Article 13, paragraph 1 is replaced by the following:

‘1. Notwithstanding paragraph 2 of this Article, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure **to comply with the obligations under this Regulation and with the cybersecurity risk management obligations under Article 18 of the Directive XXXX/XXXX [NIS2].**’

certeidas

eIDAS2 cybersecurity requirements

Standardization

Article 24, paragraph 2 (fa) is amended as follows:

‘(fa) have **appropriate policies and take corresponding measures** to manage legal**, business, operational** and other **direct or indirect risks** to the provision of the **qualified trust service**. **Notwithstanding the provisions of Article 18 of Directive EU XXXX/XXX [NIS2]**, those **measures shall include at least** the following:

i. **measures related to registration and on-boarding procedures** to a service;

ii. measures related to **procedural or administrative checks**;

iii. measures related to the **management and implementation of serv**

certeidas

eIDAS2 cybersecurity requirements

Conformity Assessment

Article 20 paragraph 1 is replaced by the following

1. **Qualified trust service providers** shall be audited at their own expense at least **every 24 months** by a conformity assessment body. The audit shall confirm that the qualified trust service providers and the qualified trust services provided by them **fulfil the requirements laid down in this Regulation and in Article 18 of Directive (EU) XXXX/XXXX [NIS2]**. Qualified trust service providers shall submit the resulting conformity assessment report to the **supervisory body within three working days of receipt**.';

certeidas

eIDAS2 cybersecurity requirements

Supervision

Article 21, paragraph 2 is replaced by the following:

2. The **supervisory body shall verify** whether the trust service provider and the trust services provided by **it comply with the requirements laid down in this Regulation**, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide.

In order to **verify the compliance of the trust service provider with the requirements laid down in Article 18 of Dir XXXX [NIS2]**, the **supervisory body** shall **request the competent authorities** referred to in **Dir XXXX [NIS2] to carry out supervisory actions** in that regard and to **provide information about the outcome within three days from their completion**.

certeidas

NIS2: Provisions related to TSPs

NIS2: Provisions related to TSPs

Scope

(9b) Some entities perform activities in the field of national security, defence or law enforcement while also providing trust services. **Trust services which are included in the scope of the Regulation (EU) No 910/2014 ("eIDAS Regulation") should be included in the scope of this Directive** in order to **secure the same level of security requirements and supervision as that previously laid out by the eIDAS Regulation**.

In line with the exclusion of certain specific services from the eIDAS Regulation, **this Directive should not apply to the provision of trust services that are used exclusively within closed systems resulting from national law** or **from agreements between a defined set of participants**.

certeidas

NIS2: Provisions related to TSPs

Scope

Article 2 Scope

2. Regardless of their size, this Directive also applies to essential and important entities, where:

(a) the services are provided by:

(ii) **trust service providers referred to point 8 of Annex I;**

certeidas

NIS2: Provisions related to TSPs

Scope

Article 2a Essential and important entities

1. For the purposes of this Directive, **essential entities shall be considered all entities of the type listed in Annex I** which exceed the ceilings for medium-sized enterprises **as well as the following entities**:

(a) **qualified trust service providers** and top-level domain name registries as well as DNS service providers regardless of their size;

certeidas

NIS2: Provisions related to TSPs

Scope

ANNEX I **SECTORS OF HIGH CRITICALITY**

Sector: **Digital infrastructure**

Type of entity: Trust service providers referred to in point (19) of Article 3 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p.73).

certeidas

NIS2: Provisions related to TSPs

Security measures

(48a) The **security obligations** laid down in this Directive should be considered **complementary** to the requirements imposed on trust service providers under Regulation (EU) No 910/2014 (**eIDAS Regulation**). **Trust-service providers** should be requested to take all **appropriate and proportionate measures to manage the risks posed to their services**, including in relation **to customers and relying third parties**, and to **report security incidents under this Directive**. Such security and **reporting obligations should also concern the physical protection of the service provided. Article 24 of Regulation (EU) 910/2014 continues to apply**.

certeidas

NIS2: Provisions related to TSPs

Security measures

Article 18 Cybersecurity risk management measures

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational **measures to manage the risks posed to the security of network and information systems** which those entities use for their operations or for the provision of their services, and to **prevent or minimise the impact of incidents** on recipients of their services and on other services.

Having regard to the state of the art and, where applicable, relevant European and international standards, as well as the cost of implementation, those measures shall ensure a level of security of network and information systems appropriate to the risk presented. **When assessing** the proportionality of those measures, due account shall be taken of

- the degree of the entity's exposure to risks,
- its size,
- the likelihood of occurrence of incidents and their severity,
- including their societal and economic impact.

certeidas

NIS2: Provisions related to TSPs

Security measures

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach aiming to protect network and information systems and their physical environment from incidents, and shall include at least the following:

(a) **risk analysis and information system security policies**;

(b) **incident handling** ;

(c**) business continuity**, such as backup management and disaster recovery, and crisis management;

(d) **supply chain** security including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers ;

(e) **security in network and information systems** acquisition, development an maintenance, including vulnerability handling and disclosure;

certeidas

NIS2: Provisions related to TSPs

Security measures

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach aiming to protect network and information systems and their physical environment from incidents, and shall include at least the following:

(f) policies and procedures to assess the effectiveness of cybersecurity risk management measures;

- (fa) basic computer hygiene practices and cybersecurity training;

(g) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

- (ga) human resources security, access control policies and asset management;
- (gb) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communications syste within the entity, where appropriate.

certeidas

NIS2: Provisions related to TSPs

Supervision

(48b) Member States **may assign the role of competent authorities for trust services to the eIDAS supervisory bodies** in order to ensure the **continuation of current practices** and to build on the knowledge and experience gained in the application of the eIDAS Regulation.

Where that **role is assigned to a different body,** the **national competent authorities** under this Directive should cooperate closely, in a timely manner, by exchanging the relevant information in order to ensure effective supervision and compliance of trust service providers with the requirements set out in this Directive and Regulation [XXXX/XXXX].

Where applicable, **the CSIRT or national competent authority** under this Directive **should immediately inform the eIDAS supervisory body about any notified significant cyber threat or incident with impact on trust services** as well as about **any non-compliance of a trust service provider with the requirements under this Directive.**

certeidas

NIS2 and ETSI EN 319401 control mapping

certeidas

Domain	Sub-domains	NIS2 Directive	ETSI EN 319 401	ISO/IEC 27002:2013 references in ETSI EN 319 401	ISO/IEC 27002:2022
Risk analysis		18.2. a) risk analysis	5 Risk Assessment		
information system security policies		18.2. a) information system security policies	6.3 Information security policy	Clause 5.1.1	5.1 Policies for information security
ISMS policies and procedures		18.2. f) policies and procedures to assess the effectiveness of cybersecurity risk management measures	Controls and policies included in section 7. Need to link section 6 with the controls and procedures of section 7.		
Internal organization	Organization reliability		7.1.1 Organization reliability		5.2 Information security roles and responsibilities
	Segregation of duties		7.1.2 Segregation of duties		5.3 Segregation of duties
Human resources	General	18.2 (ga) human resources security, access control policies and asset management;	7.2 Human resources	Clauses 6.1.1, 6.1.2 Clauses 7, 7.2.1, 7.2.3	5.4 Management responsibilities; 6.1 Screening 6.2 Terms and conditions of employment 6.3 Information security awareness, education and training 6.4 Disciplinary process 6.5 Responsibilities after termination or change of employment 6.6 Confidentiality or non-disclosure agreements 6.7 Remote working

Domain	Sub-domains	NIS2 Directive	ETSI EN 319 401	ISO/IEC 27002:2013 references in ETSI EN 319 401	ISO/IEC 27002:2022
	Training and awareness	18.2. (fa) basic computer hygiene practices and cybersecurity training	REQ-7.2-02, REQ-7.2-03, REQ-7.2-04, REQ-7.2-13		6.3 Information security awareness, education and training
Asset management	General requirements	18.2. (e) security in information systems acquisition, development and maintenance, including vulnerability handling and disclosure; 18.2 (ga) …asset management;	7.3.1 General requirements	Clauses 8, 8.1.1,	5.9 Inventory of information and other associated assets 5.10 Acceptable use of information and other associated assets 5.11 Return of assets
	Media handling		7.3.2 Media handling	Clause 8.3	7.10 Storage media
Vulnerability management		18.2. (e) security in information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	Included but not as a specific topic		5.8 Information security in project management 8.26 Application security requirements 8.7 Protection against malware 8.8 Management of technical vulnerabilities 8.9 Configuration management 8.15 Logging 8.16 Monitoring activities 8.17 Clock synchronization 8.18 Use of privileged utility programs 8.19 Installation of software on operational systems

Domain	Sub-domains	NIS2 Directive	ETSI EN 319 401	ISO/IEC 27002:2013 references in ETSI EN 319 401	ISO/IEC 27002:2022
	Training and awareness	18.2. (fa) basic computer hygiene practices and cybersecurity training	REQ-7.2-02, REQ-7.2-03, REQ-7.2-04, REQ-7.2-13		6.3 Information security awareness, education and training
Asset management	General requirements	18.2. (e) security in information systems acquisition, development and maintenance, including vulnerability handling and disclosure; 18.2 (ga) …asset management;	7.3.1 General requirements	Clauses 8, 8.1.1,	5.9 Inventory of information and other associated assets 5.10 Acceptable use of information and other associated assets 5.11 Return of assets
	Media handling		7.3.2 Media handling	Clause 8.3	7.10 Storage media
Vulnerability management		18.2. (e) security in information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	Included but not as a specific topic		5.8 Information security in project management 8.26 Application security requirements 8.7 Protection against malware 8.8 Management of technical vulnerabilities 8.9 Configuration management 8.15 Logging 8.16 Monitoring activities 8.17 Clock synchronization 8.18 Use of privileged utility programs 8.19 Installation of software on operational systems

Domain	Sub-domains	NIS2 Directive	ETSI EN 319 401	ISO/IEC 27002:2013 references in ETSI EN 319 401	ISO/IEC 27002:2022
Access control		18.2 (ga) …. access control policies...; 18.2. (gb) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communications systems within the entity, where appropriate.	7.4 Access control	Clause 9	5.15 Access control 5.16 Identity management 5.17 Authentication information 5.18 Access rights Access rights 8.2 Privileged access rights
	System and application access control		Included but not as a specific topic		5.17 Authentication information 8.3 Information access restriction 8.4 Access to source code 8.5 Secure authentication 8.18 Use of privileged utility programs
Cryptographic controls		18.2. (g) policies and procedures regarding the use of cryptography and, where appropriate, encryption;	7.5 Cryptographic controls	Clause 10	8.24 Use of cryptography

Domain	Sub-domains	NIS2 Directive	ETSI EN 319 401	ISO/IEC 27002:2013 references in ETSI EN 319 401	ISO/IEC 27002:2022
Physical and environmental security		Not included. See18.2. f)	7.6 Physical and environmental security	Clauses 11, 11.1	7.1 Physical security perimeters 7.2 Physical entry 7.3 Securing offices, rooms and facilities 7.4 New Physical security monitoring 7.5 Protecting against physical and environmental threats 7.6 Working in secure areas 7.7 Clear desk and clear screen 7.8 Equipment siting and protection 7.9 Security of assets off-premises 8.1 User endpoint devices
Supply chain		18.2. (d) supply chain security including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers ;	Not included		5.19 Information security in supplier relationships 5.20 Addressing information security within supplier agreements 5.21 Managing information security in the ICT supply chain 5.22 Monitoring, review and change management of supplier services 5.23 Information security for use of cloud services
Operation security			7.7 Operation security	Clauses 12, 14, 15	5.37 Documented operating procedures 8.6 Capacity management 8.31 Separation of development, test and production environments 8.32 Change management

certeidas

Domain	Sub-domains	NIS2 Directive	ETSI EN 319 401	ISO/IEC 27002:2013 references in ETSI EN 319 401	ISO/IEC 27002:2022
Network security		18.2. (e) security in network	7.8 Network security		8.20 Networks security 8.21 Security of network services 8.22 Segregation of networks 8.23 Web filtering
Incident management		18.2. (b) incident handling	7.9 Incident management	Clause 16	5.24 Information security incident management planning and preparation 5.25 Assessment and decision on information security events 5.26 Response to information security incidents 5.27 Learning from information security incidents 5.28 Collection of evidence 6.8 Information security event reporting
	Reporting	Under NIS2 (CERT) and eIDAS regulation Recital 48a NIS Article 24 eIDAS Regulation	Included but not as a specific topic		
Collection of evidence			7.10 Collection of evidence		5.28 Collection of evidence
Business continuity management		18.2. (c) business continuity, such as backup management and disaster recovery, and crisis management;	7.11 Business continuity management	Clause 17	8.13 Information backup 5.29 Information security during disruption 5.29 Information security during disruption 5.30 ICT readiness for business

Domain	Sub-domains	NIS2 Directive	ETSI EN 319 401	ISO/IEC 27002:2013 references in ETSI EN 319 401	ISO/IEC 27002:2022
					continuity
Compliance			7.13 Compliance		5.31 Legislation, regulations and statutory and contractual requirements 5.32 Intellectual property rights 5.33 Protection of records 5.34 Privacy and protection of PII 5.35 Independent review of information security

Conclusions

certeidas

Conclusions

- On the standardisation side, European eIDAS standards + national NIS2 development standards with a risk perspective on connectivity (information security + cybersecurity).
- On the conformity assessment side, two partially overlapping scopes if no European standardisation is achieved that homogenises the applicable information security and cybersecurity requirements.
- Unless the recommendation of recital 48b of the NIS2 Directive is followed, double supervision and, at least, double incident reporting (not counting reporting under the GDPR).

certeidas

Paloma Llaneza
pllaneza@certicar.es

Thanks!

certeidas