

EVIDEN

EVIDEN
MINDSHARE
2024

NIS2 Directive Compliant Cryptography

View of the Client's Advisor and auditor

Slawomir Pijanowski, Ph.D, Eviden

EVIDEN



Legal notice:

This publication, called further „Presentation” represents the views and interpretations of EVIDEN unless stated otherwise.

EVIDEN has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only.

All references to it or its use as a whole or partially must contain EVIDEN as its source. Third-party sources are quoted as appropriate. EVIDEN is not responsible or liable for the content of the external sources including external websites referenced in this publication.

While care has been taken in gathering the data and preparing the Presentation EVIDEN does not make any representations or warranties on behalf of themselves or others as to its accuracy or completeness and expressly exclude to the maximum extent permitted by law all those that might otherwise be implied.

Neither EVIDEN nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. Eviden accepts no responsibility or liability for any loss or damage of any nature occasioned to any person as a result of acting or refraining from acting because of, or in reliance on, any statement, fact, figure or expression of opinion or belief contained in this Presentation. This Presentation does not constitute advice or promise of any kind.

Status of information contained in this Presentation, in particular on NIS2 Directive EU Member States transposition as of 30th August 2024.

EVIDEN maintains its intellectual property rights in relation to this publication.



Contents for NIS2 Compliant Cryptography

View of the Client's Advisor and auditor

- Introduction to NIS2 and its misinterpretations
- If encryption is hardly unbreakable, why do organizations are still being hacked? Not saying about future post-quantum judgment day on the way... Role of encryption in security incidents.
- Understanding and monitoring broader context of cryptographic technical controls within ISMS (Information Security Management System) controls
- Exemplary potential scenarios of regulatory auditing use of cryptography. What could be checked, how to prepare? Ex ante and ex post NIS2 supervisory audit and enforcement measures. What evidence is critical for early warning, forensic for regulator regardless incident happens or not?
- Illusion of control compliance tick-boxing - to be compliant or to be secure does not always means the same.
Business risk originating from cryptography or encryption.
- Cryptographic, encryption control / safeguard risk vs the risk of insufficient cryptography



Customers tell us ...

- They are not aware if or to what extent they are in scope of NIS-2 / DORA / CER regulations.
- They do not know if there is right moment to do preparation work to assure compliance
- They are afraid of reporting cyber incidents to external competent authority if published, they might impact business, credibility and reputation
- They do not know how to impose on their suppliers - the compliance obligations resulting from NIS-2 / DORA / CER and how to effectively monitor them
- They do not know what should be the “reasonable” level if compliance cost or investments to be done to assure minimum but sufficient compliance needs
- They do not know how to connect cyber risk analysis, business continuity, supply chain managed into consistent framework to justify risk-based spending on compliance (“this is justified amount for which I am able to comply”).
- They are afraid how to collect evidence, how to perform documented, reasonable, balanced risk assessment to prove that implemented countermeasures are adequately, proportionally addressing the cyber resilience risks

Cyber Resilience Compliance needs proportional efforts to identified risks



New regulations are being published by EU (NIS-2/DORA/CER, ECA, CRA/AI Act, etc. – it is very easy to get lost



AI-powered compliance tools can leverage optimization of continuous compliance evidence



Connected infrastructures, supply chains and related cyber attacks might come from various sides – it is not easy to control them

NIS-2 Directive – Objective and scope - 160000 organisations in EU

Harmonise cybersecurity & resilience by coordinated regulatory framework & measures across EU



Obligations of EU Member States

- Adoption of national cybersecurity strategy
- Establish at least one competent authority responsible for cybersecurity and for the supervisory tasks
- Establish National cyber crisis management frameworks for large scale cyber incidents or crises
- Establish EU-CyCLONe – Crisis Management
- Establish Computer security incident response teams (CSIRTs) network
- Coordinated vulnerability disclosure and a European vulnerability register



Obligations for enterprises and extension of sectors

Risk management measures

- Risk analysis, InfoSec Policies
- Incident handling
- Business Continuity, Back-up, Disaster Recovery, Crisis Management
- Supply chain security
- Information Systems & Network Security,
- Security Controls' Effectiveness Assessment
- Cyber hygiene & awareness training
- Cryptography & encryption
- Asset management, HR security, Access control
- Multi-Factor or Continuous Authentication
- Secured voice, video, text communications,
- Emergency communication systems



Effective Cooperation & information sharing

- EU MS to designate a single point of contact responsible for coordinating issues on security of network & information systems, cross-border cooperation at EU level.
- At national level, the single points of contact should enable smooth cross-sectoral cooperation with other competent authorities
- Voluntary notification submitted to CSIRTs / competent authorities – on significant incidents, cyber threats and near misses

Source: Eviden SAS

- Provide effective remedies and enforcement measures for cyber resilience
- Eliminate fragmentation of the internal market affecting the cross-border provision of services and the level of cyber resilience

NIS2 Directive – Initial scope - before country transposition

Industry scope

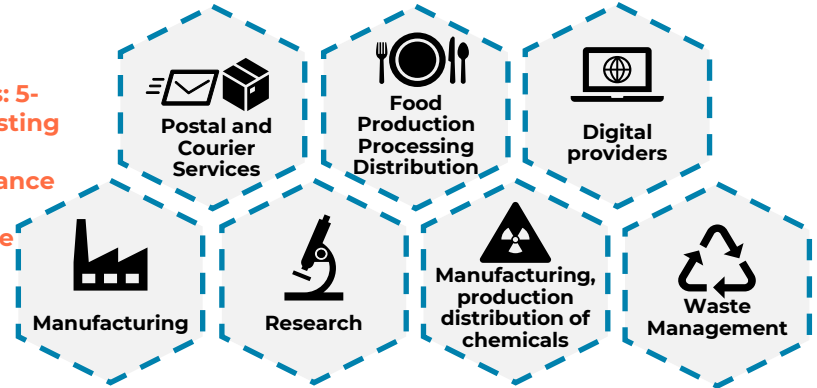
NIS 2 - 11 Essential Entities' sectors

NIS 1 – Operators of Essential Services' 7 sectors



7 Important Entities' sectors

NIS-1 entities: 5-15% existing ICT compliance budget increase



Organizations new in NIS-2: 15-30% existing ICT compliance budget increase

17th of Oct 2024

Members States (MS) translate (transpose) NIS-2 into 27 country laws

17th of April 2025

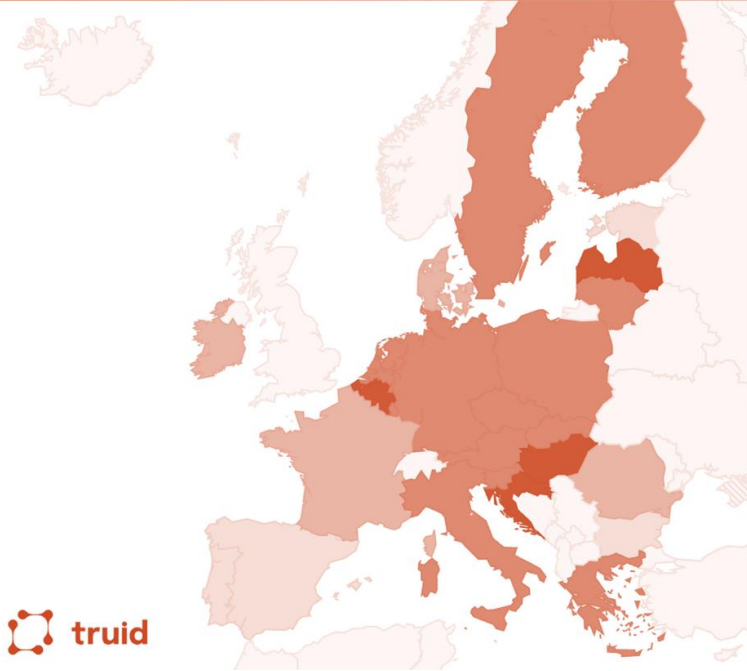
MS publish list of Essential & Important Entitie

--- New group of Important Entities in NIS-2 Directive

Source: Eviden SAS

NIS 2 Directive – current progress of transpositions to EU-countries' laws

Status of NIS 2 Directive Transposition



**Only Hungary, Belgium, Croatia, Latvia
4 of 27 Member Stated transposed
NIS2 into their national law**

- Stage 4**
Transposition of NIS 2 directive into national law
- Stage 3**
Draft has been submitted, waiting for feedback or approval
- Stage 2**
Initial stages of development announced and some progress made
- Stage 1**
Limited information available or minimal progress made

Source: <https://www.truid.app/blog/the-nis2-directive-in-eu-a-country-by-country-breakdown>

NIS-2 Directive – Potential business Impact – penalties for non compliance

Penalties for non-compliance with NIS-2

Essential Entities

10 mln EUR
or at least
2%
of global turnover *

* whichever is greater

Important Entities

7 mln EUR
or at least
1.4%
of global turnover *

* whichever is greater

Regulatory Penalties – are subject
of adoption by Member States
to local law

Eviden's Cyber Services & Products can fully cover NIS-2 compliance gap

Source: Eviden SAS

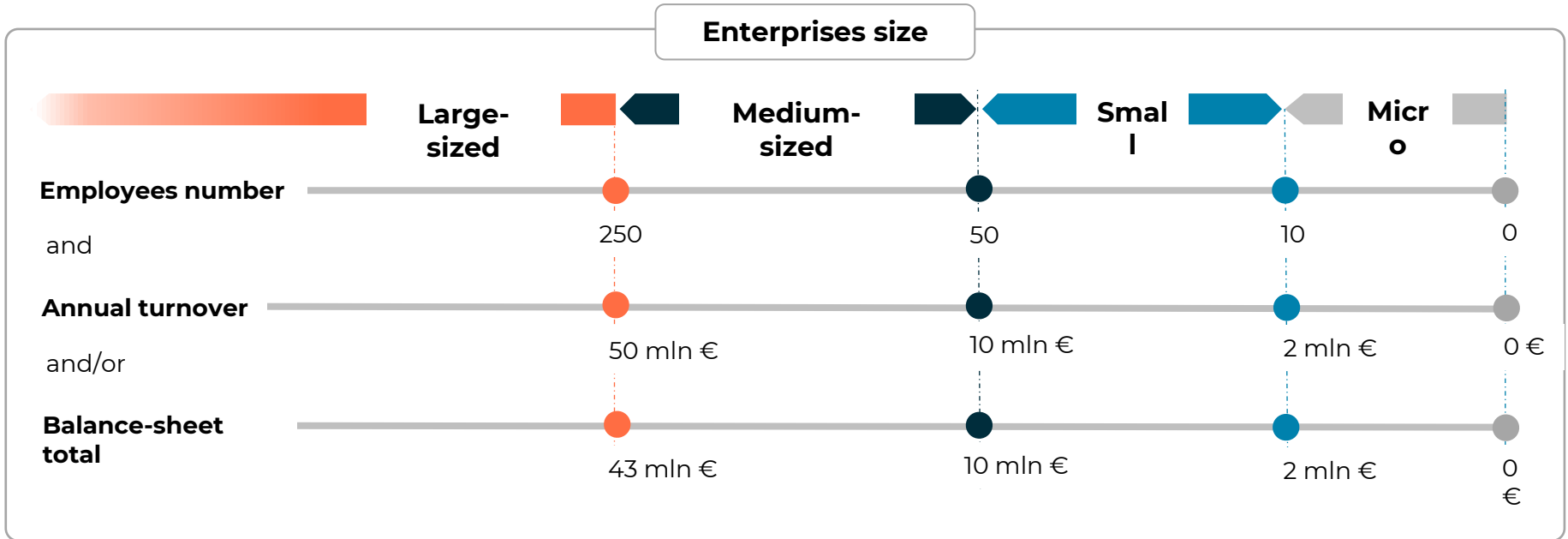
NIS-2 Directive – How compliance will be checked by Regulator

Competent authorities supervisory activities

	Essential Entities (EE)	Important Entities (IE)	
<p>Essential Entities are subject to an ex-ante and ex-post approach to supervision (i.e. before the incident happens, i.,e. any time)</p> <p>Important Entities – ex-post</p> <p>supervisory authorities will only conduct investigations into these entities if there is evidence or information that they have infringed their NIS 2 obligations (art 21 or 23 in particular)</p>	a) on-site inspections and off-site supervision, including random checks conducted by trained professionals*	a) on-site inspections and off-site ex post supervision conducted by trained professionals;	<p>* on-site inspections and off-site supervision, including the identification of weaknesses in databases, hardware, firewalls, encryption and networks. Those inspections and that supervision should be conducted in an objective manner.</p> <p>** b) shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related information</p>
	b) regular and targeted security audits carried out by an independent body or a competent authority**	b) [non-regular] targeted security audits carried out by an independent body or a competent authority	
	c) ad hoc audits, including where justified on the ground of a significant incident or an infringement of this Directive by the essential entity	Not applicable for IE	
	d) For EE security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned, For IE the same provision but indicated as c)	d) requests for information necessary to assess, ex post , ...(then the same as for IE, but indicated as d)	
	e) requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Art 27	e) the same as for IE, but indicated as e)	
f) requests to access data, documents and information necessary to carry out their supervisory tasks	f) the same as for IE, but indicated as f)		
g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.			

Source: Eviden SAS

Organisation size thresholds in NIS2











Source: Eviden SAS own elaboration Art. 2 of NIS 2 and Recommendation 2003/361/EC, art 2 defines companies large and medium

NIS2 Critical Sectors and subsectors (Annex I) mapping to Essential/Important Entities size (1)

SECTORS – ANNEX I	SUBSECTOR	LARGE ENTERPRISES	MEDIUM ENTERPRISES	SMALL & MICRO ENTERPRISES
Energy	Electricity, District heating and cooling, Oil, Gas and Hydrogen			
	Transport			
	Banking			
Financial market infrastructures	Operators of trading venues, Central counterparties			
Health	Healthcare providers, EU reference laboratories, entities carrying out research and development activities of medicinal products, entities manufacturing basic pharmaceutical products and pharmaceutical preparations and entities manufacturing medical devices considered to be critical during a public health emergency	Essential Entities	Important Entities	Not in scope
Drinking water	Suppliers and distributors of water intended for human consumption			
Digital infrastructure	Internet Exchange Point providers			
	DNS service providers, excluding operators of root name servers			
	TLD name registries			
	Cloud computing service providers			
	Data center service providers			Not in scope
	Content delivery network providers			
	Trust service providers			
Providers of public electronic communications networks				
Providers of publicly available electronic communications services				Not in scope

Source: Eviden SAS own elaboration Art. 2 of NIS 2 and Recommendation 2003/361/EC, art 2 defines companies large and medium

NIS2 Critical Sectors and subsectors (Annex I) mapping to Essential/ Important Entities size (2)

SECTORS – ANNEX I	SUBSECTOR	LARGE ENTERPRISES	MEDIUM ENTERPRISES	SMALL & MICRO ENTERPRISES
Waste water	Undertakings collecting, disposing of or treating urban waste-water, domestic waste-water or industrial waste-water			Not in scope
	Managed service providers and managed security service providers			
Public administration	Public administration entities of central governments			
	Public administration entities at regional level			
Space	Operators of ground-based infrastructure			Not in scope



Source: Eviden SAS own elaboration Art. 2 of NIS 2 and Recommendation 2003/361/EC, art 2 defines companies large and medium

There are also other specific criteria for determination applicability scope. See art. 26 of NIS2.

Final allocation of critical or important sectors as well as essential or important entity criteria are subject of member states transpositions, f.e.:

Poland (Draft version of NIS2) – Manufacturing, Chemicals, Food were moved from other critical sectors (Annex II) to Annex I, and consequently from Important Entity to Essential Entities.

NIS2 Other Critical Sectors and subsectors (Annex II) mapping to Important Entities size

SECTORS – ANNEX II	SUBSECTOR	LARGE ENTERPRISES	MEDIUM ENTERPRISES	SMALL & MICRO ENTERPRISES
Postal and courier services	Postal service providers	 Important Entities	 Important Entities	Not in scope
Waste management	Waste management companies			
Manufacture, production and distribution of chemicals	Companies involved in the manufacture of substances and the manufacture and distribution of substances or mixtures			
Production, processing and distribution of food	Wholesale distribution and industrial production and processing companies			
Manufacturing	Manufacture of medical devices and in vitro diagnostic medical devices			
	Manufacture of computer, electronic and optical products			
	Manufacture of electrical equipment			
	Manufacture of machinery and equipment n.e.c.			
	Manufacture of motor vehicles, trailers and semi-trailers			
Digital providers	Manufacture of other transport equipment			
	Providers of online marketplaces ; online search engines and social networking services platforms			
Research	Research organisations			

Source: Eviden SAS own elaboration Art. 2 of NIS 2 and Recommendation 2003/361/EC, art 2 defines companies large and medium

NIS2 Objective or Scope Misinterpretation

Frequently Addressed Questions

1. If I am ISO 27001 or ISO 22301 certified does that mean I am compliant with NIS2?
2. Is your organisation / company already NIS2 certified?
3. Do I need to be ISO 27001 or 22301 certified to be NIS2 Compliant?
4. If I am already in NIS1 scope, does that mean I automatically certified?
5. Vendors – is my product NIS2 certified or should it be „NIS2 certified“?
6. Customers – is your product „NIS2 certified“?

NIS2 and products:
Essential entities must use some certified products by ECA ENISA
Details in European Cybersecurity Act and Product, Cloud, 5G Certifications Schemes

NIS2 addresses the process of security Secure Development Lifecycle which will be also partially regulated via **Cyber Resilience Act**

Source: Eviden SAS



ENISA Products and CRA Products

NIS2 on using certified products by essential or important entities

Article 24 Use of European cybersecurity certification schemes

1. In order to demonstrate compliance with particular requirements of Article 21, Member States may require essential and important entities to use particular ICT products, ICT services and ICT processes, developed by
- the essential or important entity (here Digital Infrastructure Sector under NIS2) or
 - **procured from third parties, that are certified under European cybersecurity certification schemes** adopted pursuant to Article 49 of Regulation (EU) 2019/881 (European Cybersecurity Act).
 - Furthermore, Member States shall encourage essential and important entities to use qualified trust services.



Network & Information System Directive 2 & DORA

Manufacturers of ICT Products, ICT Services indicated as critical sector in NIS2

NIS2 Group 8. Digital Infrastructure	Internet Exchange Point providers
	DNS service providers, excluding operators of root name servers
	TLD name registries
	Cloud computing service providers
	Data centre service providers (collocation services)
	Content delivery network providers
	Trust service providers (in Article 3, point (19), of Regulation (EU) No 910/2014) e-IDAS – electronic signatures, seals, time stamps, etc.
	Providers of public electronic communications networks
Providers of publicly available electronic communications services	
NIS2 Group 9. ICT service management (business-to-business)	Managed service providers
	Managed security service providers
DORA Regulation	ICT Third Party Service Provider SSC, BPO of Financial Institutions being in scope of DORA – if they are part of essential service

Art 6. 10. RMF: DORA Financial entities may,

in accordance with Union and national sectoral law,

outsource the tasks of verifying compliance with ICT risk management requirements to intra-group or external undertakings.

In case of such outsourcing, the financial entity remains fully responsible for the verification of compliance with the ICT risk management requirements.

Source: Eviden SAS

Products in scope of Cyber Resilience Act

ANNEX III CRITICAL PRODUCTS WITH DIGITAL ELEMENTS

Class I

1. Identity management systems software and privileged access management software;
2. Standalone and embedded browsers;
3. Password managers;
4. Software that searches for, removes, or quarantines malicious software;
5. Products with digital elements with the function of virtual private network (VPN);
6. Network management systems;
7. Network configuration management tools;
8. Network traffic monitoring systems;
9. Management of network resources;
10. Security information and event management (SIEM) systems;
11. Update/patch management, including boot managers;
12. Application configuration management systems;
13. Remote access/sharing software;
14. Mobile device management software;
15. Physical network interfaces;
16. Operating systems not covered by class II;
17. Firewalls, intrusion detection and/or prevention systems not covered by class II;
18. Routers, modems intended for the connection to the internet, and switches, not covered by class II;
19. Microprocessors not covered by class II;
20. Microcontrollers;
21. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];
22. Industrial Automation & Control Systems (IACS) not covered by class II, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);
23. Industrial Internet of Things not covered by class II.

Class II

1. Operating systems for servers, desktops, and mobile devices;
2. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments;
3. Public key infrastructure and digital certificate issuers;
4. Firewalls, intrusion detection and/or prevention systems intended for industrial use;
5. General purpose microprocessors;
6. Microprocessors intended for integration in programmable logic controllers and secure elements;
7. Routers, modems intended for the connection to the internet, and switches, intended for industrial use;
8. Secure elements;
9. Hardware Security Modules (HSMs);
10. Secure cryptoprocessors;
11. Smartcards, smartcard readers and tokens;
12. Industrial Automation & Control Systems (IACS) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)], such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);
13. Industrial Internet of Things devices intended for the use by essential entities of the type referred to in [Annex I to the Directive (NIS2)];
14. Robot sensing and actuator components and robot controllers;
15. Smart meters.

Source: [Cyber Resilience Act Annex III](#)



A	<ul style="list-style-type: none">• Policies on risk analysis,• Policies on information system security
B	<ul style="list-style-type: none">• Incident & Crisis Management
C	<ul style="list-style-type: none">• Crisis management• Business continuity, backup mgt• Disaster recovery
D	<ul style="list-style-type: none">• Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
E	<ul style="list-style-type: none">• ICT Security (IS & Network Security),• S-SDLC / DevSecOps,• Coordinated Vulnerability Disclosure
F	<ul style="list-style-type: none">• Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
G	<ul style="list-style-type: none">• Cybersecurity training
H	<ul style="list-style-type: none">• Policies and procedures regarding the use of cryptography and, where appropriate, encryption
I	<ul style="list-style-type: none">• Human resources security (HR)• Access control policies (ACP)• Asset management (AM)
J	<ul style="list-style-type: none">• The use of multi-factor authentication or continuous authentication solutions,• Secured voice, video and text communications• Secured emergency communication systems within the entity

NIS2 Directive Art. 21 Risk Management Measures



Governance IS & Network Security & Resilience Policies People	A	<ul style="list-style-type: none"> • Policies on risk analysis, • Policies on information system security
	F	<ul style="list-style-type: none"> • Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
	H	<ul style="list-style-type: none"> • Policies and procedures regarding the use of cryptography and, where appropriate, encryption
Incident & Crisis Management	G	<ul style="list-style-type: none"> • Cybersecurity training & Cyber Hygiene
Business Continuity	B	<ul style="list-style-type: none"> • Incident & Crisis Management
	C	<ul style="list-style-type: none"> • Crisis management • Business continuity, backup mgt • Disaster recovery
Supply chain	D	<ul style="list-style-type: none"> • Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
ICT Life cycle Security,	E	<ul style="list-style-type: none"> • ICT Security (IS & Network Security), • S-SDLC / DevSecOps, • Coordinated Vulnerability Disclosure
People	I	<ul style="list-style-type: none"> • Human resources security (HR) • Access control policies (ACP) • Asset management (AM)
Asset Management IAM & Secure Digital Workplace	J	<ul style="list-style-type: none"> • The use of multi-factor authentication or continuous authentication solutions, • Secured voice, video and text communications • Secured emergency communication systems within the entity

NIS2 Directive Art. 21 Risk Management Measures

Eviden Grouping

Source: Eviden SAS



Eviden's approach to NIS2 Compliance – Cyber Hygiene & Zero Trust



*Cyber hygiene minimum scope based on Motive/Recital (89) of NIS-2. Source: Eviden own elaboration Source: Eviden SAS

NIS2 Delegated Act – Cryptography, Encryption - Guidance

Governance	A	<ul style="list-style-type: none">• Policies on risk analysis,• <u>Policies on access control, cryptography</u>• Policies on information system security
IS & Network Security & Resilience Policies	F	<ul style="list-style-type: none">• Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
	H	<ul style="list-style-type: none">• Policies and procedures regarding the use of cryptography and, where appropriate, encryption
People	G	<ul style="list-style-type: none">• Cybersecurity training• <u>Basic cyber hygiene practices</u>
Incident & Crisis Management	B	<ul style="list-style-type: none">• Incident & <u>Crisis</u> Management
Business Continuity	C	<ul style="list-style-type: none">• Crisis management• Business continuity, backup mgt• Disaster recovery
Supply chain	D	<ul style="list-style-type: none">• Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
ICT Life cycle Security,	E	<ul style="list-style-type: none">• ICT Security (IS & Network Security),• S-SDLC (DevSecOps),• Coordinated Vulnerability Disclosure
People	I	<ul style="list-style-type: none">• Human resources security (HR)• <u>Access control policies (ACP)</u>• <u>Asset management (AM)</u>
Asset Management IAM & Secure Digital Workplace	J	<ul style="list-style-type: none">• the use of multi-factor authentication or continuous authentication solutions,• secured voice, video and text communications• secured emergency communication systems within the entity



9. CRYPTOGRAPHY (ARTICLE 21(2), POINT (H), OF DIRECTIVE (EU) 2022/2555)

9.1.1. For the purpose of Article 21(2), point (h) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply **a policy and procedures related to cryptography**, with a view to ensuring adequate and effective use of cryptography to protect the confidentiality, authenticity and integrity of information **in line with the relevant entities' information classification** and the **results of the risk assessment**.

9.1.2. The policy and procedures referred to in point 9.1 shall establish:
(a) in accordance with the relevant entities' **classification of assets, the type, strength and quality of the cryptographic measures required to protect the relevant entities' assets**;
(b) based on point (a), **the protocols** to be adopted, as well as cryptographic **algorithms, cipher strength, cryptographic solutions** and usage practices to be approved and required for use in the entities, following, where appropriate, a **cryptographic agility** approach;

(c) the relevant entities' approach **to key management**, including methods for the following:
(i) generating keys for different cryptographic systems and applications;
(ii) issuing and obtaining public key certificates;
(iii) distributing keys to intended entities, including how to activate keys when received;
(iv) storing keys, including how authorised users obtain access to keys;
(v) changing or updating keys, including rules on when and how to change keys;
(vi) dealing with compromised keys;
(vii) revoking keys including how to withdraw or deactivate keys;
(viii) recovering lost or corrupted keys;
(ix) backing up or archiving keys;
(x) destroying keys;
(xi) logging and auditing of key management-related activities;
(xii) setting activation and deactivation dates for keys ensuring that the keys can only be used for the specified period of time according to the organization's rules on key management;
(xiii) handling legal requests for access to cryptographic keys.

9.1.3. The relevant entities shall **review and, where appropriate, update their policy and procedures at planned intervals**, taking into **account the state of the art in cryptography**.

Source: NIS2 Delegated Act - precisng what to do with Art 21 (10 risk management measures) and 23 (incidents thresholds)
https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-Cybersecurity-risk-management-reporting-obligations-for-digital-infrastructure-providers-and-ICT-service-managers_en

NIS2 Delegated Act – Cryptography, Encryption - Guidance

Governance	A	<ul style="list-style-type: none"> • Policies on risk analysis, • <u>Policies on access control, cryptography</u> • Policies on information system security
	F	<ul style="list-style-type: none"> • Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
	H	<ul style="list-style-type: none"> • Policies and procedures regarding the use of cryptography and, where appropriate, encryption
IS & Network Security & Resilience Policies	G	<ul style="list-style-type: none"> • Cybersecurity training • <u>Basic cyber hygiene practices</u>
	B	<ul style="list-style-type: none"> • Incident & <u>Crisis</u> Management
People	C	<ul style="list-style-type: none"> • Crisis management • Business continuity, backup mgt • Disaster recovery
Incident & Crisis Management	D	<ul style="list-style-type: none"> • Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
Business Continuity	E	<ul style="list-style-type: none"> • ICT Security (IS & Network Security), • S-SDLC (DevSecOps), • Coordinated Vulnerability Disclosure
Supply chain	I	<ul style="list-style-type: none"> • Human resources security (HR) • <u>Access control policies (ACP)</u> • <u>Asset management (AM)</u>
ICT Life cycle Security,	J	<ul style="list-style-type: none"> • the use of multi-factor authentication or continuous authentication solutions, • secured voice, video and text communications • secured emergency communication systems within the entity
People		
Asset Management IAM & Secure Digital Workplace		

9. CRYPTOGRAPHY (ARTICLE 21(2), POINT (H), OF DIRECTIVE (EU) 2022/2555)



ACCESS CONTROL (ARTICLE 21(2), POINT (I), OF DIRECTIVE (EU) 2022/2555)

11.4. Administration systems

11.4.1. The relevant entities shall restrict and control the use of system administration systems.

11.4.2. For that purpose, the relevant entities shall:

- (a) only use system administration systems for system administration purposes, and not for any other operations;
- (b) separate logically such systems from application software not used for system administrative purposes,
- (c) protect access to system administration systems through authentication and encryption.**



Source: NIS2 Delegated Act - precisising what to do with Art 21 (10 risk management measures) and 23 (incidents thresholds)
https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-Cybersecurity-risk-management-reporting-obligations-for-digital-infrastructure-providers-and-ICT-service-managers_en

Cryptography in DORA RTS for Pillar 1

Draft RTS RMF:

Article 6 Encryption and cryptographic controls

2. (a) [...] rules for the encryption of data at rest, in transit and, where relevant, in use, taking into account the results of the approved data classification [...] If encryption of data in use is not possible, financial entities shall process data in use in a separated and protected environment or take other equivalent measures[...]

b. [...] encryption of internal network connections and traffic with external parties [...]

Article 7 Cryptographic key management

1. [...] cryptographic key management policy [...] **requirements for managing cryptographic keys through their whole lifecycle**, including generating, storing, backing up, archiving, retrieving, transmission, retiring, revoking and destroying keys [...]

Source: BaFin: Was bedeutet DORA in der Praxis? Highlights im IKT-Risikomanagementrahmenwerk Jan Kiefer (BaFin), Dominik Schäfer (Deutsche Bundesbank)



Cryptography, encryption in security incidents

6 encryption mistakes that lead to data breaches

#1: Assuming your developers are security experts

#2: Believing that regulatory compliance means you're secure (see shared responsibility models)

#3: Relying on cloud providers to secure your data (see shared responsibility models)

#4: Relying on low-level encryption disk or file encryption can seem like a tempting one-click-fix. However, many organizations rely solely on these solutions which is downright dangerous. For starters, disk encryption only kicks in when the server is turned off. While the server is on, the operating system goes about decrypting sensitive data for anyone who is logged in...including the bad guys.

#5: Using the wrong cipher modes and algorithms

- Using random numbers that are not cryptographically secure (or, in the case of the Sony PS3 hack, a *constant*)
- Using AES-ECB mode for data larger than 128 bits
- Reusing an Initialization Vector (IV) multiple times which can nullify the entire encryption process itself
- Using deterministic encryption to make sensitive data searchable without factoring for dictionary attacks.

#6: Getting key management wrong

Leaving the key unprotected

Fetching the key insecurely

Using the same key for all your data

Never changing the key

Source: [Yaron Guez](#)



NIS2 Auditing scenarios

Dependent on used security control framework and audit method scenarios may differ

- ISO 27001/2 Audit Scenarios
- ENISA EECC Audit Scenarios
- Spanish AEPD Guidelines (used for GDPR Personal Data Encryption – In NIS2 data are extended to whole organisation's data based on its classification)

Source: Eviden SAS



Cryptographic controls in ISMS

Related assets and risk scenarios per security objective or combined

According to ISO/IEC 27002:2022 - Cryptography can be used to achieve different information security objectives, for example:

- a) confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;
- b) integrity or authenticity: using digital signatures or message authentication codes to verify the authenticity or integrity of stored or transmitted sensitive or critical information. Using algorithms for the purpose of file integrity checking;
- c) non-repudiation: using cryptographic techniques to provide evidence of the occurrence or nonoccurrence of an event or action;
- d) authentication: using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources.

The ISO/IEC 11770 series provides further information on key management.

Source: Eviden SAS Based on ISO 27002:2022



ISO 27002:2022 ISMS controls addressing cryptography or encryption

5. Organizational Controls	6. Peoples controls	8. Technological controls
<p>5.1. Policies for information security (encryption, key management policy, privacy policy) 5.5. Contact with authorities (foreign jurisdictions)</p> <p>5.9. Inventory of information and other associated assets (assets discovery, IP country related information) 5.10. Acceptable use of information and other associated assets (by foreign jurisdictions)</p> <p>5.11. Return of assets 5.12. Classification of information (sensitive for Sovereignty, PII, IP, R&D) 5.13. Labelling of information</p> <p>5.14. Information transfer 5.15. Access control (from which country data are accessed)</p> <p>5.16. Identity management (Self Sovereign Identity, Distributed ID)</p> <p>5.17. Authentication information 5.18. Access rights</p>	<p>n/a</p>	<p>8.1. User endpoint devices</p> <p>8.2. Privileged access rights 8.3. Information access restriction 8.5. Secure authentication 8.7. Protection against malware</p> <p>8.10 Information deletion 8.11. Data masking (anonymization, hashing for sovereignty reasons) (AWS DMS) 8.12. Data leakage prevention 8.13. Information backup (Atos Cyber Recovery / Cloud Vault)</p>
<p>5.19. Information security in supplier relationships (requirements for encryption communicated to suppliers) 5.20. Addressing information security within supplier agreements (SCC – sovereignty requirements, audits, reviews, monitoring included in contracts)</p> <p>5.21. Managing information security in the ICT supply chain 5.22. Monitoring, review and change management of supplier services (use encryption against lawful access or data sharing to foreign governments) 5.23. Information security for use of cloud services (set-up encryption configuration specific to shared responsibility model with Cloud Service Provider)</p> <p>5.26. Response to information security incidents (in case of access or sharing data with foreign government)</p> <p>5.31. Legal, statutory, regulatory and contractual requirements (Country/Regional Sovereignty regulations) 5.32. Intellectual property rights 5.33. Protection of records (Storage encryption, Cloud Vault) 5.34. Privacy and protection of PII (hashing, masking of PII data) 5.35. Independent review of information security 5.36. Compliance with policies, rules and standards for information security (compliance to sovereignty laws, regulations) 5.37. Documented operating procedures</p>	<p>7. Physical controls</p> <p>7.1. Physical security perimeters (cloud provider data center locations, where data are stored) 7.3. Securing offices, rooms and facilities 7.8. Equipment siting and protection (HSM) 7.10. Storage media (Data Sanctuary/Air gapped vault) ISO 27040. 7.11. Supporting utilities</p> <p>7.13. Equipment maintenance (HSM) 7.14. Secure disposal or re-use of equipment</p>	<p>8.15. Logging (encryption of logs) 8.16. Monitoring activities (of sovereignty policies enforcement)</p> <p>8.20. Networks security 8.21. Security of network services 8.22. Segregation of networks 8.23. Web filtering</p> <p>8.24. Use of cryptography (Encryption key management, ISO 11770) 8.25. Secure development life cycle</p> <p>8.26. Application security requirements 8.27. Secure system architecture and engineering principles 8.28. Secure coding. 8.29. Security Testing</p> <p>Source: Eviden SAS Based on ISO 27002:2022</p>

ISO 27002:2022 ISMS controls related to cryptography 25 of 93 – 25%+ of all controls

ISO/IEC 27002 control ID	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.1	Policies for information security	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_ and_Ecosystem #Resilience
5.11	Return of assets	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management	#Protection
5.14	Information transfer	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Protection
5.17	Authentication information	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_ access_management	#Protection
5.19	Information security in supplier relationships	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_ and_Ecosystem #Protection
5.21	Managing information security in the ICT supply chain	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_ and_Ecosystem #Protection
5.22	Monitoring, review and change management of supplier services	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_ and_Ecosystem #Protection #Defence #Information_ security_assurance
5.31	Legal, statutory, regulatory and contractual requirements	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_ compliance	#Governance_ and_Ecosystem #Protection
5.33	Protection of records	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_ compliance #Asset_management #Information_protection	#Defence
5.36	Compliance with policies, rules and standards for information security	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_ compliance #Information_ security_assurance	#Governance_ and_Ecosystem
7.10	Storage media	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_ management	#Protection
7.14	Secure disposal or re-use of equipment	#Preventive	#Confidentiality	#Protect	#Physical_security #Asset_ management	#Protection

Source: Eviden SAS Based on ISO 27002:2022

ISO 27002:2022 ISMS controls related to cryptography 25 of 93 – 25%+ of all controls

ISO/IEC 27002 control ID	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
8.1	User endpoint devices	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Protection
8.3	Information access restriction	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection
8.7	Protection against malware	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security #Information_protection	#Protection #Defence
8.10	Information deletion	#Preventive	#Confidentiality	#Protect	#Information_protection #Legal_and_compliance	#Protection
8.11	Data masking	#Preventive	#Confidentiality	#Protect	#Information_protection	#Protection
8.12	Data leakage prevention	#Preventive #Detective	#Confidentiality	#Protect #Detect	#Information_protection	#Protection #Defence
8.13	Information backup	#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection
8.15	Logging	#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_event_management	#Protection #Defence
8.21	Security of network services	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection
8.24	Use of cryptography	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration	#Protection
8.26	Application security requirements	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection #Defence
8.27	Secure system architecture and engineering principles	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
8.28	Secure coding	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
8.29	Security testing in development and acceptance	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Application_security #Information_security_assurance #System_and_network_security	#Protection

European Electronic Communications Code (EECC)*

D1: GOVERNANCE AND RISK MANAGEMENT

- SO1: Information security policy
- SO2: Governance and risk management
- SO3: Security roles and responsibilities
- SO4: Security of third party dependencies

D2: HUMAN RESOURCES SECURITY

- SO5: Background checks
- SO6: Security knowledge and training
- SO7: Personnel changes
- SO8: Handling violations

D3: SECURITY OF SYSTEMS AND FACILITIES

- SO9: Physical and environmental security
- SO10: Security of supplies
- SO11: Access control to network and information systems
- SO12: Integrity of network and information systems
- SO13: Use of encryption**
- SO14: Protection of security critical data**

*Technical guidance to the national authorities tasked with supervising the security of electronic communication networks and services (hereinafter Competent Authorities), and in particular the security measures mentioned in Article 40 the European Electronic Communications Code (EECC)

Source: [ENISA Guideline on Security Measures under EECC](#)

D4: OPERATIONS MANAGEMENT

- SO15: Operational procedures
- SO16: Change management
- SO17: Asset management

D5: INCIDENT MANAGEMENT

- SO18: Incident management procedures
- SO19: Incident detection capability
- SO20: Incident reporting and communication

D6: BUSINESS CONTINUITY MANAGEMENT

- SO21: Service continuity strategy and contingency plans
- SO22: Disaster recovery capabilities

D7: MONITORING, AUDITING AND TESTING

- SO23: Monitoring and logging policies
- SO24: Exercise contingency plans
- SO25: Network and information systems testing
- SO26: Security assessments
- SO27: Compliance monitoring

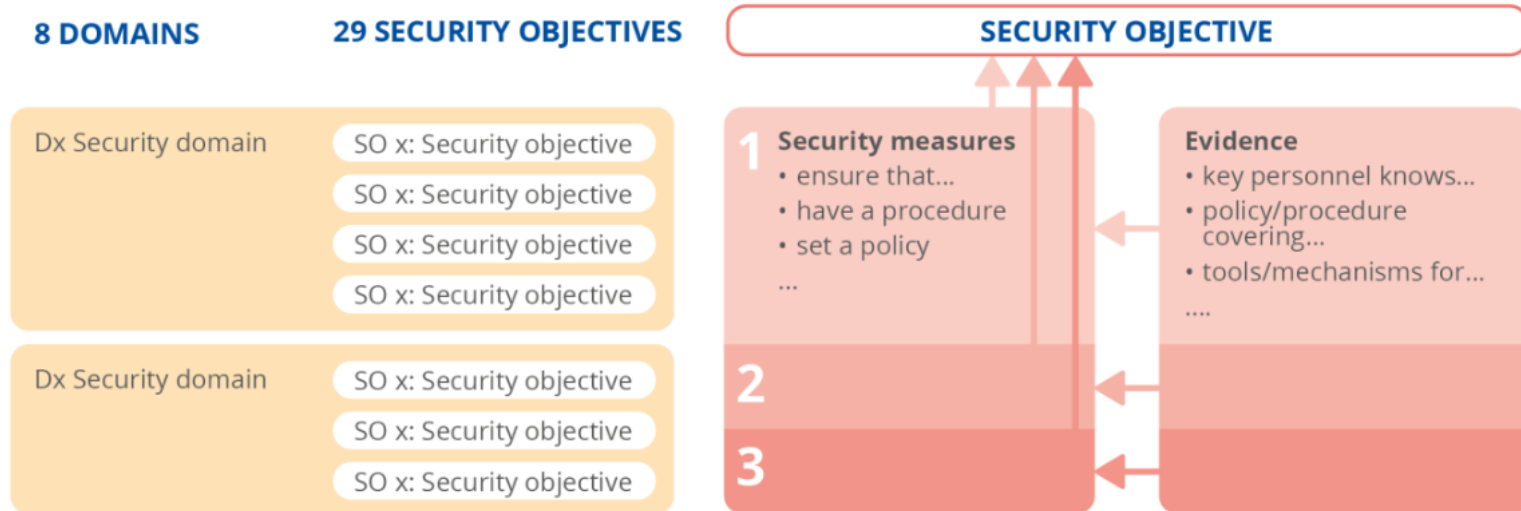
D8: THREAT AWARENESS

- SO28: Threat intelligence
- SO29: Informing users about threats



Security objectives

Figure 4: Overall structure of the security objectives and security measures



Source: [ENISA Guideline on Security Measures under EEC](#)



„State of the art.” in EU Regulations: EECC

1 Sophistication level 1 (basic)

- Basic security measures that could be implemented.
- Evidence that basic measures are in place

2 Sophistication level 2 (industry standard)

- Industry standard security measures and an ad-hoc review of the implementation, following changes or incidents.
- Evidence of industry standard measures and evidence of reviews of the implementation following changes or incidents.

3 Sophistication level 3 (state of the art)

- State of the art (advanced) security measures, and continuous monitoring of implementation, structural review of implementation, taking into account changes, incidents, tests and exercises, to proactively improve the implementation of security measures.
- Evidence of state of the art (advanced) implementation, evidence of a structural review process, and evidence of pro-active steps to improve the implementation of security measures.

[Source: ENISA Guideline on Security Measures under EECC](#)



The European Electronic Communications Code

	Security measures	Evidence
1	a) Where appropriate to prevent and/or minimise the impact of security incidents on users and on other networks and services, encrypt data ²⁶ during its storage in and/or transmission via networks.	<ul style="list-style-type: none"> i. Description of main data flows, and the encryption protocols and algorithms used for each flow. ii. Description of justified exclusions and limitations²⁷ in implementing encryption.
2	<ul style="list-style-type: none"> b) Implement encryption policy. c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys. 	<ul style="list-style-type: none"> iii. Documented encryption policy including details about the cryptographic algorithms and corresponding cryptographic keys, according to international best practices and standards. iv. Documented justified exclusions that provide rationale for when data is not encrypted, including the related impact assessment.
3	<ul style="list-style-type: none"> d) Review and update the encryption policy. e) Use state of the art encryption algorithms. 	<ul style="list-style-type: none"> v. Updated encryption policy, review comments and/or change logs. vi. Encryption policy includes details about the state of the art cryptographic protocols used.

4.4.3.5 SO13: Use of encryption

Ensure adequate use of encryption to prevent and/or minimise the impact of security incidents

on users and on other networks and services.

5 Including reliable identification, monitoring and tracking of changes and the status of patches.

26 The type and scope of data to be encrypted should be determined based on the risk assessment performed and will typically include communication data, customer critical data (e.g. unique identifiers), relevant management and signalling traffic and any other data or metadata, the disclosure or tampering of which may cause security incidents.

27 Ability to implement encryption may also be influenced by technological limitations, like in the case of legacy networks or when old equipment and network protocols are used

Source: [ENISA Guideline on Security Measures under EEC](#)



The European Electronic Communications Code

	Security measures	Evidence
1	<ul style="list-style-type: none"> a) Make sure that cryptographic key material and secret authentication information (including cryptographic key material used for authentication) are not disclosed or tampered with. b) Access to private keys is strictly controlled and monitored. 	<ul style="list-style-type: none"> i. Cryptographic key material and secret authentication information are protected using security best practices and standards for protection mechanisms (like split knowledge and dual control, encryption, hashing, secure hardware etc.). ii. Description of mechanisms for controlling and monitoring access to private keys.
2	<ul style="list-style-type: none"> c) Implement policy for management of cryptographic keys. d) Implement policy for management of user passwords. 	<ul style="list-style-type: none"> iii. Key management policy including roles, responsibilities and controls for the use, protection and lifetime of cryptographic keys throughout their life cycle including controls for access to and backup and recovery of private keys. iv. User password management policy including processes, methods and techniques for secure storing of user passwords using industry best practices²⁸.
3	<ul style="list-style-type: none"> e) Review and update of key management policy. f) Review and update of user password management policy. 	<ul style="list-style-type: none"> v. Updated key management policy, review comments and/or change logs. vi. Updated user password management policy, review comments and/or change logs.

4.4.3.6 SO14: Protection of security critical data

Ensure that cryptographic key material and secret authentication information are adequately protected

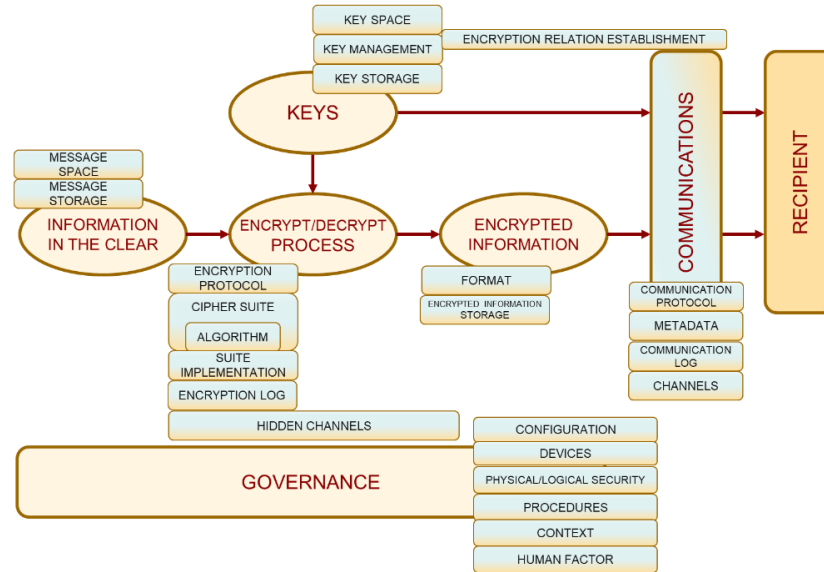
E.g. hashing using appropriate hashing algorithms, salting etc.

Source: [ENISA Guideline on Security Measures under EECC](#)



Audit Scope – Controls of Encryption System

Element of Encryption System according to AEPD Guidelines for the validation of cryptographic systems in data protection processing



Source: Guidelines for the validation of cryptographic systems in data protection Processing May 2023 Agencia Española de Protección de Datos (Spanish Data Protection Agency) in collaboration with the Asociación Profesional Española de Privacidad (APEP) and the Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum)



Audit Scope – Controls of Encryption System

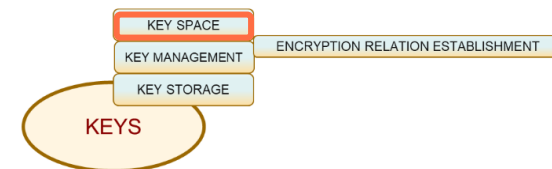
Element of Encryption System according to AEPD Guidelines

Key space controls

Control

1. Key security requirements have to be defined, e.g., length over a number of bits (see Annex), format etc
2. There is a procedure to avoid reuse of keys.
3. It is not possible to use manually generated keys.
4. Passwords are not used as keys.
5. Keys are not generated from user passwords using key derivation functions.
6. There is a procedure for the detection and elimination of weak and predictable keys.
7. High entropy in the key selection process and potential coverage of the entire key space, with uniform distribution, is ensured.
8. The absence of correlation between the keys of different users is guaranteed.
9. Key generation takes place in a protected environment (e.g., in hardware security modules or HSM).
10. Key generation shall be isolated from the operating environment.
11. Key generation protects forward secrecy.
12. Key generation protects future secrecy.
13. The key generation mechanisms shall be certified and subject to the applicable sectorial regulations.
14. Whether or not the generated keys should be implemented on physical devices or tokens

Source: Guidelines for the validation of cryptographic systems in data protection Processing May 2023 Agencia Española de Protección de Datos

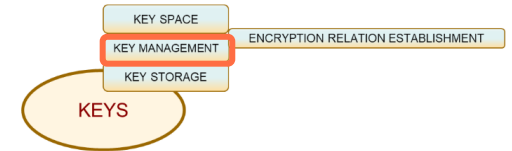


Audit Scope – Controls of Encryption System

Element of Encryption System according to AEPD Guidelines

Encryption Key Management Controls

1. The management and lifecycle of the key and certificate relationship is documented: generation, distribution, storage, change or update, revocation, management of compromised, forgotten, or lost keys, activation periods, expiry, recovery of lost or corrupted keys, storage33, backup and destruction of keys.
2. There are extracts from the management documentation oriented to the different roles involved in the encryption process.
3. If a cryptographic medium or token is not used, the entry of the key and its representation on the screen must not be in a format readable by other persons or users who may be around.
4. Internal key distribution is done through confidential channels and by authenticating the recipients.
5. There are procedures in place to train users never to disclose keys or passwords to third parties on request, even if they identify themselves as administrators of the service.
6. A user management procedure is in place, both for authorisation and termination procedures or for those whose privileges have been temporarily (absent) or permanently withdrawn.
7. There is a procedure defining the use of keys that limits reuse in multiple messages, use in different procedures and systems or in different roles.
8. There is a procedure that guarantees a large distance between two keys of consecutive use.
9. A pyramid/hierarchical key structure exists.
10. There is a key or certificate revocation protocol that takes into account not only the time of use, but also the amount of information exchanged, the context of breaches or attacks, the sensitivity of the information, etc.
11. Revoked keys or certificates to be stored shall be stored on media isolated from the operational media.



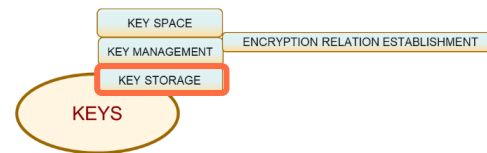
Source: Guidelines for the validation of cryptographic systems in data protection...AEPD

NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Encryption Key Storage Controls

1. The keys are not recorded in clear on any type of media.
2. Keys are not stored in a non-volatile or external form when the key is not encrypted (key wrapped).
3. There is specific key management used to protect keys.
4. There is a protection or cryptographic devices (HSM, hardware security module) to preserve the confidentiality of the keys.
5. The protection mechanisms themselves are subject to periodic review.
6. Storage, backup and key recovery procedures are in place.
7. Access to passwords is subject to access control and logging
8. Automatic procedures are in place to detect and alert to improper access to key stores.
9. Secure key deletion and erasure procedures are in place.



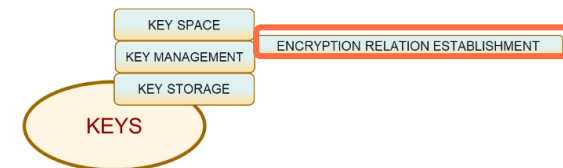
Source: Guidelines for the validation of cryptographic systems in data protection Processing May 2023 Agencia Española de Protección de Datos

NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Management of the Encryption and Certificate Relationship Controls

1. If two parties agree to exchange information to establish a key relationship, both parties must be certain of the identity and origin of the other party's messages.
2. In the case of authentication in a Public Key Infrastructure (PKI), the PKI must be trusted.
3. In the case of symmetric keys, if two parties agree to exchange information to establish a key relationship, the keys they establish between them must be different from the keys that one of the parties establishes with another third party.
4. If there are common keys for groups of people there must be different keys for different groups not allowed to communicate with each other.
5. The received certificates and the chain of trust are properly validated.
6. While two parties are exchanging information to establish a key relation, no other third-party entity should be able to infer the identity of both parties.
7. The establishment of the key relationship (algorithms, suite elements, etc.) is to be done in a confidential manner.



Source: Guidelines for the validation of cryptographic systems in data protection Processing May 2023 Agencia Española de Protección de Datos



NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Messages Space Controls

The message space is the set of possible messages being encrypted. The more predictable the messages are, the lower the strength of the message. This predictability has more impact the more it affects the initial part of the message to be transmitted.

1. Static headers do not exist or are avoided in the messages or set of messages to be encrypted.
2. Messages should avoid predictable and identifiable message structure, such as patterns, abbreviations, public or obvious information.
3. If the message in clear consists of a set of files, the files are preprocessed in order to hide the structure.
4. Compression of the message in the clear is performed before encryption.
5. The adjustment of the message to the block size of the encryption algorithm is done using appropriate padding and without known vulnerabilities.
6. The message space guarantees by design a high entropy (e.g., with the inclusion of random segments especially at the beginning and at the end of the message to be encrypted)

Source: Guidelines for the validation of cryptographic systems in data protection Processing May 2023 Agencia Española de Protección de Datos



NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Message Storage Controls

Controls:

1. The confidentiality of the storage of permanent messages and temporary copies is protected.
2. There is a procedure for controlling access to the storage of messages in the clear.
3. There is a log of access to message in the clear message's storage.
4. Automatic procedures are in place to detect and alert to improper access to the message store.
5. For certain types of messages, there are expiry procedures for messages in the clear that were transmitted or received encrypted.
6. Temporary copies are not accessible by third parties or third-party applications and are subject to secure deletion.
7. Access to message in the clear storage, when enabled, is limited in the set of applications that can exploit it.
8. Secure deletion procedures are in place for messages in the clear and temporary copies.
9. There is no link between messages in the clear and the keys used to encrypt them.
10. There is no link between messages in clear and their encryption



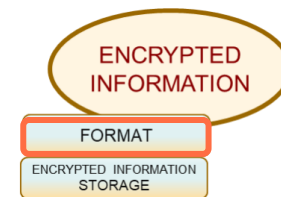
Source: Guidelines for the validation of cryptographic systems in data protection Processing May 2023 Agencia Española de Protección de Datos

NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Encrypted Information Format Controls

1. The format of the cryptogram does not include unencrypted information, nor information related to the process or nature of the encrypted information.
2. The key is not included in the header of the text before it is encrypted.
3. When the encrypted message consists of several independent files, a description of their contents is not stored in clear.
4. In case steganographic or deniable encryption techniques are used, their effectiveness has been analysed.



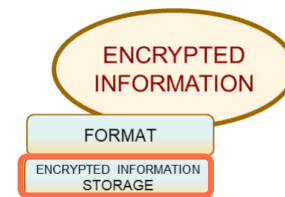
Source: Guidelines for the validation of cryptographic systems in data protection
Processing May 2023 Agencia Española de Protección de Datos

NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Encryption Storage Controls:

1. Physical and logical access controls to encrypted information repositories are in place.
2. Authentication mechanisms are in place to prevent impersonation of the user who has entered the access keys to the encryption store.
3. There is no other side storage in which it is possible to find encrypted messages but in clear, whole or just a fragment.
4. There is a backup of the encryption storage.



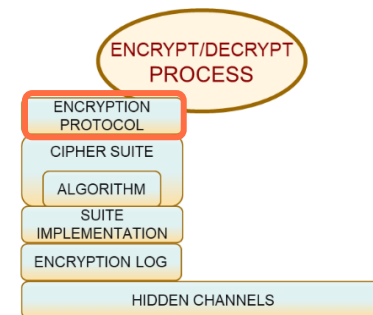
Source: Guidelines for the validation of cryptographic systems in data protection
Processing May 2023 Agencia Española de Protección de Datos

NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Encryption Protocol Controls

1. The protocol must be well documented, third party audited or certified.
2. The protocol does not use insecure block processing (e.g., ECB)
3. The protocol includes authenticated encryption mechanisms. (e.g., GCM)
4. The protocol ensures that not only a fragment of the message is encrypted.
5. The protocol ensures that the same message is not sent encrypted and unencrypted.
6. The protocol ensures that the same message is not encrypted using different keys or algorithms.
7. The protocol ensures that the same key is not used for different recipients.
8. The protocol guarantees a maximum of information encrypted with the same key.
9. The protocol ensures that different blocks of the encrypted text cannot be replaced, deleted or jumbled without being detected.



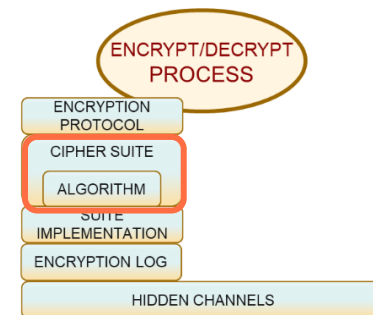
Source: Guidelines for the validation of cryptographic systems in data protection Processing May 2023 Agencia Española de Protección de Datos

NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Encryption Cipher Suite Controls

1. The elements of the suite are identified in name and version and inventoried. In particular, encryption algorithms, MACs, key exchange, padding, random number generators, key generators, certificates, automatic protocols, key management tools, etc.
2. The security of the suite is provable.
3. Criteria are identified to determine the elements of the suite appropriate to the context of the application and the life of the personal data.
4. The elements of the suite are properly certified and comply with sectoral regulations.
5. Certifications are up to date.
6. No compromised, non-certified or “ad-hoc” developed algorithms are used in the suite.
7. The generation of random numbers must be adequate, with a strong algorithm (software or hardware), certified or in accordance with regulations, and verified the next bit test and state commitment.
8. Random number generation seeds must be user-configurable or, there is a seed creation functionality with sufficient entropy and unpredictability.
9. Prime number generation must be unpredictable.
10. The configuration of the suite used to encrypt each message in clear is controlled
11. There is a backup of the elements of the suite.
12. Information about the suite is confidential.



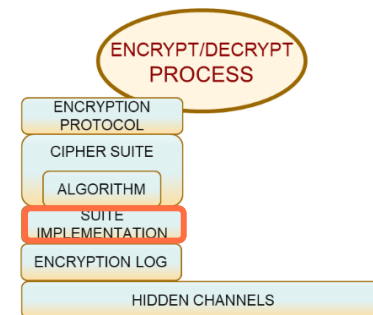
Source: Guidelines for the validation of cryptographic systems in data protection Processing May 2023
Agencia Española de Protección de Datos

NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Encryption Cipher Suite Implementation Controls

1. Vulnerability testing of the Hw/Sw elements of the encryption system has been carried out.
2. It has been verified that there is no persistence in memory of keys or clear texts used in the encryption process.
3. It is analysed that there are no keys included in the code (hardcoded).
4. There is a checking procedure to avoid leaking of system behavioural information.
5. There are measures to prevent detection and manipulation of the implementation: non-deterministic duration operations, shielding of circuits, homogenisation of consumption, modifying implementation of registered algorithms, adding noise and useless operations.
6. Implementations use appropriate, certified (FIPS 140-2, 197), or authorised libraries (CCN-STIC-807).
7. The generation of initialisation vectors, "salt" and "nonces" ensures that they are safe (minimum sizes and non-repetitive) and are not reused.
8. Block padding methods are up to date and appropriate for the type of processing. For example, do not use PKCS v1 or v1.5.
9. The hash functions used are suitable for cryptographic use, are modern and not obsolete. For example, do not use MD5 or SHA1.
10. The implementation of the certificate validation is secure

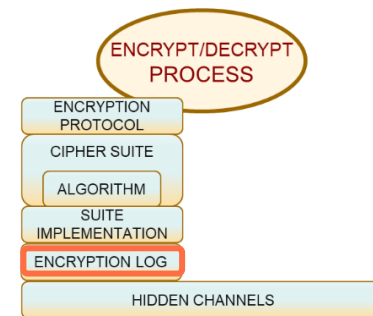


Source: Guidelines for the validation of cryptographic systems in data protection Processing May 2023
Agencia Española de Protección de Datos

NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Encryption Log Controls



1. There is a log of encryption activities.
2. Do not store keys, text in clear, encrypted text or any other information that can be used for cryptanalysis.
3. Recorded data should be kept to a minimum, with strict criteria for destruction, storage and copying.
4. Encryption logs must be protected in terms of confidentiality and integrity.
5. Very restrictive and traceable access control with real-time alerts is guaranteed.

Source: Guidelines for the validation of cryptographic systems in data protection Processing May 2023 Agencia Española de Protección de Datos

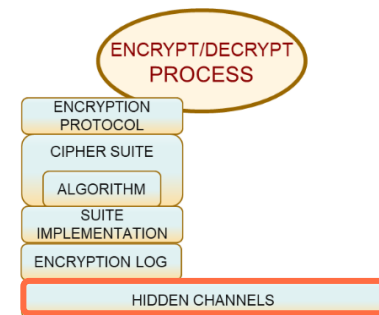
NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Hidden Channels

1. There is a hidden channel checking of the suite.
2. There is a checking of hidden channels in automated and non-automated protocols.
3. There is a checking of hidden channels in the communication channels, such as error messages.
4. There is a checking of hidden channels in the implementation in software (libraries) and hardware.
5. There is a checking of hidden channels in the operating system running the encryption system.
6. In processing implemented on complex information systems, including for storage at rest, the security of information flows between load balancers, web servers, back-end systems, and other internal and external systems must be determined.
7. If the organisation uses hidden channels in the encryption system for monitoring and inspection of content, the monitoring must be real-time, logged data must be minimised, with strict criteria for early destruction, logs must be protected in terms of confidentiality, and very restrictive and traceable access control with real-time alerts must be ensured.

Source: Guidelines for the validation of cryptographic systems in data protection Processing May 2023 Agencia Española de Protección de Datos



NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Communication Protocol Controls

1. Authentication is ensured at the establishment of each session and at each exchange within a session.
2. Procedures are in place to prevent and detect impersonation of interlocutors. (MITM).
3. Procedures are in place to prevent and detect delays, reordering or deletion of encrypted fragments, selective modification of encrypted information, fabrication of dummy messages from fragments of authentic messages, message invention, message repetition, reflection (return of message to sender), alteration of message recipient, etc



Source: Guidelines for the validation of cryptographic systems in data protection Processing May 2023 Agencia Española de Protección de Datos

NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Communication Metadata & Communication Log Controls

Metadata Controls:

1. Metadata in communications is minimised and known.
2. The impact of metadata on cryptanalysis has been assessed.

Communication Log Controls:

1. Log files must not store keys or ciphertext.
2. Where communication is not direct, the log information generated in the proxy systems must be known and controlled.
3. Recorded data should be kept to a minimum, with strict criteria for destruction, storage and copying.
4. Logs must be protected in terms of confidentiality.
5. Very restrictive and traceable access control is guaranteed (alarms for suspicious access)
6. The log management tool is audited and/or certified.
7. Procedures are in place to prevent log poisoning attacks

Source: Guidelines for the validation of cryptographic systems in data protection Processing May 2023 Agencia Española de Protección de Datos



NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Channel as physical medium (and its virtual extensions) Controls

1. Procedures are in place to prevent and detect the use of open channels.
2. Procedures are in place to prevent and detect the use of private channels.
3. Procedures are in place to prevent and detect eavesdropping and collection of encrypted information.
4. Procedures are in place to prevent and detect traffic analysis and information linkage.
5. Procedures are in place to prevent and detect attacks on DNS services.
6. Procedures are in place to prevent and detect denial-of-service attacks.
7. Procedures are in place to prevent and detect channel outages (physical and logical).
8. Physical and/or virtual network segmentation mechanisms are implemented (VLAN).



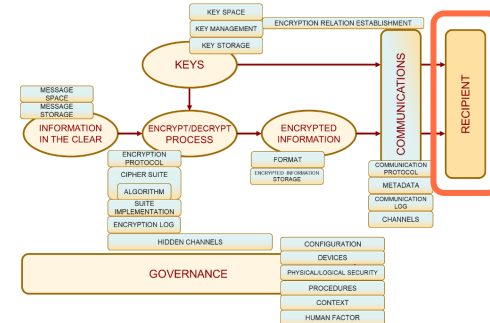
Source: Guidelines for the validation of cryptographic systems in data protection Processing May 2023 Agencia Española de Protección de Datos

NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Encrypted Messages Receipt Controls:

1. The recipient is authenticated.
2. Open sessions with the recipient expire. Session keys used are not predictable.
3. Re-authentication during an open session is performed randomly.
4. The receiver's level of compliance of the encryption system is equivalent to that of the sender.
5. The recipient has been assessed with audits and/or certifications.
6. The recipient's personnel have been trained and have policies and practical manuals for the proper handling of encrypted material.
7. The history of personal data breaches has been checked.



Source: Guidelines for the validation of cryptographic systems in data protection Processing May 2023 Agencia Española de Protección de Datos

NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Configuration Control of the Encryption System Components

1. The elements of the cryptographic system have to be properly configured prior to the production start-up of the processing where the encryption system is used.
2. The configuration of each element is documented.
3. The encryption system cannot be run with default settings, or the default settings do not exist.
4. Automatic updates of any item do not alter the configuration or reset it.
5. There is an access control policy in place and access to the configuration of each element is logged.



Source: Guidelines for the validation of cryptographic systems in data protection Processing May 2023 Agencia Española de Protección de Datos

NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Devices used in the Encryption System

1. There is a security policy and control over BYOD devices that are used in the encryption system, or they are not allowed at all.
2. There is a control or prohibition on installing applications on devices running encryption systems without the security officer's authorisation.
3. Operating system versions specially configured for high security are used.
4. Devices on which the encryption system is running are scanned for device-specific vulnerabilities.
5. The use of devices that prevent the full encryption system from being kept up to date is not permitted.
6. Encryption system devices shall only be used in protected environments.



Source: Guidelines for the validation of cryptographic systems in data protection Processing May 2023 Agencia Española de Protección de Datos

NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Physical/logical security of the Encryption System

1. There is a policy and definition of restricted areas.
2. Policies define the allowed storage devices.
3. There is authorised physical and logical access control to encryption devices and equipment, message and key files, temporary files, encryption procedures, etc.
4. There is a log of access to encryption devices and equipment, message and key files, temporary files, encryption procedures, etc..
5. There is a list of personnel involved in the execution of the cryptosystem and their roles.
6. There is a protocol for the confidential destruction of all material related to the encryption system.
7. Black-bag attack prevention measures are in place.
8. There is no direct display of the elements of the cipher system
9. All backups are controlled.
10. Doesn't exist third-party storage.
11. Hot (Heartbleed SSL) or cold start memory scans are performed.
12. The use of keyloggers and measures to prevent keylogging have been sought.
13. Measures are in place to prevent manipulations of intermediate operations.
14. Tempest attack prevention measures are in place.



Source: Guidelines for the validation of cryptographic systems in data protection
Processing May 2023 Agencia Española de Protección de Datos

NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Management of policies & procedures in the Encryption System (1)

1. The encryption system fulfil in its design, implementation and validation, the policies and procedures established by the controller (in GDPR meaning).
2. The life cycle of the data in the processing is documented (data categories, data flow from inception to destruction).
3. An assessment of the necessary strength and quality of the encryption system is documented for each processing operation in terms of the risk to fundamental rights and freedoms.
4. There is a unit/person (u/p) in charge of the encryption system.
5. The u/p maintains an adequate and documented policy on the use of encryption in processing in relation to all items and control.
6. Processing is categorised by their necessary strength and different implementations and policies appropriate to how criticality is the encryption system are implemented.
7. The policy reflects the recommendations of the DPO or the data protection advisor.
8. This policy is subject to be recorded and approval cycle of the entity's management.
9. Such a policy states the flow/life cycle of all components of the suite's inventory (as indicated above).
10. Third parties/providers involved (e.g., certificate validators, SaaS, ...) are identified.
11. Contracts with intervening third parties are included.



Source: Guidelines for the validation of cryptographic systems in data protection
Processing May 2023 Agencia Española de Protección de Datos

NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Management of policies & procedures in the Encryption System (2)

12. In contracts with third parties, to the extent that they perform encryption of personal data, instructions on data encryption are set out, all information necessary to demonstrate compliance with the controls of the cryptosystem selected by the data controller are made available to the data controller, as well as mechanisms for monitoring and auditing tchem.

13. Regular monitoring of encryption system providers is in place (e.g., with a vendor assessment).

14. This policy reflects the data protection requirements set by the DPO or the data protection advisor.

15. It includes role definition (administrator, user), access control, authentication, user procedures, destruction of cryptographic material, integrity management, incidents and alerts and contingency plans.

16. The policy sets out the timeframes and events that trigger a validation, maintenance, remove from inventory and/or audit process

17. The policy provides for re-encryption strategies for information at rest appropriate to the technical context and data breaches.

18. The policy includes a procedure for auditing and testing of updated encryption system elements.

19. Updates of procedures, hardware or software are not automatically incorporated into production systems.



Source: Guidelines for the validation of cryptographic systems in data protection
Processing May 2023 Agencia Española de Protección de Datos



NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Management of policies & procedures in the Encryption System (3)

20. There is an implemented backup management policy for the suite, configuration and keys.
21. A key escrow policy is in place.
22. This policy is integrated in the security policy.
23. Policy does not rely exclusively on automation.
24. Access to the policy or parts of the policy is restricted on a need-to-know basis.
25. The policy establishes a process for identifying and continually assessing changes in the sensitivity of encrypted information, whether due to changes in data categories, subject categories, volume of affected individuals or other changes.
26. There are communication channels for incidents about the overall encryption process that reach that unit/person.
27. There are channels for internal communication and for communications with external sources.
28. The data protection officer is included in all cryptosystem definition and validation procedures.
29. The administrator cannot bypass encryption procedures.
30. Procedures are in place to prevent the transmission of unencrypted confidential information.
31. The process of receiving and attending to applications by authorities for material of figure is in place.
32. If the organisation implements hidden channels in the encryption system for monitoring and inspection of content, the management is subject to strict criteria for continuous auditing with DPO involvement.
33. Exists a contingency plan in place in case it is detected that the cryptosystem may be compromised.
34. There is a procedure for complying with GDPR obligations in the event that a compromise of the encryption system affecting personal data is detected.



Source: Guidelines for the validation of cryptographic systems in data protection
Processing May 2023 Agencia Española de Protección de Datos



NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Context controls of personal (or other type of) data breaches in the Encryption System

1. There is an ongoing collection and analysis of encryption-related gaps and incidents in organisations, processing or similar systems.
2. There is a continuous collection and analysis of new known vulnerabilities that may affect the entire encryption system.
3. Changes in the legal framework affecting the entity or the processing are identified and assessed on an ongoing basis, and legal risks of future regulation are identified.
4. Technological developments relating to cryptanalysis, both current and estimated changes in the medium term, are identified and assessed on an ongoing basis



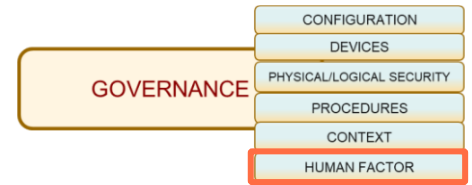
Source: Guidelines for the validation of cryptographic systems in data protection Processing May 2023 Agencia Española de Protección de Datos

NIS2 Auditing scenarios

Element of Encryption System according to AEPD Guidelines

Human factor controls in the Encryption System

1. There are written procedures available for personnel handling encryption material.
2. Staff are required to sign confidentiality undertakings informing them of their duties and responsibilities.
3. Staff are trained to carry out the procedures for which they are responsible.
4. There are plans for continuous training on the procedures.
5. There is training and specific procedures in place to detect the existence and cataloguing of social engineering attacks, as well as possible extortion or coercion.
6. There is supervision of the manual execution of procedures.
7. There is an internal sanction procedure for non-compliance with encryption procedures.
8. In internal/external staff selection processes for positions in charge of the most critical operations, a vetting process and background checks must be completed.
9. Personnel in charge of the most critical operations regularly undergo a technical and reliability reassessment process.



Source: Guidelines for the validation of cryptographic systems in data protection Processing May 2023 Agencia Española de Protección de Datos



EU Standardisation Regulation – Implications for NIS 2 – Where to search

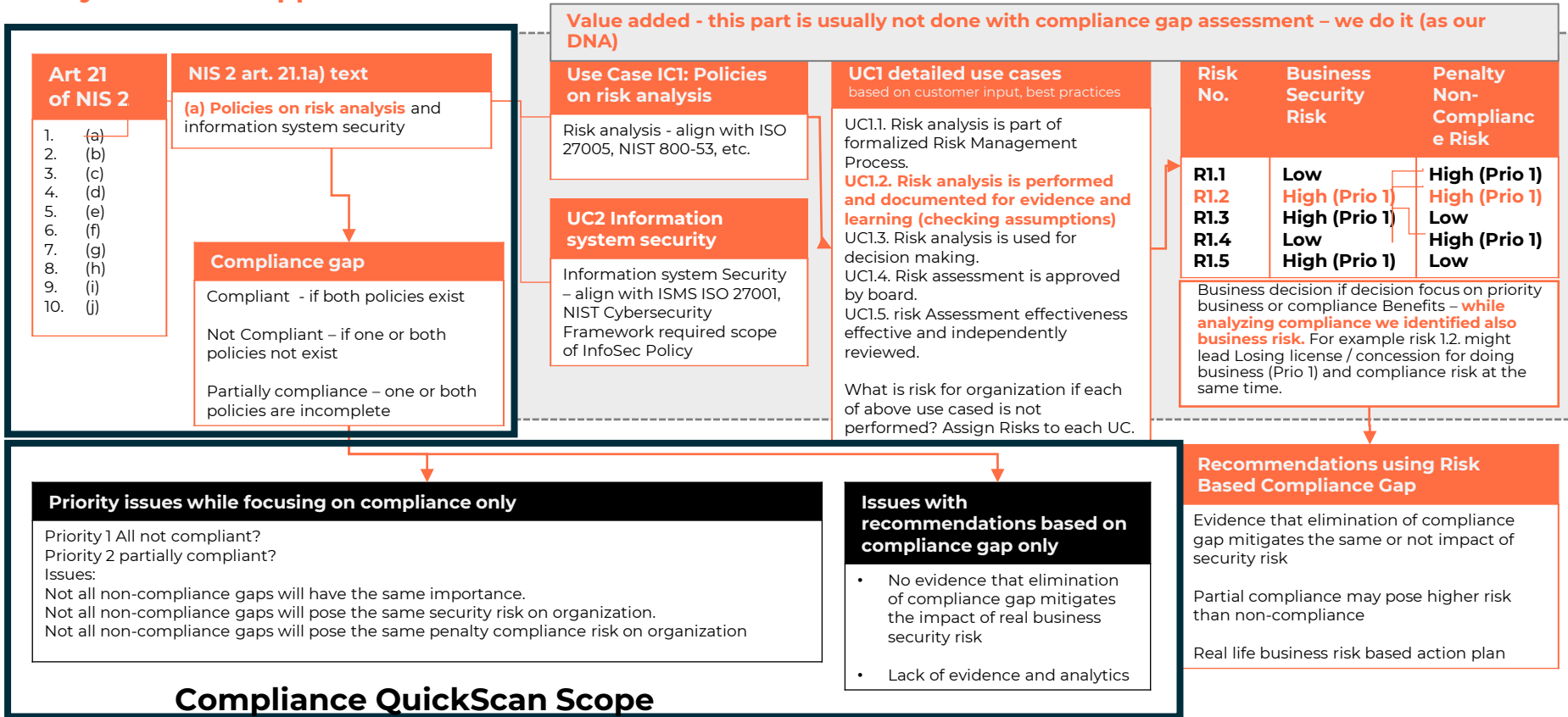
Type of Standards in [Regulation \(EU\) No 1025/2012](#) of the European Parliament and of the Council of 25 October 2012 on European standardization



Source: Eviden SAS

NIS2 Risk based Compliance Gap Assessment

Why risk-based approach?



Compliance QuickScan Scope

NIS2 Directive – Evidens' Website

Evidens' Comprehensive Compliance Journey



Your NIS2 Advantage



Tailored NIS2 Compliance Solutions for Your Critical Infrastructure

We recognize the



Holistic NIS2 Compliance Approach

Move beyond simple checklists with our comprehensive



Seamlessly Integrate IT & OT Security

The convergence of Information Technology (IT) and Operational

Secure NIS2 Compliance with Evidens' Expert Cyber Solutions

What is Evidens' NIS2 compliance service?

Evidens' NIS2 compliance service is your tailored solution for navigating the complexities of NIS2 regulations. We combine expert advisory services, customized to your organization's unique needs, with cutting-edge cybersecurity solutions to protect your critical services and ensure seamless compliance.

Partnering with Evidens, you gain a strategic advantage:

NIS2 Applicability Assessment
Determine if your organization falls under the NIS2 Directive and, if so, whether it will be classified as an essential or important entity.

Compliance Gap Analysis
Pinpoint gaps in your documentation, technical and organizational controls, and evidence collection processes, highlighting potential compliance risks and providing actionable insights for NIS2 readiness.

Actionable Implementation
Develop and execute a robust roadmap to address identified gaps, leveraging our expertise and industry best practices to fortify your defenses.

Continuous Risk Management
Proactively monitor and adapt your cybersecurity framework to evolving threats and regulatory changes, ensuring ongoing compliance and resilience.

By proactively embracing NIS2 compliance with Evidens, you not only mitigate the risk of costly fines and reputational damage but also gain a competitive edge through enhanced operational resilience and a demonstrable commitment to cybersecurity excellence.

Elevate your organization's cybersecurity maturity and lead with confidence – partner with Evidens to achieve NIS2 compliance that empowers your business.

[Consult now](#)



Our Comprehensive NIS2 Compliance Services



- **NIS-2 Quick Scan and Risk-based Assessments:** Pinpoint vulnerabilities, compliance gaps, and potential areas of improvement against NIS2 requirements through a tailored assessment approach, utilizing either a rapid scan or a deep-dive analysis. Expose both organizational and technical weaknesses with optional penetration testing for a comprehensive view.
- **NIS-2 Compliance Program Development and Implementation:** Create and implement a tailored compliance program that addresses risk mitigation, incident response, and ongoing security management, aligning with your organization's unique risk profile and operational objectives.
- **Budgeting and ROI Analysis:** Strategically allocate resources and showcase the tangible return on investment in cybersecurity measures, ensuring your NIS2 compliance efforts are both effective and financially sound.
- **Managed NIS2 Compliance Services:** Proactively monitor your systems, adapt to evolving threats, and ensure ongoing compliance with NIS2 requirements through expert, ongoing support.



- **Integrated Cyber Incident & Disaster Recovery:** Equip your team with the tools and knowledge to effectively detect, respond to, and recover from cyber incidents or disruptions, integrating cyber resilience with your broader business continuity planning, disaster recovery and crisis management.
- **Tailored Supply Chain & Third-Party Risk Management:** Tailor a risk management strategy based on specific supplier groups and assurance criteria, ensuring a comprehensive approach to mitigating risks originating from third-party vendors and partners.
- **NIS2 Network Security and Information Systems (NIS):** Fortify your defenses against evolving threats with hands-on assistance in implementing state-of-the-art cybersecurity technologies and access management measures.
- **Cybersecurity Awareness and Training Programs:** Foster a culture of cybersecurity awareness and vigilance through comprehensive training programs that transform your employees into your first line of defense.

Source: Evidens SAS

NIS2 Directive Global Landing Page

NIS2 Compliance Readiness Assessment

forms.office.com/pages/responsepage.aspx?id=hXccfYotfUO4Qh7V2PvgCqp6shwPbqFHvzGtiAPHZ55UQRUOFpPTkFSWTI5R1VPWUZSRE0wOk0wTC4u&route=shorturl

EVIDEN

English (United States)

NIS 2 DIRECTIVE

Sep 4, 2024

Start now

* Required

Get ready for NIS 2

Preparing for NIS2 is not a task to be taken lightly. By starting early, understanding the legislation, implementing crucial security measures, and educating the entire organization, affected entities can navigate the complexities and ensure compliance with the forthcoming directive.

It is time to embark on the journey toward a secure and resilient cybersecurity future. Here are 5 actions to get you started:

1. Check the minimum requirements of NIS2.
2. Check whether you have certifications in place and conduct a gap analysis.
3. Map and engage with suppliers.
4. Educate the organization.
5. Budget and reporting for success.

1. Please provide your company name:

Enter your answer

Source: Eviden SAS

Questions?

Slawomir Pijanowski, Ph.D, Eviden



Our presentation was kind of simulation of NIS2 Directive audit scope prediction – but it should be sufficient for situational awareness...

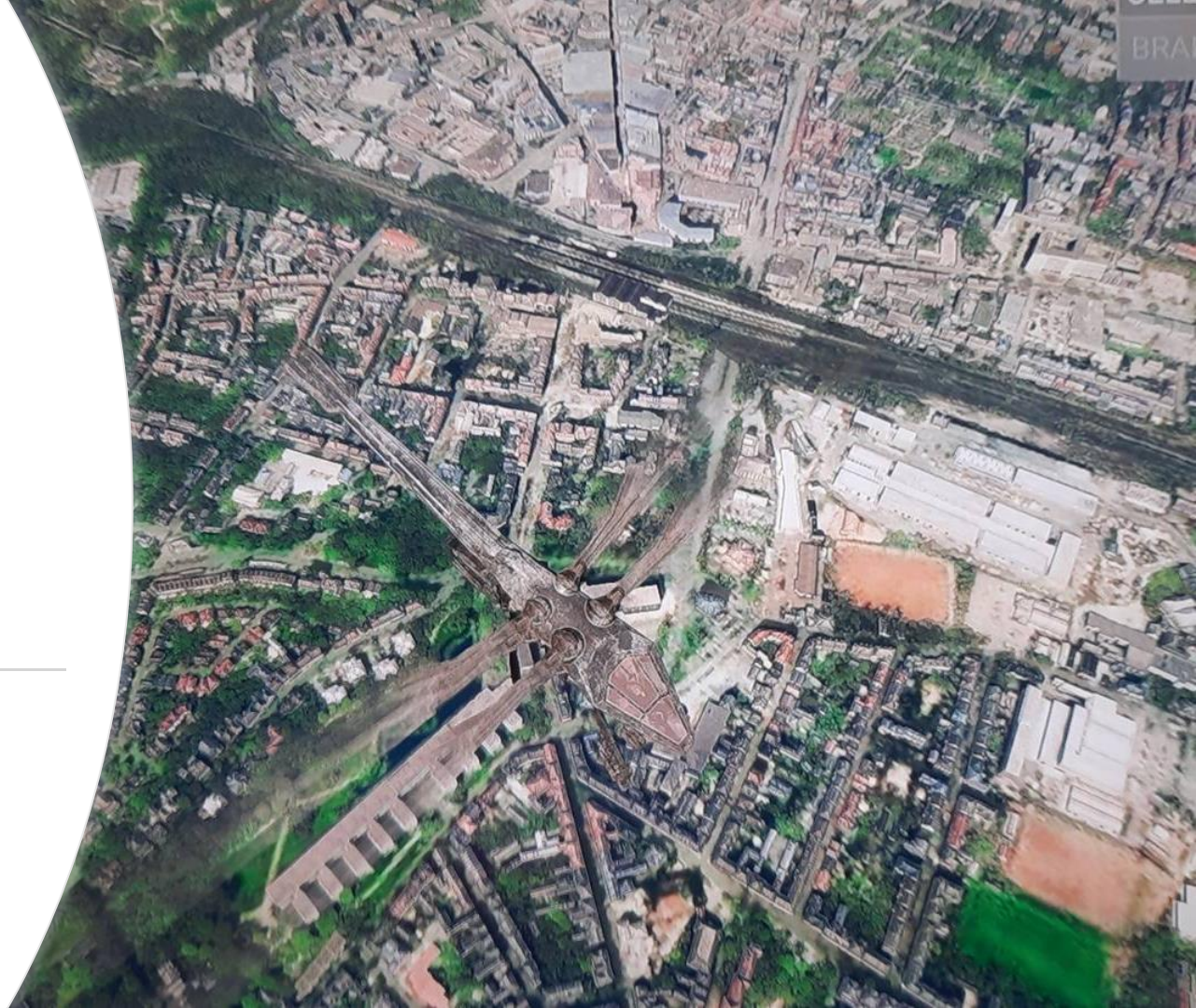


Source of Photos: Slawomir Pijanowski
© Microsoft Simulator 2021 view of Gelsenkirchen
with © Dune Ornithopter.

That's all

**I have to fly
back
to Capital
City of
Arrakis...**

Source of Photos: Slawomir Pijanowski
© Microsoft Simulator 2021 view of Gelsenkirchen
with © Dune Ornithopter.



EVIDEN

Thank you

For more information please contact:



Slawomir PIJANOWSKI, Ph.D. [in](#)

Global GRC Practice Leader,
Global Cybersecurity Consulting,
M +48 513 095 352

slawomir.pijanowski@eviden.com

Confidential information owned by Eviden SAS, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Eviden SAS.

© Eviden SAS – For internal use

Follow Eviden Digital Security:

eviden.com

