CENTRE FOR CYBERSECURITY BELGIUM

TLP:CLEAR

9 April 2026

REF.: NCCA/JK/INS-001

EX-ANTE SUPERVISION OF ESSENTIAL ENTITIES: Request for information for the deadline of 18 April 2026

To all essential NIS2 entities,

With the present letter, the NIS2 inspection service[1] of the Centre for Cybersecurity Belgium (CCB)[2] **clarifies what information must be communicated to the CCB by 18 April 2026 and formally requests all essential NIS2 entities to communicate said information to the CCB** via email to the address certification@ccb.belgium.be. In case of sensitive information, a secure link for file transfer can be requested first.

Since the NIS2 Law entered into force on 18 October 2024, all NIS2 entities must notably take the necessary cybersecurity measures in order to protect their networks and information systems. This includes policies and procedures for assessing the effectiveness of cybersecurity risk-management measures[3]. At the same time, the inspection service has the authority to supervise these entities[4].

The NIS2 inspection service is empowered to monitor compliance by essential and important entities with cybersecurity risk-management measures, in particular by requesting access to and obtaining a copy of any document or information necessary for the performance of its supervisory duties; by conducting, on-site or remotely, any examination, inspection or hearing; and by requesting any information they deem necessary to assess the cybersecurity risk-management measures adopted by the entity concerned. When exercising these powers to request information, the inspection service shall specify the purpose of the request, the precise information or evidence required, and the deadline by which these must be provided[5].

The NIS2 inspection service (NCCA) requests that all essential entities provide the necessary information, as set out below, by 18 April 2026 at the latest, so that it can thoroughly verify the implementation of the cybersecurity risk-management measures.

[1] See the law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security (NIS2 Law).
[2] Designated as the national cybersecurity authority under Article 3, § 1 of the Royal Decree of 9 June 2024 implementing the law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security (NIS2 RD).
[3] Art. 30, § 3, 6° NIS2 Law.
[4] Title 4 of the NIS2 Law.
[5] See notably articles 44, § 1 to 2; 48, § 1; and 50, § 1 of the NIS2 Law.

Information to be communicated to the CCB

Entities that have chosen ISO/IEC 27001 (3 possible scenarios)[6]

1) Scenario 1: The organisation holds an ISO/IEC 27001 certificate issued by an authorised CAB

Your organisation does not need have to do anything else. The CAB will handle the administrative formalities.

2) Scenario 2: The organisation holds an ISO/IEC 27001 certificate issued by a non-authorised CAB

Your organisation must send the following documents to the CCB[7]:

a. Scope of the certificate
b. Statement of Applicability - SoA (including all cybersecurity measures that are being or have been implemented, equivalent to CyFun® Basic level)
c. Latest (internal) audit report in which the implementation of these cybersecurity measures is assessed

Note: from 18 April 2027, the organisation must obtain a certificate issued by an accredited and authorised CAB (the transfer of existing certifications can be carried out if necessary; CABs have procedures in place for this).

3) Scenario 3: The organisation does not yet have an up-to-date ISO/IEC 27001 certification

Your organisation must send the following documents to the CCB[8]:

a. Scope of the future certificate
b. Statement of Applicability - SoA of the future certificate (including all cybersecurity measures that are being or have been implemented, equivalent to CyFun® Basic level)
c. Latest (internal) audit report in which the implementation of these cybersecurity measures is assessed

Note: from 18 April 2027, the organisation must obtain a certificate issued by an accredited and authorised CAB.

Entities that have chosen the CyberFundamentals (CyFun®) Framework (2 possible scenarios)[9]

1) Scenario 1: The organisation already has obtained proof of compliance with at least the CyFun® Basic assurance level from an authorised CAB

The CAB handles the administrative formalities. Your organisation does not need to do anything else.

2) Scenario 2: The organisation has not yet received proof of compliance with at least the CyFun® Basic assurance level from an authorised CAB

We require at least a signed agreement with a CAB for the assurance level CyFun® Basic to be in place before the deadline of 18 April 2026, even if the actual verification will happen only later. You do not need to take any further action than said verification[10].

Entities that have chosen to be directly inspected by the CCB[11]

Your organisation must submit a formal request for an inspection to the CCB (inspection@ccb.belgium.be).

Inspection by the CCB is an alternative option offered to essential entities as part of the regular conformity assessment process, which does not involve the use of a CAB. It should nevertheless be noted that this option is less advantageous for the entities concerned, as it **does not provide a presumption of conformity**. It is therefore a purely ad hoc control which the entity cannot rely on in the same way as a verification or certification carried out

[6] Art. 39, subpar. 1, 1° NIS2 Law and art. 5, § 1, 2° NIS2 RD.
[7] Art. 22, § 1, 2° NIS2 RD, read together with art. 44, § 1 to 2; 48, § 1; and 50, § 1 NIS2 Law.
[8] Art. 22, § 1, 2° NIS2 RD, read together with art. 44, § 1 to 2; 48, § 1; and 50, § 1 NIS2 Law.
[9] Art. 39, subpar. 1, 1° NIS2 Law and art. 5, § 1, 1° NIS2 RD.
[10] Art. 22, § 1, 1° NIS2 RD
[11] Art. 39, subpar. 1, 2° NIS2 Law; art. 5, § 1 and 23, § 1 NIS2 RD.

by a CAB to defend itself in the event of an incident. Indeed, it will **still be up to the entity to prove that it is complying with its obligations**[12]. If an essential entity holds a certification, for example, it is up to the CCB to prove that the entity is not meeting its obligations. It is therefore a considerable advantage to have such a presumption of conformity.

The conformity assessment carried out directly by the CCB **takes the form of an inspection procedure (with possible administrative measures and sanctions)**[13] **and is not free of charge**[14] - except for entities in the public administration sector referred to in Annex I of the NIS2 law, and which are not covered by Article 1 of the Royal Decree of 4 May 2016 establishing the Federal Internal Audit Service (audit by the FIA as a NIS2 CAB).

Yours sincerely,

Johan Klykens (Signature)
Digitally signed by Johan Klykens (Signature)
Date: 2026.04.09 13:17:17 +02'00'

Johan KLYKENS
Director
National Cybersecurity Certification Authority (NCCA) – NIS2 Inspection Service
Centre for Cybersecurity Belgium

[12] Art. 42 NIS2 Law.
[13] Art. 48 and following NIS2 Law.
[14] Art. 20 NIS2 RD.

What is your response deadline?

You are required to respond within the specified deadline[15]. We may extend the response deadline upon receipt of a formal written request from you. However, you must demonstrate that you have legitimate grounds for doing so:

- a valid reason showing that more time is needed to gather evidence
- a serious illness or long-term absence
- a case of force majeure

How should you respond?

You may send your response to us:

- by post: CCB - NCCA – NIS2 Inspection service
  Rue de la Loi 18, 1000 Brussels
- by email: certification@ccb.belgium.be

  Does your response contain files that are too large or too sensitive to be sent by email? In that case, please contact us so that we can provide you with a data transfer service.

Are you late, failing to respond, or providing an incomplete response?

As the law requires you to respond within the specified deadline, we may then impose an administrative measure[16] or a fine[17].

What supporting documents are required?

You may choose not to send the requested supporting documents with your reply. In that case, we will verify these documents at your address. This will not result in any administrative measure or fine. However, you must contact us within the specified deadline to arrange an appointment.

Do you have any questions?

You can always contact us for further information. The legislation referred to in this letter can be consulted at the following address: https://www.ejustice.just.fgov.be/.

Protection of your personal data?

To find out more about how we process your personal data in accordance with privacy regulations, please visit the CCB website: https://ccb.belgium.be/personal-data.

[15] Article 44, § 2 NIS2 law.
[16] Article 58 NIS2 law.
[17] Article 59 NIS2 law.