De nieuwe cybersecuritynorm ISO 27001

7 december 2022

Standaard voor vooruitgang

Code of Conduct

- Het webinar wordt opgenomen
- De presentaties worden na afloop beschikbaar gesteld
- Tijdens het webinar staan je camera en microfoon automatisch uit
- Vragen stellen via de Q&A
- Mogelijkheid gestelde vragen te upvoten met duimpje
- Indien je inbelt via de laptop/mobiel ipv de zoomlink kun je alleen luisteren

Programma

16.00 Welkom
16.10 Nieuwe versie van ISO 27001
16.30 Gevolgen van certificatie op basis van ISO 27001
16.50 Afsluiting

Sprekers

Theo de Breed

Risk Knowledge

Christian Oudenbroek

Brand Compliance

Inge Piek

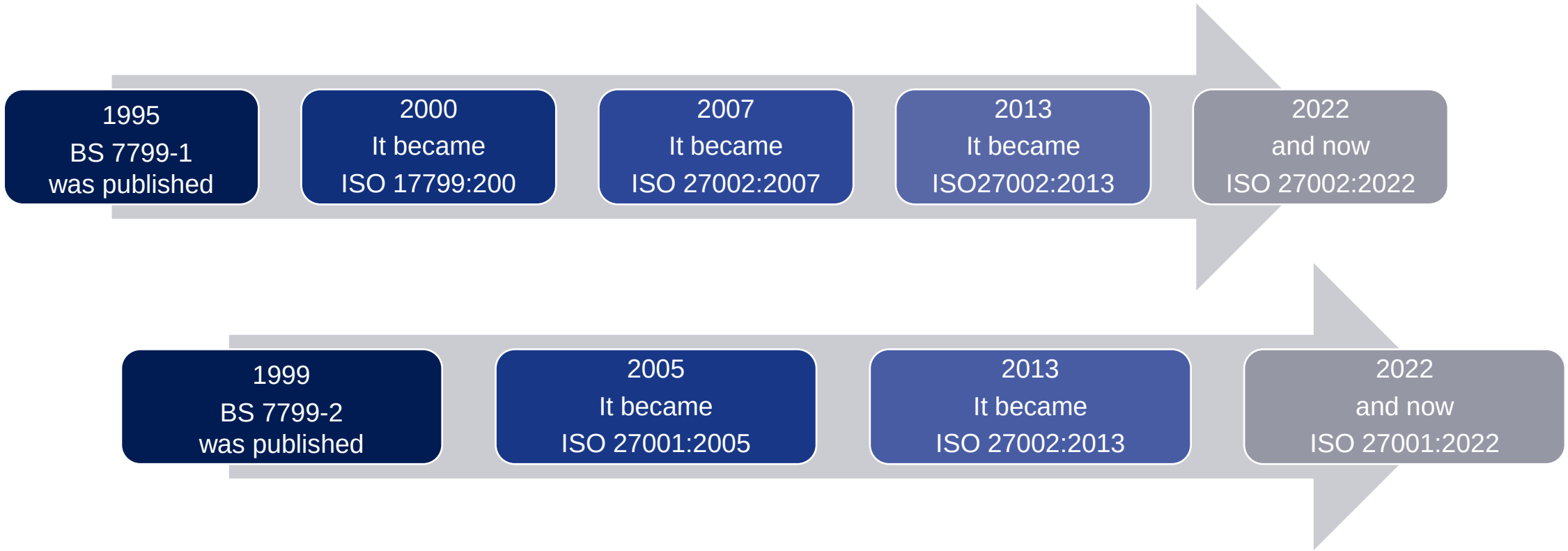
NEN

Nieuwe editie van ISO 27001

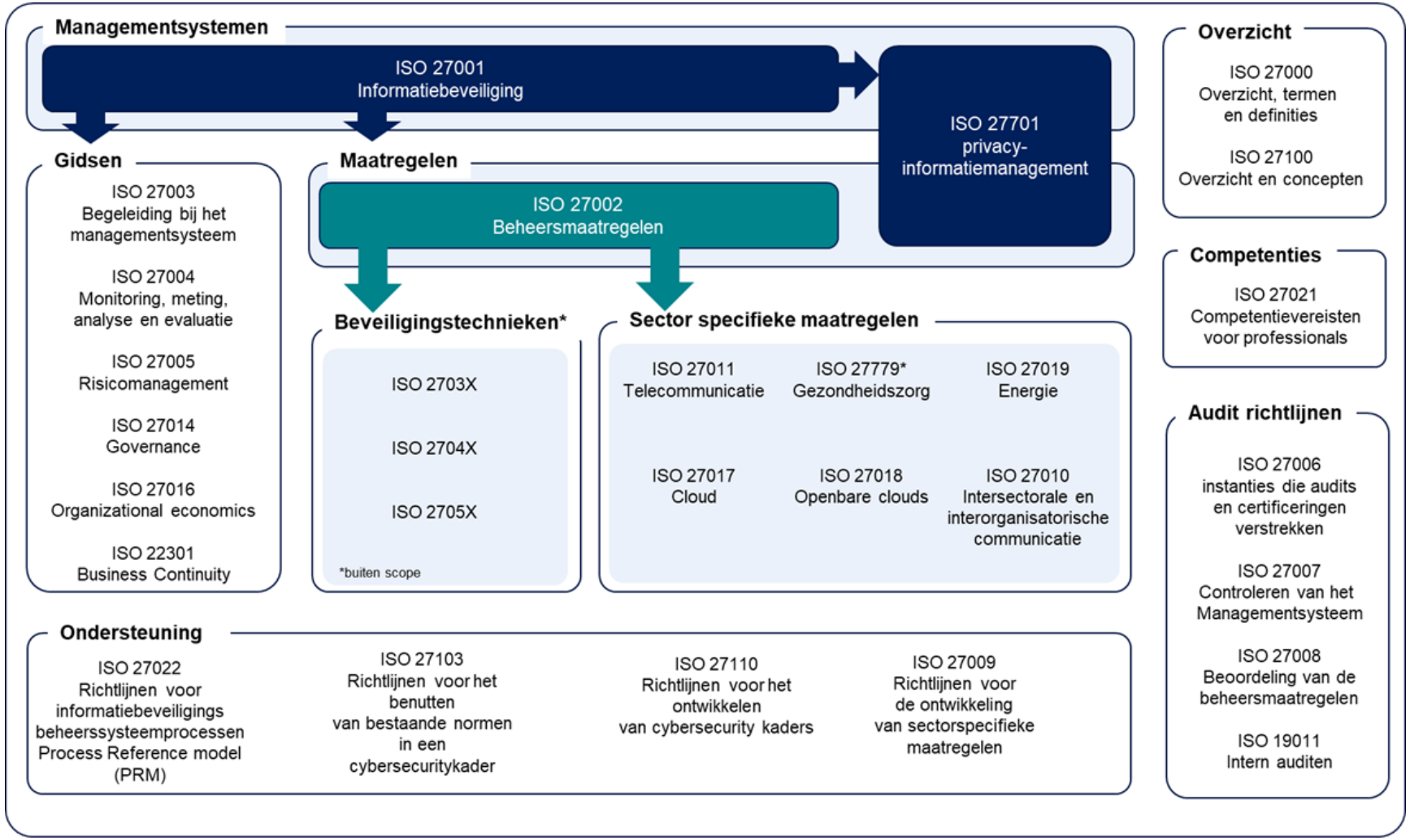
Theo de Breed

Risk Knowledge

Geschiedenis ISO 27002 / 27001



De ISO27K familie

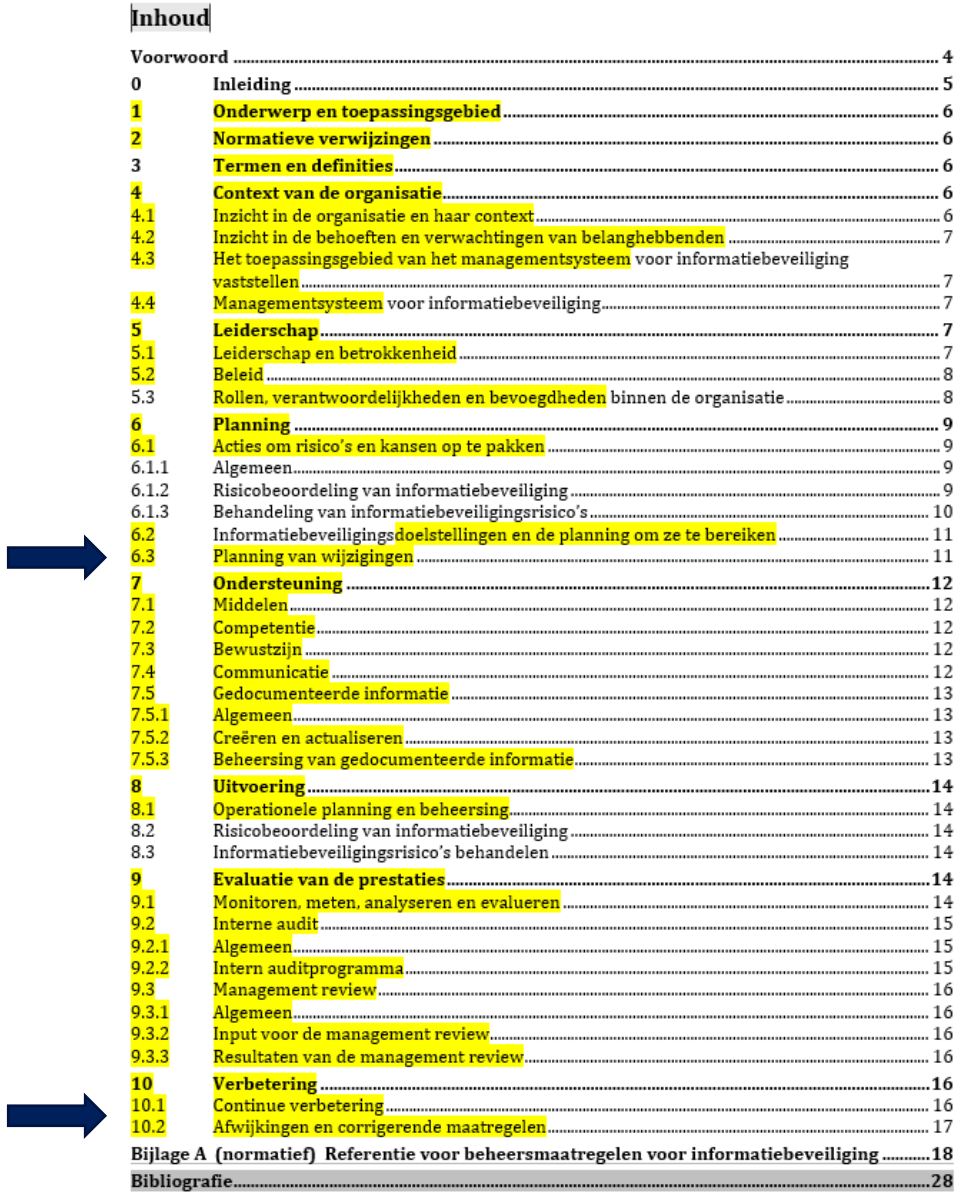


Wijzigingen ISO 27001 - naamgeving

ISO/IEC 27001:2013	ISO/IEC 27001:2022
Information technology – Security techniques – Information security management systems - Requirements	Information security, cybersecurity and privacy protection – Information security management systems - Requirements

Wijzigingen ISO 27001: Indeling

- Nieuw paragraaf 6.3 planning van wijzigingen
- Paragraaf 10.1 and 10.2 zijn gewisseld



Inhoud

Voorwoord 4
0 Inleiding 5
1 Onderwerp en toepassingsgebied 6
2 Normatieve verwijzingen 6
3 Termen en definities 6
4 Context van de organisatie 6
4.1 Inzicht in de organisatie en haar context 6
4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden 7
4.3 Het toepassingsgebied van het managementsysteem voor informatiebeveiliging vaststellen 7
4.4 Managementsysteem voor informatiebeveiliging 7
5 Leiderschap 7
5.1 Leiderschap en betrokkenheid 7
5.2 Beleid 8
5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie 8
6 Planning 9
6.1 Acties om risico's en kansen op te pakken 9
6.1.1 Algemeen 9
6.1.2 Risicobeoordeling van informatiebeveiliging 9
6.1.3 Behandeling van informatiebeveiligingsrisico's 10
6.2 Informatiebeveiligingsdoelstellingen en de planning om ze te bereiken 11
6.3 Planning van wijzigingen 11
7 Ondersteuning 12
7.1 Middelen 12
7.2 Competentie 12
7.3 Bewustzijn 12
7.4 Communicatie 12
7.5 Gedocumenteerde informatie 13
7.5.1 Algemeen 13
7.5.2 Creëren en actualiseren 13
7.5.3 Beheersing van gedocumenteerde informatie 13
8 Uitvoering 14
8.1 Operationele planning en beheersing 14
8.2 Risicobeoordeling van informatiebeveiliging 14
8.3 Informatiebeveiligingsrisico's behandelen 14
9 Evaluatie van de prestaties 14
9.1 Monitoren, meten, analyseren en evalueren 14
9.2 Interne audit 15
9.2.1 Algemeen 15
9.2.2 Intern auditprogramma 15
9.3 Management review 16
9.3.1 Algemeen 16
9.3.2 Input voor de management review 16
9.3.3 Resultaten van de management review 16
10 Verbetering 16
10.1 Continue verbetering 16
10.2 Afwijkingen en corrigerende maatregelen 17
Bijlage A (normatief) Referentie voor beheersmaatregelen voor informatiebeveiliging 18
Bibliografie 28

Wijzigingen ISO 27001: Termen en definities

ISO/IEC 27001:2013	ISO/IEC 27001:2022
3 Terms and definitions For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.	**3 Terms and definitions** For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply. ISO and IEC maintain terminology databases for use in standardization at the following addresses: • ISO Online browsing platform: available at https://www.iso.org/obp • IEC Electropedia: available at https://www.electropedia.org

Wijzigingen ISO 27001
Nieuwe relevante eisen, 4.2

ISO/IEC 27001:2013	ISO/IEC 27001:2022
4.2 Understanding the needs and expectations of interested parties The organization shall determine: a) interested parties that are relevant to the information security management system; b) and the requirements of these interested parties relevant to information security.	**4.2 Understanding the needs and expectations of interested parties** The organization shall determine: a) interested parties that are relevant to the information security management system; b) the relevant requirements of these interested parties; c) which of these requirements will be addressed through the information security management system.

Wijzigingen ISO 27001
Meer focus op processen, 4.4

ISO/IEC 27001:2013	ISO/IEC 27001:2022
4.4 Information security management system The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.	**4.4 Information security management system** The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document.

Wijzigingen ISO 27001
Nieuwe eisen, 6.2 Objectives

ISO/IEC 27001:2013	ISO/IEC 27001:2022
6.2 Information security objectives and planning to achieve them The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall: a) be consistent with the information security policy; b) be measurable (if practicable); c) take into account applicable information security requirements, and results from risk assessment and risk treatment; d) be communicated; and e) be updated as appropriate.	**6.2 Information security objectives and planning to achieve them** The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall: a) be consistent with the information security policy; b) be measurable (if practicable); c) take into account applicable information security requirements, and results from risk assessment and risk treatment; d) be monitored; e) be communicated; f) be updated as appropriate; g) be available as documented information.

Wijzigingen ISO 27001
Planning van wijzigingen, 6.3

ISO/IEC 27001:2013	ISO/IEC 27001:2022
-	**6.3 Planning of changes** When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.

Wijzigingen ISO 27001
Nieuwe eisen, 7.4 Communicatie

ISO/IEC 27001:2013	ISO/IEC 27001:2022
7.4 Communication The organization shall determine the need for internal and external communications relevant to the information security management system including: a) on what to communicate; b) when to communicate; c) with whom to communicate; d) who shall communicate; and e) the processes by which communication shall be effected.	**7.4 Communication** The organization shall determine the need for internal and external communications relevant to the information security management system including: a) on what to communicate; b) when to communicate; c) with whom to communicate; **d) how to communicate.**

Wijzigingen ISO 27001
Nieuwe eisen, 8.1 Operationele planning

ISO/IEC 27001:2013	ISO/IEC 27001:2022
8.1 Operational planning and control The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2. The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned. The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. The organization shall ensure that outsourced processes are determined and controlled.	**8.1 Operational planning and control** The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by: • establishing criteria for the processes; • implementing control of the processes in accordance with the criteria. Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned. The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.

Wijzigingen ISO 27001
Nieuwe eisen, 9.1 Monitoring

ISO/IEC 27001:2013	ISO/IEC 27001:2022
9.1 Monitoring, measurement, analysis and evaluation … The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.	**9.1 Monitoring, measurement, analysis and evaluation** … Documented information shall be available as evidence of the results. The organization shall evaluate the information security performance and the effectiveness of the information security management system.

Wijzigingen ISO 27001
Nieuwe structuur, 9.2 en 9.3

ISO/IEC 27001:2013	ISO/IEC 27001:2022
9.2 Internal audit **9.3 Management review**	**9.2 Internal audit** **9.2.1 General** **9.2.2 Internal audit programme** **9.3 Management review** **9.3.1 General** **9.3.2 Management review inputs** **9.3.3 Management review results** + new input for management review c) changes in needs and expectations of interested parties that are relevant to the information security management system

Wijzigingen ISO 27001
Nieuwe bijlage A. Beheersmaatregelen

Annex A
(normative)

Information security controls reference

The information security controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2022[1], Clauses 5 to 8, and shall be used in context with 6.1.3.

Table A.1 — Information security controls

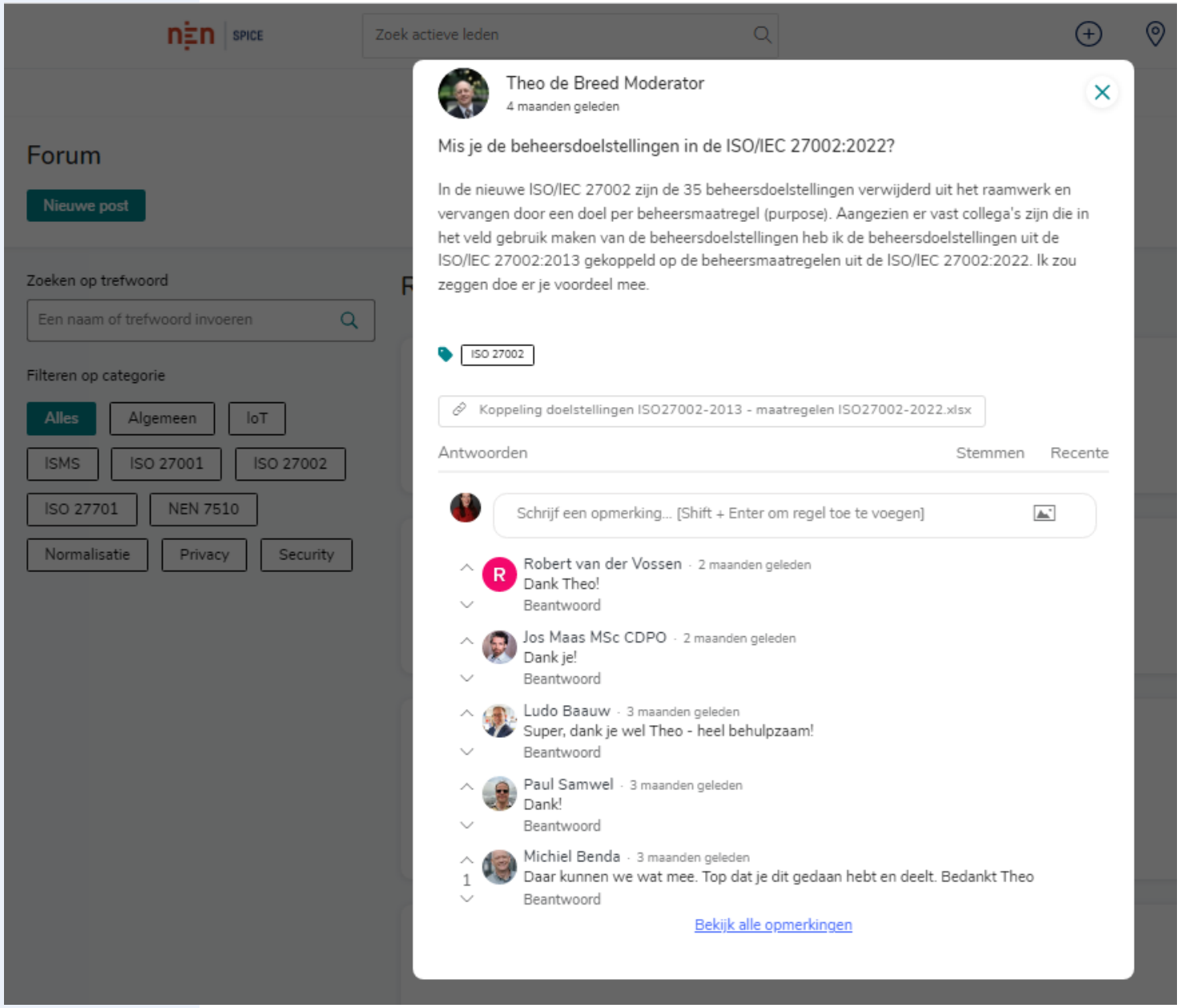
A.5	**Organizational controls**	
A.5.1	Policies for information security	**Control** Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.
A.5.2	Information security roles and responsibilities	**Control** Information security roles and responsibilities shall be defined and allocated according to the organization needs.
A.5.3	Segregation of duties	**Control** Conflicting duties and conflicting areas of responsibility shall be segregated.

SPICE - community

Standards, Privacy, Information & Cyber Engagement

Vragen en antwoorden

https://nen.hivebrite.com/page/welcome



Tijd voor vragen

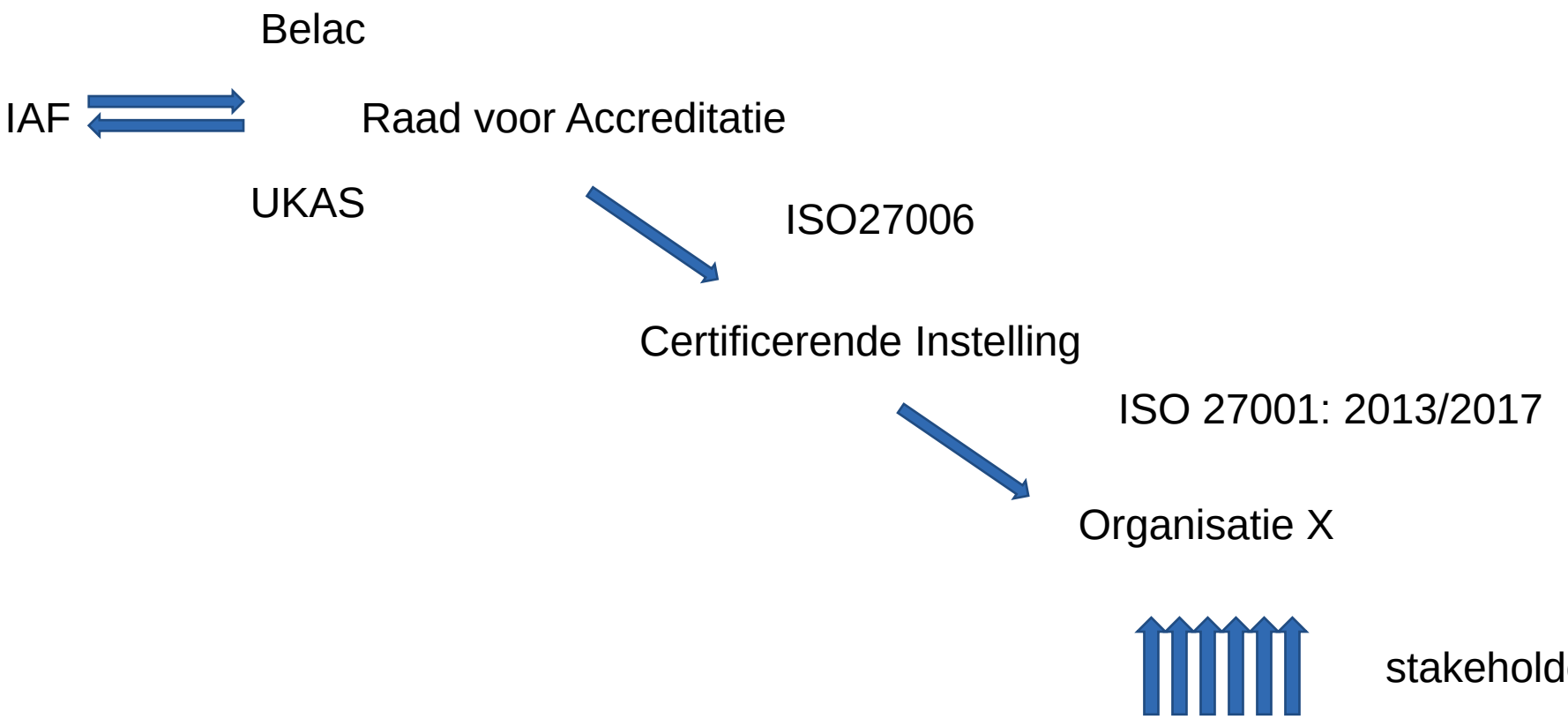
Standaard voor vooruitgang

Gevolgen voor certificatie op basis van ISO 27001

Christian Oudenbroek

CEO Brand Compliance BV

Borging en uniformiteit



IAF Mandatory Document

TRANSITION REQUIREMENTS FOR ISO/IEC 27001:2022

Issue 1

(IAF MD 26:2022)

Regels voor:

- Accreditatie Instelling
- Certificerende Instelling
- Gecertificeerde organisatie X

Data

Belangrijkste data uit de MD26:

• Voor 1 november 2023 moeten de CI's geaccrediteerd zijn voor certificatie tegen de nieuwe versie.

• De certificaathouders kunnen uiterlijk tot eind oktober 2025 tegen de oude versie van de norm zijn gecertificeerd.

• Vanaf 12 maanden na publicatie, dus vanaf 1 november 2023 mogen door CI's geen initiële (of hercertificatie audits) meer worden uitgevoerd tegen de ISO/IEC 27001:2013 of NEN-EN ISO/IEC 27001:2017+A11:2020.

Gelijk speelveld

Simultaan besluit

De uitbreidingsaanvragen die voor 15 december 2022 zijn aangeleverd bij de RvA, zullen in een simultaan traject worden beoordeeld.

Er is gekozen voor een simultaan besluit om het speelveld voor de geaccrediteerde certificerende instellingen zo gelijk mogelijk te houden.

Voor de CI’s waar geen afwijking(en) worden vastgesteld in dit onderzoek, wordt op 1 februari 2023 een simultaan besluit genomen.

De CI’s waar wel afwijkingen worden vastgesteld, krijgen de gelegenheid om corrigerende maatregelen te nemen. Voor deze CI’s zal het simultaan besluit op 1 juni 2023 genomen worden.

IAF MD26 Transition audit

1) De CI’s kunnen de overgangsaudit uitvoeren in combinatie met de toezichtsaudit, de hercertificeringsaudit of via een afzonderlijke audit.

2) De overgangsaudit is niet alleen gebaseerd op een documentenbeoordeling, met name voor de beoordeling van de technologische controles.

IAF MD26 Transition audit

3) De overgangsaudit omvat, maar is niet beperkt tot het volgende:

- GAP analyse van ISO/IEC 27001:2022, alsmede de noodzaak van wijzigingen in het ISMS;
- De actualisering van de verklaring van toepasselijkheid (SoA)
- Indien van toepassing, het bijwerken van het risicobehandelingsplan
- De uitvoering en doeltreffendheid van de nieuwe of gewijzigde controles die door de organisatie zijn gekozen.

4) De CI’s kunnen de overgangsaudit op afstand uitvoeren indien zij ervoor zorgen dat de doelstellingen van de overgangsaudit gehaald worden.

Tijd voor vragen

Standaard voor vooruitgang

Afsluiting

Inge Piek

Normcommissie Cybersecurity en privacy

1. Informatiebeveiliging
2. Cryptografie
3. Testing en controls
4. IoT Product security
5. Privacy en Data protection

https://www.nen.nl/normcommissie-cybersecurity-privacy

Normcommissie Cybersecurity en privacy

Nederlandse vertalingen

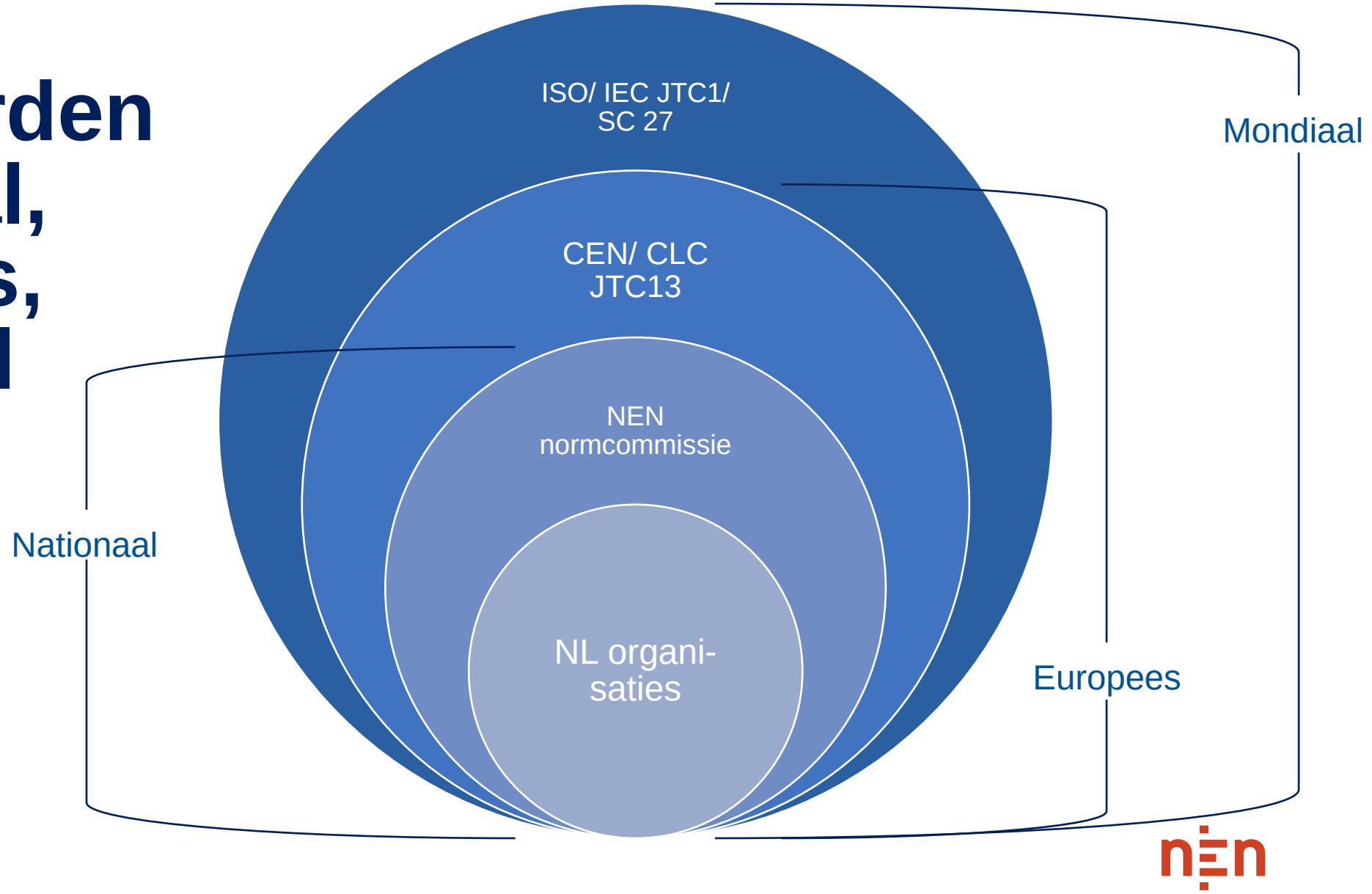
- **ISO/IEC 27001:2022 nl** (Link)

Informatiebeveiliging, cybersecurity en bescherming van de privacy - Managementsysteem voor informatiebeveiliging – Eisen

- **NEN-EN-ISO/IEC 27002:2022 nl** (Link)

Informatiebeveiliging, cybersecurity en bescherming van de privacy - Beheersmaatregelen voor informatiebeveiliging

Standaarden Nationaal, europees, mondiaal

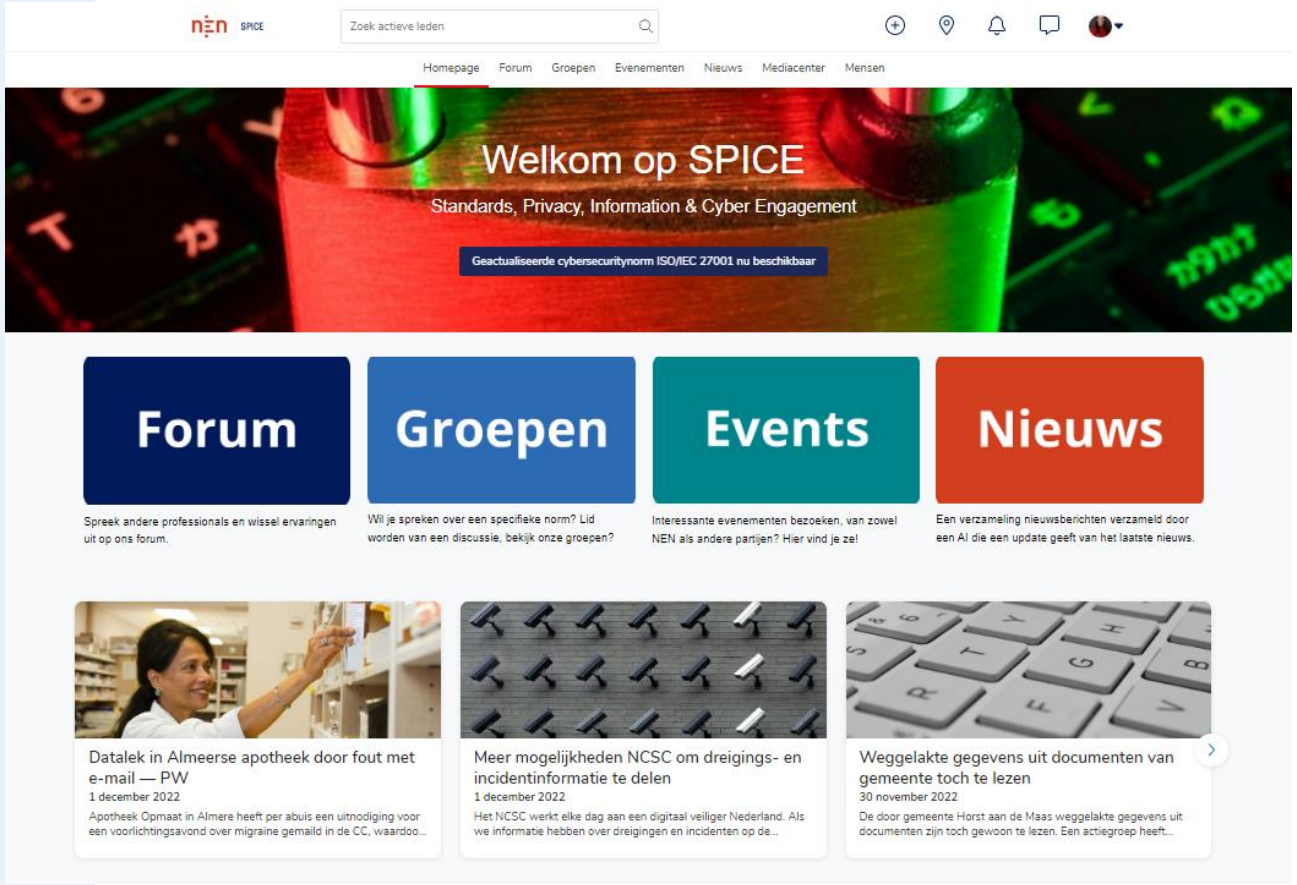


SPICE - COMMUNITY

Standards, Privacy,

Information & Cyber Engagement

https://nen.hivebrite.com/page/welcome



NEN – ICT Standards

- Informatiebeveiliging, cybersecurity en privacy
- Informatiebeveiliging in de zorg
- Artificial intelligence
- Data opslaan en uitwisselen
- Digitale vaardigheden

www.nen.nl

https://www.nen.nl/ict/normcommissies

Informatiebijeenkomsten

- NEN 7545 Gegevensuitwisseling in de zorg - verpleegkundige overdracht
- Richtlijn voor inzicht in resultaten agile softwareontwikkeling
- Europese standaarden voor quantum technologieën

https://www.nen.nl/agenda-evenementen

Bedankt voor het deelnemen!

De presentaties en de opname worden zo snel mogelijk toegestuurd.

Voor meer informatie, neem contact op met:

Inge Piek, kid@nen.nl

Standaard voor
vooruitgang

De nieuwe cybersecuritynorm ISO 27001

7 december 2022

Standaard voor vooruitgang