# NEN Meets PvIB

Themabijeenkomst

2021-11-11

Standaard voor vooruitgang

# Agenda

**Normalisatie**

Het normenlandschap van informatiebeveiliging

**Privacy**

Privacy normen, ISO 27701 en de verfijningen

**Certificatie**

Het certificeringsproces en de waarde van ISO 27701

Normalisatie

# Profielschets

Stichting

# Nederlands Normalisatie Instituut

1916

Opgericht

2016

Koninklijk

300

Medewerkers

550

Commissies

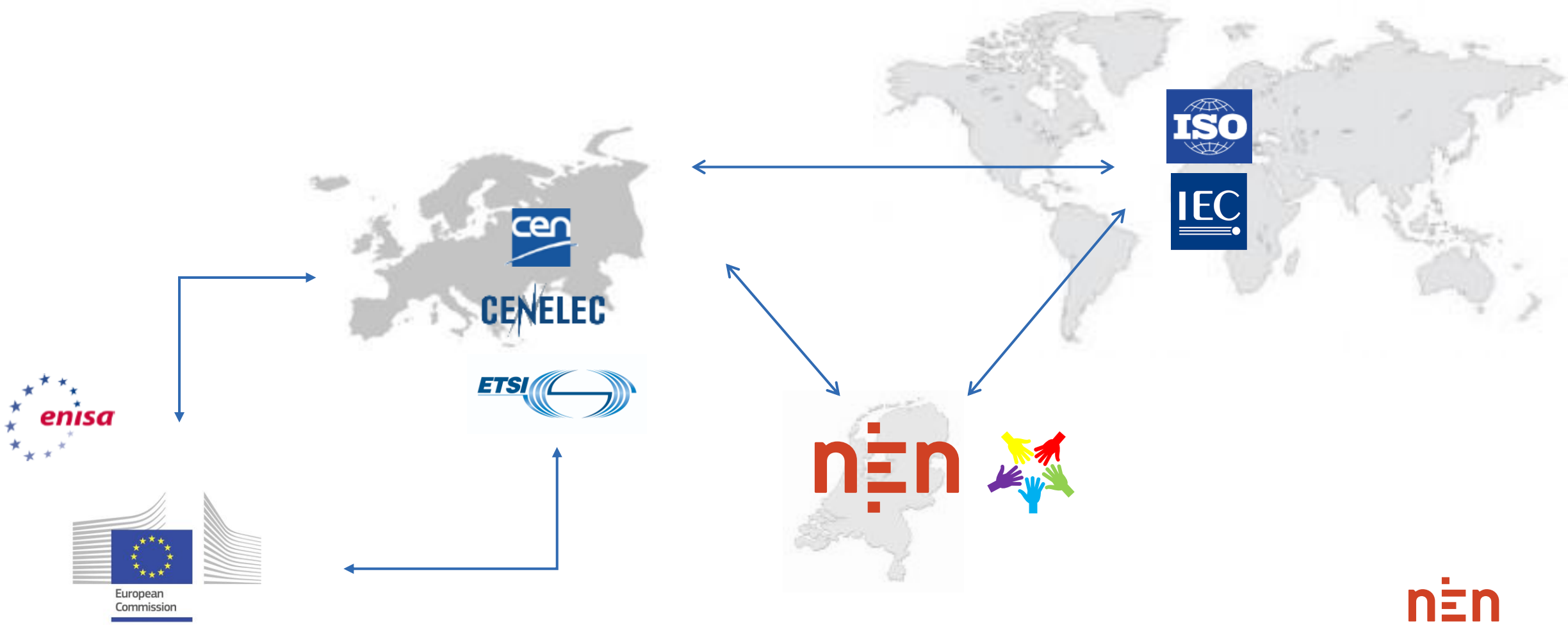
6.200

Experts

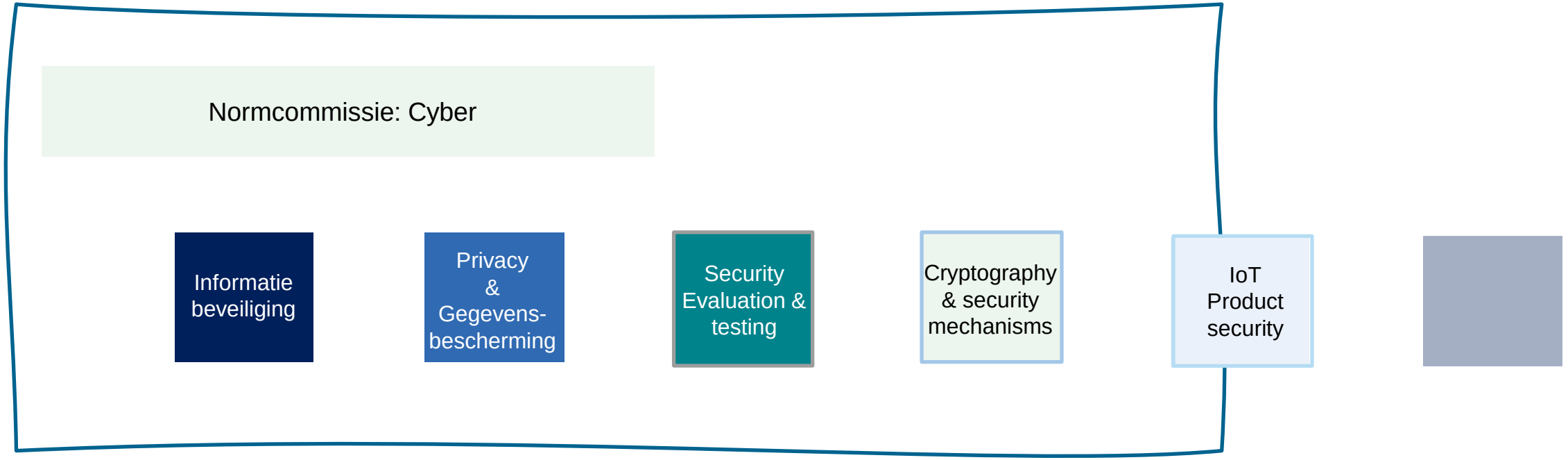
30.000

Normen

# Omgeving normalisatie



# Commissie & werkgroepen




Sterre Bierens

Tom Hoogendijk

Roeland Roeterdink

Pim Pasman

# Normalisatie

asdf


*NEN webinar, september 2020, Martin Vliem

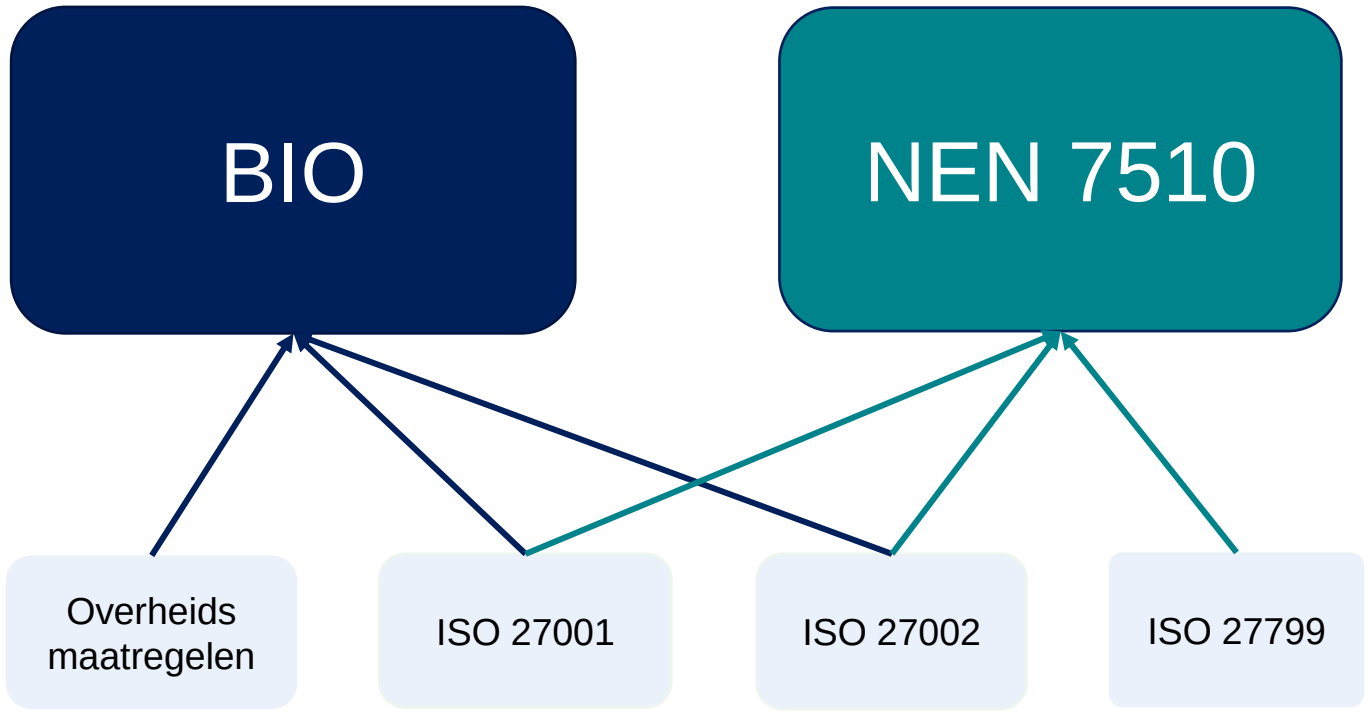
# Bekende normen?

ISO 27001

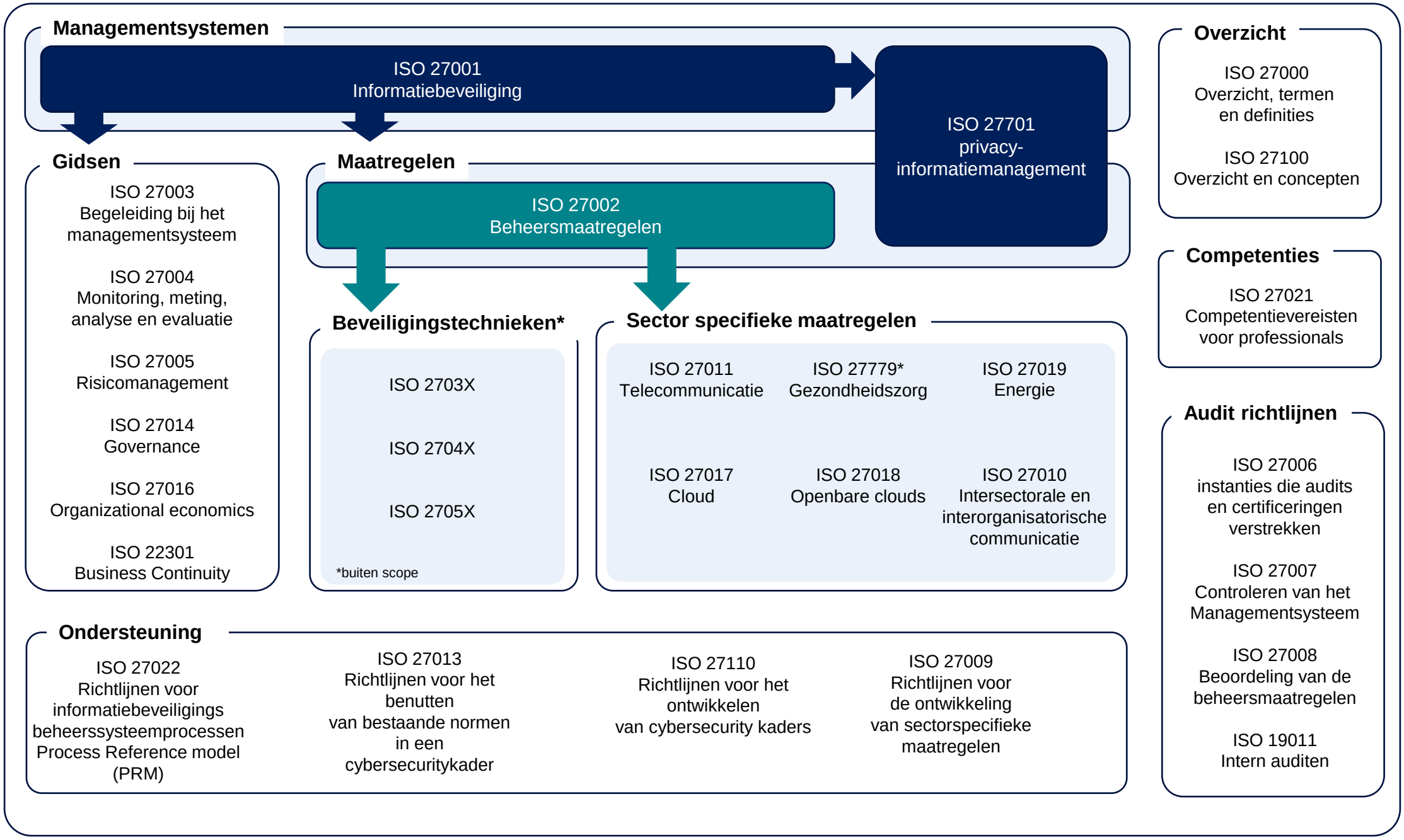
ISO 27002

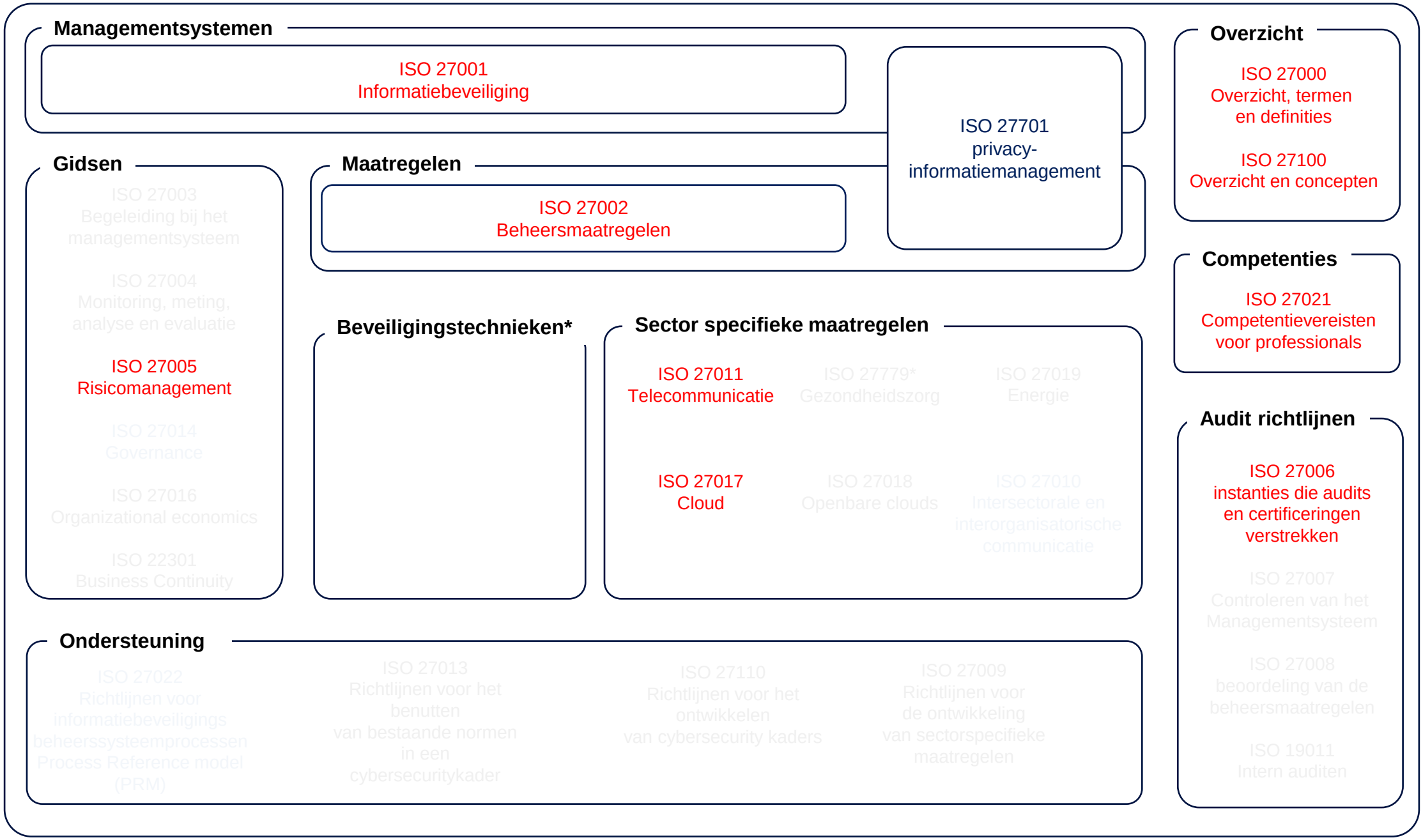
ISO 27701

# Overheid & Zorg



# Bekende normen in perspectief


Managementsystemen
ISO 27001
Informatiebeveiliging
ISO 27701
privacy-
informatiemanagement
Gidsen
ISO 27003
Begeleiding bij het managementsysteem
ISO 27004
Monitoring, meting, analyse en evaluatie
ISO 27005
Risicomanagement
ISO 27014
Governance
ISO 27016
Organizational economics
ISO 22301
Business Continuity
Maatregelen
ISO 27002
Beheersmaatregelen
Beveiligingstechnieken*
ISO 2703X
ISO 2704X
ISO 2705X
*buiten scope
Sector specifieke maatregelen
ISO 27011
Telecommunicatie
ISO 27779*
Gezondheidszorg
ISO 27019
Energie
ISO 27017
Cloud
ISO 27018
Openbare clouds
ISO 27010
Intersectorale en interorganisatorische communicatie
Ondersteuning
ISO 27022
Richtlijnen voor informatiebeveiligings beheerssysteemprocessen Process Reference model (PRM)
ISO 27013
Richtlijnen voor het benutten van bestaande normen in een cybersecuritykader
ISO 27110
Richtlijnen voor het ontwikkelen van cybersecurity kaders
ISO 27009
Richtlijnen voor de ontwikkeling van sectorspecifieke maatregelen
Overzicht
ISO 27000
Overzicht, termen en definities
ISO 27100
Overzicht en concepten
Competenties
ISO 27021
Competentievereisten voor professionals
Audit richtlijnen
ISO 27006
instanties die audits en certificeringen verstrekken
ISO 27007
Controleren van het Managementsysteem
ISO 27008
Beoordeling van de beheersmaatregelen
ISO 19011
Intern auditen


Managementsystemen
ISO 27001
Informatiebeveiliging
ISO 27701
privacy-
informatiemanagement
Overzicht
ISO 27000
Overzicht, termen
en definities
ISO 27100
Overzicht en concepten
Gidsen
ISO 27003
Begeleiding bij het
managementsysteem
ISO 27004
Monitoring, meting,
analyse en evaluatie
ISO 27005
Risicomanagement
ISO 27014
Governance
ISO 27016
Organizational economics
ISO 22301
Business Continuity
Maatregelen
ISO 27002
Beheersmaatregelen
Competenties
ISO 27021
Competentievereisten
voor professionals
Beveiligingstechnieken*
Sector specifieke maatregelen
ISO 27011
Telecommunicatie
ISO 27779*
Gezondheidszorg
ISO 27019
Energie
ISO 27017
Cloud
ISO 27018
Openbare clouds
ISO 27010
Intersectorale en
interorganisatorische
communicatie
Audit richtlijnen
ISO 27006
instanties die audits
en certificeringen
verstrekken
ISO 27007
Controleren van het
Managementsysteem
ISO 27008
beoordeling van de
beheersmaatregelen
ISO 19011
Intern auditen
Ondersteuning
ISO 27022
Richtlijnen voor
informatiebeveiligings
beheerssysteemprocessen
Process Reference model
(PRM)
ISO 27013
Richtlijnen voor het
benutten
van bestaande normen
in een
cybersecuritykader
ISO 27110
Richtlijnen voor het
ontwikkelen
van cybersecurity kaders
ISO 27009
Richtlijnen voor
de ontwikkeling
van sectorspecifieke
maatregelen

# Aanleiding

*De huidige 27002 te veel werd gebruikt als checklist en het te weinig uitnodigde tot nadenken*


*ISO/IEC 27002:2021 EN*

# Gevolg Europees

**Europese overname**

~~*ISO/IEC 27002:2021 EN*~~

***EN*** *ISO/IEC 27002 :2021 EN*

# Gevolg nationaal

**Vertaling**
**ISO 27002**

**Herziening**
**NEN 7510**

***NEN-****EN-ISO/IEC 27002:2021 EN*
***NEN-****EN-ISO/IEC 27002:2021 NL*

# Route & voortgang

Informatiebeveiliging

# Structuur ISO 27002

| | |
|---|---|
| 0 | Introduction |
| 1 | Scope |
| 2 | Normative references |
| 3 | Terms, definitions and abbreviated terms |
| 4 | Structure of this document |
| ***5*** | |
| ***6*** | |
| ***7*** | |
| ***8*** | |
| A | Using attributes |
| B | Correspondence with 27002:2013 |



***5. Organizational controls***

***6. People controls***

***7. Physical controls***

***8. Technological controls***

Informatiebeveiliging

# Maatregelen

5.7 Threat Intelligence
5.23 Information security for use of cloud services
5.30 ICT readiness for business continuity

7.4 Physical security monitoring

8.9 Configuration management
8.10 Information deletion
8.11 Data masking
8.12 Data leakage prevention
8.16 Monitoring activities
8.23 Web filtering
8.28 Secure coding

*Totaal aantal maatregelen*

**93**

*Nieuwe maatregelen*

**11**

# Invloed op ISO standaarden

**ISO 27001**

**Aanpassing bijlage A**

**ISO documenten**

**Stroomlijnen overige**

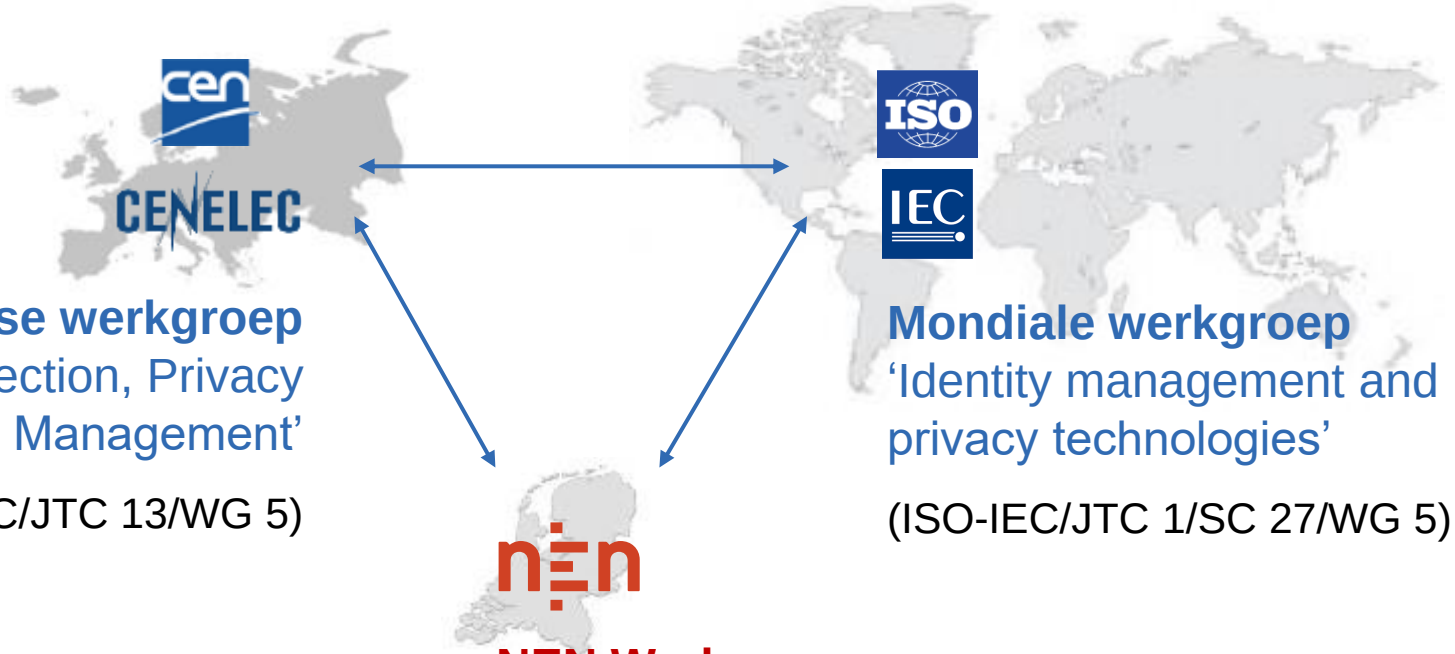
# Hoe ziet de overgang eruit?

Er zal sprake zijn van een overgangsperiode, dit is gebruikelijk bij de herziening van een norm.
Bij de vorige herziening was dit een periode van 2 jaar.

Eventueel behaalde certificeringen op de oude versie zijn niet waardeloos bij de publicatie van de nieuwe versie.


ISO 27701
Privacy en gegevensbescherming

# De wereld van normalisatie



**Europese werkgroep**
‘Data protection, Privacy and Identity Management’

(CEN-CLC/JTC 13/WG 5)

**Mondiale werkgroep**
‘Identity management and privacy technologies’

(ISO-IEC/JTC 1/SC 27/WG 5)

**NEN Werkgroep**
‘Privacy en gegevensbescherming’

(Onderdeel van normcommissie ‘Cybersecurity & Privacy’)

## Privacy en gegevensbescherming

# Wat is ISO 27701?

De norm specificeert eisen en geeft richtlijnen voor het inrichten, implementeren, onderhouden en continu verbeteren van een Privacy Informatie Management Systeem (PIMS).

De norm is ontwikkeld waarbij een expliciete koppeling mogelijk wordt gemaakt tussen een ISMS en de AVG.

Met ISO 27701 waarborg je niet alleen je eigen informatie, maar maak je ook aantoonbaar dat je de privacy van anderen beschermd.

Een wereldwijde standaard.

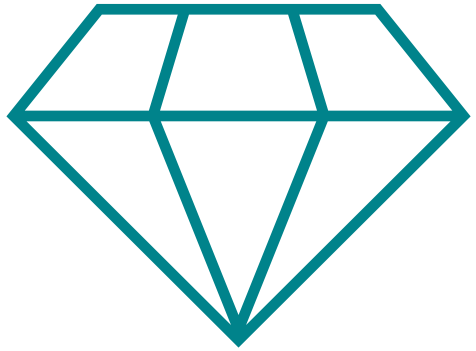
Voor wie:

- Organisaties die werken met PII.
- Verwerkingsverantwoordelijke en/of verwerker.

# Waarde van ISO 27701

Het is een goede manier om privacy in te bedden in uw organisatie door het op te nemen als managementsysteem.

Praktisch kader waarmee het bestaande *ISMS* met een *PIMS* wordt uitgebreid.

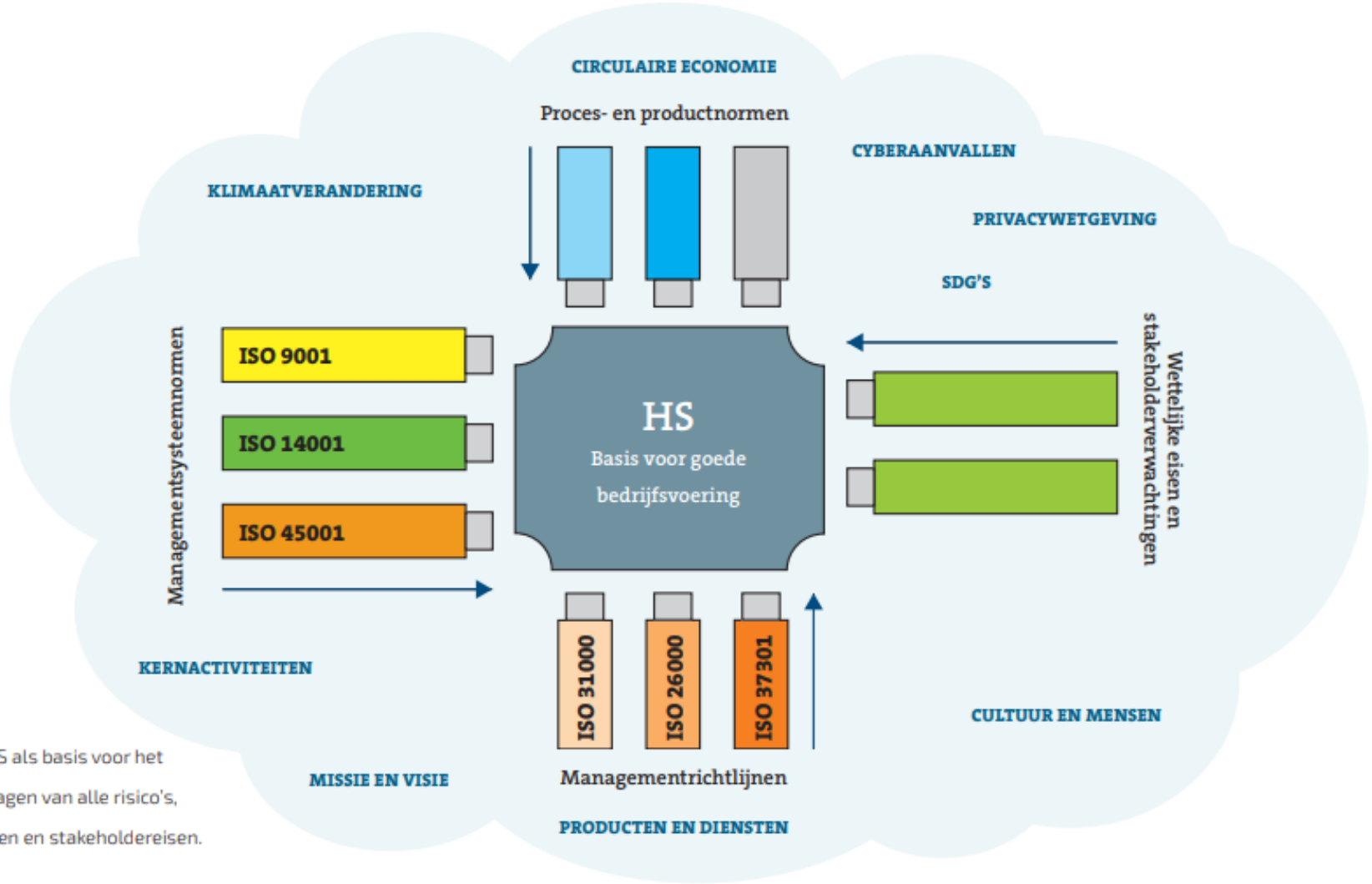


Biedt transparantie over huidige controles voor het beheer van de privacy.

Vergemakkelijkt overeenkomsten met zakelijke partners waar de verwerking van PII's wederzijds relevant is.

Verduidelijkt rolverdeling en verantwoordelijkheden bij het managen van persoonsgegevens.

# Geharmoniseerde structuur




De HS als basis voor het managen van alle risico's, kansen en stakeholdereisen.

De basisstructuur van alle ISO managementsystemen

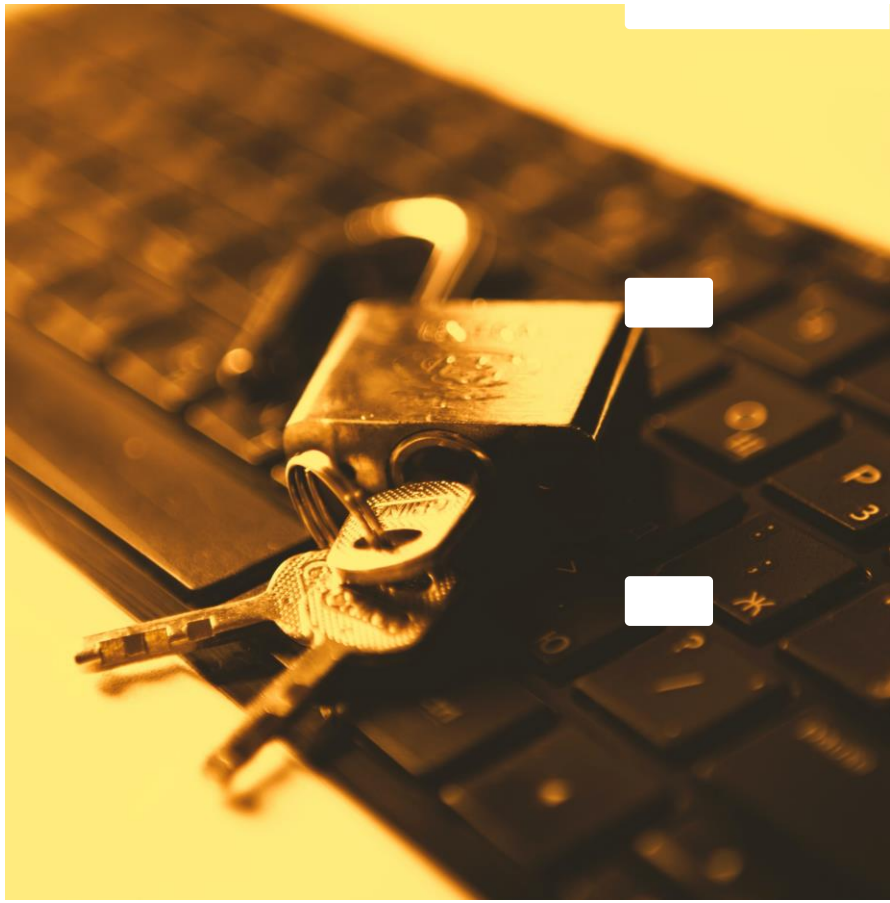
Eenduidige structuur

Vergemakkelijkt het integreren van managementsystemen

# Relatie met ISO 27001?


- Uitbreiding (extensie) van de ISO27001.
- Toetsing op de eisen is alleen mogelijk in combinatie met de eisen uit ISO 27001 en ISO 27002.

# Relatie met de AVG



- Bijlage D van ISO 27701: ‘mapping to the GDPR’.

- Toekomst:
  - EU komt met meer wetgeving op digitaal en privacy gebied
  - Blijven ISO en CEN in lijn? Welke zou meeste invloed hebben op praktijk in NL?

ISO 27001
ISO 27002

**Information technology - Security Techniques - Information security management systems**

+

ISO/IEC 27701

**Extension to ISO 27001 and ISO/IEC 27002 for privacy information management**

ISO 27006

**Requirements for bodies providing audit and certification of information security management systems**

+

ISO 27006-2
*in ontwikkeling*

**Part 2: PIMS**

Gepubliceerd:
ISO/IEC TS 27006-2

**Aansluiting van NEN experts op Europees werk**

NCS 27701

**Eisen aan instellingen die audits ten behoeve van certificatie van PIMS uitvoeren conform ISO/IEC 27701**

EN 17529
*in afronding*

**Data protection and privacy by design and by default**

**Aansluiting van NEN experts op Europees werk**





ISO/IEC 27701

**Extension to ISO 27001 and ISO/IEC 27002 for privacy information management**

EN xxxxx

**Refinement of ISO 27701 in European context**

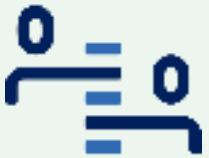
**Aansluiting van NEN experts op Europees werk**

# Certificatie

# Wanneer is certificatie slim?

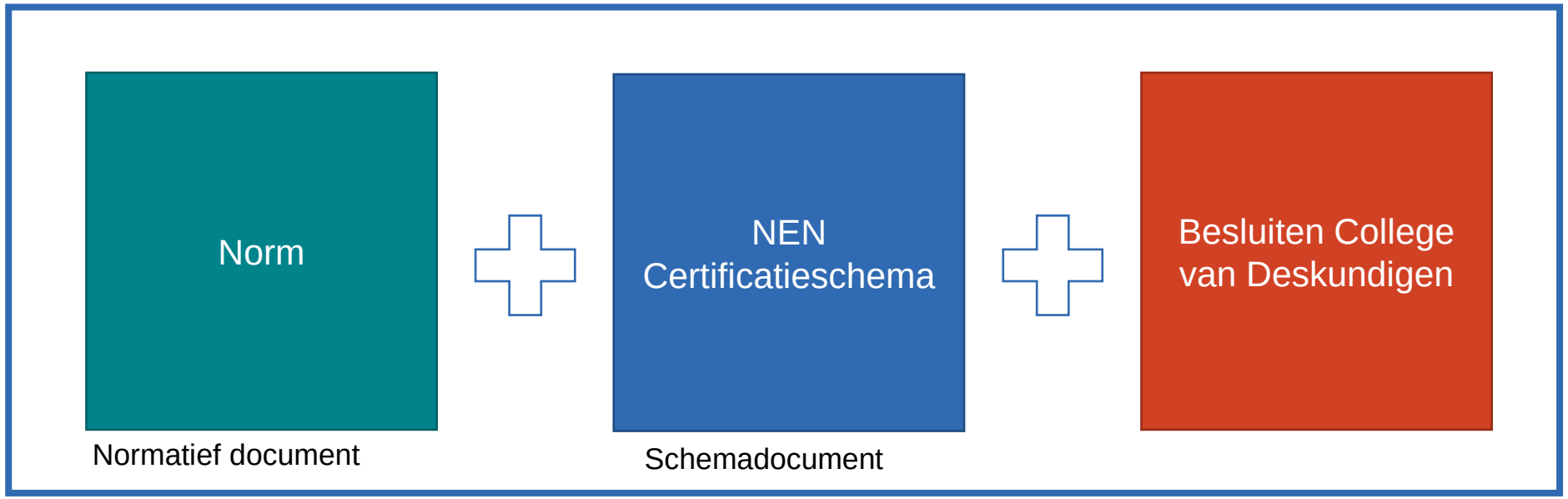
**Er is een behoefte om zich te onderscheiden met betrouwbaar bewijs waarmee kan worden aangetoond te voldoen aan de eisen uit de norm.**

**Partijen (brancheverenigingen, overheid) gaan het certificaat/keurmerk of het (aantoonbaar) voldoen aan een norm verplicht stellen.**



**Er gaat iets mis! Een certificaat of keurmerk biedt garantie dat het goed geregeld is.**

# De basis van een certificaat



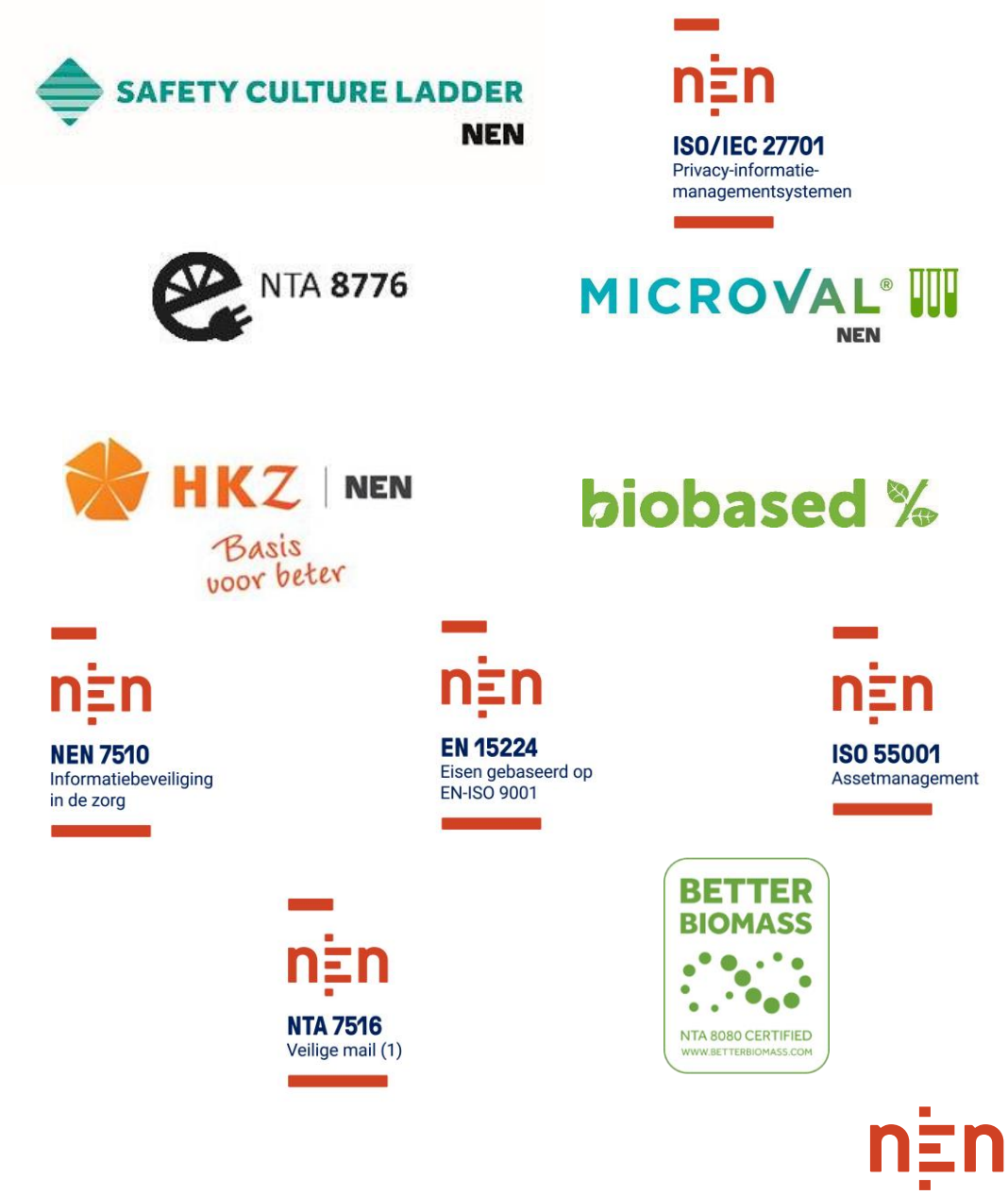

Bron: NTA 8813 art 3.6

# Vertrouwen toevoegen

Certificatie

# Zichtbaar bewijs

Een certificaat of keurmerk toont aan dat een product, systeem, persoon of proces voldoet aan de eisen van een norm.



Certificatie

# ISMS-familie van normen

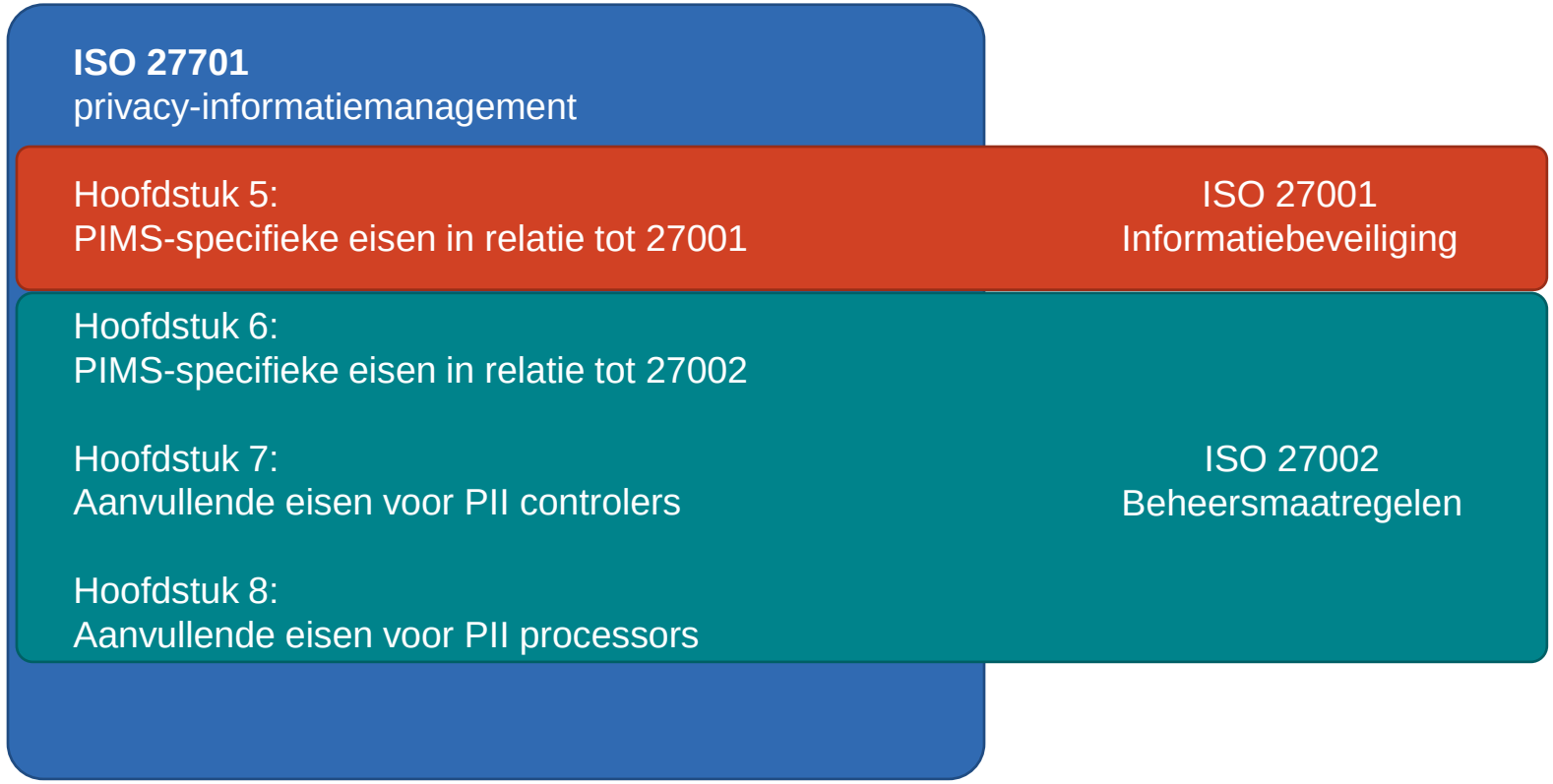
- **NEN-EN-ISO/IEC 27001** Information technology - Security techniques - Information security management systems – Requirements
- **NEN-EN-ISO/IEC 27002** Information technology - Security techniques - Code of practice for information security controls
- **NEN-EN-ISO/IEC 27006** Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems

- **NEN-EN-ISO/IEC 27701** Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines
- …

Certificatie

# Controle als organisatie

# Koppeling


ISO 27701
privacy-informatiemanagement
Hoofdstuk 5:
PIMS-specifieke eisen in relatie tot 27001
ISO 27001
Informatiebeveiliging
Hoofdstuk 6:
PIMS-specifieke eisen in relatie tot 27002
Hoofdstuk 7:
Aanvullende eisen voor PII controlers
Hoofdstuk 8:
Aanvullende eisen voor PII processors
ISO 27002
Beheersmaatregelen

# Certificatie

# Perspectief

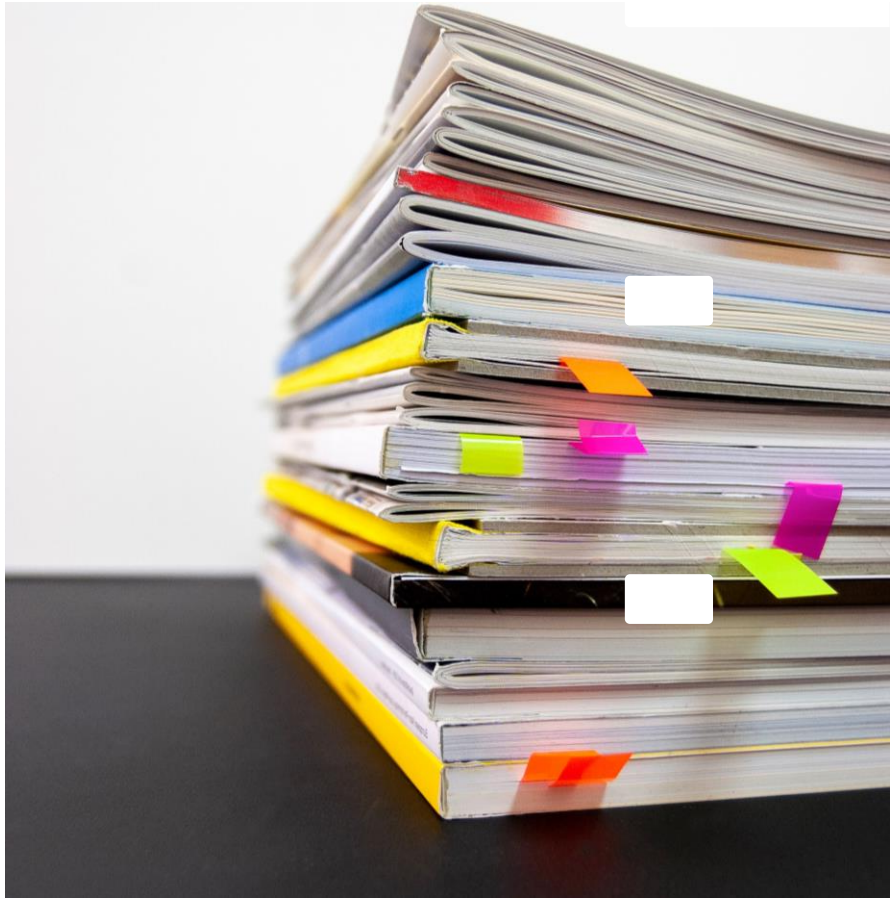
- Uitbreiding met gevolgen?
  - Welke aspecten toegevoegd?
  - Welke overwegingen anders?
  - Welke belangen anders?

- Scope van het 27001 certifcaat

Certificatie

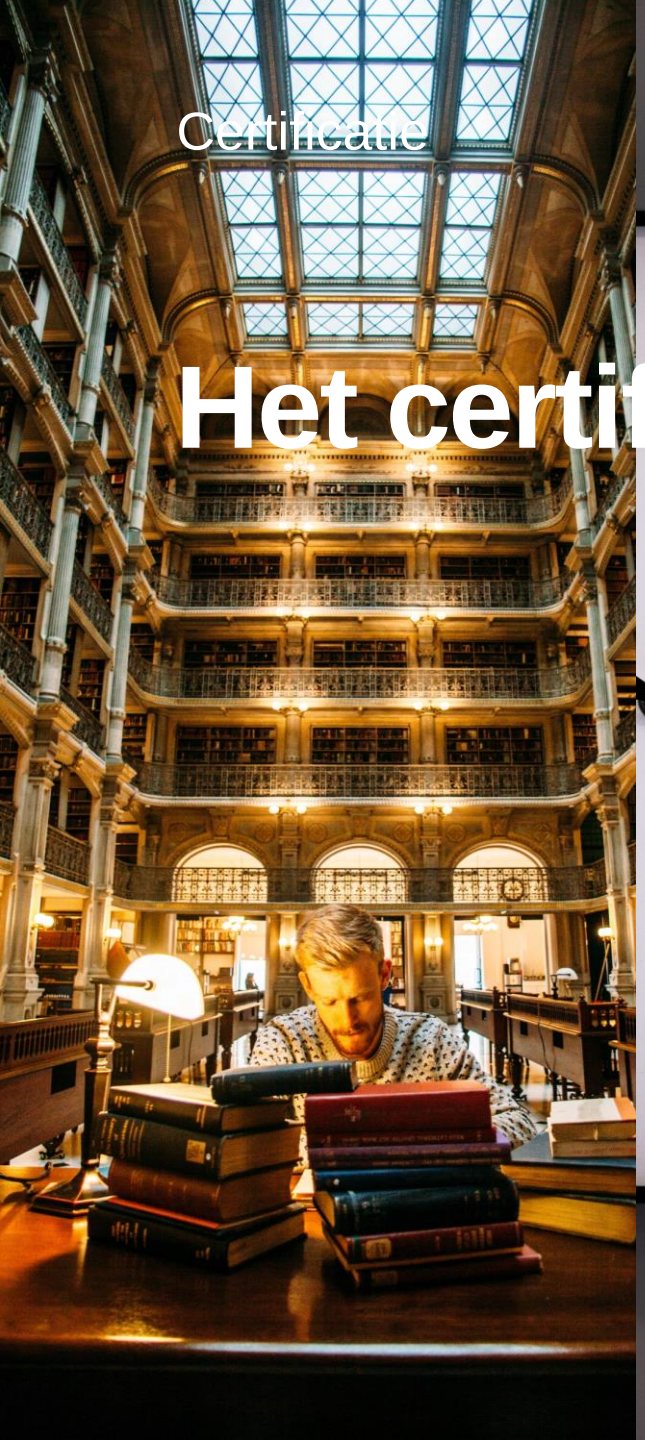
# Certificatieschema

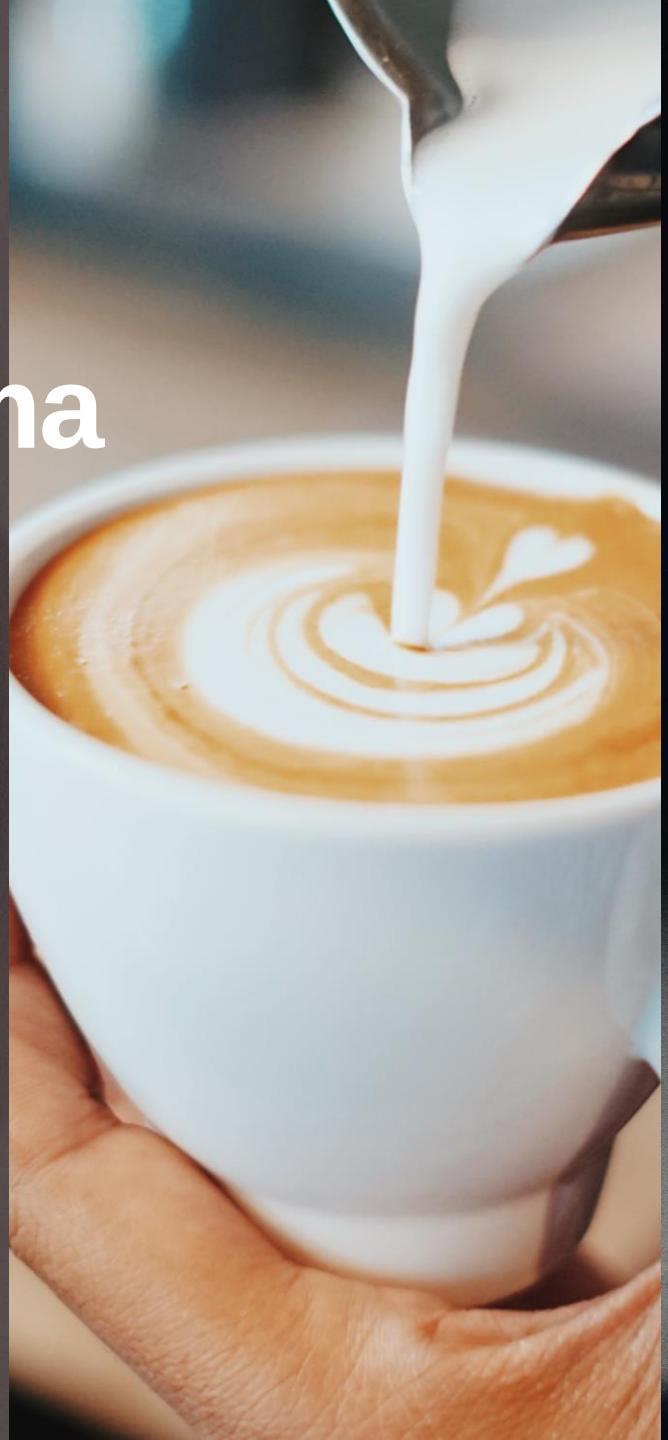
Toetsing door certificerende instelling van ISO 27701

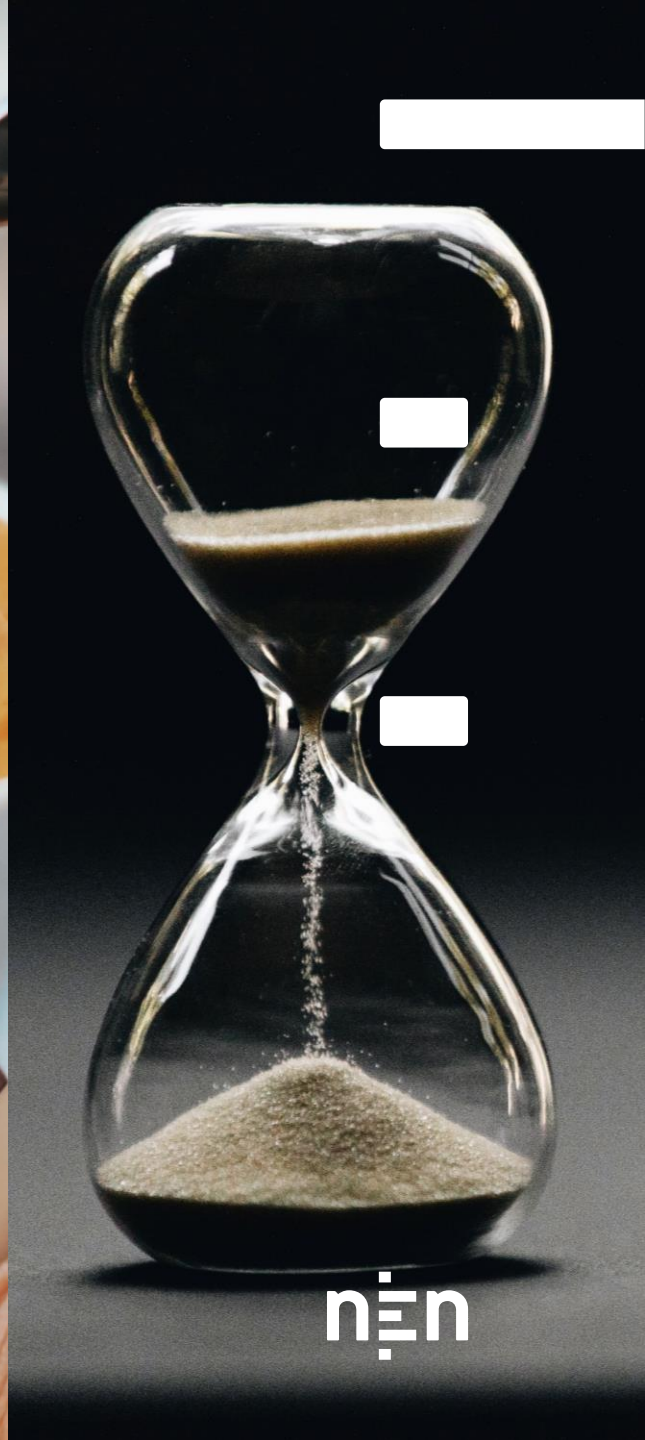


Certificatie

# Het certificatieschema







# NEN register

- Drie certificerende instellingen:
  - TüV Nederland
  - Kiwa
  - Brand Compliance
- Openbaar register

## Wie zijn gecertificeerd?

**Bekijk hieronder het overzicht.**

Het register bevat alle organisaties die in het bezit zijn van een certificaat. Certificaten worden afgegeven voor een periode van drie jaar, waarbij tenminste jaarlijks een opvolgingsonderzoek plaatsvindt.

Zoeken:

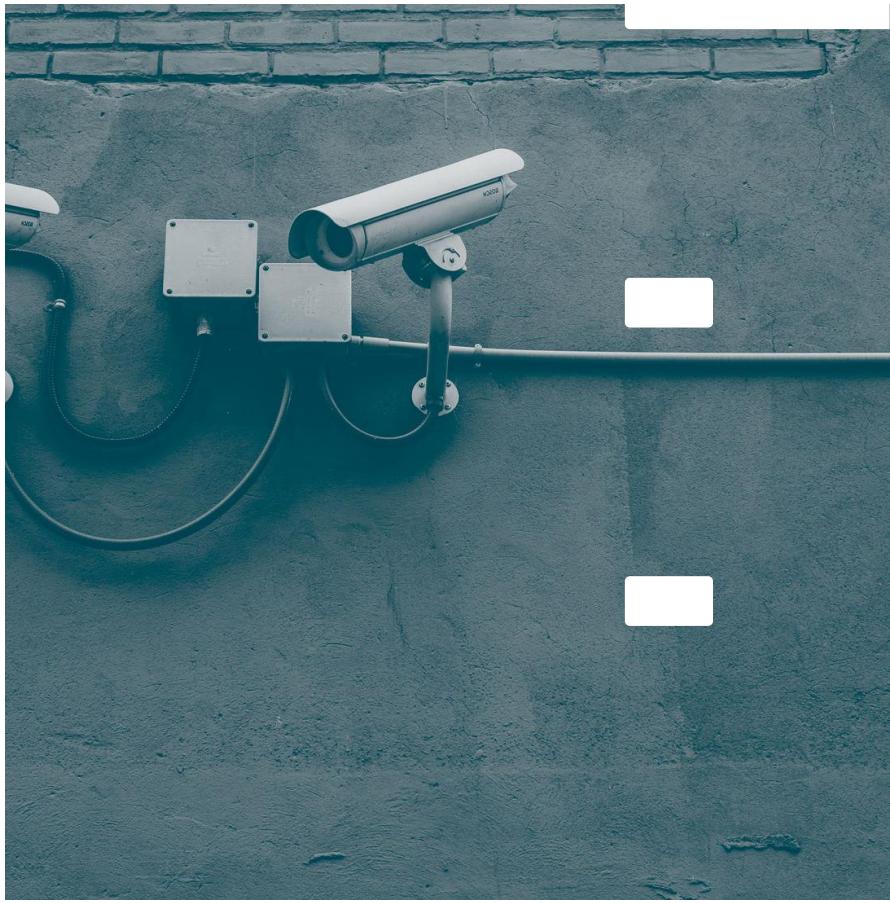
| Organisatie | Gecertificeerd sinds | Certificerende instelling | Status |
|---|---|---|---|
| Alterdesk B.V. | 2020-12-16 | TÜV Nederland | Valid |
| Hartis Telezorg B.V. | 2020-12-16 | KIWA Nederla | Valid |
| Zaurus B.V. | 2020-12-16 | TÜV Nederland | Valid |

25 resultaten weergeven

Vorige 1 Volgende

# Wat is nodig voor certificering?

- ISO 27001 is verplicht
- Analyse en uitbreiding van het managementsysteem
- Scope van certificering eventueel aanpassen
- Interne audits



# Vragen aan de zaal

- Wat is jullie ervaring met 27701?
- Waar lopen jullie tegen aan?
- Hoe zien jullie de ontwikkelingen van Europese wetgeving op privacy?
- Hoe kan NEN helpen?


Interesse in de mogelijkheden van certificaten en keurmerken?
Voor meer informatie ga direct naar
nen.nl/certificaten >
Standaard voor vooruitgang
nen

Standaard voor
vooruitgang