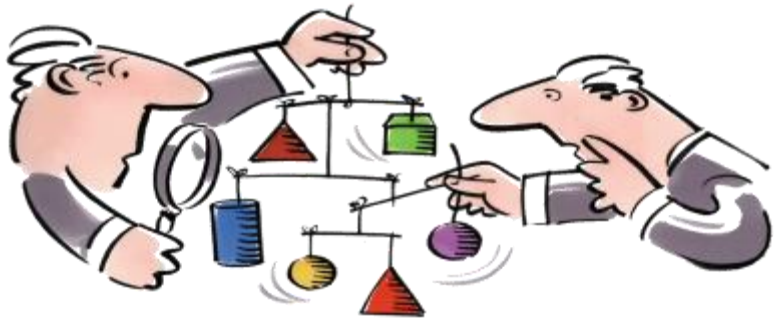
De nieuwe NEN7510: 2017 – een introductie

Jan Willem Schoemaker,

CISO/Business Continuity Manager Erasmus MC

Agenda

1. ‘Schoten voor de boeg’
2. Nut van de NEN7510
3. Uitgangspunten en inhoud nieuwe NEN 7510
4. Consequenties voor certificatie
5. Vragen / discussie



World's Biggest Data Breaches

Selected losses greater than 30,000 records

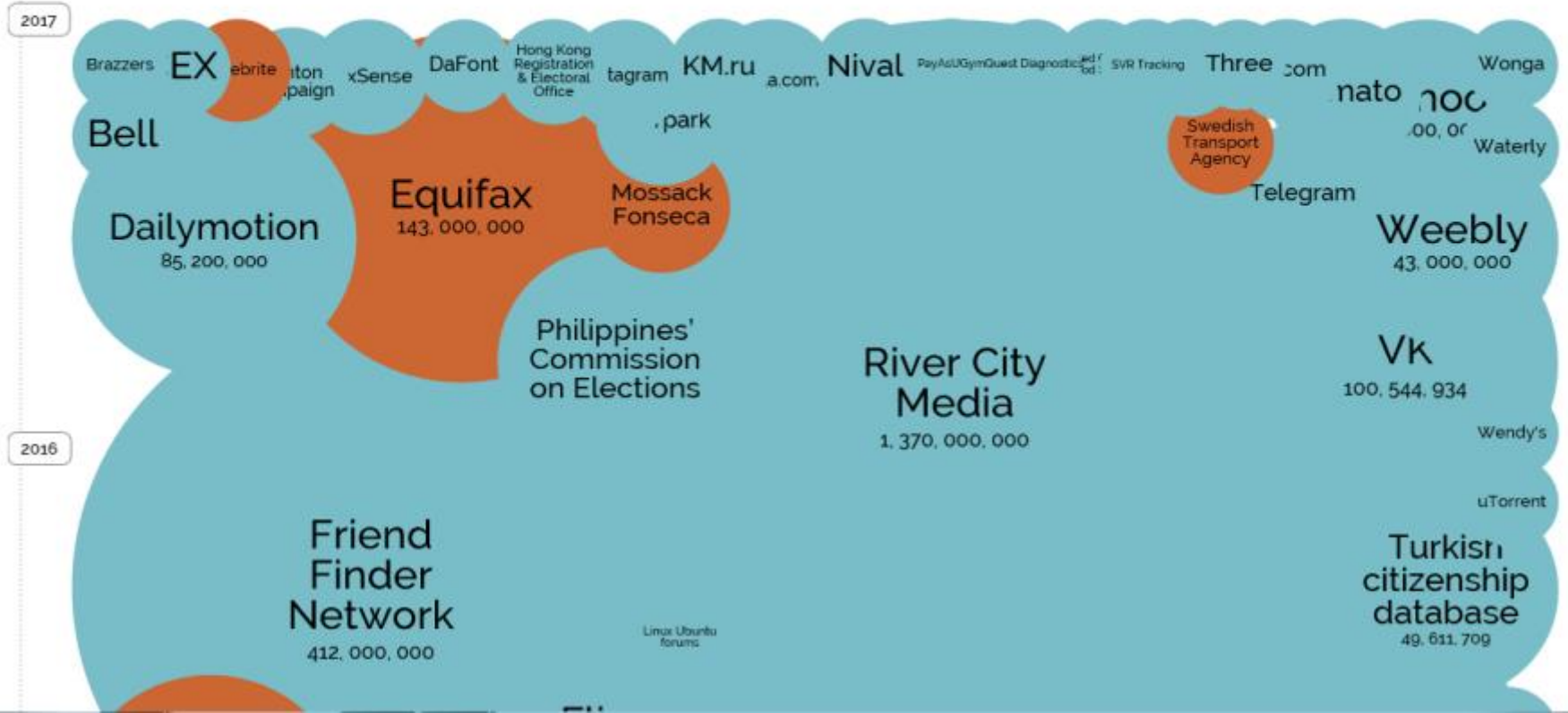
(updated 10th Sep 2017)

interesting story

YEAR

BUBBLE COLOUR YEAR METHOD OF LEAK BUBBLE SIZE NO OF RECORDS STOLEN DATA SENSITIVITY

SHOW FILTER



NHS 'could have prevented' WannaCry ransomware attack

27 October 2017 | Technology | Share

WannaCry was the biggest cyber-attack that has affected the NHS to date

NHS trusts were left vulnerable in a major ransomware attack in May because cyber-security recommendations were not followed, a government report has said.

More than a third of trusts in England were disrupted by the WannaCry ransomware, according to the National Audit Office (NAO).

Top Stories

Trump victory as Senate backs tax overhaul

1 hour ago

Yemen ex-president offers talks to Saudis

1 hour ago

N Korea threat prompts Hawaii siren test

3 hours ago

Nut van de NEN7510

- De NEN7510 biedt structuur
- Basis voor benchmark / audit
- Referentie in wetgeving
- Aantoonbaarheid d.m.v. certificering
- Bevordert de samenwerking binnen de zorg
- NEN7510 is hiermee een begrip in de gezondheidszorg

NEN 7510

- Sinds 2004 beschikbaar
- Managementsysteem en risicoanalyse
- Combinatie van:
  - Organisatorische maatregelen
  - Technische maatregelen
  - Fysieke maatregelen
- Gericht op:
  - Bedrijfsprocessen
  - Informatievoorziening
  - Informatietechnologie
  - Geautomatiseerd en niet-geautomatiseerd

Uitgangspunten nieuwe NEN 7510 (1)

- **Doelgroep:**
  - Zorginstellingen
  - Andere beheerders van persoonlijke gezondheidsinformatie

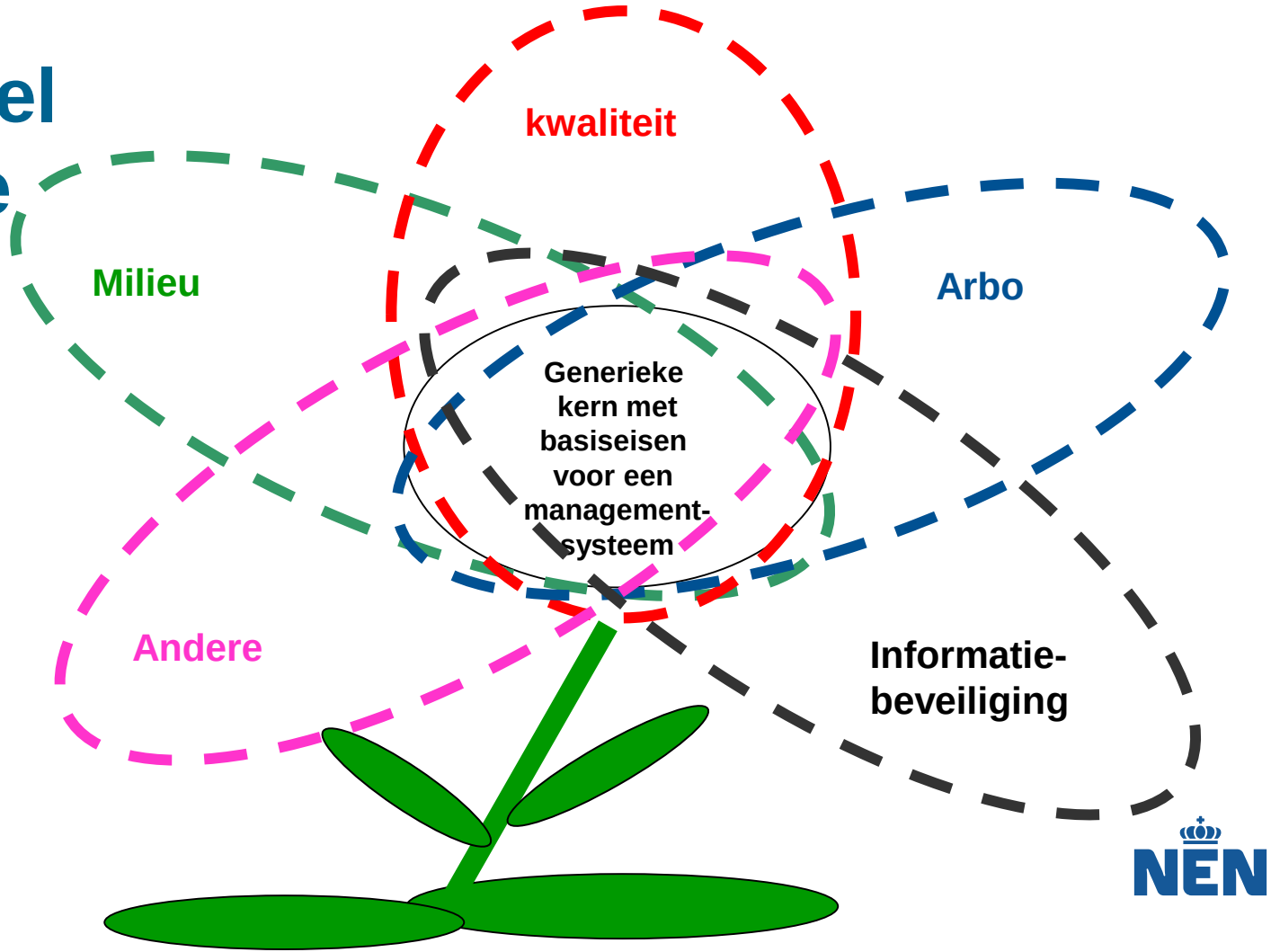
- **Twee delen**:
  - Deel I: inleiding, scope, managementsysteem, incl. risicoanalyse
  - Deel II: beheersmaatregelen

NEN 7510 | Informatiebeveiliging in de zorg

Uitgangspunten nieuwe NEN 7510 (2)

- **Bronnen**:
  - **NEN 7510: 2011**, Informatiebeveiliging in de zorg
  - **ISO 27001: 2015**, Managementsystemen voor informatiebeveiliging
  - **ISO 27002: 2015**: Praktijkrichtlijn beheersmaatregelen informatiebeveiliging
  - **ISO 27799: 2016**, Informatiebeveiligingsmanagement in de gezondheidszorg

High Level Structure



Nederlandse norm

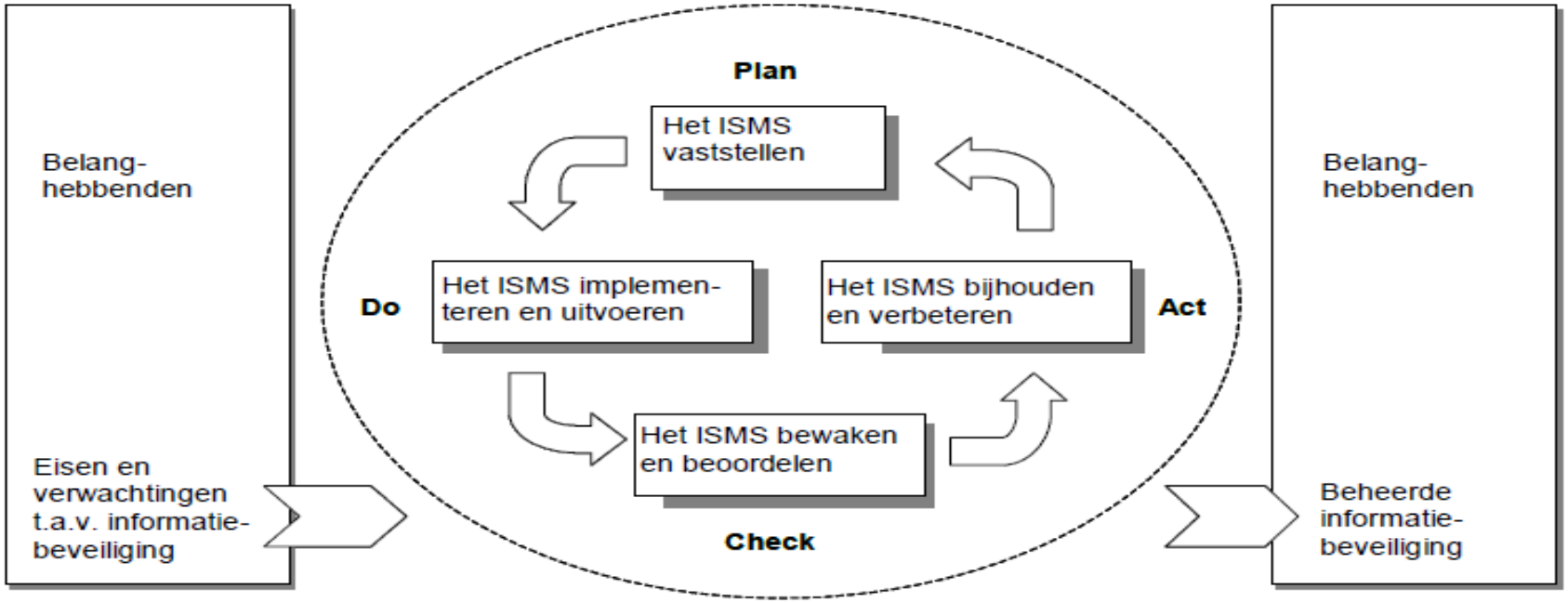
NEN 7510-1

(nl)

Medische informatica -
Informatiebeveiliging in de zorg -
Deel 1: Managementsysteem

Health informatics -
Information security management in healthcare -
Part 1: Management system

Managementsysteem

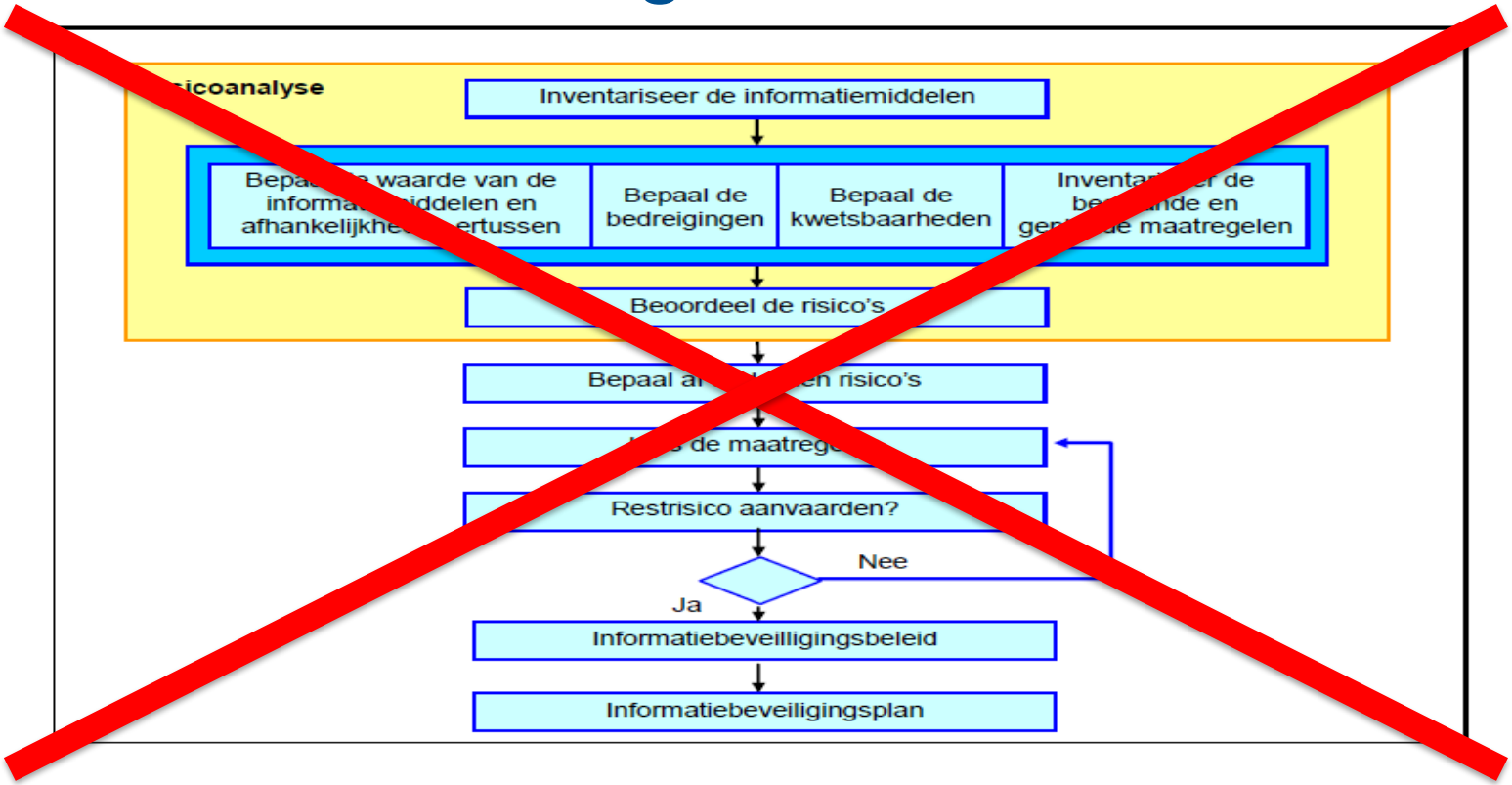


Managementsysteem

Eisen aan het managementsysteem (ISO 27001)

4. Context van de organisatie
5. Leiderschap
6. Planning
7. Ondersteuning
8. Uitvoering
9. Evaluatie van de prestaties
10. Verbetering

Risicobeoordeling



Risicobeoordeling

- Risicocriteria vaststellen en onderhouden
- Waarborgen consistentie risicobeoordelingen
- Identificeren informatiebeveiligingsrisico's
- Analyseren informatiebeveiligingsrisico's
- Evalueren informatiebeveiligingsrisico's
- Informatiebeveiligingsrisico's behandelen
  - Behandelprocedure definiëren en toepassen

Risicobeoordeling

- Behandelen informatiebeveiligingsrisico's
  - Passende opties kiezen
  - Beheersmaatregelen vaststellen
  - Gekozen beheersmaatregelen toetsen op ISO 27002
  - Verklaring van toepasselijkheid opstellen
  - Behandelplan informatiebeveiligingsrisico's formuleren
  - Goedkeuring verkrijgen van risico-eigenaren voor:
    - > Behandelplan
    - > Acceptatie restrisico's

Nederlandse norm

NEN 7510-2

(nl)

Medische informatica -
Informatiebeveiliging in de zorg -
Deel 2: Beheersmaatregelen

Health informatics -
Information security management in healthcare -
Part 2: Controls

Indeling beheersmaatregelen (1)

- Beheersmaatregel
- Zorgspecifieke beheersmaatregel

- Implementatierichtlijn
- Zorgspecifieke implementatierichtlijn

- Overige informatie
- Overige zorgspecifieke informatie

Indeling beheersmaatregelen (2)

- Informatiebeveiligingsbeleid
- Organiseren van informatiebeveiliging
- Veilig personeel
- Beheer van bedrijfsmiddelen
- Toegangsbeveiliging
- Cryptografie
- Fysieke beveiliging en beveiliging van de omgeving
- Beveiliging bedrijfsvoering
- Communicatiebeveiliging
- Acquisitie, ontwikkeling en onderhoud van informatiesystemen
- Leveranciersrelaties
- Beheer van informatiebeveiligingsincidenten
- Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
- Naleving

Hoofdstuk	Aantal maatregelen	Inclusief Aanvullend ISO 27799
05. Informatiebeveiligingsbeleid	2	2
06. Organiseren van Informatiebeveiliging	7	3
07. Veilig personeel	6	3
08. Beheer van bedrijfsmiddelen	10	6
09. Toegangsbeveiliging	14	4
10. Cryptografie	2	
11. Fysieke beveiliging en beveiliging van de omgeving	15	4
12. Beveiliging bedrijfsvoering	14	6
13. Communicatiebeveiliging	7	1
14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen	13*	4
15. Leveranciersrelaties	5	1
16. Beheer van informatiebeveiligingsincidenten	7	1
17. Informatiebeveiligingsaspecten van continuïteitsbeheer	4	1
18. Naleving	8	1
***= 3 maatregelen toegevoegd alleen voor de zorg**	114	37

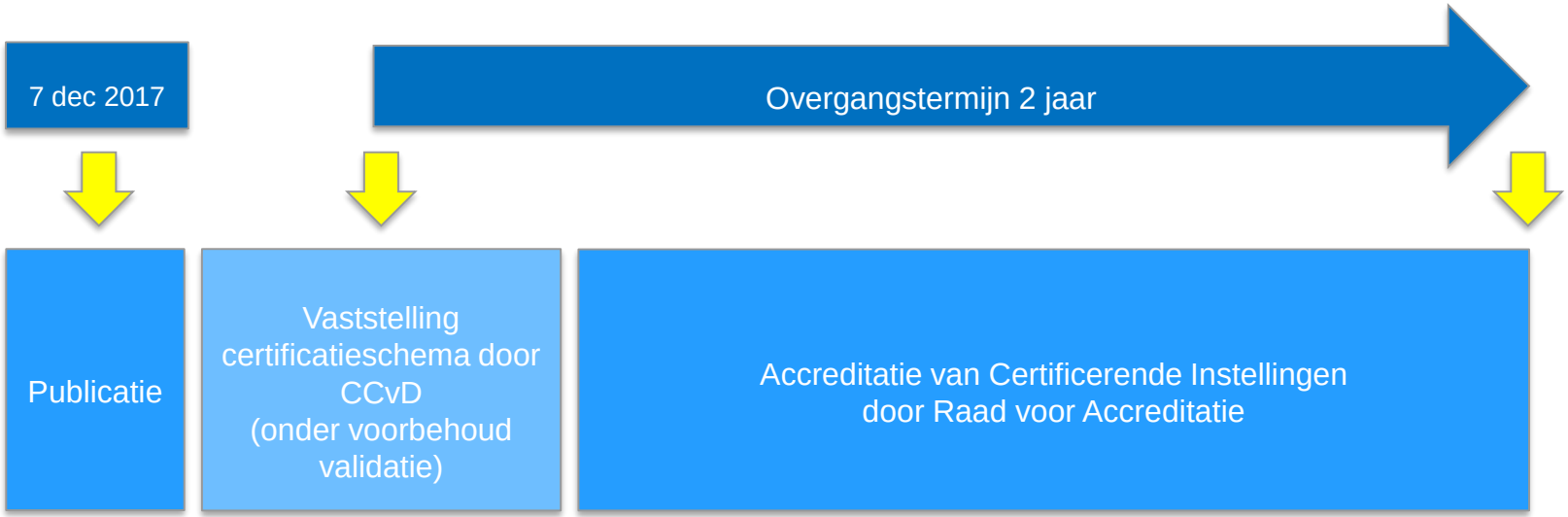
Voorbeeld beheersmaatregel (1)

- **Beheersmaatregel**
  - Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
- **Zorgspecifieke beheersmaatregel**
  - De toegang tot gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoort onderhevig te zijn aan een formeel gebruikersregistratieproces. Procedures voor het registreren van gebruikers behoren te garanderen dat het **vereiste niveau van authenticatie** van de geclaimde identiteit van gebruikers overeenkomt met het (de) toegangsniveau(s) waarover de gebruiker zal gaan beschikken.
  - De gebruikersregistratiegegevens behoren **regelmatig te worden beoordeeld** om te garanderen dat ze volledig en juist zijn en dat toegang nog altijd vereist is.

Voorbeeld beheersmaatregel (2)

- **Beheersmaatregel**
  - Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.
- **Zorgspecifieke beheersmaatregel**
  - Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren de **geïnformeerde toestemming** van cliënten te beheren.
  - Waar mogelijk behoort **geïnformeerde toestemming** van cliënten te worden verkregen **voordat** persoonlijke gezondheidsinformatie per e-mail, fax of telefonisch wordt gecommuniceerd of anderszins bekend wordt gemaakt aan partijen buiten de zorginstelling.

Overgangstermijn certificatie NEN 7510:2011 naar NEN 7510:2017



Meer weten over certificatie? *Kom naar de NEN-stand of vraag na bij de aanwezige Verschillende Certificerende Instellingen*

Tot slot

- Informatiebeveiliging is en wordt steeds belangrijker, ook in de zorg
- NEN7510 helpt hierbij en biedt houvast
- Certificering wordt makkelijker
- Praktijkgids / website:
  https://www.werkenmetnen7510.nl/
- Niets houdt ons tegen om aan de slag te gaan en te blijven