Avensus - AuditConnect

Boeklancering "NEN 7510"

Abram Schermer

Agenda

- Welkom
- Avensus – AuditConnect
- Intro Cees van der Wens
- Presentatie “NEN 7510”
- Vraag en antwoord
- Het boek!

Wat doet Avensus?

avensus

	Technologie	Proces
Cloud	Cloud Transitie	Managed Cloud AuditConnect
Security	Security Transitie High Grade Security	Managed security AuditConnect

avensus

Deskundig
Betrokken
Plezier
No nonsense
Samenwerking

CEES VAN DER WENS

Opleiding en ervaring:

- Studie: Industriële Automatisering
- Technisch schrijver, Kwaliteitsmanager, Security Officer
- ISO 27001, NEN 7510, NEN 7512, NEN 7513, ISO 27006, ISO 17021, NCS 7510, ISAE 3402, ISAE 3000

In 2015 nauw betrokken bij de opzet van de certificatie-instelling **DigiTrust**. Tientallen certificatie-audits uitgevoerd.

Huidige activiteiten:

- ISO 27001 & NEN 7510: certificatie-auditor, consultant, implementaties, interne audits, trainingen, boeken
- ISEA3000 en ISAE3402 audits

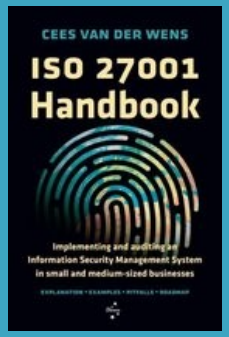
Movares adviseurs & ingenieurs

Alcatel·Lucent

TRUE hostingprovider

auditconnect

DigiTrust CERTIFICATION OF MANAGEMENT SYSTEMS



avensus

NEN

NEN Shop | Normontwikkeling | Trainingen

NEN 7510

Home › header › Zoekresultaten

135 resultaten gevonden voor

Ingestelde filters:

Filter resultaat

- **Type**
  - Norm (33)
  - Training (14)
  - NEN Connect (2)
  - Publicatie (3)
  - Meer..
- **Categorie**
  - NEN (28)
  - ISO (5)
  - IEC (1)
  - ASTM (2)
- **Status**
  - Definitief (11)
  - Ingetrokken (25)
- **Taal**
  - Nederlands (29)
  - Engels (7)
- **Publicatiejaar**
  - 2020 (1)

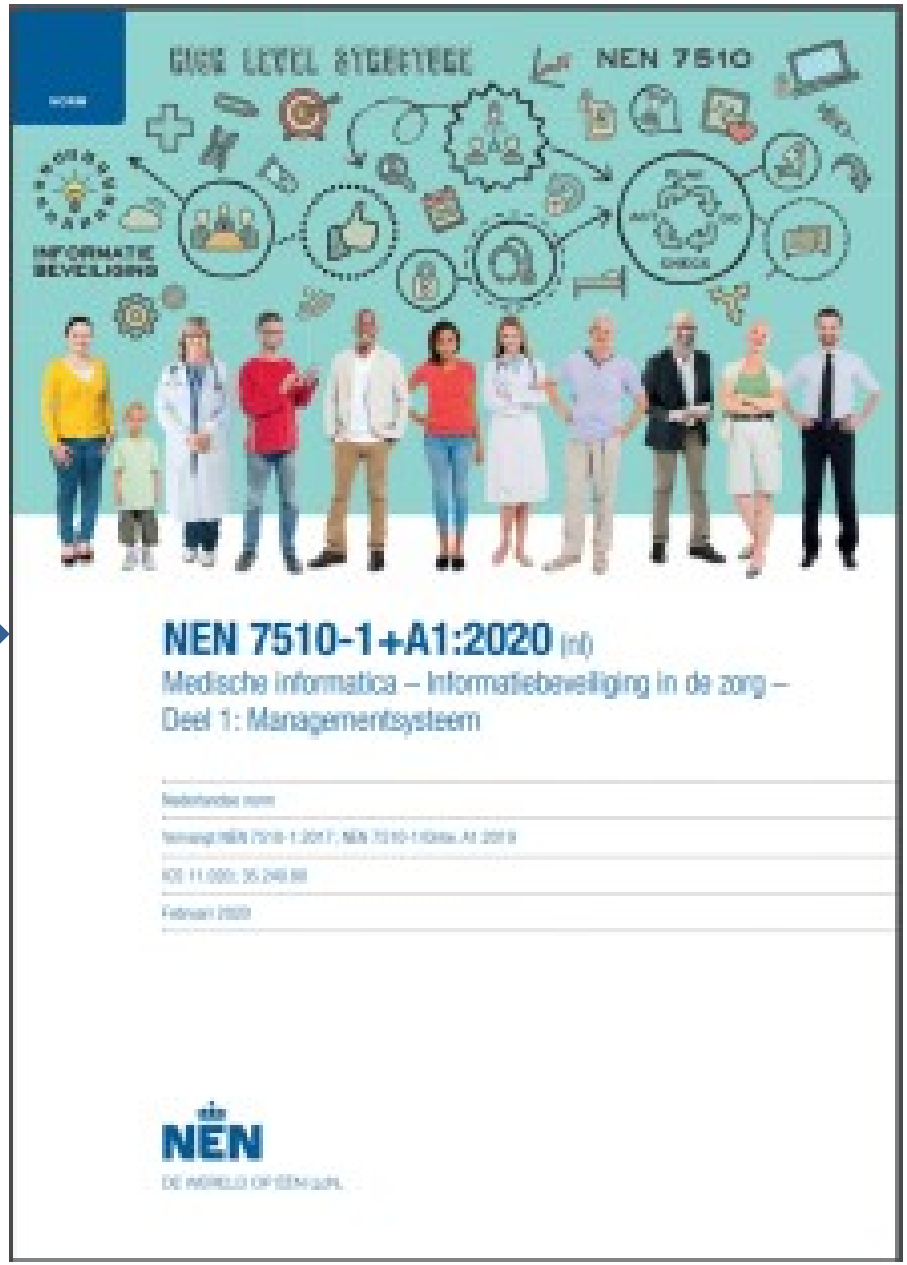
TRAIN
NEN
op de l
Belang

TRAIN
ISO
. BTW
vanuit

PUBL
UIT
Werl
Status
Aantal

TRAIN
NEN
van be

GRATIS



NEN 7510 is wettelijk verplicht voor zorginstellingen

Regeling gebruik burgerservicenummer in de zorg

Artikel 2: De gegevensverwerking, bedoeld in de artikelen 8 en 9 van de wet, in artikel 9.1.1, vierde lid, van de Wet langdurige zorg, in artikel 86, eerste, vierde en vijfde lid, van de Zorgverzekeringswet en in de artikelen 28, tweede lid, en 29 van het 'Besluit gebruik burgerservicenummer in de zorg' voldoet aan de **NEN 7510**.

Besluit van 10 november 2017, houdende nadere regels over functionele, technische en organisatorische maatregelen bij elektronische gegevens-verwerking door en tussen zorgaanbieders (Besluit elektronische gegevensverwerking door zorgaanbieders)

Artikel 2: Een zorgaanbieder draagt overeenkomstig het bepaalde in **NEN 7510 en NEN 7512**, zorg voor een veilig en zorgvuldig gebruik van het zorginformatiesysteem en een veilig en zorgvuldig gebruik van het elektronisch uitwisselingssysteem waarop hij is aangesloten.

NEN 7510-1+A1:2020 (nl)

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

NEN 7510-1+A1:2020 (nl)

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

NEN 7510-1 (normatief)
Managementsysteem +
Beheersmaatregelen.
CERTIFICEERBAAR

NEN 7510-2
Beheersmaatregelen +
implementatierichtlijnen.
NIET CERTIFICEERBAAR

avensus

NEN 7510-1+A1:2020 (nl)

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

NEN 7510-1
Kopie van ISO/IEC 27001
+
Kopie van de NEN 7510-2
(zonder de guidelines)

NEN

De organisatie NEN
wijzigt in principe niets aan
deze normen!

NEN 7510-2
Kopie van ISO/IEC 27002
+ ISO 27799 (health)

NEN 7510-1+A1:2020 (nl)

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

Dit betekent:

- de norm NEN 7510-1 (uit 2017)
- inclusief aanpassing nummer 1,
- die is toegevoegd in het jaar 2020

Aanpassingen betreffen alleen inleidende teksten, vertalingen of omissies

NEN 7510-1+A1:2020 (nl)

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

De norm geldt alleen voor Nederland en is alleen verkrijgbaar in de Nederlandse taal

NEN 7510-1+A1:2020 (nl)

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

De NEN 7510-1 gaat over de beveiliging van:

- persoonlijke gezondheidsinformatie, en
- alle andere relevante informatie

… binnen een gekozen toepassingsgebied

NEN 7510-1+A1:2020 (nl)

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

NEN 7510-1: Het begrip *informatiebeveiliging* kan worden opgesplitst in de volgende drie dimensies:

- Het beschermen van de **vertrouwelijkheid** van informatie
- Het beschermen van de **integriteit** (juistheid) van informatie
- Het beschermen van de **beschikbaarheid** van informatie

NEN 7510-1+A1:2020 (nl)

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

- **Zorginstellingen**

  Ziekenhuizen, GGZ-instellingen, klinieken, zelfstandige behandelcentra, ouderenzorginstellingen, jeugdzorginstellingen, gehandicapten-zorginstellingen, revalidatiecentra, huisartsenpraktijken en apotheken

- **Gemeenten**

  Wmo, Jeugdzorg

- **Toeleveranciers**

  Hosting providers, Zorgserviceproviders (netwerkleveranciers), SaaS providers

avensus

NEN 7510-1+A1:2020 (nl)

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

Hoofdstuk 0 t/m 2: inleiding

Hoofdstuk 3: termen en definities

H4 t/m H10: managementsysteem

Bijlage-A

117 beheersmaatregelen

Hoofdstuk 0 t/m 2: inleiding

Hoofdstuk 3: termen en definities

H4 t/m H10: managementsysteem

Bijlage-A

117 beheersmaatregelen

Maar de norm gaat toch eigenlijk alleen om deze 117 beheersmaatregelen?

Eh… nee.

In Bijlage-A van de norm NEN 7510-1 staan 117 maatregelen die (indien van toepassing) geïmplementeerd moeten worden.

NEN 7510-1:2017

Bijlage-A

(normatief)

Referentiebeheersdoelstellingen en -maatregelen

De beheersdoelstellingen en beheersmaatregelen die zijn opgenomen in tabel A.1, zijn overgenomen uit *NEN 7510-2* [21], hoofdstukken 5 tot en met 18, en moeten worden gebruikt in samenhang met 6.1.3.

In die laatste internationale norm zijn zorgspecifieke aanscherpingen van het dwingende *moeten* (*shall*) voorzien op basis van een universele risicobeoordeling voor de zorg. Aangezien in de systematiek van deze NEN 7510 een verklaring van toepasselijkheid (6.1.3 van deel 1) de selectie van beheersmaatregelen bepaalt, is die formuleringswijze hier niet overgenomen.

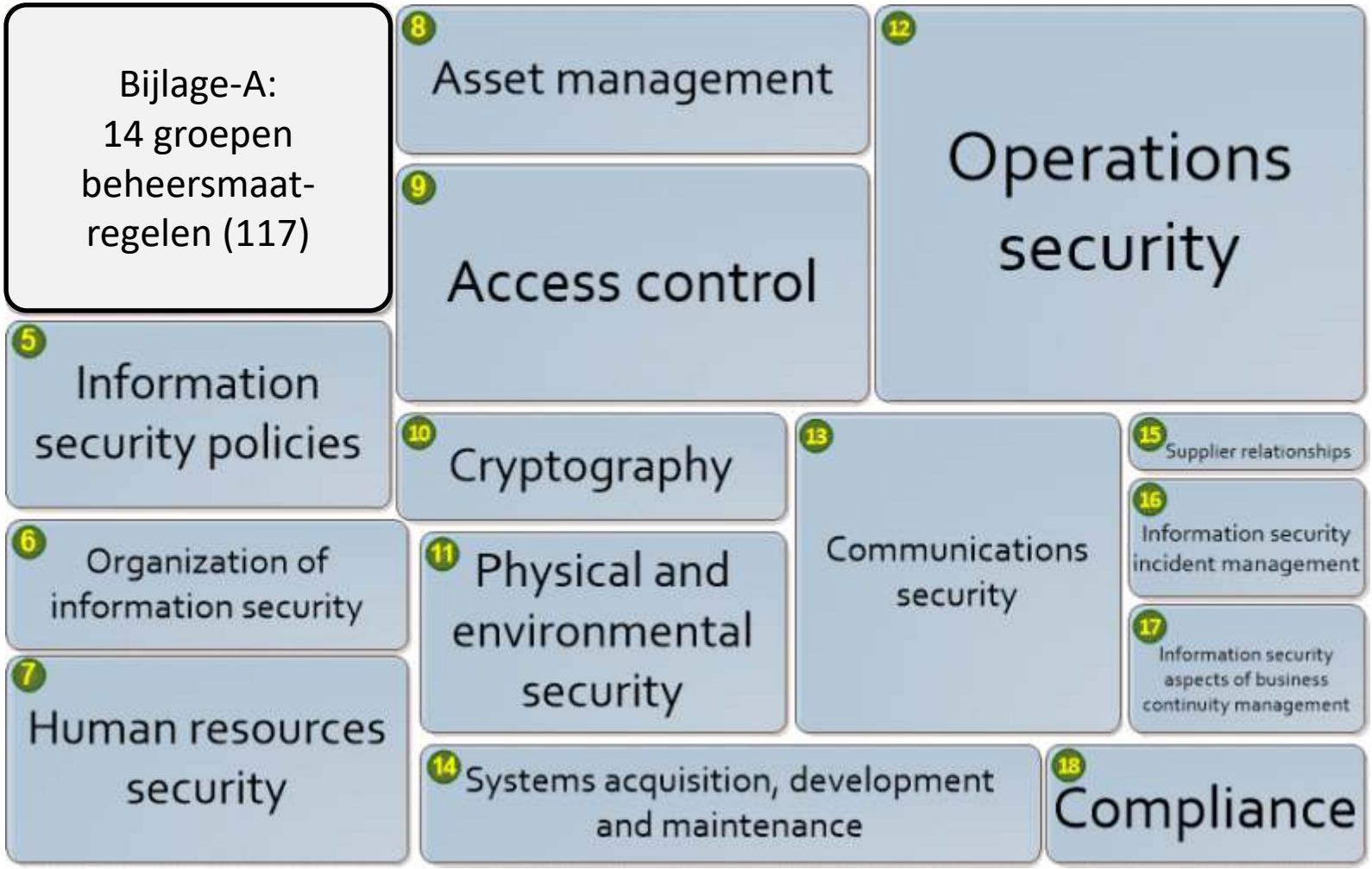
In deel 2 staan immers 'best practices' of richtlijnen om aan de doelvoorschriften te voldoen. Dit zijn mogelijke keuzes, dus in deel 2 staan de beheersmaatregelen *niet normatief* beschreven; er staat dus geen *moeten*, maar er staat *behoren*.

Daarin ligt ook het verschil met de doelvoorschriften in deze bijlage. Zorginstellingen *moeten* deze doelvoorschriften selecteren op basis van de risicoanalyse en dit vastleggen in de verklaring van toepasselijkheid en daarmee kunnen aantonen dat de doelvoorschriften wel of niet van toepassing zijn. In deze bijlage A staan de beheersmaatregelen daarom wel normatief beschreven (*moeten* en niet *behoren*).

Tabel A.1 — Beheersdoelstellingen en beheersmaatregelen

A.5	**Informatiebeveiligingsbeleid**	
A.5.1	**Aansturing door de directie van de informatiebeveiliging**	
Doelstelling: Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.		
A.5.1.1	**Beleidsregels voor informatiebeveiliging**	*Beheersmaatregel* Ten behoeve van informatiebeveiliging moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. ZORGSPECIFIEKE BEHEERSMAATREGEL

Bijlage-A
(normatief)



Bijlage A
(normatief)

A.10.1.1: Beleid inzake het gebruik van cryptografie

Ter bescherming van informatie moet ***een beleid*** *voor het gebruik van* ***cryptografische beheersmaatregelen*** *worden ontwikkeld en geïmplementeerd.*

NEN 7510-1:2017

Bijlage A
(normatief)

Referentiebeheersdoelstellingen en -maatregelen

De beheersdoelstellingen en beheersmaatregelen die zijn opgenomen in tabel A.1, zijn overgenomen uit *NEN 7510-2* [21)], hoofdstukken 5 tot en met 18, en moeten worden gebruikt in samenhang met 6.1.3.

NEN 7510-1:2017

Bijlage A
(normatief)

Referentiebeheersdoelstellingen en -maatregelen

De beheersdoelstellingen en beheersmaatregelen die zijn opgenomen in tabel A.1, zijn overgenomen uit *NEN 7510-2* [21)], hoofdstukken 5 tot en met 18, en moeten worden gebruikt in samenhang met 6.1.3.

Alle 117 beheersmaatregelen van Bijlage-A moeten worden gebruikt in **samenhang** met de eisen bij normelement 6.1.3 van het **managementsysteem:** behandeling van informatiebeveiligingsrisico's.

avensus

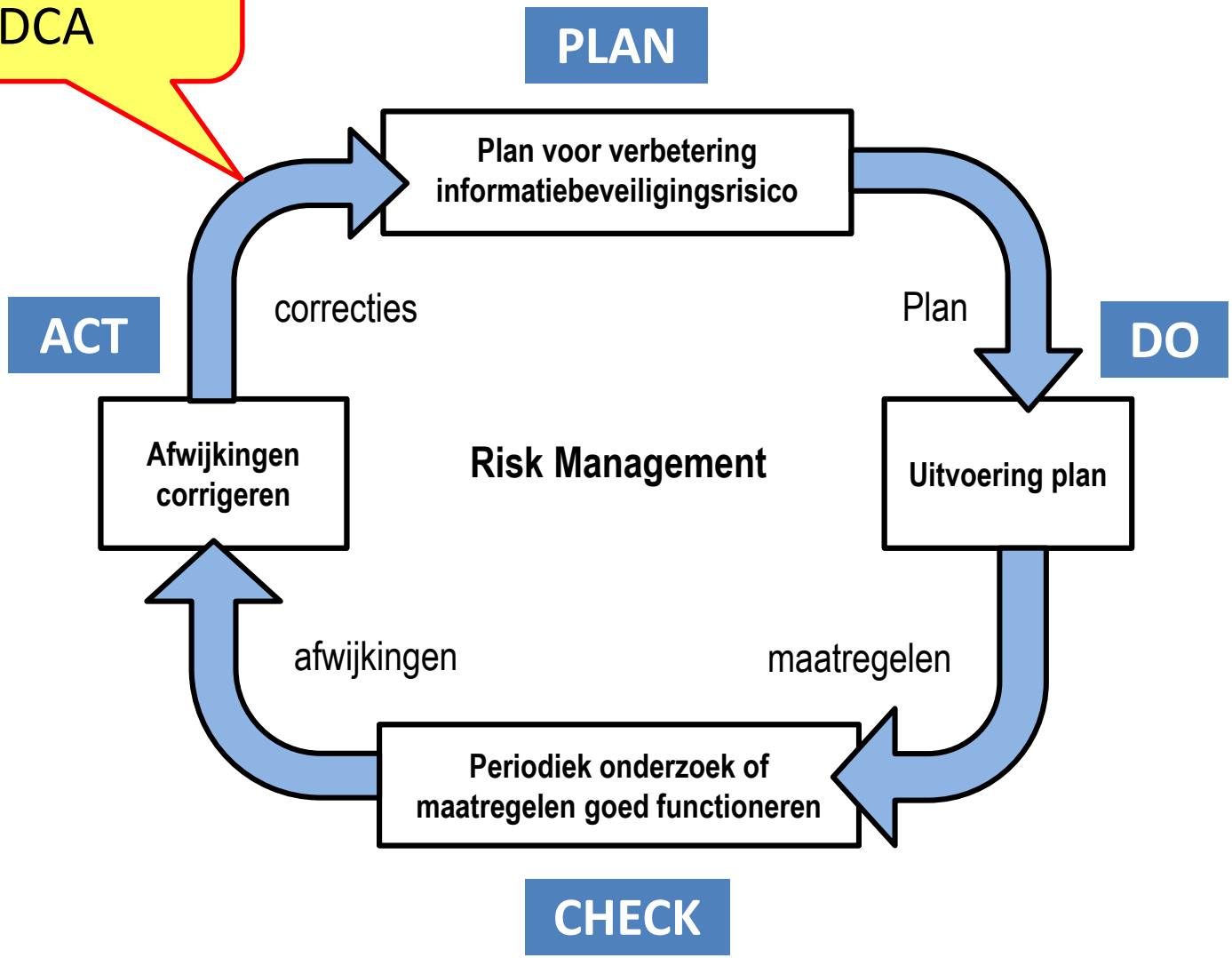
egelen van Bijlage-A
t in **samenhang** met
nent 6.1.3 van het
managementsysteem: behandeling van informatiebeveiligingsrisico's.

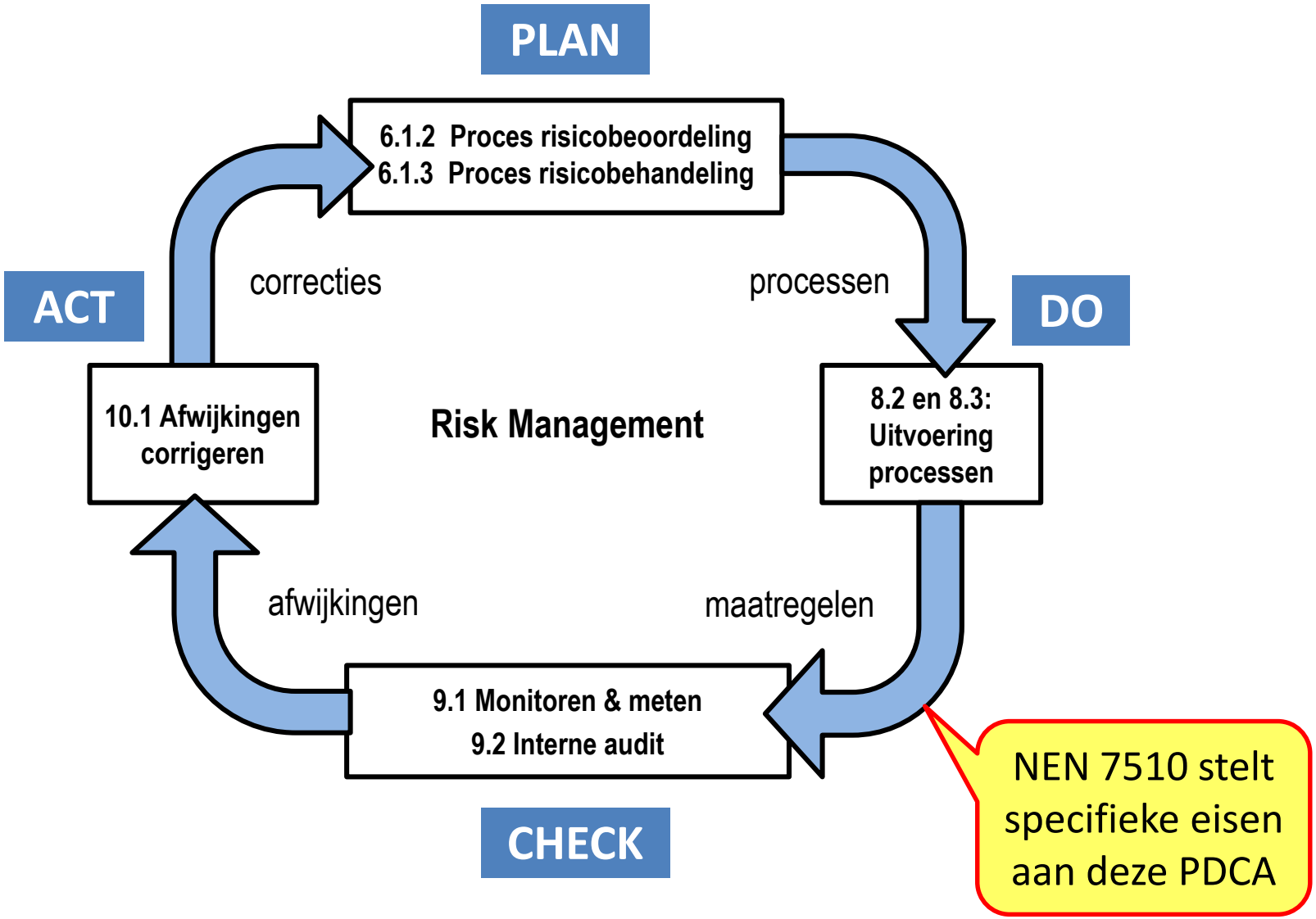
avensus

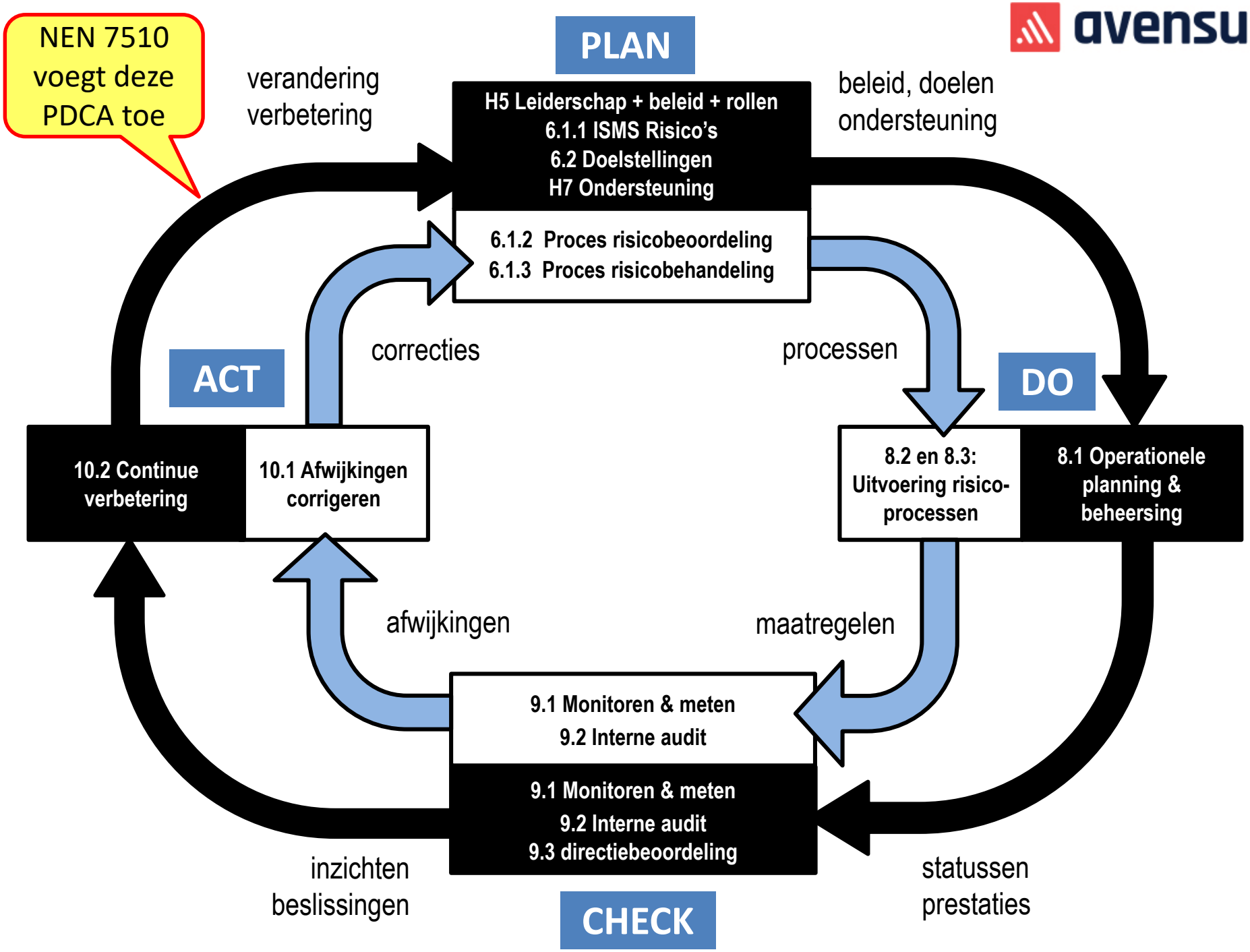
Natuurlijk heeft u al maatregelen getroffen om informatiebeveiligingsrisico's te verlagen:

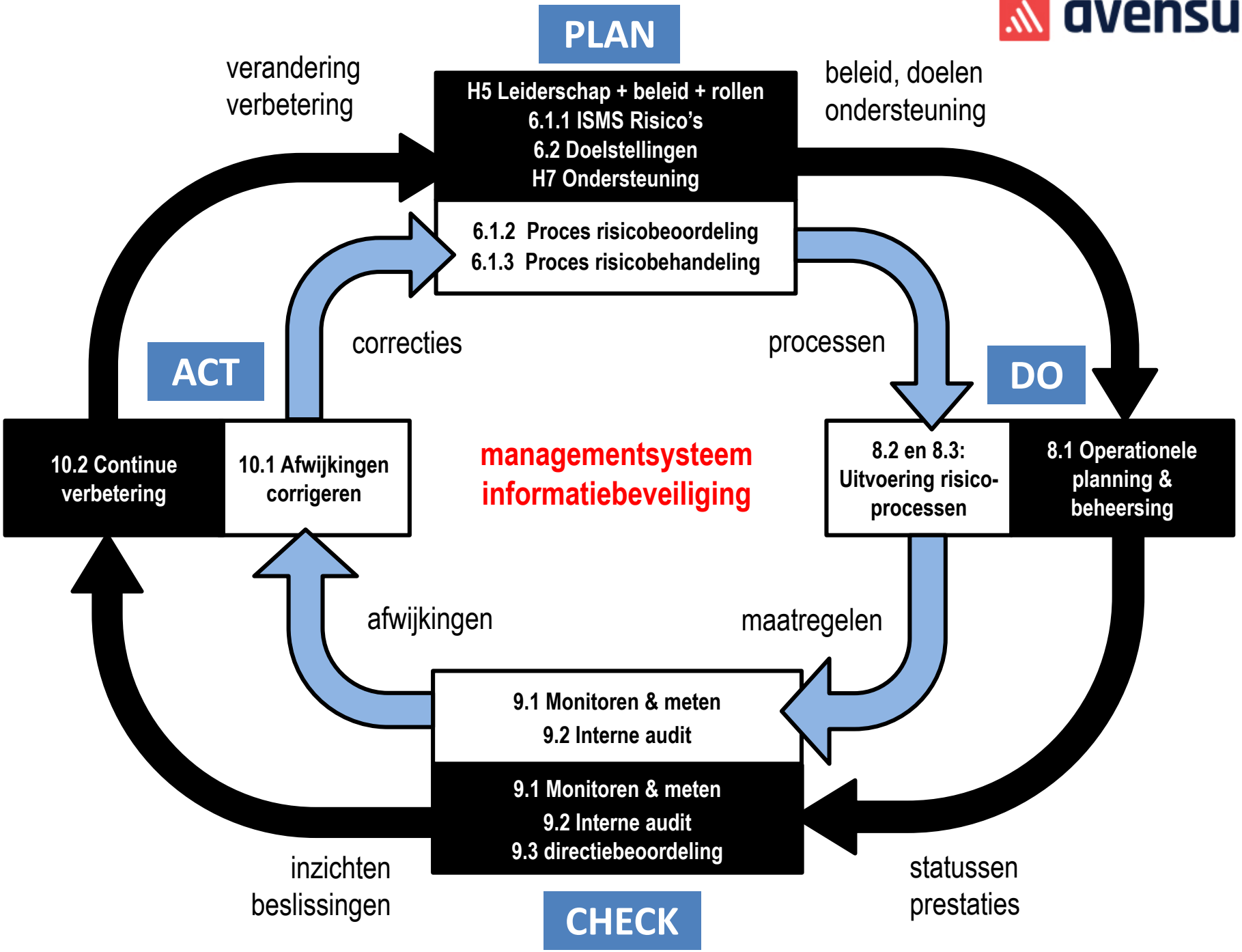
Hoe bent u tot die maatregelen gekomen?

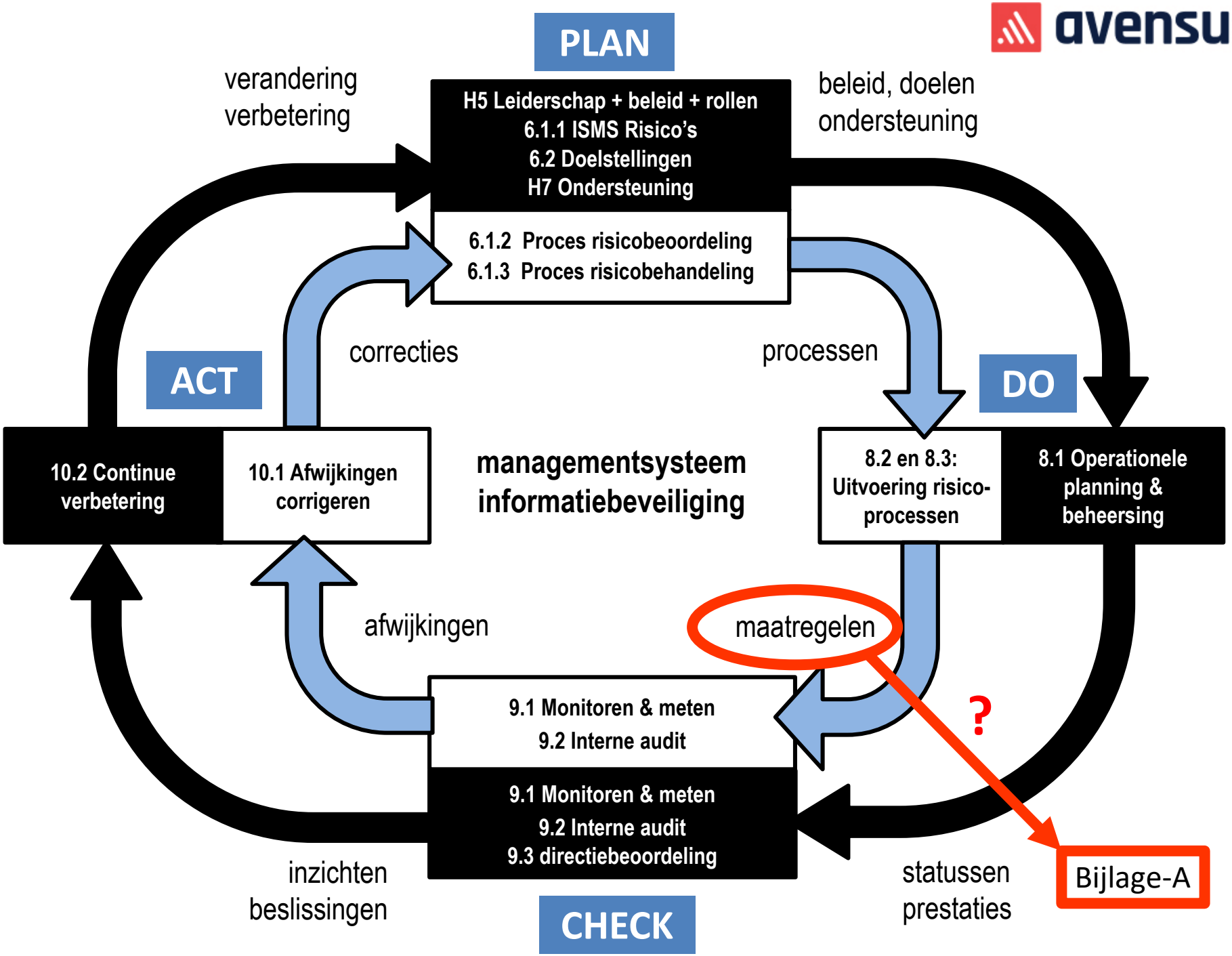
Elke organisatie gebruikt deze PDCA




PLAN
6.1.2 Proces risicobeoordeling
6.1.3 Proces risicobehandeling
processen
DO
8.2 en 8.3: Uitvoering processen
maatregelen
CHECK
9.1 Monitoren & meten
9.2 Interne audit
afwijkingen
ACT
10.1 Afwijkingen corrigeren
correcties
Risk Management
NEN 7510 stelt specifieke eisen aan deze PDCA


NEN 7510 voegt deze PDCA toe
verandering verbetering
PLAN
H5 Leiderschap + beleid + rollen
6.1.1 ISMS Risico's
6.2 Doelstellingen
H7 Ondersteuning
beleid, doelen ondersteuning
6.1.2 Proces risicobeoordeling
6.1.3 Proces risicobehandeling
correcties
processen
ACT
DO
10.2 Continue verbetering
10.1 Afwijkingen corrigeren
8.2 en 8.3: Uitvoering risico-processen
8.1 Operationele planning & beheersing
afwijkingen
maatregelen
9.1 Monitoren & meten
9.2 Interne audit
9.1 Monitoren & meten
9.2 Interne audit
9.3 directiebeoordeling
inzichten beslissingen
statussen prestaties
CHECK


PLAN
verandering
verbetering
H5 Leiderschap + beleid + rollen
6.1.1 ISMS Risico's
6.2 Doelstellingen
H7 Ondersteuning
beleid, doelen
ondersteuning
6.1.2 Proces risicobeoordeling
6.1.3 Proces risicobehandeling
correcties
processen
ACT
DO
10.2 Continue verbetering
10.1 Afwijkingen corrigeren
managementsysteem informatiebeveiliging
8.2 en 8.3: Uitvoering risico-processen
8.1 Operationele planning & beheersing
afwijkingen
maatregelen
9.1 Monitoren & meten
9.2 Interne audit
9.1 Monitoren & meten
9.2 Interne audit
9.3 directiebeoordeling
inzichten
beslissingen
statussen
prestaties
CHECK


PLAN
verandering
verbetering
H5 Leiderschap + beleid + rollen
6.1.1 ISMS Risico's
6.2 Doelstellingen
H7 Ondersteuning
beleid, doelen
ondersteuning
6.1.2 Proces risicobeoordeling
6.1.3 Proces risicobehandeling
correcties
processen
ACT
DO
10.2 Continue verbetering
10.1 Afwijkingen corrigeren
managementsysteem informatiebeveiliging
8.2 en 8.3: Uitvoering risico-processen
8.1 Operationele planning & beheersing
afwijkingen
maatregelen
?
9.1 Monitoren & meten
9.2 Interne audit
9.1 Monitoren & meten
9.2 Interne audit
9.3 directiebeoordeling
inzichten
beslissingen
statussen
prestaties
Bijlage-A
CHECK

NEN 7510-1:2017

Bijlage A
(normatief)

Referentiebeheersdoelstellingen en -maatregelen

De beheersdoelstellingen en beheersmaatregelen die zijn opgenomen in tabel A.1, zijn overgenomen uit *NEN 7510-2* [21)], hoofdstukken 5 tot en met 18, en moeten worden gebruikt in samenhang met 6.1.3.

Alle 117 beheersmaatregelen van Bijlage-A moeten worden gebruikt in **samenhang** met de eisen bij normelement 6.1.3 van het **managementsysteem:** behandeling van informatiebeveiligingsrisico's.

Eis 6.1.3b: De organisatie moet alle beheersmaatregelen vast te stellen die nodig zijn voor het behandelen van informatiebeveiligingsrisico's te implementeren. **Organisaties kunnen beheersmaatregelen naar behoefte ontwerpen of ze uit een bepaalde bron halen**.

Eis 6.1.3c: **De organisatie moet de beheersmaatregelen die hiervoor in 6.1.3b zijn vastgesteld vergelijken met die in Bijlage-A, om te verifiëren dat geen noodzakelijke beheersmaatregelen zijn weggelaten.**

Dus mogelijk heb je Bijlage-A helemaal niet nodig?

Klopt!

Moet ik alle 117 beheersmaatregelen implementeren?

- Je bent verplicht een **Verklaring van Toepasselijkheid** (VvT) op de stellen, waaruit blijkt welke van de 117 maatregelen wel en niet van toepassing zijn.
- In de VvT moet je voor elke maatregel een **rechtvaardiging** geven **waarom** deze **wel of niet** van toepassing is.
- Het is niet ongebruikelijk dat een **klant** de VvT van een leverancier opvraagt.
- Naast de beheersmaatregelen van Bijlage-A mag je ook **eigen beheersmaatregelen** aan de VvT toevoegen.

Verklaring van toepasselijkheid NEN7510:2017 [Naam organisatie] [Versie] [Datum]			Van toepassing?	Geimplementeerd?	Wet	Contract	Risico analyse	Niet van toepassing want:
A.5	**Beveiligingsbeleid**							
A.5.1	**Managementaanwijzing voor informatiebeveiliging**	Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.						
A.5.1.1	**Beleidsregels voor informatiebeveiliging**	Ten behoeve van informatiebeveiliging moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. **Zorgspecifieke beheersmaatregel:** Organisaties moeten beschikken over een schriftelijk informatiebeveiligingsbeleid dat door het management wordt goedgekeurd, wordt gepubliceerd en vervolgens wordt gecommuniceerd aan alle werknemers en relevante externe partijen.	Ja	Ja			X	
A.5.1.2	**Beoordeling van het Informatiebeveiligingsbeleid**	Het beleid voor informatiebeveiliging moet met geplande tussenpozen of als zich significante veranderingen voordoen, worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is. **Zorgspecifieke beheersmaatregel:** Het informatiebeveiligingsbeleid moet aan voortdurende, gefaseerde beoordelingen worden onderworpen zodat het volledige beleid ten minste eenmaal per jaar wordt beoordeeld. Het beleid moet worden beoordeeld als er zich een ernstig beveiligingsincident heeft voorgedaan.	Ja	Ja			X	
A.6	**Organisatie van informatiebeveiliging**							
A.6.1	**Interne organisatie**	Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.						
A.6.1.1	**Rollen en verantwoordelijkheden bij informatiebeveiliging**	Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen. **Zorgspecifieke beheersmaatregel:** Organisaties moeten: a) duidelijk verantwoordelijkheden op het gebied van	Ja	Ja			X	

ISO 27003 (ISMS-implementatierichtlijnen):

“Elke beheersmaatregel die in Bijlage-A staat en die niet bijdraagt aan het wijzigen van een risico, behoort te worden uitgesloten.”

avensus

Bijlage A
(normatief)

A.10.1.1: Beleid inzake het gebruik van cryptografie

Ter bescherming van informatie moet ***een beleid*** *voor het gebruik van* ***cryptografische beheersmaatregelen*** *worden ontwikkeld en geïmplementeerd.*

Dus ik mag zelf bepalen wat er in dit beleid komt te staan?

Wat u hier moet doen hangt af van uw specifieke risico's op het gebied van informatiebeveiliging

Bijlage A
(normatief)

A.6.1.1: Rollen en verantwoordelijkheden

*Zorgspecifiek: Organisaties moeten over een informatie-beveiligingsmanagementforum (**IBMF**) beschikken om te garanderen dat er duidelijke aansturing en zichtbare ondersteuning vanuit het management is (…). Het gezondheidsinformatiebeveiligingsforum moet regelmatig, maandelijks of bijna maandelijks, vergaderen.*

Ik ben een hostingprovider.
Moet ik dit doen?

Tja…

NEN 7510 - Implementatie

	Norm	→ *inrichten*			→ *implementeren*	
H4 t/m H10	H4 - Context					
	H5 - Leiderschap	→	Eigen eisen	*structuur, beleid, planning, verantwoordelijk-heden, werkwijzen, procedures, processen en middelen*	→	Toepassing
	H6 - Planning	→	Eigen eisen		→	Toepassing
	H7 - Ondersteuning	→	Eigen eisen		→	Toepassing
	H8 - Uitvoering	→	Eigen eisen		→	Toepassing
	H9 - Evaluatie	→	Eigen eisen		→	Toepassing
	H10 - Verbetering	→	Eigen eisen		→	Toepassing
Bijlage-A	A.5.1.1 Beleid	→	Eigen eisen	*een proces, beleid, voorziening, werkwijze of andere maatregel waarmee het risico wordt gewijzigd*	→	Toepassing
	A.5.1.2 Beleid	→	Eigen eisen		→	Toepassing
	A.6.1.1 Rollen	→	Eigen eisen		→	Toepassing
	Etc. ……	→	Eigen eisen		→	Toepassing
	A.18.2.2 Naleving	→	Eigen eisen		→	Toepassing
	A.18.2.3 Naleving	→	Eigen eisen		→	Toepassing

NEN 7510 – Initiële certificatieaudit

Fase-1 audit

	Norm	→ *inrichten*			→ *implementeren*
H4 t/m H10	H4 - Context				
	H5 - Leiderschap	→ Eigen eisen	*structuur, beleid, planning, verantwoordelijk-heden, werkwijzen, procedures, processen en middelen*	→	Toepassing
	H6 - Planning	→ Eigen eisen		→	Toepassing
	H7 - Ondersteuning	→ Eigen eisen		→	Toepassing
	H8 - Uitvoering	→ Eigen eisen		→	Toepassing
	H9 - Evaluatie	→ Eigen eisen		→	Toepassing
	H10 - Verbetering	→ Eigen eisen		→	Toepassing
Bijlage-A	A.5.1.1 Beleid	→ Eigen eisen	*een proces, beleid, voorziening, werkwijze of andere maatregel waarmee het risico wordt gewijzigd*	→	Toepassing
	A.5.1.2 Beleid	→ Eigen eisen		→	Toepassing
	A.6.1.1 Rollen	→ Eigen eisen		→	Toepassing
	Etc. ……	→ Eigen eisen		→	Toepassing
	A.18.2.2 Naleving	→ Eigen eisen		→	Toepassing
	A.18.2.3 Naleving	→ Eigen eisen		→	Toepassing

NEN 7510 – Initiële certificatieaudit

Fase-2 audit

	Norm	→ *inrichten*		→ *implementeren*
H4 t/m H10	H4 - Context			
	H5 - Leiderschap	→ Eigen eisen	*structuur, beleid, planning, verantwoordelijk-heden, werkwijzen, procedures, processen en middelen*	→ Toepassing
	H6 - Planning	→ Eigen eisen		→ Toepassing
	H7 - Ondersteuning	→ Eigen eisen		→ Toepassing
	H8 - Uitvoering	→ Eigen eisen		→ Toepassing
	H9 - Evaluatie	→ Eigen eisen		→ Toepassing
	H10 - Verbetering	→ Eigen eisen		→ Toepassing
Bijlage-A	A.5.1.1 Beleid	→ Eigen eisen	*een proces, beleid, voorziening, werkwijze of andere maatregel waarmee het risico wordt gewijzigd*	→ Toepassing
	A.5.1.2 Beleid	→ Eigen eisen		→ Toepassing
	A.6.1.1 Rollen	→ Eigen eisen		→ Toepassing
	Etc. ……	→ Eigen eisen		→ Toepassing
	A.18.2.2 Naleving	→ Eigen eisen		→ Toepassing
	A.18.2.3 Naleving	→ Eigen eisen		→ Toepassing

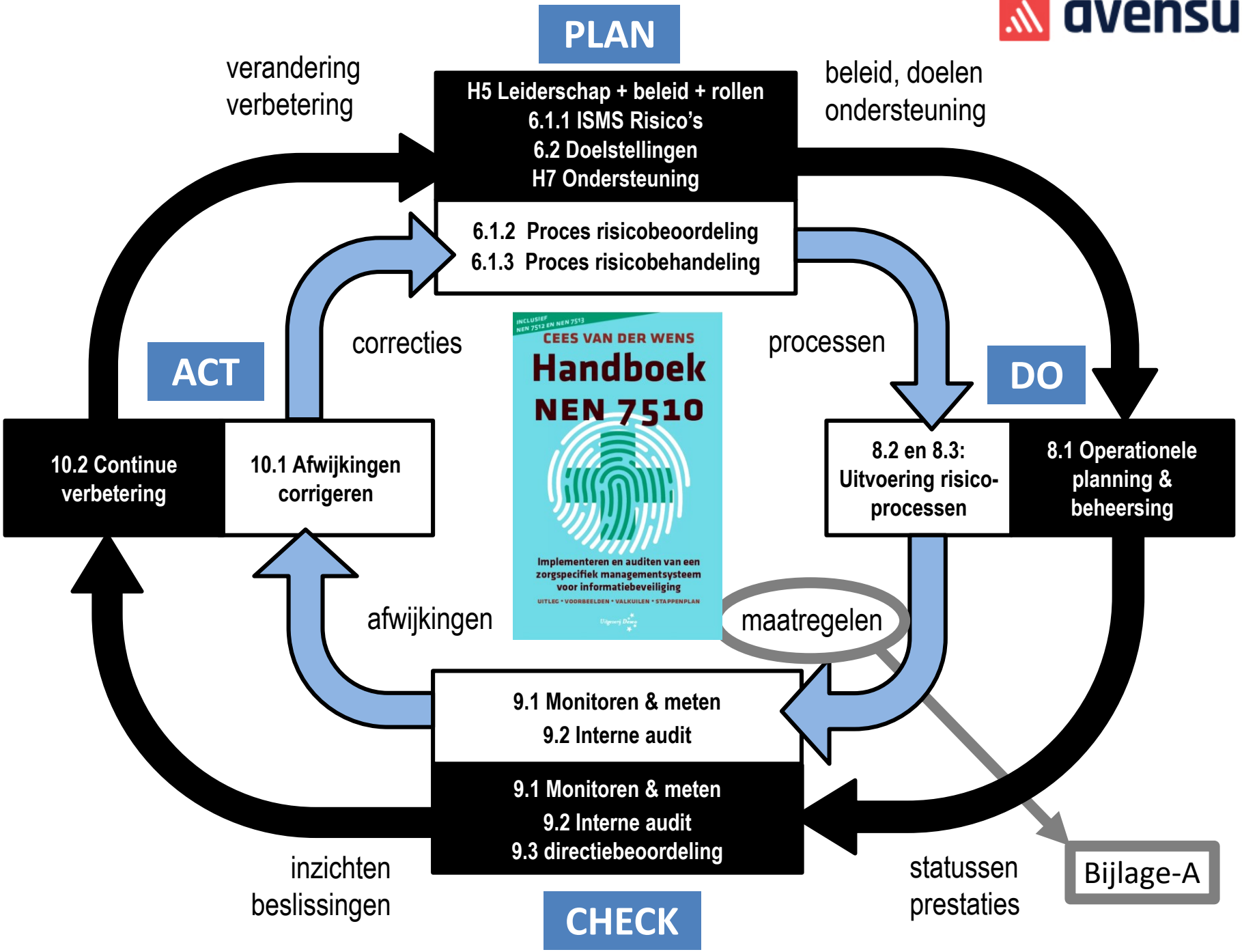
NEN 7510 – Certificatie-instellingen (CI)

1. CI zonder RvA-accreditatie voor NEN 7510-1
2. CI met RvA-accreditatie voor NEN 7510-1 Cluster B
3. CI met RvA-accreditatie voor NEN 7510-1 Cluster Z+B

B = Beheerder (Hostingprovider, Zorgserviceprovider, etc.)

Z = Zorginstellingen

Let op: Elke beheerder (B) moet sinds april 2019 aan CI type 2 en 3 kunnen aantonen dat hij beheerder is van **persoonlijke gezondheids-informatie** en dat hij **interfaces** heeft met één of meer zorginstellingen, hetgeen moet blijken uit zijn Verklaring van Toepasselijkheid.


PLAN
verandering
verbetering
H5 Leiderschap + beleid + rollen
6.1.1 ISMS Risico's
6.2 Doelstellingen
H7 Ondersteuning
beleid, doelen
ondersteuning
6.1.2 Proces risicobeoordeling
6.1.3 Proces risicobehandeling
correcties
processen
ACT
DO
10.2 Continue verbetering
10.1 Afwijkingen corrigeren
8.2 en 8.3: Uitvoering risico-processen
8.1 Operationele planning & beheersing
INCLUSIEF NEN 7512 EN NEN 7513
CEES VAN DER WENS
Handboek NEN 7510
Implementeren en auditen van een zorgspecifiek managementsysteem voor informatiebeveiliging
UITLEG • VOORBEELDEN • VALKUILEN • STAPPENPLAN
afwijkingen
maatregelen
9.1 Monitoren & meten
9.2 Interne audit
9.1 Monitoren & meten
9.2 Interne audit
9.3 directiebeoordeling
inzichten
beslissingen
statussen
prestaties
Bijlage-A
CHECK

Dank voor uw aandacht

avensus
auditconnect

Wij helpen u graag verder!