Handboek NEN 7510

Implementeren en auditen van een zorgspecifiek managementsysteem voor informatiebeveiliging

Uitgeverij: Deseo / Brave New Books
ISBN 9789402129908
BISAC COM053000
NUR 982
Versie: 20200616
Trefwoord: Informatiebeveiliging

Boekomslag: Rob Westendorp – WSTNDRP grafisch ontwerp & illustratie
Foto auteur: Heleen Rozeveld
Afbeeldingen in het boek: Cees van der Wens
Omslagillustratie: iStock.com/Physicx

© 2020 - Cees van der Wens

Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt worden in enige vorm of op enige wijze, hetzij elektronisch, mechanisch of door fotokopieën, opname, of op enige andere manier, zonder voorafgaande schriftelijke toestemming van de auteur.

Inhoud

Inleiding

Doel van dit boek

Het organiseren van informatiebeveiliging wordt steeds complexer. Dit geldt zeker binnen de zorgsector waar met vitale en gevoelige gegevens wordt gewerkt, waar ICT en e-health een steeds belangrijkere rol spelen en waar veel partijen een stem hebben. Een systematische aanpak voor de beveiliging van informatie is daarom een noodzaak geworden.

Dit handboek is geschreven met als doel zorginstellingen, gemeenten en toeleveranciers te helpen bij het inrichten, implementeren, onderhouden en continu verbeteren van een *zorgspecifiek managementsysteem voor informatiebeveiliging* volgens de norm NEN 7510-1:2017. In dit boek vindt u uitleg, voorbeelden en valkuilen met betrekking tot het voldoen aan alle eisen van deze norm, en aan alle eisen van de NEN 7512 en NEN 7513.

Tegelijkertijd is dit handboek ook bedoeld om ondersteuning te bieden aan auditoren die moeten onderzoeken of een zorgspecifiek managementsysteem voor informatiebeveiliging aan alle eisen voldoet en doeltreffend geïmplementeerd is. Dit boek biedt de auditor informatie over alle na te leven eisen, wijst de auditor op veel voorkomende tekortkomingen en bevat specifieke aanwijzingen voor het uitvoeren van audits.

De uitleg in dit handboek houdt voortdurend rekening met de mogelijkheid dat u uw managementsysteem voor informatiebeveiliging uiteindelijk wilt laten certificeren. Speciaal voor dit doel is een apart hoofdstuk opgenomen over de specifieke spelregels en het verloop van een certificatie-audit.

Dit handboek mengt zich niet in de grote discussies over security en privacy in de zorg, zoals deze bijvoorbeeld worden gevoerd over de veiligheid van de elektronische uitwisseling van gegevens of over het opslaan van gegevens in de cloud. Het boek beperkt zich bewust tot het aanreiken van informatie die van belang is om te voldoen aan de eisen van de norm.

Dit boek is een bewerking van het eerder verschenen ‘Handboek ISO 27001’. Bij de bewerking zijn alle teksten aangepast en uitgebreid om aan te sluiten bij het zorgspecifieke karakter van de norm NEN 7510-1:2017.

Leeswijzer voor dit boek

De nummers en titels van hoofdstuk 4 t/m 10 van dit boek komen overeen met de nummers en titels van hoofdstuk 4 t/m 10 van de norm. Hierdoor kunnen boek en norm gemakkelijk naast elkaar worden gebruikt.

Bij het lezen van de hoofdstukken 4 t/m 10 van dit boek zult u zien dat de norm nauwgezet wordt gevolgd, maar daarvan niet de letterlijke tekst laat zien. De reden hiervoor is dat dit boek geen vervanging is van de norm. Om gedetailleerd kennis te nemen van de normteksten zult u een exemplaar van de norm moeten aanvragen bij de NEN (zie hoofdstuk 1 van dit boek).

De hoofdstukken 4 t/m 10 behandelen elk één of meerdere normelementen. Het in dit boek gebruikte woord *normelement* komt niet uit de norm, het is een door de auteur gehanteerde term om de norm op te delen in logische eenheden. Binnen een normelement komen één of meerdere *eisen* aan de orde. *Eisen* zijn voorwaarden waaraan u moet voldoen om conformiteit met de norm te kunnen claimen.

Om geen extra ruis te introduceren, is in dit boek het woordgebruik bewust zo dicht mogelijk bij dat van de norm gehouden. Waar nodig worden woorden en begrippen uitgelegd. Teksten die beginnen met een ➢-symbool zijn bedoeld als verduidelijking of aanvulling op de hoofdtekst.

De hoofdstukken 4 t/m 10 in dit boek beginnen elk met een schematische weergave van de norm. In het schema zijn de normelementen gemarkeerd die deel uitmaken van het betreffende hoofdstuk. De schema's zijn van de auteur van dit boek en zijn dus niet afkomstig uit de norm.

Bij elk normelement komen de volgende vaste onderwerpen aan de orde:

- *Uitleg, voorbeelden en valkuilen*
  Welke eisen staan er in dit normelement? Wat betekenen ze? Wat moet u doen? Wat moet u niet doen?
- *Verplichte documentatie*
  Welke gedocumenteerde informatie eist dit normelement?
- *Aanwijzingen voor het uitvoeren van audits*
  Wat zou een (interne) auditor kunnen onderzoeken met betrekking tot de eisen van dit normelement?

De 'Aanwijzingen voor het uitvoeren van audits', hebben als doel u te helpen bij het voldoen aan de eisen van normelement 9.2. Bij dit normelement staat dat u met geplande tussenpozen *interne audits* moet uitvoeren om te bepalen of uw managementsysteem voor informatiebeveiliging doeltreffend is en aan alle eisen voldoet. De aanwijzingen aan het einde van elk normelement bevatten concrete informatie ten behoeve van deze audits.

Dit handboek volgt de norm op de voet, maar waar de norm bij Bijlage-A stopt, gaat dit boek nog een aantal hoofdstukken verder. Deze extra hoofdstukken bevatten praktische tips en aanvullende informatie, waaronder een stappenplan voor implementatie.

Soms komt u in de tekst van dit boek een blokje met een nummer tegen, bijvoorbeeld: [2]. Het nummer in het blokje verwijst naar een van de bronnen die door de auteur zijn gebruikt en die achter in dit boek bij het hoofdstuk *Bronnen* worden gespecificeerd.

Disclaimer

De uitleg en voorbeelden in dit boek komen voort uit persoonlijke meningen en ervaringen van de auteur en kunnen ter discussie worden gesteld door anderen. De auteur kan niet verantwoordelijk worden gesteld voor eventuele negatieve gevolgen die voortvloeien uit het toepassen van de informatie in dit boek.

1. Over de norm NEN 7510-1

DE NORM NEN 7510-1

De norm NEN 7510-1 [1] is een document van ongeveer 90 pagina's dat u gratis kunt verkrijgen via de webshop van de NEN. De norm geldt alleen voor Nederland en is alleen verkrijgbaar in de Nederlandse taal [18].

De norm NEN 7510-1 is een uitgave van de NEN (NEderlandse Norm), een organisatie die de ontwikkeling van certificatieschema's faciliteert. Daarnaast beheert NEN deze schema's zodra ze gereed zijn en toegepast worden voor het uitvoeren van certificatie-audits (zie de uitleg in hoofdstuk 14). NEN certificeert zelf niet, maar fungeert als onafhankelijk platform om certificatieschema's op te zetten en te beheren.

In de praktijk wordt de aanduiding 'NEN 7510-1' voor het gemak vaak ingekort tot 'NEN 7510' (zie ook de titel van dit boek). In dit boek is de aanduiding 'NEN 7510' voor het gemak bijna overal afgekort tot 'de norm'.

- *Om de uitleg en afbeeldingen in dit boek goed te kunnen begrijpen, is het noodzakelijk dat u over de norm NEN 7510-1 beschikt. Bestel de norm, lees hem een keer door en houd hem bij het lezen van dit boek onder handbereik.*

ONTWIKKELING VAN DE NEN 7510-1

In het jaar 2017 vond de herziening van NEN 7510:2011 plaats en viel de nieuwe norm NEN 7510:2017 (naar analogie met de norm ISO/IEC 27001 [6]) uiteen in de volgende twee delen:

- NEN 7510-1:2017. Deze norm bevat de normatieve voorschriften voor het managementsysteem volgens NEN-ISO/IEC 27001 (nl).
- NEN 7510-2:2017. Deze norm vormt de Nederlandse weergave van de Europese en internationale norm NEN-ISO/IEC 27002 (nl) en NEN-EN-ISO 27799 (en).

Dit handboek gaat over het eerste deel, de NEN 7510-1:2017, dus over het inrichten van een managementsysteem voor informatiebeveiliging.

Net als bij eerdere versies van de norm, zullen er in de NEN 7510-1:2017 gaandeweg fouten en kansen voor verbetering worden ontdekt. In februari 2020 heeft de NEN een eerste aanpassing doorgevoerd, waarna de norm de volgende (uitgebreide) naam heeft gekregen: 'NEN 7510-1:2017+A1:2020'. Dit moet gelezen worden als: *de norm NEN 7510-1:2017, inclusief de eerste aanpassing (A1) op de oorspronkelijke versie uit 2017, welke in het jaar 2020 is doorgevoerd*.

◆ DOELGROEPEN

DOELGROEP: ZORGINSTELLINGEN

De norm is primair bedoeld voor *zorginstellingen*. Een zorginstelling wordt volgens art. 1 van de Wet kwaliteit, klachten en geschillen zorg (Wkkgz) gedefinieerd als 'een rechtspersoon die bedrijfsmatig zorg verleent, een organisatorisch verband van natuurlijke personen die bedrijfsmatig zorg verlenen of doen verlenen, alsmede een natuurlijke persoon die bedrijfsmatig zorg doet verlenen'.

Onder *zorginstellingen* vallen bijvoorbeeld ziekenhuizen, GGZ-instellingen, klinieken, zelfstandige behandelcentra, ouderenzorginstellingen, jeugdzorginstellingen, gehandicaptenzorginstellingen, revalidatiecentra, huisartsenpraktijken en apotheken.

DOELGROEP: TOELEVERANCIERS

Naast zorginstellingen bestaat de doelgroep van de norm ook uit 'andere beheerders van persoonlijke gezondheidsinformatie'. Dit zijn bijvoorbeeld zorgserviceproviders, hostingproviders en andere toeleveranciers van zorginstellingen [1].

- *Een zorgserviceprovider is een netwerkleverancier van een beveiligde netwerkverbinding tussen een zorginformatiesysteem en een elektronisch uitwisselingssysteem.*

Voor toeleveranciers is het relevant te onderzoeken of zij beheerder zijn van persoonlijke gezondheidsinformatie (een bijzondere vorm van persoonsgegevens) en daarmee daadwerkelijk een toeleverancier zijn zoals door de

norm wordt bedoeld. Omdat leveranciers niet altijd geacht worden zich toegang te verschaffen tot de door hen verwerkte gegevens (denk aan een hostingprovider) zal dit onderzoek soms in samenspraak met de verwerkingsverantwoordelijke (de klant) moeten plaatsvinden.

- *Volgens de AVG is er sprake van 'verwerking' bij [17]: 'een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens'.*

- *Om in aanmerking te komen voor NEN 7510-certificatie onder accreditatie van de Raad van Accreditatie zal een leverancier moeten kunnen aantonen dat hij daadwerkelijk beheerder is van persoonlijke gezondheidsinformatie en dat er interfaces zijn met zorginstellingen (zie de uitleg in hoofdstuk 14 van dit boek).*

DOELGROEP: GEMEENTEN

Onder de in de norm genoemde 'andere beheerders van persoonlijke gezondheidsinformatie' vallen ook Nederlandse gemeenten, indien en voor zover ze persoonlijke gezondheidsinformatie verwerken (zie ook paragraaf 0.5 van de norm).

Gemeenten zijn volgens de Wet maatschappelijke ondersteuning (Wmo) verplicht om kwetsbare en hulpbehoevende groepen te compenseren door het aanbieden van voorzieningen en ondersteuning, bijvoorbeeld huishoudelijke hulp of aanpassing van de woning. Gemeenten werden in 2015 ook verantwoordelijk voor de jeugdzorg Binnen beide verantwoordelijkheden, Wmo en jeugdzorg, kan met persoonlijke gezondheidsinformatie worden gewerkt die met passende maatregelen moet worden beschermd.

Daarnaast kan een gemeente bijvoorbeeld opdracht geven aan VECOZO tot het ten behoeve van de Gemeente verzorgen van de aansluiting van (zorg)aanbieders en diens ingeschakelde tussen- en softwarepartijen op het Gegevensknooppunt voor zorgaanbieders (GKZ). In dat geval zal VECOZO in de verwerkersovereenkomst eisen dat de gemeente kan aantonen te werken volgens de norm NEN 7510-1 (zie ook normelement 4.2).

◆ VERPLICHTINGEN

IS DE NORM VERPLICHT VOOR ZORGINSTELLINGEN?

Het antwoord is: ja. Een zorgaanbieder moet volgens de *Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg* het burgerservicenummer van een cliënt gebruiken. In de aanvullende *Regeling gebruik burgerservicenummer* is bepaald dat:

> *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.*

Wat wordt hier bedoeld met de NEN 7510? Bij de NEN 7510-2 gaat het over beheersmaatregelen en richtlijnen voor de implementatie daarvan. Maar deze maatregelen en richtlijnen zijn, zoals de norm zelf zegt [2], 'mogelijk niet in alle situaties geheel passend of toereikend en voldoen mogelijk niet aan de specifieke eisen met betrekking tot beheersmaatregelen van de organisatie.' Om die reden moet ook de NEN 7510-1 worden toegepast.

Er zijn nog steeds zorginstellingen die denken dat ze aan de norm NEN 7510 voldoen door beheersmaatregelen te implementeren die genoemd worden in de NEN 7510-2. Dit is een misvatting. Uiteindelijk is het treffen van maatregelen wel het doel, maar de eisen in de NEN 7510-1 gaan verder en dwingen u na te denken over de volgende belangrijke vragen:

- Wat zijn in uw geval passende maatregelen?
- Hoe zorgt u dat uw maatregelen passend blijven?
- Hoe weet u of uw maatregelen compleet zijn?
- Hoe en hoe vaak onderzoekt u of geïmplementeerde maatregelen doeltreffend zijn?
- Wat doet u als een maatregel niet doeltreffend blijkt te zijn?
- Hoe weet u dat u met uw maatregelen alle wettelijke en contractuele eisen naleeft?
- Hoe kunt u, indien gevraagd, aantonen dat u er alles aan gedaan hebt om te zorgen dat uw maatregelen passend, doeltreffend, compleet en conform wettelijke en contractuele eisen zijn?

IS DE NORM VERPLICHT VOOR TOELEVERANCIERS?

De wet verplicht dit niet, maar omdat zorginstellingen vanuit de NEN 7510 verplicht zijn hun uitbestede processen te beheersen, kunnen toeleveranciers via hun contract met zorginstellingen verplicht zijn om aan (delen van) de norm te voldoen.

IS NEN 7510-CERTIFICATIE VERPLICHT?

Certificatie van een NEN 7510-managementsysteem is niet wettelijk verplicht, maar zorginstellingen moeten wel steeds vaker kunnen aantonen dat ze voldoen aan de norm NEN 7510 (zie de voorbeelden bij normelement 4.2). Voor dat doel kan certificatie een geschikt middel zijn.

De NEN houdt op haar website een register bij van gecertificeerde organisaties [18]. Hieruit blijkt dat zowel zorginstellingen als toeleveranciers zich in groten getale laten certificeren (begin 2020 waren er circa twaalfhonderd organisaties met een NEN-7510-certificaat). Hierbij kan een onderscheid worden gemaakt tussen 'gewone certificatie' en 'certificatie onder accreditatie van de Raad van Accreditatie'.

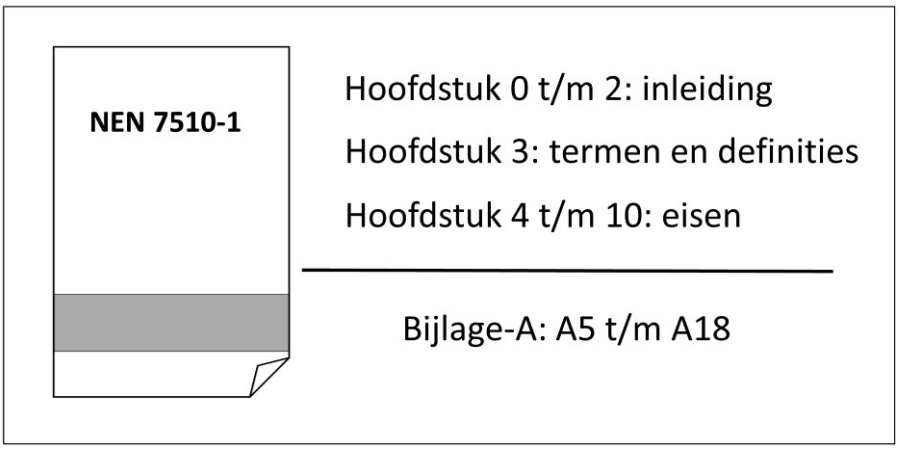
In hoofdstuk 14 van dit boek vindt u uitgebreide informatie over certificatie. Tevens wordt op diverse plekken in dit boek uitgelegd hoe u met het oog op certificatie aan bepaalde eisen moet voldoen.

◆ INHOUD VAN DE NORM

OPBOUW VAN DE NORM

Vooral voor beginners is de norm niet eenvoudig te doorgronden. Hij bevat geen lijstjes met onderwerpen die u kunt afvinken en geeft nauwelijks uitleg over wat u precies moet doen. Het is de bedoeling dat u zelf betekenis geeft aan de norm, een betekenis die past bij uw specifieke activiteiten, verplichtingen, risico's en doelstellingen. Daarover later meer.

De norm begint met hoofdstuk nul. In de hoofdstukken 0 t/m 3 van de norm vindt u inleidende teksten en een definitielijst. Het kan verhelderend zijn om deze teksten te lezen.



In de hoofdstukken 4 t/m 10 van de norm staan de eisen beschreven waaraan u moet voldoen 'om conformiteit met de norm te kunnen claimen', ofwel: om te mogen beweren dat uw managementsysteem voor informatiebeveiliging aan de norm voldoet.

In paragraaf 1.1 van de norm kunt u lezen dat uitsluiting van een van de eisen genoemd in de hoofdstukken 4 t/m 10 niet is toegestaan. Kortom, voor elk type organisatie geldt: alle eisen zijn verplicht.

BIJLAGE-A

De norm bevat ook een Bijlage-A. De 117 beheersmaatregelen die in de onderwerpen 5 t/m 18 van deze bijlage staan, zijn overgenomen uit de NEN 7510-2 [2]. Moet u alle 117 maatregelen toepassen en naleven? Dat ligt eraan. In dit boek wordt bij normelement 6.1.3 uitgebreid uitgelegd hoe u moet omgaan met Bijlage-A.

Valkuil 1 'We voldoen aan Bijlage-A, dus aan de norm NEN 7510'

Sommige organisaties denken aan de norm NEN 7510-1 voldoen omdat ze (een deel van) de beheersmaatregelen hebben geïmplementeerd die in Bijlage-A staan. In werkelijkheid voldoet een organisatie pas aan de norm als er ook een managementsysteem voor informatiebeveiliging is geïmplementeerd volgens de eisen in de hoofdstukken 4 t/m 10.

WAT BEDOELT DE NORM MET HET WOORD 'ORGANISATIE'?

In hoofdstuk 1 van de norm kunt u lezen dat de eisen in de norm bedoeld zijn voor alle *organisaties*, ongeacht type, omvang of aard. Wat verstaat de norm onder een *organisatie*?

Het begrip *organisatie* omvat, maar is niet beperkt tot: eenmanszaak, bedrijf, vennootschap, firma, onderneming, autoriteit, partnerschap, liefdadigheidsinstelling of genootschap, of een deel of combinatie daarvan, hetzij als rechtspersoon erkend of niet, publiek of privaat [1].

Merk op dat een *organisatie* geen rechtspersoon (juridische entiteit) hoeft te zijn en dat een managementsysteem voor informatiebeveiliging ook kan worden toegepast bij een eenmanszaak.

WAAROM IS DE TEKST VAN DE NORM ZO VAAG?

In paragraaf 0.6.1 van de norm kunt u lezen dat de volgorde van de eisen die in de norm worden gepresenteerd, niet de volgorde impliceert waarin deze eisen moeten worden geïmplementeerd, en ook niets zegt over het belang van die eisen. Dat klinkt een beetje als een kookboek waarin staat dat de volgorde van de ingrediënten die in de recepten staan, niets zegt over het belang van die ingrediënten, en ook niets zegt over de volgorde waarin ze tijdens het koken moeten worden gebruikt.

Behalve dat de volgorde van de eisen verwarrend kan overkomen, worden de teksten door velen als 'vaag' ervaren. Waarom staat er niet concreet wat u moet doen zodat u het kunt uitvoeren en van uw lijst kunt schrappen? Waarom moet u het allemaal zelf uitzoeken en bedenken?

De belangrijkste oorzaak van de 'vaagheid' is dat de norm bedoeld is voor alle typen organisaties en de eisen van de norm dus niet al te specifiek kunnen zijn. De norm kan bijvoorbeeld wel eisen dat er een informatiebeveiligingsbeleid moet zijn, maar niet wat er in dat beleid moet staan. Dat hangt namelijk af van wat er aan beleid nodig is binnen uw organisatie. De norm kan ook geen passende beheersmaatregelen voorschrijven, want wat passend is hangt af van uw specifieke informatiebeveiligingsrisico's.

U moet daarom zelf een managementsysteem voor informatiebeveiliging gaan definiëren dat voldoet aan de norm, dat past bij uw activiteiten, verplichtingen, risico's en doelstellingen, en dat geïntegreerd kan worden

met uw bedrijfsprocessen en met uw managementstructuur. Dat is nogal wat en in de praktijk blijkt dit niet altijd eenvoudig. Dit boek is bedoeld om u hierbij te helpen.

TERMEN EN DEFINITIES

In hoofdstuk 3 van de norm staat een lijst met zeventig definities. Deze kunt u gebruiken om meer duidelijkheid te krijgen over de betekenis van bepaalde termen die in de norm worden gebruikt. In dit boek wordt soms verwezen naar deze lijst.

BIBLIOGRAFIE

Achter in de norm staat onder de titel *Bibliografie* een lijst met documenten opgenomen die aanvullende informatie bieden op de norm NEN 7510-1. Dit boek verwijst regelmatig naar deze documenten (zie ook het hoofdstuk *Bronnen* achter in dit boek).

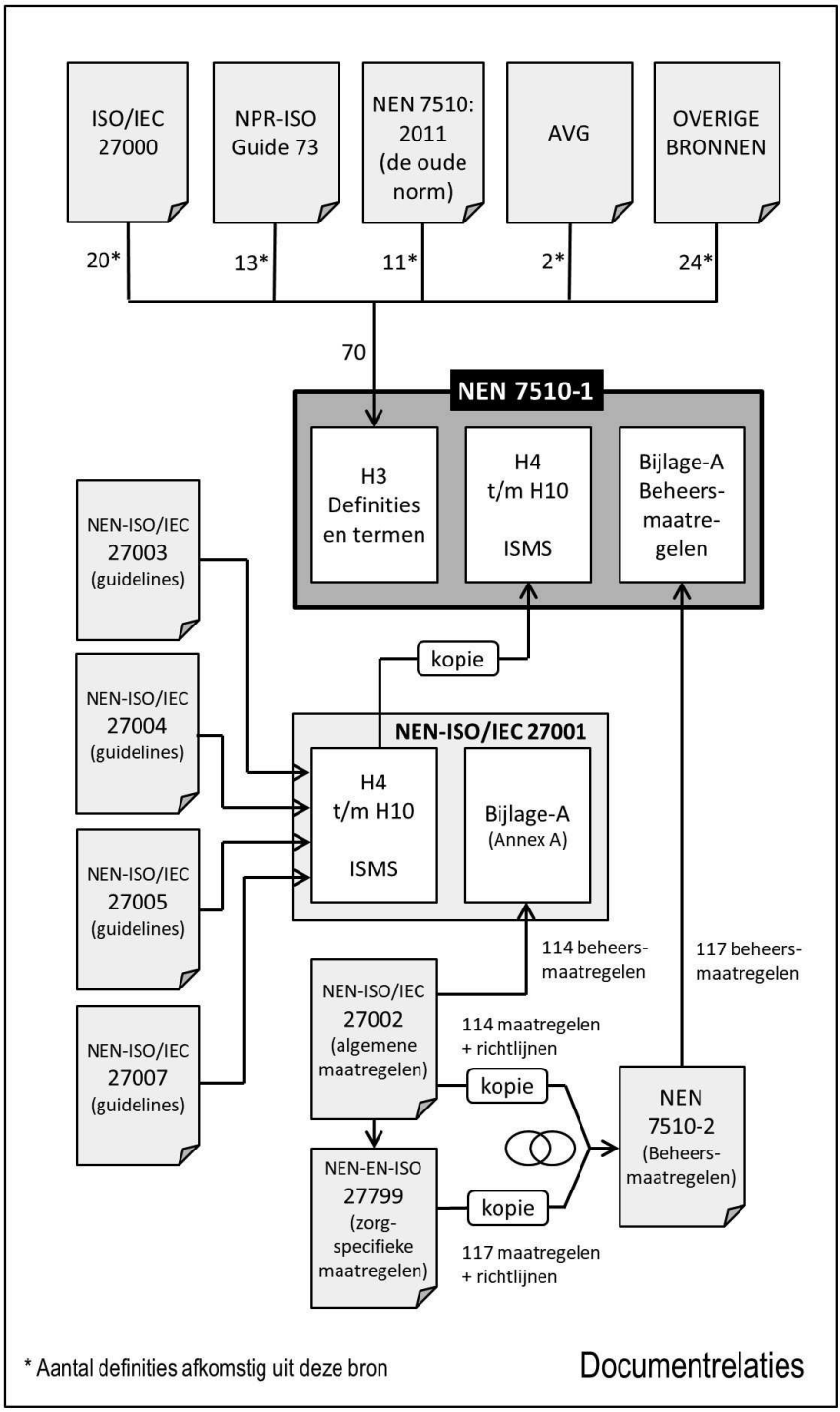
◆ CONTEXT VAN DE NORM

DOCUMENTRELATIES

Bij het lezen van dit boek is het van belang te weten dat de hoofstukken 4 t/m 10 van de norm NEN 7510-1 ongewijzigd zijn overgenomen uit de norm NEN-ISO/IEC 27001 [6]. Hierdoor zijn sommige documenten die implementatierichtlijnen voor de NEN-ISO/IEC 27001 bevatten automatisch ook relevant bij het implementeren van de norm NEN 7510-1. Dit geldt voor de volgende documenten:

- NEN-ISO/IEC 27003 [8]
- NEN-ISO/IEC 27004 [9]
- NEN-ISO/IEC 27005 [10]
- NEN-ISO/IEC 27007 [12]

Daar waar deze documenten waardevolle informatie bieden voor het implementeren van de norm NEN 7510-1, maakt dit boek gebruik van deze informatie.


ISO/IEC 27000
NPR-ISO Guide 73
NEN 7510: 2011 (de oude norm)
AVG
OVERIGE BRONNEN
20*
13*
11*
2*
24*
70
NEN 7510-1
H3 Definities en termen
H4 t/m H10 ISMS
Bijlage-A Beheers-maatre-gelen
NEN-ISO/IEC 27003 (guidelines)
NEN-ISO/IEC 27004 (guidelines)
NEN-ISO/IEC 27005 (guidelines)
NEN-ISO/IEC 27007 (guidelines)
kopie
NEN-ISO/IEC 27001
H4 t/m H10 ISMS
Bijlage-A (Annex A)
114 beheers-maatregelen
117 beheers-maatregelen
NEN-ISO/IEC 27002 (algemene maatregelen)
114 maatregelen + richtlijnen
kopie
NEN 7510-2 (Beheers-maatregelen)
NEN-EN-ISO 27799 (zorg-specifieke maatregelen)
kopie
117 maatregelen + richtlijnen
* Aantal definities afkomstig uit deze bron
Documentrelaties

HOOFDSTRUCTUUR (HIGH LEVEL STRUCTURE – HLS)

Het voorwoord van de norm gaat in op 'de compatibiliteit van de norm met de andere managementsysteemnormen'. Wat wordt hiermee bedoeld?

De norm NEN 7510-1 is niet de enige *managementsysteemnorm*. Andere managementsysteemnormen zijn bijvoorbeeld ISO/IEC 27001 (informatiebeveiliging), ISO/IEC 9001 (kwaliteit), ISO/IEC 14001 (milieu) en ISO/IEC 22301 (bedrijfscontinuïteit).

De norm NEN 7510-1 past de zogenaamde *hoofdstructuur* toe (Engels: High Level Structure - HLS), dat wil zeggen dat de norm dezelfde paragraaftitels, identieke tekst, gemeenschappelijke termen en kerndefinities gebruikt als de andere ISO/IEC-managementsysteemnormen. Deze compatibiliteit is nuttig voor organisaties die ervoor kiezen een enkelvoudig managementsysteem uit te voeren dat voldoet aan de eisen van twee of meer managementsysteemnormen.

- *Dit boek besteedt geen speciale aandacht aan het combineren van meerdere managementsysteemnormen.*

◆ NEN 7512 EN NEN 7513

De norm NEN 7510 wordt vaak in één adem genoemd met de normen NEN 7512 [14] en NEN 7513 [15]. Zijn deze twee normen ook verplicht?

NEN 7512 (GEGEVENSUITWISSELING)

De aanduiding 'NEN 7510' heeft volgens de wettelijke *Regeling gebruik burgerservicenummer* 'betrekking op de norm NEN 7510 zelf, en op uitwerkingen daarvan in de NEN 7511 en de NEN 7512'.

- *De norm NEN 7511 is inmiddels vervallen.*

De NEN 7512, die betrekking heeft op het uitwisselen van gegevens en een uitwerking is van de NEN 7510, is voor zorginstellingen dus ook verplicht.

Praktische informatie over het toepassen van de norm NEN 7512 is te vinden bij de uitleg van de normelementen 6.1.2 en 6.1.3 in dit boek.

NEN 7513 (LOGGING)

In 2018 kwam de NEN 7513 beschikbaar met eisen voor het 'vastleggen van acties op elektronische patiëntdossiers' (logging). In hetzelfde jaar werd het *Besluit elektronische gegevensverwerking door zorgaanbieders* van kracht 'houdende nadere regels over functionele, technische en organisatorische maatregelen bij elektronische gegevensverwerking door en tussen zorgaanbieders'.

Het genoemde besluit eist dat zorgaanbieders die aan elektronische verwerking van persoonsgegevens doen, moeten werken 'overeenkomstig het bepaalde in NEN 7510, NEN 7512 en NEN 7513'. Naast de NEN 7510 en de NEN 7512 is er dus ook een verplichting om te voldoen aan de NEN 7513.

Praktische informatie over het toepassen van de norm NEN 7513 is te vinden bij de uitleg van normelement 6.1.3 in dit boek.

- *De NEN 7512 en NEN 7513 zijn, net als de NEN 7510-1 en NEN 7510-2, gratis te verkrijgen via de webshop van NEN. De normen gelden alleen voor Nederland en zijn alleen verkrijgbaar in de Nederlandse taal.*

2. Informatiebeveiliging

WAT IS INFORMATIEBEVEILIGING?

Het begrip *informatiebeveiliging* kan worden opgesplitst in de volgende drie dimensies [1]:

- Het beschermen van de *vertrouwelijkheid* van informatie
- Het beschermen van de *integriteit* van informatie
- Het beschermen van de *beschikbaarheid* van informatie

BEHOUD VAN DE VERTROUWELIJKHEID VAN INFORMATIE

Als het om informatiebeveiliging gaat, wordt het begrip *vertrouwelijkheid* meestal als eerste genoemd. Bij het behoud van vertrouwelijkheid gaat het erom dat informatie niet beschikbaar of bekend wordt gemaakt aan onbevoegde personen, entiteiten of processen [1]. In plaats van het woord *vertrouwelijkheid* wordt ook wel het woord *exclusiviteit* gebruikt.

Verlies van vertrouwelijkheid van informatie kan op veel manieren plaatsvinden. Organisaties kunnen vertrouwelijke gegevens zonder toestemming delen met anderen. Een e-mail met vertrouwelijke informatie kan per ongeluk naar de verkeerde persoon worden gestuurd. Personen met kwade bedoelingen kunnen vertrouwelijke gegevens stelen of kopiëren en daar hun voordeel mee doen. Soms kunnen cliënten in de wachtkamer meeluisteren met vertrouwelijke gesprekken. Een indringer kan ongemerkt spionagesoftware installeren. Loslippige personen kunnen bewust of per ongeluk vertrouwelijke informatie delen. Een verloren, gestolen of onzorgvuldig afgedankte computer kan een schat aan vertrouwelijke gegevens bevatten.

Een verlies van vertrouwelijkheid van informatie kan niet alleen leiden tot een verlies van privacy, maar bijvoorbeeld ook tot identiteitsfraude.

Valkuil 2 'Informatiebeveiliging gaat over vertrouwelijkheid'

Soms wordt gedacht dat informatiebeveiliging alleen over het beschermen van de *vertrouwelijkheid* van informatie gaat. Binnen de context van de norm gaat informatiebeveiliging echter ook over de *integriteit* en de *beschikbaarheid* van informatie.

BEHOUD VAN DE INTEGRITEIT VAN INFORMATIE

Met de *integriteit* van informatie wordt de nauwkeurigheid en volledigheid van informatie bedoeld [1]. Het woord *integriteit* leidt nog wel eens tot verwarring omdat het ook buiten de context van informatiebeveiliging bestaat, namelijk in de vorm van een persoonlijke eigenschap (eerlijk, oprecht, niet omkoopbaar). Je zou kunnen zeggen dat integere informatie een eerlijk beeld geeft: nauwkeurig (juist) en volledig (compleet).

Verlies van integriteit van informatie kan bijvoorbeeld optreden door een onjuiste invoer, verwerking of presentatie van gegevens (handmatig of geautomatiseerd). Personen met kwade bedoelingen kunnen de juistheid en compleetheid van informatie opzettelijk aantasten om er beter van te worden of om schade te berokkenen. Iemand kan een verkeerde back-up terugplaatsen, waardoor informatie niet meer klopt of compleet is. Bedenk dat zelfs grote banken, ondanks hun talloze maatregelen, af en toe kampen met het probleem van onjuiste saldo's.

Vooral in de zorg is de juistheid van informatie van groot belang. Zo kan bijvoorbeeld onjuiste informatie verstrekt over een patiënt, of onjuiste informatie verstrekt aan een patiënt, ziekte, letsel of de dood tot gevolg hebben. Op een heel ander vlak, maar mogelijk met dezelfde gevolgen, kan onjuiste informatie binnen het ICT-beheer ertoe leiden dat informatiesystemen uitvallen, waardoor zorginformatie niet meer beschikbaar is.

BEHOUD VAN DE BESCHIKBAARHEID VAN INFORMATIE

Als het om informatiebeveiliging gaat, wordt het aspect *beschikbaarheid* vaak als laatste genoemd. Niet omdat het beschikbaar zijn van informatie als onbelangrijk wordt beschouwd, maar omdat het niet altijd meteen wordt gekoppeld aan het beveiligen van informatie. Bij het behoud van beschikbaarheid gaat het erom dat informatie toegankelijk en bruikbaar is op verzoek van een bevoegde entiteit [1], ofwel: de organisatie of de persoon die (of het proces dat) over de informatie wil en mag beschikken.

Verlies van beschikbaarheid van informatie kan tijdelijk of permanent zijn. Een verlies kan veroorzaakt worden door onbedoelde oorzaken zoals foutieve handelingen, technische storingen of natuurrampen. Uitval van systemen kan leiden tot verlies van gegevens en uitval van spreekuren of operatieprogramma's. Personen met kwade bedoelingen kunnen informatie vernietigen, ontoegankelijk maken of onleesbaar maken. Iemand kan een

DDoS-aanval opzetten om informatiesystemen opzettelijk te verstoren. Informatiedragers zoals papier, tapes, harde schrijven en usb-sticks kunnen door veroudering hun informatie verliezen. Soms is informatie niet meer beschikbaar omdat een overleden persoon als enige bepaalde wachtwoorden kende.

Een verlies van beschikbaarheid van informatie kan grote gevolgen hebben. Zo hebben artsen bij ICT-uitval soms geen toegang meer tot patiëntendossiers en moeten belangrijke gegevens, zoals laboratoriumuitslagen, handmatig worden vastgelegd en telefonisch worden doorgegeven, wat tot vertraging kan leiden en de kans op het maken van fouten groter maakt. Bij ICT-uitval moeten ziekenhuizen soms behandelingen uitstellen, patiënten verplaatsten of een opnamestop afkondigen. In het kader van de geneeskundige hulpverlening hebben basis-SEH's de verplichting om, ook bij uitval van nutsvoorzieningen, apparatuur en ICT-middelen, de zorg te continueren, wat hoge eisen stelt aan de beschikbaarheid van informatie.

- *Na de uitbraak van het coronavirus in 2020 probeerden criminelen wereldwijd ziekenhuizen plat te leggen en af te persen. In sommige gevallen lukte dit, zoals bij het universitair ziekenhuis in de Tsjechische stad Brno.*

BIV / BIV-CLASSIFICATIE

Om de drie dimensies van informatiebeveiliging af te korten, wordt in de praktijk vaak de afkorting BIV gebruikt. De volgorde van de letters is daarbij willekeurig gekozen (in het Engels wordt de afkorting CIA gebruikt: Confidentiality, Integrity, Availability).

Informatiesystemen, bedrijfsprocessen en gegevens worden soms geclassificeerd volgens een zogenaamde BIV-classificatie. Het hoogst geclassificeerd systeem kent dan bijvoorbeeld een BIV-klasse van 333, het laagst geclassificeerd systeem de BIV-klasse 111. Op basis van deze classificatie worden dan passende beheersmaatregelen getroffen.

De norm schrijft het gebruikt van een BIV-classificatie niet voor, maar beschrijft in Bijlage-A wel iets wat erop lijkt. Volgens beheersmaatregel A.8.2.1 moet informatie worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking en wijziging. Zie hoofdstuk 11 'Bijlage-A' in dit boek voor meer informatie over het classificeren van informatie.

OVERIGE ASPECTEN

Informatiebeveiliging kan ook andere eigenschappen betreffen, zoals [1]:

- *Onweerlegbaarheid*. Hiermee wordt het vermogen bedoeld om te bewijzen dat een geclaimde gebeurtenis of actie zich daadwerkelijk heeft voorgedaan. Denk bijvoorbeeld aan het laten plaatsen van een handtekening voor ontvangst bij het afleveren van een postpakket.
- *Authenticiteit*: Hierbij gaat het om de eigenschap dat een entiteit is wat zij claimt te zijn. Denk bijvoorbeeld aan het gebruik van een digitaal certificaat dat zorgt dat iemand weet dat berichten van een bepaalde verzender afkomstig zijn (bronauthenticiteit).
- *Betrouwbaarheid*. Hiermee wordt de eigenschap bedoeld van consistent beoogd gedrag en consistente resultaten. Denk bijvoorbeeld aan informatie die de ene keer snel en de andere keer traag op een beeldscherm verschijnt, of waarbij de getoonde informatie per keer verschilt, terwijl dat niet de bedoeling is.

OVER WELKE INFORMATIE GAAT HET BIJ DE NORM NEN 7510-1?

Paragraaf 0.1 van de norm legt uit dat het bij informatiebeveiliging om alle soorten informatie gaat waarvan de beschikbaarheid, integriteit en vertrouwelijkheid moet worden beschermd, maar dat bij het toepassen van de norm op eerste plaats moet gedacht worden aan het beschermen van *persoonlijke gezondheidsinformatie*.

Persoonlijke gezondheidsinformatie is informatie over een identificeerbare persoon die verband houdt met de lichamelijke of geestelijke gesteldheid van, of de verlening van zorgdiensten aan, de persoon in kwestie [1].

Toch gaat het bij informatiebeveiliging in de zorg niet alleen om het beschermen van persoonlijke gezondheidsinformatie. Denk bijvoorbeeld aan gegevens over zorgverleners, personeel en vrijwilligers. Denk ook aan gegevens ter ondersteuning van klinische besluiten, aan statistische gegevens en aan onderzoeksgegevens. Denk ook aan technische informatie over de werking van zorginformatiesystemen en aan informatie over de fysieke en logische beveiliging daarvan. Al deze gegevens moeten worden beschermd.

Valkuil 3 'Informatiebeveiliging gaat over persoonsgegevens'

Bij informatiebeveiliging gaat het niet alleen om het beschermen van persoonsgegevens. Bij informatiebeveiliging gaat het om het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie die relevant is voor de activiteiten, diensten en producten van een organisatie (zie ook de uitleg bij normelement 4.3 in dit boek).

- *In een later stadium moet u risico's gaan identificeren voor alle informatie binnen het toepassingsgebied (zie eis 6.1.2-c1 in de norm, en de uitleg bij normelement 6.1.2 in dit boek).*

Paragraaf 0.3 van de norm gaat in op alle soorten informatie binnen de zorg waarvan de beschikbaarheid, integriteit en vertrouwelijkheid behoort te worden beschermd.

INFORMATIEBEVEILIGING EN DE AVG

Hiervoor zagen we dat het begrip *informatiebeveiliging* betrekking kan hebben op alle soorten informatie, dus ook op persoonsgegevens. Zodra het over de bescherming van persoonsgegevens gaat, is in Europees verband de GDPR en in Nederland de daarvan afgeleide Algemene Verordening Gegevensbescherming (AVG) van belang. Behalve over gewone persoonsgegevens spreekt de AVG ook over bijzondere persoonsgegevens in de vorm van 'persoonsgegevens over gezondheid'.

Artikel 32 van de AVG gaat over *Beveiliging van de verwerking*. In dit artikel spreekt de verordening over [17]:

> *(…) het treffen van passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten: (…) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen.*

Zoals u bij het lezen van dit boek zult zien, komt 'het treffen van maatregelen die afgestemd zijn op risico's' en 'het op gezette tijden evalueren van de doeltreffendheid van die maatregelen' overeen met de aanpak van de norm NEN 7510-1.

INFORMATIEBEVEILIGING EN DATALEKKEN

In Nederland kennen we het woord *datalek*. In de AVG komt het woord 'datalek' niet voor en wordt er in plaats daarvan gesproken over een 'inbreuk in verband met persoonsgegevens'.

In de praktijk wordt vaak gedacht dat een *datalek* alleen betrekking heeft op het aspect *vertrouwelijkheid*, maar volgens de Autoriteit Persoonsgegevens zijn er drie categorieën *datalekken* te onderscheiden [19]:

- inbreuk op de vertrouwelijkheid van persoonsgegevens;
- inbreuk op de integriteit van persoonsgegevens;
- inbreuk op de beschikbaarheid van persoonsgegevens.

Zoals u ziet sluiten de definities van de drie verschillende soorten datalekken volledig aan bij de drie eerder besproken dimensies van informatiebeveiliging.

➢ *Dit boek gaat niet over de AVG, maar zal daar soms wel naar verwijzen.*

INFORMATIEBEVEILIGING EN DE NORM ISO/IEC 27701

In het jaar 2019 kwam de internationale norm ISO/IEC 27701 beschikbaar. Deze norm gaat over het opzetten van een Privacy Information Management System (PIMS) en wordt door velen beschouwd als 'de schakel tussen informatiebeveiliging en de AVG'.

De norm ISO/IEC 27701 is een uitbreiding op de normen ISO/IEC 27001 (vaak wordt de term 'add-on' of 'plug-in' gebruikt) en beschrijft hoe het aspect *privacy* in het ISO/IEC 27001-managementsysteem moet worden geïntegreerd.

Vanwege de nauwe verwantschap tussen NEN 7510-1 en ISO/IEC 27001, is een dergelijke integratie ook mogelijk met NEN 7510-1.

3. Managementsysteem

ALGEMEEN

In paragraaf 0.6.1 van de NEN 7510-1 kunt u lezen dat de norm eisen bevat voor een *managementsysteem voor informatiebeveiliging*. Zoals u in dit boek stap voor stap zult zien, is dit een systeem dat een organisatie kan helpen bij het inrichten, implementeren, onderhouden en continu verbeteren van de informatiebeveiliging.

Om een beetje warm te lopen voor het door u in te richten managementsysteem voor informatiebeveiliging, besteedt dit hoofdstuk aandacht aan het doel en de achterliggende gedachte van dit systeem. Specifieke uitleg vindt u vanaf hoofdstuk 4 in dit boek.

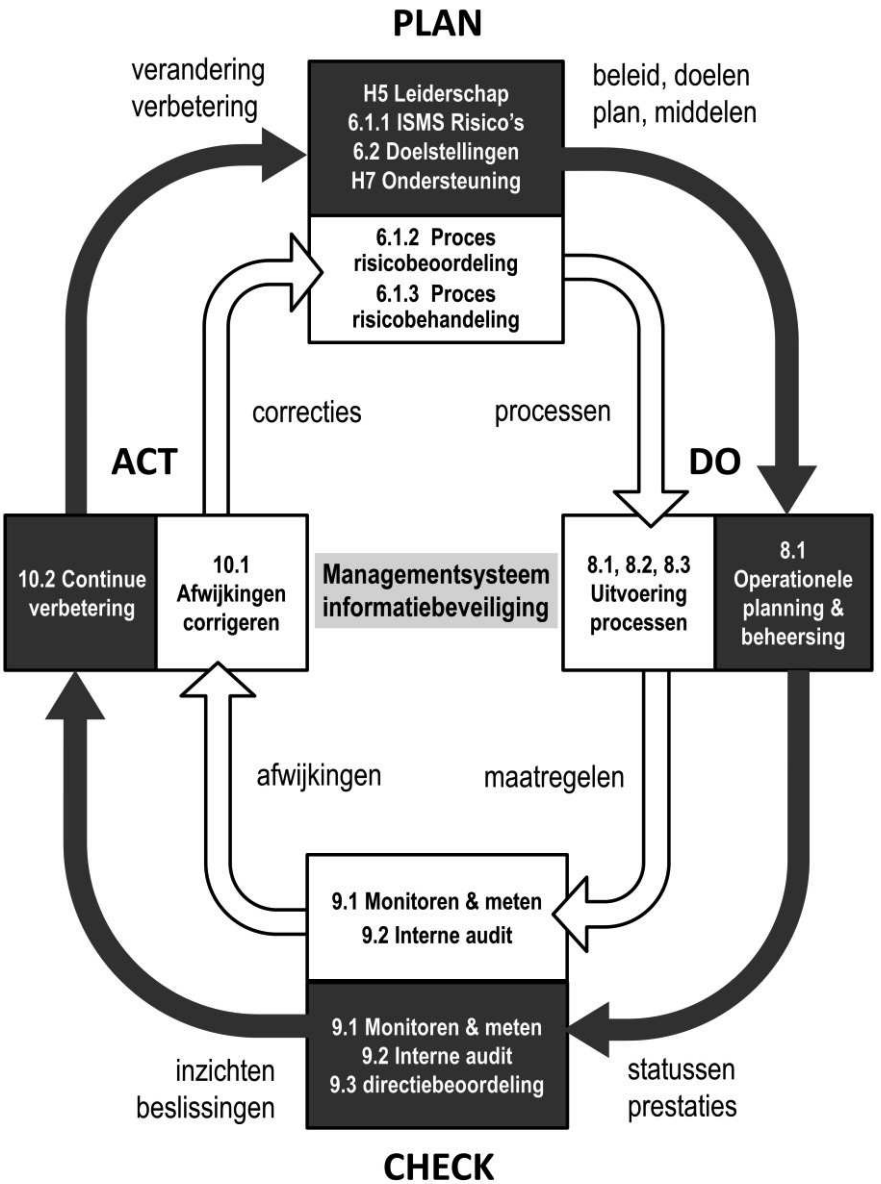
ISMS

Voor het aanduiden van een managementsysteem voor informatiebeveiliging wordt vaak de afkorting *ISMS* gebruikt (van het Engelse 'Information Security Management System'). Om verwarring te voorkomen en om aan te blijven sluiten bij het taalgebruik van de norm, wordt de aanduiding ISMS in dit boek niet gebruikt.

PDCA

Hoewel de norm zelf geen verwijzing maakt naar de kwaliteitscirkel van Deming (een wereldwijd bekend en veel toegepast model voor kwaliteitsverbetering), zijn de onderdelen van het managementsysteem duidelijk te linken aan de Plan-Do-Check-Act-fasen van dit model.

In de afbeelding op de volgende pagina is de norm vertaald naar de cirkel van Deming. In het model staan twee PDCA-cirkels: een binnen-cirkel (de witte) en een buiten-cirkel (de zwarte). De nummers en titels in het model verwijzen naar de hoofdstukken en paragrafen van de norm én naar de gelijknamige hoofdstukken en paragrafen van dit boek.


PLAN
verandering
verbetering
H5 Leiderschap
6.1.1 ISMS Risico's
6.2 Doelstellingen
H7 Ondersteuning
beleid, doelen
plan, middelen
6.1.2 Proces
risicobeoordeling
6.1.3 Proces
risicobehandeling
correcties
processen
ACT
DO
10.2 Continue
verbetering
10.1
Afwijkingen
corrigeren
Managementsysteem
informatiebeveiliging
8.1, 8.2, 8.3
Uitvoering
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

- *Het model van het managementsysteem met de twee cirkels is van de auteur van dit boek en is dus niet afkomstig uit de norm.*

De binnenste PDCA-cirkel van het getoonde model heeft rechtstreeks betrekking op het managen van informatiebeveiligingsrisico's. Deze cirkel is bij alle organisaties in zekere mate al aanwezig: er zijn ideeën over het omgaan met informatiebeveiligingsrisico's (plan), er worden maatregelen getroffen om die risico's te beheersen (do), er wordt gecontroleerd of de maatregelen het gewenste resultaat opleveren (check) en er wordt actie ondernomen als dit niet het geval is (act).

Helaas blijkt de binnenste cirkel in de praktijk niet altijd even goed te functioneren. Door een gebrek aan discipline, systematiek en ondersteuning kunnen er onzichtbare gevaren in de organisatie sluipen die plotseling toeslaan en grote schade aanrichten. Hiervan zien we dagelijks de gevolgen in de vorm van een verlies van vertrouwelijkheid, integriteit en beschikbaarheid van informatie bij talloze organisaties.

Daarom is er een tweede PDCA-cirkel. Deze buitenste cirkel biedt ondersteuning aan de binnenste cirkel in de vorm van leiderschap en ondersteuning (plan), planning en beheersing (do), een systematische evaluatie van prestaties (check) en een continue verbetering van het systeem als geheel (act).

De omloopsnelheden van de twee PDCA-cirkels kunnen verschillen, maar de buitenste cirkel zoekt regelmatig contact met de binnenste, voedt hem en bewaakt hem nauwlettend (zoals u in dit boek kunt lezen).

Zodoende biedt invoering van een managementsysteem voor informatiebeveiliging op twee fronten verbetering: de introductie van een formeel proces voor het managen van informatiebeveiligingsrisico's (de binnenste cirkel) en het gebruik van een ondersteunend proces daar omheen (de buitenste cirkel). Het geheel vormt een zeer krachtig systeem dat overal ter wereld wordt toegepast en nog steeds in populariteit groeit.

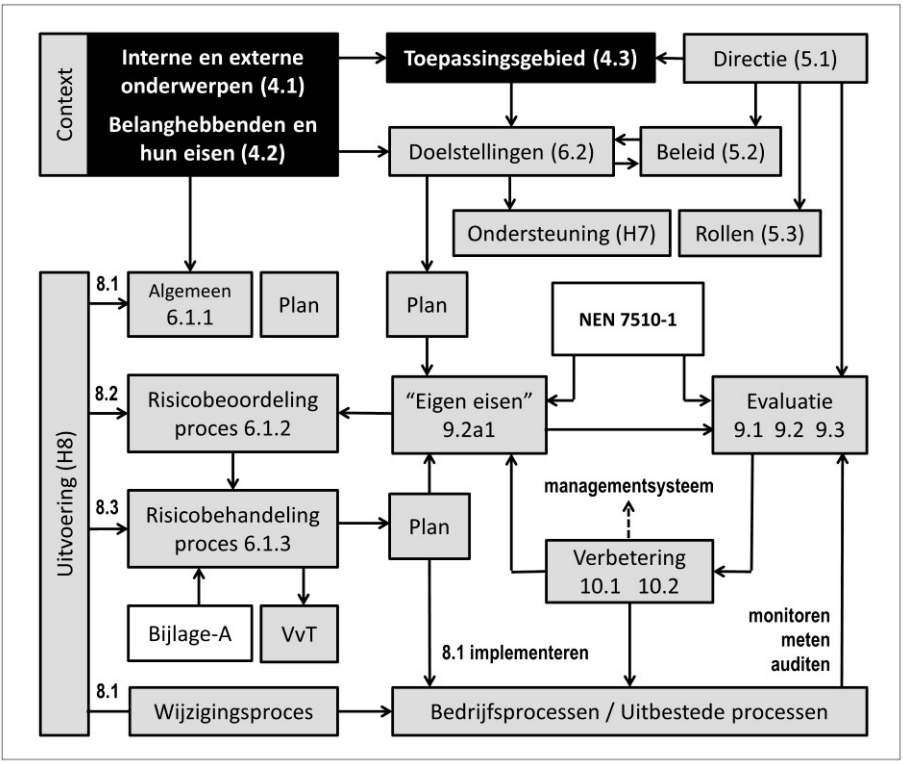
Ten aanzien van het gebruik van de binnenste cirkel, die u waarschijnlijk al heeft, is het mogelijk dat u de touwtjes wat strakker moet aantrekken dan u op dit moment doet: alle processen van het systeem moeten worden gedocumenteerd en volgens een planning worden toegepast. De buitenste cirkel is bij veel organisaties nog onvoldoende aanwezig of onvoldoende aantoonbaar.

Voor wie de kwaliteitscirkel van Deming een handige methode vindt, is in dit boek aan het begin van de hoofdstukken 5 t/m 10 met een PDCA-afbeelding aangegeven bij welke fase van de cirkel het hoofdstuk hoort.

4. Context

In hoofdstuk 4 van de norm draait het om de volgende vragen:

1) Welke interne en externe factoren zijn relevant voor uw management-systeem voor informatiebeveiliging?
2) Welke behoeften en verwachtingen van belanghebbenden zijn relevant voor uw managementsysteem voor informatiebeveiliging?
3) Wat is een geschikt toepassingsgebied voor uw managementsysteem voor informatiebeveiliging?
4) Hoe gaat u een managementsysteem voor informatiebeveiliging inrichten, implementeren, onderhouden en continu verbeteren in overeenstemming met de eisen van de norm?



4.1 De organisatie en haar context

INLEIDING

Normelement 4.1 eist dat u alle *externe en interne onderwerpen* vaststelt:

- die relevant zijn voor uw *doelstelling*;
- die het vermogen van uw organisatie kunnen beïnvloeden om de *beoogde resultaten* van uw managementsysteem voor informatiebeveiliging te behalen.

➢ *De norm spreekt bij 4.1 over 'onderwerpen'. De Engelstalige norm ISO/IEC 27001 [6], die de brontekst van de norm NEN 7510-1 bevat, spreekt over 'issues' (vraagstukken). Omdat het woord 'onderwerpen' vrij neutraal is en het in werkelijkheid om bepalende factoren gaat, wordt in de praktijk vaak over 'factoren' gesproken. Voor een beter begrip spreekt dit boek daarom vanaf hier steeds over 'externe en interne factoren'.*

De door u vast te stellen *externe en interne factoren* moet u in een later stadium gebruiken tijdens het implementeren van uw managementsysteem voor informatiebeveiliging. U wordt verwacht dit te doen bij:

- het vaststellen van het toepassingsgebied van uw managementsysteem (zie de uitleg bij normelement 4.3);
- het vaststellen en behandelen van risico's die voorkomen dat het managementsystemen voor informatiebeveiliging zijn beoogde resultaten behaalt (zie de uitleg bij normelement 6.1.1);
- het vaststellen van meetbare informatiebeveiligingsdoelstellingen [8] (zie de uitleg bij normelement 6.2).

EXTERNE EN INTERNE FACTOREN: DOELSTELLING ORGANISATIE

Het woord *doelstelling* dat bij normelement 4.1 wordt genoemd, gaat over uw strategische doelstelling met betrekking tot informatiebeveiliging. Bijvoorbeeld: 'het leveren van veilige en betrouwbare zorg en het vertrouwen bieden dat risico's adequaat worden beheerst'. De vraag waar het bij dit normelement om gaat is: welke positieve en negatieve factoren zijn relevant voor het behalen van uw doelstelling?

Voorbeeld

Een zorginstelling met twee vestigingen heeft als doelstelling 'het leveren van veilige en betrouwbare zorgdiensten en het vertrouwen bieden aan patiënten en andere belanghebbenden dat risico's adequaat worden beheerst. Tijdens een brainstorm komen de volgende interne factoren naar voren die relevant zijn voor deze doelstelling:

Zorginstelling: Interne factoren
De twee vestigingen denken verschillend over informatiebeveiliging en de wijze waarop dit moet worden gemanaged.
Proces van besluitvorming is soms erg traag.
Een deel van de medewerkers is zich onvoldoende bewust van informatiebeveiligingsrisico's.
Hoge werkdruk. Op de werkvloer is er regelmatig sprake van spanning tussen veiligheid en werkbaarheid.
Informatiebeveiliging is nog te weinig omgezet naar uitgewerkt beleid, er wordt nog veel 'in de praktijk' geregeld.
Te weinig controle op gedrag van medewerkers.
Verantwoordelijkheden ten aanzien van informatiebeveiliging zijn niet altijd duidelijk.
5 medewerkers beheersen niet de Nederlandse taal.

Tijdens dezelfde brainstorm komen de volgende externe factoren naar voren die relevant zijn voor de doelstelling:

Zorginstelling: Externe factoren
Groeiend eisenpakket informatiebeveiliging overheid en andere belanghebbenden.
Krapte op de arbeidsmarkt, te weinig capaciteit voor informatiebeveiliging.
We zien steeds weer nieuwe vormen van 'social engineering' op ons afkomen.
Patiënten worden zich bewuster van hun privacyrechten en spreken ons daarop aan.

Het voorgaande voorbeeld ging over een zorginstelling, het volgende voorbeeld gaat over de interne en externe factoren bij een toeleverancier:

Voorbeeld

Een hostingprovider met klanten in de zorg heeft als bedrijfsdoelstelling 'veilige en betrouwbare IT-diensten leveren en vertrouwen bieden aan (zorg)klanten dat risico's adequaat worden beheerst'. Tijdens een brainstorm komen de volgende interne factoren naar voren die relevant zijn voor deze doelstelling:

Sterktes (intern)
Gunstige financiële positie.
Gemotiveerd personeel.
Nooit ernstige incidenten gehad.
Veel IT-kennis.
Goede tools.

Zwaktes (intern)
Weinig formele processen en regels.
Weinig interne controles.
Weinig inzicht in risico's.
Laag bewustzijn bij sommige medewerkers.

Om een beter beeld te krijgen van de context, betrekt de organisatie de door haar vastgestelde factoren in een bredere analyse. Hiervoor wordt een zogenaamde *SWOT-analyse* gebruikt (Strength, Weakness, Opportunity, Threat).

	FACTOREN VOOR HET BEHALEN VAN HET BEDRIJFSDOEL	
	POSITIEF	**NEGATIEF**
INTERN	**Sterktes** • Gunstige financiële positie. • Gemotiveerd personeel. • Nooit ernstige incidenten gehad. • Veel IT-kennis. • Goede tools.	**Zwaktes** • Weinig inzicht in risico's. • Weinig formele processen en regels. • Weinig interne controles op doeltreffendheid van maatregelen. • Laag bewustzijn t.a.v. informatiebeveiliging bij sommige medewerkers.
EXTERN	**Kansen** • Een NEN 7510-certificaat is een kans om klanten nog meer vertrouwen te bieden.	**Bedreigingen** • Probleem bij leverancier X. • Krapte op de arbeidsmarkt. • Veranderende wetgeving. • Steeds nieuwe vormen cybercrime.

- *Let op: de norm verplicht u niet om een SWOT-analyse uit te voeren. In principe hoeft u bij normelement 4.1 alleen maar interne en externe factoren vast te stellen.*

INTERNE EN EXTERNE FACTOREN: BEOOGDE RESULTATEN

Zodra het strategische besluit is genomen om binnen een bepaalde tijd een managementsysteem voor informatiebeveiliging te gaan invoeren, komt de volgende vraag naar voren: welke positieve en negatieve factoren beïnvloeden het vermogen van uw organisatie 'om de beoogde resultaten van uw managementsysteem te behalen'? (zie norm-eis 4.1).

Voorbeeld

Dezelfde hostingprovider als in het vorige voorbeeld organiseert ook een brainstorm over de interne factoren die 'de beoogde resultaten van het managementsysteem' beïnvloeden. De uitkomsten worden in een SWOT-analyse geplaatst.

INTERNE FACTOREN VOOR HET MANAGEMENTSYSTEEM	
POSITIEF	**NEGATIEF**
Sterktes • Betrokkenheid directie. • Kleine organisatie, snelle beslissingen. • Gemotiveerd personeel. • Veel IT-kennis. • Goede tools.	**Zwaktes** • Beperkte mankracht. • Weinig kennis van NEN 7510. • Weinig kennis van de wet. • Laag bewustzijn t.a.v. informatiebeveiliging bij sommige medewerkers. • Documentatie is rommelig.
Kansen • Vermindering aantal incidenten. • Verbetering bestaande processen. • Betere samenwerking met klanten en leveranciers. • Beter voldoen aan wettelijke en contractuele eisen.	**Bedreigingen** • Project X gaat dit jaar veel mankracht eisen wat ten koste kan gaan van het managementsysteem. • Dit jaar gaan drie ervaren medewerkers met pensioen.

Het is logisch dat er bij het bepalen van interne en externe factoren soms een overlap is tussen de doelstelling van de organisatie en de beoogde resultaten van het managementsysteem. De resultaten van het managementsysteem dragen immers bij aan het behalen van uw bedrijfsdoelstelling.

INTERNE FACTOREN VASTSTELLEN

Denk bij het vaststellen van interne factoren bijvoorbeeld aan:

- de omvang van uw organisatie;
- uw bedrijfscultuur;
- de volwassenheid van leiderschap, beleid, processen en procedures;
- uw verplichtingen, doelstellingen en plannen voor de toekomst;
- uw beschikbare middelen zoals kapitaal, mankracht en tijd.

Bij grotere organisaties spelen vaak andere interne factoren dan bij kleinere.

EXTERNE FACTOREN VASTSTELLEN

Denk bij het vaststellen van externe factoren bijvoorbeeld aan;

- de invloed van de economische situatie en het politieke klimaat;
- wet- en regelgeving op het gebied van informatiebeveiliging;
- technologische ontwikkelingen die buiten uw organisatie spelen;
- ontwikkelingen bij uw leveranciers.

Kenmerkend voor externe factoren is dat u er meestal geen of weinig invloed op kan uitoefenen. Dit betekent dat u een manier moet vinden om met deze factoren om te gaan.

Valkuil 4 Factoren bepaald voor het beoogde toepassingsgebied

Kijk bij het vaststellen van interne en externe factoren nog niet naar het beoogde *toepassingsgebied* van uw managementsysteem (zie de uitleg bij normelement 4.3). Het is juist de bedoeling dat u dit *toepassingsgebied* mede op basis van de interne en externe factoren gaat bepalen.

🕮 VERPLICHTE DOCUMENTATIE

In de eisen van normelement 4.1 wordt nergens gesteld dat er iets gedefinieerd of gedocumenteerd moet worden (woorden die u bij veel andere normelementen wel tegenkomt).

Om te kunnen aantonen dat aan de eisen van de norm wordt voldaan, kunt u een gedocumenteerd overzicht maken van uw externe en interne factoren.

☑ AANWIJZINGEN VOOR HET UITVOEREN VAN AUDITS

Met betrekking tot de hiervoor besproken eisen van normelement 4.1 zou een auditor kunnen onderzoeken:

- of de organisatie een 'doelstelling' heeft geformuleerd met betrekking tot informatiebeveiliging (dit is geen eis, maar volgens normelement 4.1 wel een noodzakelijke voorwaarde om interne en externe factoren te kunnen vaststellen);
- of de organisatie interne en externe factoren heeft vastgesteld die relevant zijn voor haar doelstelling met betrekking tot informatiebeveiliging (zie het punt hierboven);
- of de organisatie 'beoogde resultaten' heeft geformuleerd met betrekking tot het managementsysteem voor informatiebeveiliging (dit is geen eis, maar volgens normelement 4.1 wel een noodzakelijke voorwaarde);
- of de organisatie interne en externe factoren heeft vastgesteld die haar vermogen kunnen beïnvloeden om de beoogde resultaten van haar managementsysteem voor informatiebeveiliging te behalen;
- of de organisatie regelmatig onderzoekt of de vastgestelde informatie over interne en externe factoren compleet en actueel is.

4.2 Belanghebbenden en hun eisen

INLEIDING

Normelement 4.2 eist dat u vaststelt welke *belanghebbenden* relevant zijn voor uw managementsysteem voor informatiebeveiliging en welke eisen van deze belanghebbenden relevant zijn voor informatiebeveiliging. De vastgestelde informatie moet u in een later stadium gebruiken tijdens het implementeren van uw managementsysteem voor informatiebeveiliging. Net als bij de interne en externe factoren (zie normelement 4.1) wordt u verwacht dit te doen bij:

- het vaststellen van het toepassingsgebied van uw managementsysteem (zie de uitleg bij normelement 4.3);
- het vaststellen en behandelen van algemene risico's om te zorgen dat het managementsystemen voor informatiebeveiliging zijn beoogde resultaten behaalt (zie de uitleg bij normelement 6.1.1);
- het vaststellen van informatiebeveiligingsdoelstellingen [8] (zie de uitleg bij normelement 6.2).

◆ SOORTEN BELANGHEBBENDEN

Wat bedoelt de norm met *belanghebbenden*? Een belanghebbende is [1]:

- een persoon of organisatie die invloed kan hebben op een beslissing of activiteit van uw organisatie;
- een persoon of organisatie die beïnvloed kan worden door een beslissing of activiteit van uw organisatie;
- een persoon of organisatie die ervaart dat hij wordt beïnvloed (positief of negatief) door een beslissing of activiteit van uw organisatie.

➢ *De norm gebruikt het woord 'belanghebbenden'. De Engelstalige norm ISO/IEC 27001 [6], die de brontekst van de norm NEN 7510-1 bevat, spreekt over 'interested parties'. In de praktijk wordt in Nederland in plaats van het woord 'belanghebbende' ook wel het woord 'stakeholder' gebruikt. Het onderzoek dat in het kader van normelement 4.2 moet worden uitgevoerd met betrekking tot belanghebbenden en hun eisen, wordt om die reden ook wel een 'stakeholderanalyse' genoemd. Om verwarring te voorkomen en om aan*

te blijven sluiten bij het taalgebruik van de norm, wordt de aanduiding 'stakeholder' in dit boek niet gebruikt.

De volgende soorten belanghebbenden kunnen onderscheiden worden:

- *Intern*: personen of partijen binnen uw organisatie.
- *Extern*: externe personen of organisaties, zoals klanten, partners, leveranciers en crediteuren.
- *Interface*: partijen die niet betrokken zijn bij de organisatie, maar die een specifiek (legitiem) belang hebben en invloed uitoefenen. Denk aan de overheid, toezichthouders, Kamer van Koophandel, brancheorganisaties, de maatschappij, etc.

Hieronder zijn enkele voorbeelden van belanghebbenden opgenomen die invloed kunnen hebben op, of invloed kunnen ondervinden vanuit uw organisatie.

◆ INTERNE BELANGHEBBENDEN

BELANGHEBBENDEN (INTERN): DIRECTIE

De directie van een organisatie is de eerste relevante belanghebbende voor het managementsysteem voor informatiebeveiliging. De directie heeft er alle belang bij dat de bedrijfsdoelstelling niet in gevaar komt en dat het managementsysteem zijn beoogde resultaten behaalt. Als het aan de norm ligt, dan speelt de directie een zeer belangrijke rol bij informatiebeveiliging (zie de uitleg bij de normelementen 5.1, 5.2, 5.3 en 9.3).

BELANGHEBBENDEN (INTERN): RVC, RVT, RVB

Een onderneming of instelling heeft doorgaans naast een directie een toezichthoudend orgaan. Dit orgaan benoemt en ontslaat directieleden en speelt een belangrijke rol bij directiebesluiten, zoals het vaststellen van de begroting of het doen van grote investeringen.

De naam van het toezichthoudend orgaan verschilt per sector en rechtsvorm van de organisatie. Bij zorginstellingen is de raad van toezicht (RvT) verantwoordelijk voor het toezicht op het beleid van de raad van bestuur