NEN 7510 stappenplan: Hoe u kwetsbare gegevens in de zorg beschermt

Leer van onze experts welke stappen nodig zijn om gevoelige informatie te beschermen en tot NEN 7510 certificering te komen

Inhoudsopgave

1.	Bepaal uw doel	6
2.	Stel een projectplan op	9
3.	Breng de huidige en gewenste situatie in kaart	17
4.	Het managementsysteem opzetten	22
5.	De informatiebeveiligingsrisico's aanpakken	45
6.	De informatiebeveiligingsrisico's behandelen	53
7.	Het managementsysteem certificeren	58

Hoe dit stappenplan u gaat helpen

Als zorgspecialist bent u het liefst alleen maar met uw vak bezig. Normeringen, regelgevingen en informatiebeveiliging heeft niet uw focus en het kan knap lastig zijn dit goed te organiseren. Want hoe krijgt u beschikking over de benodigde kennis? En waar haalt u de tijd vandaan?

We merken dat het voor zorginstellingen een uitdaging is om grip te krijgen op het beveiligen van patiëntgegevens en andere gevoelige patiënteninformatie. In de zorg worden ontzettend veel gegevens uitgewisseld die een hoge mate van privacy bevatten. Als hier iets mee gebeurd heeft dit direct impact op mensen en soms zelfs mensenlevens.

Om u te ondersteunen hebben we het Stappenplan NEN 7510 gepubliceerd. Dit helpt u een idee te krijgen van de te nemen stappen om tot certificering te komen.

Dit stappenplan is geen vervanging van de norm, maar kunt u bij de hand houden als ondersteunend document en wellicht zelfs als basis gebruiken voor uw implementatieplan.

Stap 1 - Wat wilt u bereiken?

1. Bepaal uw doel

U bent als zorgverlener verantwoordelijk voor de beveiliging van gevoelige informatie van uw patiënten. Om de beveiliging van informatie goed in te richten, dient u de nodige investeringen te doen in zowel tijd als geld. U wilt dan ook dat het proces soepel verloopt. En daar is een duidelijke route voor nodig.

Daarom beginnen we bij het begin: wat is uw doel?

Het doel lijkt misschien vanzelfsprekend, maar de invulling van het managementsysteem kan er wezenlijk anders uitzien afhankelijk van uw zienswijze. Stel uzelf de vraag wat u wilt bereiken met het project en welke meerwaarde het heeft voor uw organisatie. Denk aan het vergroten van het vertrouwen bij patiënten, het terugdringen van informatiebeveiligingsrisico's, afbreukrisico's beperken of imagoschade voorkomen.

U of uw directie zullen commitment en leiderschap moeten tonen en het behalen van de doelstellingen moeten ondersteunen. Het draagvlak van de directie heeft u bovendien nodig om elders in de organisatie mensen mee te krijgen.

De betrokkenheid van de directie kan worden vastgesteld op basis van de bijdrage aan onderstaande aspecten:

- Het vaststellen van het informatiebeveiligingsbeleid en de doelstellingen
- Zorg dragen voor integratie van eisen van het managementsysteem voor informatiebeveiliging in processen
- Het beschikbaar stellen van benodigde middelen om doelstellingen te behalen
- Communicatie over (eisen aan) het managementsysteem
- Mede zorgdragen voor het behalen van beoogde resultaten
- Benodigde sturing en ondersteuning van mensen
- Het bevorderen van continue verbetering van prestaties
- Het communiceren van prestaties
- Verantwoordelijkheid nemen voor het management-systeem voor informatiebeveiliging

Stap 2 - De planning maken

2. Stel een projectplan op

Het is verstandig een planning te maken voordat u aan de slag gaat. Het loopt nooit helemaal zoals verwacht en juist om deze reden is het goed de zaken vooraf in kaart te brengen. Wanneer de omvang van het project verandert door bijvoorbeeld een miscommunicatie of veranderende verwachtingen, wilt u risico's rondom het overschrijden van tijdsplanningen en budgetten beperken.

Let wel, een projectplan stelt u in het beginstadium op, maar wordt continu bijgewerkt aan de hand van de laatste wijzigingen. U kunt zelf bepalen op basis van welke methode u uw project gaat plannen en uitvoeren.

2.1 Bepaal de omvang

Goede afspraken maken over wat wel en wat niet onder uw verantwoordelijkheden valt en onder die van het project, zorgt ervoor dat u later in het proces miscommunicaties voorkomt. Daarom is het verstandig vooraf de definitieve scope van het project te bepalen. Hoe doet u dit?

U kunt dit bijvoorbeeld doen door de vastgelegde details over de eisen en wensen van de directie en andere betrokkenen als uitgangspunt te nemen. Stel uzelf de vraag: Welke onderwerpen zijn onderdeel van het project - en vooral ook welke niet?

2.2 Stel eisen en doelstellingen op

Om de eisen uit de NEN 7510 norm en van uw eigen organisatie - en de doelstellingen scherp te krijgen, kunt u een antwoord formuleren op de volgende vraag:

Welke doelstellingen moet het managementsysteem bereiken om te kunnen zeggen dat het succesvol is?

Deze vraag heeft betrekking op de verwachtingen die uw directie heeft uitgesproken over het managementsysteem - maar ook eisen vanuit belanghebbenden en wetgeving.

Bepaal welke rollen, verantwoordelijkheden en bevoegdheden u moet toekennen. Definieer in elk geval de rollen en verantwoordelijkheden van:

- **De projectleider**

Wie is verantwoordelijk voor het organiseren van het project en dat het project op tijd, op basis van de vastgestelde doelstellingen en binnen budget wordt afgerond?

- **Teamleden**

Bepaal welke mensen daadwerkelijk het project mee helpen uitvoeren en taken toe bedeeld krijgen. Weeg hierin af welke expertise of inzichten er cruciaal zijn voor het project.

- **Sponsor**

Zorg dat u voor deze stap al met de directie om tafel hebt gezeten omdat zij sponsor van het project moeten zijn en zorgen voor de juiste ondersteuning en commitment.

- **De project-partner (optioneel)**

Indien u heeft bepaald dat er een projectpartner, zoals een adviseur, betrokken is bij het project - kunt u mogelijk afspraken maken over het verder uit handen geven van de projectbegeleiding en het implementatieplan.

- **Financiële middelen**

Houd rekening met mogelijke operationele uitgaven voor informatiebeveiliging op het gebied van infrastructuur en mogelijke voorzieningen.

Hoewel de meeste kosten zitten in de voorbereidingen en implementatie van het project, dient u ook rekening te houden met de uiteindelijke kosten voor het certificaat.

Houdt in dat geval rekening met mogelijke kosten voor:

- Training
- Advies en/of begeleiding

2.3 Maak een tijdsplanning

Om een goede planning te kunnen maken, kan een tijdsplan hierin niet ontbreken. Denk daarom in deze fase na over de volgende zaken:

- Hoe zorg ik dat ik exact weet wat er wanneer moet gebeuren?
- Wat is de inhoud van mijn projectplanning?
- Welke deadlines zijn er voor acties en maatregelen?
- Hoe en op welke momenten communiceer ik met (interne) stakeholders?
- Welke informatie verwachten stakeholders?
- Welke beslissingen moeten stakeholders nemen en welke kan ik zelfstandig nemen?
- Hoe en wanneer evalueer ik het managementsysteem voor informatiebeveiliging?
- Is de tijdsplanning realiseerbaar voor iedereen die deelneemt aan het project?

Hulp nodig bij begroten?

Wanneer u een managementsysteem opzet, wilt u een zo gedetailleerd mogelijk beeld krijgen van alle bijbehorende kosten. Het is dan niet vreemd als u een aantal vragen heeft, zoals:

- Hoe zorg ik dat ik me niet verkijk op de verschillende kosten van implementatie van het managementsysteem en certificering?
- Wanneer kan ik het beste starten met budgetteren?
- Hoe voorkom ik dat invloeden binnen en buiten de organisatie het traject vertragen?

Natuurlijk wilt u het liefst niets aan het toeval over laten. Een ervaren specialist van TÜV Nederland denkt daarom graag met u mee:

Stel uw vraag

Vraag uw certificering aan

Stap 3 - De brug bouwen

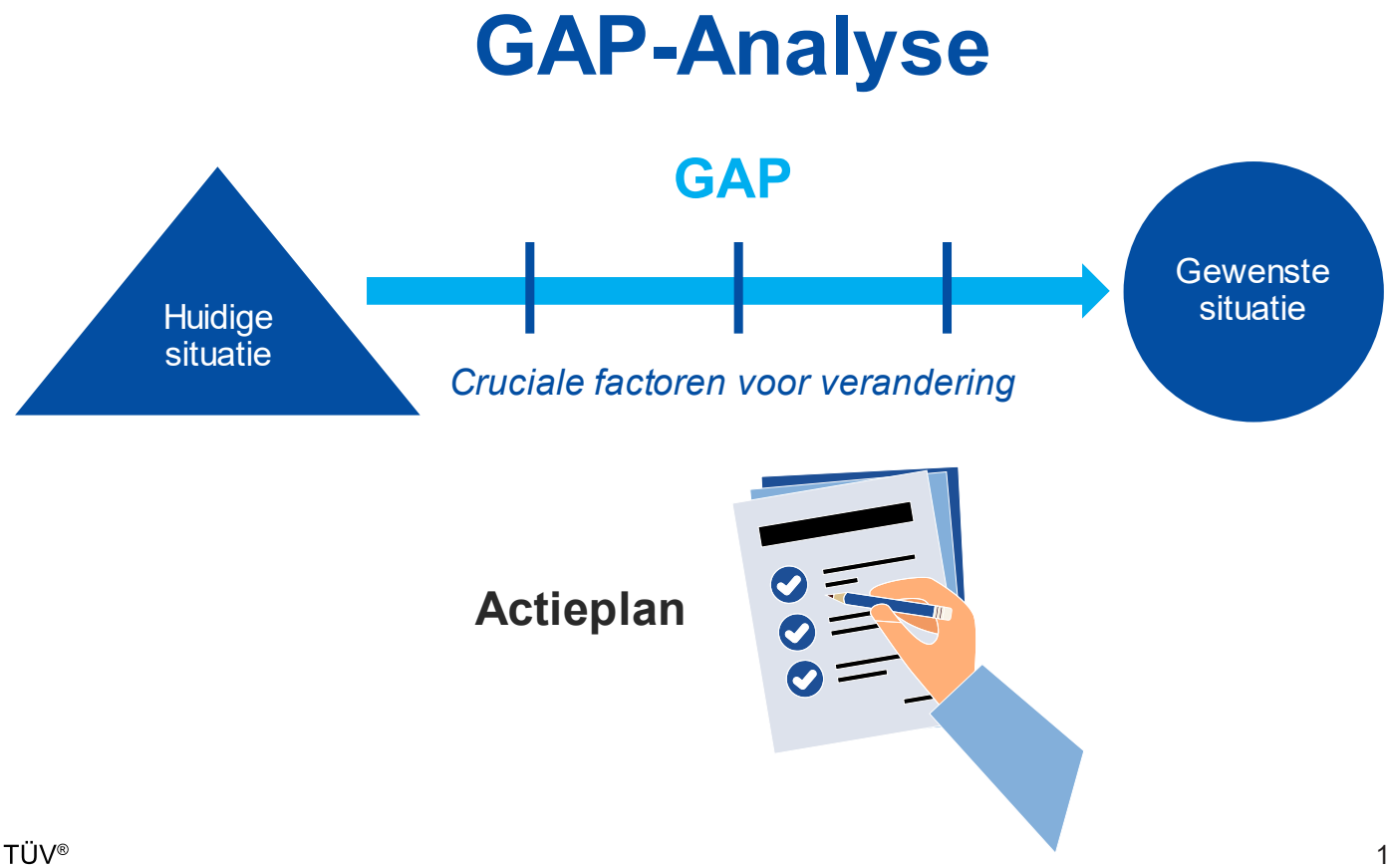
TÜV NORD GROUP

3. Breng de huidige en gewenste situatie in kaart

Om op de plek te komen waar u wilt zijn, is het goed om eerst te kijken waar u nu staat. In deze stap gaat u de huidige en gewenste situatie in kaart brengen. Deze situaties legt u vervolgens naast elkaar om de ‘gaten’ die zich hiertussen bevinden te constateren.

De gaten maken duidelijk welke stappen nodig zijn om uw doel te bereiken (het doel dat u als het goed is al heeft vastgesteld).

Een veel gebruikte methode om de huidige en gewenste situatie in kaart te brengen is de zogeheten ‘GAP-analyse’. Hieronder geven we aan hoe u deze kunt inzetten in uw eigen organisatie.



3.1 De huidige situatie

Het is zaak de huidige situatie te inventariseren. De NEN 7510 norm kan u hierbij goed ondersteunen. Door de norm te gebruiken als referentiekader zult u ook merken dat u moet vaststellen welke eisen en wensen voor informatiebeveiliging er zijn vanuit belanghebbenden.

Daarnaast gaat u vaststellen welke wettelijke en contractuele eisen met betrekking tot informatiebeveiliging relevant zijn in uw organisatie. Het nagaan of en hoe er binnen uw organisatie al aan die eisen wordt voldaan vormt een verdere verdiepingsslag bij het in kaart brengen van de huidige situatie.

U gaat achterhalen welke processen in de organisatie al zijn beschreven of gedocumenteerd op het gebied van informatiebeveiliging. Dit alles geeft al een duidelijk beeld van de huidige situatie.

Let wel, het is van belang om zo objectief mogelijk de situatie in kaart te brengen, zodat u in een later stadium de juiste stappen zet naar de gewenste situatie.

3.2 De gewenste situatie

De gewenste situatie is dat er een managementsysteem ontstaat, waarmee uw organisatie in staat is patiëntgegevens doeltreffend te beschermen. Dit door het invoeren en onderhouden van geschikte beheersmaatregelen. Het is belangrijk dat u vaststelt welk doel u wilt bereiken met uw managementsysteem voor informatiebeveiliging. Uitgangspunten voor de gewenste situatie kunnen zijn dat uw organisatie:

- De benodigde en verplichte documenten en registraties heeft opgesteld en ingevoerd
- Geschikte beheersmaatregelen heeft vastgesteld en ingevoerd
- Voldoet aan de eisen van NEN 7510 en het certificaat behaald

Op basis van de huidige situatie (3.1), uw doelstelling en uitgangspunten voor informatiebeveiliging kunt u vaststellen welke acties u nog moet ondernemen. Bijvoorbeeld het beschrijven van processen die nog niet gedocumenteerd zijn. Of het opstellen van eisen op het gebied van informatiebeveiliging waaraan u wilt voldoen. Deze neemt u op in de gewenste profielschets.

Het resultaat is dat u nu weet waar u staat en wat u nog te doen staat om te voldoen aan de minimale of door uw organisatie bepaalde eisen.

Werknemers kunnen u ook wijzen op zaken die al zijn gedocumenteerd. Zoals bijvoorbeeld de bestaande werkinstructies waarin de toegang tot bepaalde documenten in beschreven staat.

Stap 4 - Aan de slag

TÜV NORD GROUP

4. Het managementsysteem opzetten

Een managementsysteem bevat voor iedere organisatie unieke aspecten. Daarom kunnen we niet precies aangeven waar u rekening mee moet houden. Wel kunnen we u wijzen op onderstaande onderdelen van een managementsysteem waar u in ieder geval naar kunt kijken.

Een managementsysteem voor informatiebeveiliging opzetten bestaat in grote lijnen uit de volgende onderdelen, waar we in dit hoofdstuk op ingaan:

- De basis leggen van het managementsysteem
- De beoordeling op de informatiebeveiliging uitvoeren
- De informatiebeveiligingsrisico's identificeren en behandelen

Wilt u meer weten over het opzetten van een managementsysteem? Bekijk dan ook eens ons blog.

4.1 Wat is informatiebeveiliging?

Voordat we het inhoudelijke gedeelte induiken, maken we eerst nog eens duidelijk wat we nu precies verstaan onder informatie-beveiliging. Informatiebeveiliging gaat over het beschermen van kwetsbare (bedrijfs)informatie. Belangrijk om voor ogen te houden is dat het in de basis uit drie componenten bestaat, namelijk:

- Vertrouwelijkheid
- Integriteit
- Beschikbaarheid

Om een helder beeld te geven van de verschillen tussen deze drie, laten we drie voorbeelden zien met een korte toelichting. Het is belangrijk het verschil te begrijpen omdat u de informatie ook op deze drie elementen dient te beveiligen.

Vertrouwelijkheid

Is en blijft de informatie vertrouwelijk?

Vertrouwelijke informatie betekent dat alleen geautoriseerden toegang hebben tot de (gevoelige) informatie. Het gaat hierbij niet alleen om digitale informatie maar ook informatie op papier.

Integriteit

Is de informatie actueel, correct en volledig?

Integriteit gaat om informatie die actueel, correct en volledig is. Is de informatie een van deze dingen niet (meer)? Dan vormt dit een risico. Wanneer u de route uitstippelt en informatie niet meer leesbaar is op de landkaart, kan dit de route blokkeren of u een verkeerde richting in sturen.

Beschikbaarheid

Is de informatie beschikbaar?

Bij beschikbaarheid gaat het om de toegankelijkheid van de informatie en de bruikbaarheid als de informatie nodig is. Wanneer u bijvoorbeeld informatie bewaart in een gesloten kast is dit veilig, echter heeft u hier niets aan wanneer de sleutel niet beschikbaar is.

4.2 Leg de basis voor het managementsysteem

De eerste stap in het opzetten van een managementsysteem voor informatiebeveiliging betreft het leggen van een stevige fundering. Hoe sterker u deze legt, hoe stabieler u hier verder op kunt bouwen.

Daarom gaat u in deze fase de kaders scheppen van het managementsysteem - waardoor u helder krijgt hoe deze er in grote lijnen uit gaat zien.

U bepaalt zelf hoe u dit aanvliegt. Wel kunnen we u op weg helpen door het geven van bruikbare handvatten en tips.

Informatiebeveiiging gaat niet alleen over technische maatregelen, het is mensenwerk. En waar mensen zijn, worden fouten gemaakt. Help uw werknemers daarom een handje en gebruik bijvoorbeeld de password cards voor wachtwoordbeheer. Hiermee heeft iedereeen altijd zijn of haar persoonlijke wachtwoord bij de hand. Het werkt zo dat alleen de gebruiker weet welke rij, kleur en aantal cijfers je gebruikt als wachtwoord.

4.2.1 Processen inrichten voor informatiebeveiliging

U dient geschikte methoden en werkafspraken binnen de organisatie toe te passen die ervoor zorgen dat de informatie-beveiliging op het gewenste pijl komt én blijft. U bepaalt zelf de invulling, zo lang de informatiebeveiliging maar op een voor uw organisatie acceptabel niveau verkeert.

Om tot deze geschikte methoden en afspraken te komen, gaat u daarom in deze fase bedenken hoe het managementsysteem straks gaat functioneren en wat de taakverdeling is.

Let op: De norm stelt het in veel gevallen niet verplicht om deze zaken te documenteren. Echter helpt het u later in het proces wel om mogelijke onduidelijkheden te voorkomen.

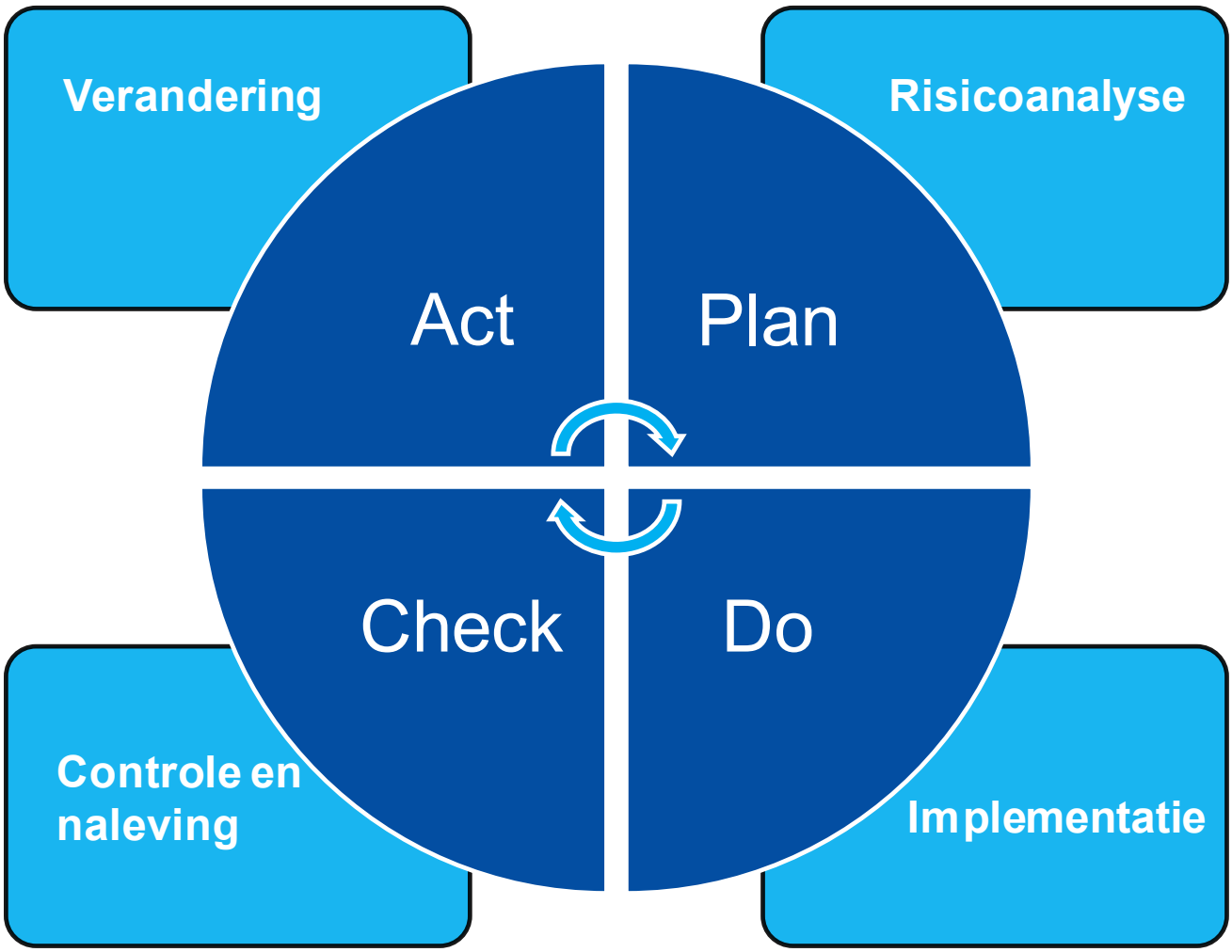
U gaat in deze stap niet alleen bedenken (en eventueel vastleggen) hoe u het managementsysteem gaat opzetten, maar ook de uiteindelijke situatie waarin het managementsysteem functioneert. U gaat daarom o.a. nadenken over de volgende zaken:

- Welke activiteiten zijn er nodig om het managementsysteem te laten functioneren?
- Hoe gaat u deze activiteiten inrichten binnen de organisatie?
- Wie stelt het beleid op?
- Hou houdt u vinger aan de pols of het beleid ook wordt nageleefd?
- Hoe gaat u de risicobeoordeling uitvoeren?
- Hoe gaat u de risico's behandelen?
- Hoe houdt u toezicht op het functioneren van het managementsysteem?

Houdt hierbij in gedachten dat het managementsysteem dynamisch is en geen voorgeschreven 'boekje'. De afspraken die u heeft gemaakt en de activiteiten die u hebt ingevoerd maken het managementsysteem. De informatie uit de norm die u vastlegt is belangrijk, maar is niet het hoofddoel.

Wat is een proces?
Onder een proces verstaan we het verloop van een activiteit in uw organisatie. Een proces wil niets meer zeggen dan *input* die

wordt omgezet in *output*. Het primaire proces van uw organisatie beslaat de activiteiten om uw product of dienst voort te brengen en te realiseren richting de klant. Dit zijn eigenlijk de kernactiviteiten van uw organisatie.



Een versimpelde weergave van een verbeteringsproces voor informatiebeveiliging

4.2.2 Informatie vastleggen zoals in de norm vereist

In de NEN 7510 norm staat onder andere dat er bepaalde informatie van het managementsysteem als gedocumenteerde informatie **beschikbaar** moet zijn en dat de organisatie gedocumenteerde informatie moet **onderhouden**. Daarnaast staat in de norm dat u gedocumenteerde informatie moet **bijhouden**.

Met het beschikbaar hebben en onderhouden van informatie bedoelen we documenten die het functioneren van het managementsysteem uitleggen en ondersteunen. U gaat vervolgens registreren dat u deze informatie heeft bijgehouden. Dit is de bewijslast. Naast het feit dat de norm dit vereist, is het voor uzelf ook nog eens een stuk gemakkelijker om activiteiten aantoonbaar te maken, bijvoorbeeld richting een certificerende instelling.

U legt deze informatie (zoals in de norm vereist) vast middels elke gewenste methode, zolang deze voor uw organisatie geschikt is. In de praktijk zien we vaak een handboek met procedures. Maar ook steeds vaker zien we dat er digitale (intranet)applicaties worden gebruikt, zoals sharepoint. Een bijkomend voordeel van het vastleggen van informatie is dat u het kunt inzetten als communicatiemiddel. Het helpt u bij het creëren van eenduidigheid en transparatie binnen de organisatie.

4.2.3 Het informatiebeveiligingsbeleid opstellen

U wilt aan het management of directie kunnen aangeven wat uw zorgorganisatie in grote lijnen met informatiebeveiliging wil bereiken. Dit doet u door het informatiebeveiligingsbeleid op te stellen. In dit beleid legt u vast wat u wilt gaan bereiken en dit hangt samen met uw doelstellingen.

Wanneer u een reden aangeeft als “het is een vereiste van de opdrachtgever” dan zal dit een wezenlijk andere invulling aan het systeem geven dan wanneer u stelt “onze zorginstelling wil de informatiebeveiliging continu blijven verbeteren”.

Uw zienswijze bepaalt in grote mate de invalshoek waarmee naar het managementsysteem wordt gekeken. Uw doelstelling bepaalt vervolgens weer de invulling van het management-systeem. U kunt NEN 7510 op minimaal niveau toepassen (en voldoen aan de compliance verplichtingen), maar u kunt ook een managementsysteem opstellen dat verder gaat dan de minimale vereisten en uw organisatie helpt continu te verbeteren. Het beleid beschrijft uw intenties.

Wat is een informatiebeveiligingsbeleid?
In de basis zou u kunnen zeggen dat een beleid altijd richtinggevend is aan de organsatie. Het helpt bij het varen van de koers van de organisatie en de doelen die het wil behalen. Het beleid voegt waarde toe aan de organisatie.

U dient het beleid te communiceren en beschikbaar te stellen voor alle medewerkers.

In de NEN 7510 norm vindt u een aantal zaken die sowieso aangestipt moeten zijn. Onder andere:

- Hoe gaat u aan de eisen voor informatiebeveiliging voldoen?
- Hoe gaat u het managementsysteem voor informatie-beveiliging continu verbeteren?

De directie moet een informatiebeveiligingsbeleid vaststellen dat:

- Passend is voor het doel van de organisatie
- Doelstellingen bevat voor de informatiebeveiliging of een kader biedt voor het vaststellen hiervan
- Laat zien hoe u gaat voldoen aan van toepassing zijnde informatiebeveiligingseisen
- Laat zien hoe u uw managementsysteem voor infor-matiebeveiliging continu verbetert

Hoe pakt u dit aan?
U kunt verschillende formats en templates gebruiken als basis. Dit gaat met name om de opzet en opbouw van het beleid. Inhoudelijk is het belangrijkste dat u zelf (of met de projectgroep) nadenkt over het eindpunt dat u wilt bereiken en de weg die daar naartoe leidt. Hiervoor stelt u doelen op en dit alles bespreekt u met de directie.

Commitment van de directie
Een goed informatiebeveiligingsbeleid dient uiteindelijk van u of uw directie af te komen. Dit is vaak ook direct de uitdaging.

Het valt niet altijd mee om de betrokkenheid en prioriteit te krijgen die nodig is. Het kan u daarom helpen een voorzet te maken van hoe het beleid er volgens u uit zou moeten zien. Leg dit vervolgens voor aan de betrokkenen en zorg dat er overeenstemming komt, zodat het benodigde commitment aanwezig is om het project ook daadwerkelijk uit te voeren.

Heeft u aanvullende ondersteuning nodig om dit onderdeel - of andere onderdelen - invulling te geven? Dan kunt u altijd overwegen een adviseur aan te haken.

4.2.4 Doelstellingen formuleren

U heeft het algemene doel voor het opzetten van het managementsysteem in de vorige stappen al vastgesteld. In deze stap gaat u het algemene doel verder uitwerken in concrete - inhoudelijk te bereiken - resultaten (doelstellingen).

Wat moet een goede doelstelling omvatten?
De norm stelt dat uw doelstellingen meetbaar moeten zijn waar dit praktisch uitvoerbaar is. Het dient daarnaast vooral ook in overeenstemming te zijn met het informatiebeveiligingsbeleid.

Het is daarom van belang dat een doelstelling geen kale vertaling is van een normelement waaraan u dient te voldoen. Uw organisatie dient actief en op continue basis de informatie veilig te houden en te verbeteren.

Een doelstelling SMART formuleren
Om de verbeterdoelstellingen uiteindelijk meetbaar te maken, kan het helpen de doelstellingen SMART te formuleren. Hiermee zet u doelstellingen neer die u in staat stellen ook daadwerkelijk te meten of uw doelen bereikt zijn.

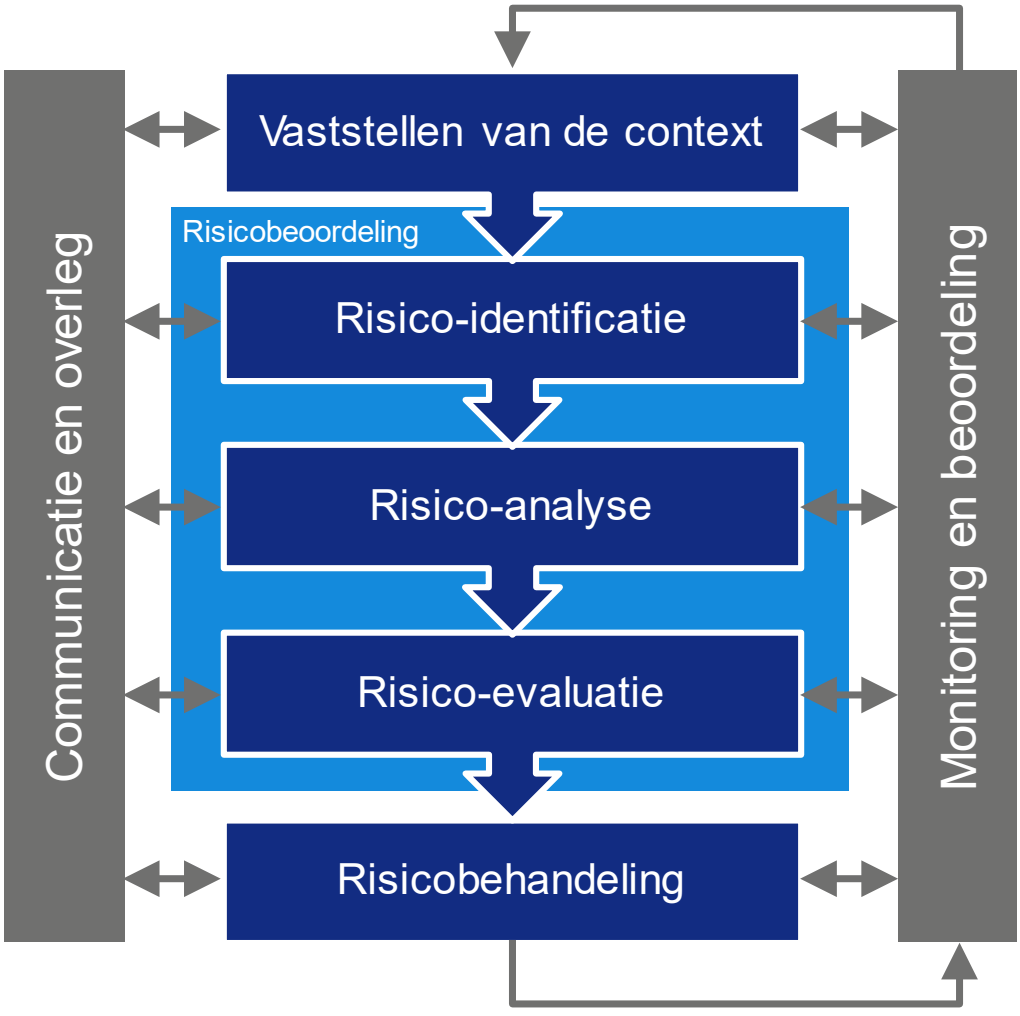
- **Specifiek:** is de doelstelling eenduidig?
- **Meetbaar:** onder welke (meetbare/observeerbare) voorwaarden of vorm is het doel bereikt?
- **Acceptabel:** is deze doelstelling acceptabel voor de doelgroep en/of het management?
- **Realistisch:** is het doel haalbaar?
- **Tijdgebonden:** wanneer moet het doel bereikt zijn

Een voorbeeld van een SMART-doelstelling voor informatiebeveiliging is bijvoorbeeld:

Komend jaar willen we een daling van 50% van het aantal informatiebeveiligingsincidenten binnen de organisatie

4.3 De risicobeoordelingsmethode vaststellen

Een risicobeoordelingsmethode helpt u met overzicht over welke risico's u als eerste gaat aanpakken. Het heeft als doel om risico's voor informatiebeveiliging te beoordelen en in te schalen. U kunt risico's op verschillende manieren en in verschillende niveau's inschalen. Dit is afhankelijk van de methode die u hiervoor gaat hanteren.



Informatie 'scope' identificeren

Om ervoor te zorgen dat u de risico's straks kunt beoordelen, kunt u ervoor kiezen om eerst alle informatie die uw organisatie bezit – de informatie 'scope' – te identificeren. Ga na wat de informatiedragers zijn, welke informatieverwerkingssystemen en informatiestromen er binnen uw organisatie zijn. Dit schept het kader waarbinnen u straks de risico's gaat beoordelen.

Let op: de norm stelt het niet verplicht de informatiescope op deze manier te identificeren. Het helpt u echter wel met het verkrijgen van overzicht.

4.3.1 Hoe stelt u een methode vast voor risicobeoordeling?

Er bestaan verschillende methoden die u kunt hanteren om de risico's te beoordelen. Het is gebruikelijk dat een risicobeoordelingsmethode rekening houdt met:

- Informatie en de waarde van deze informatie
- Kosten indien er zich een situatie voordoet van inbreuk op beveiligde informatie
  (met inbreuk bedoelen we een verlies van beschikbaarheid, integriteit of vertrouwelijkheid van de gegevens)
- Imagoschade
- Wettelijke eisen, contractuele eisen en eisen van andere belanghebbenden

Wanneer u een risicobeoordelingsmethode vaststelt is het belangrijk ook na te denken over de risico acceptatiecriteria. Dit zijn criteria die u zelf opstelt. Ze helpen te bepalen welke risico's er zijn, hoe groot de kans is dat ze zich voordoen én wanneer u een risico acceptabel vindt (en wanneer niet).

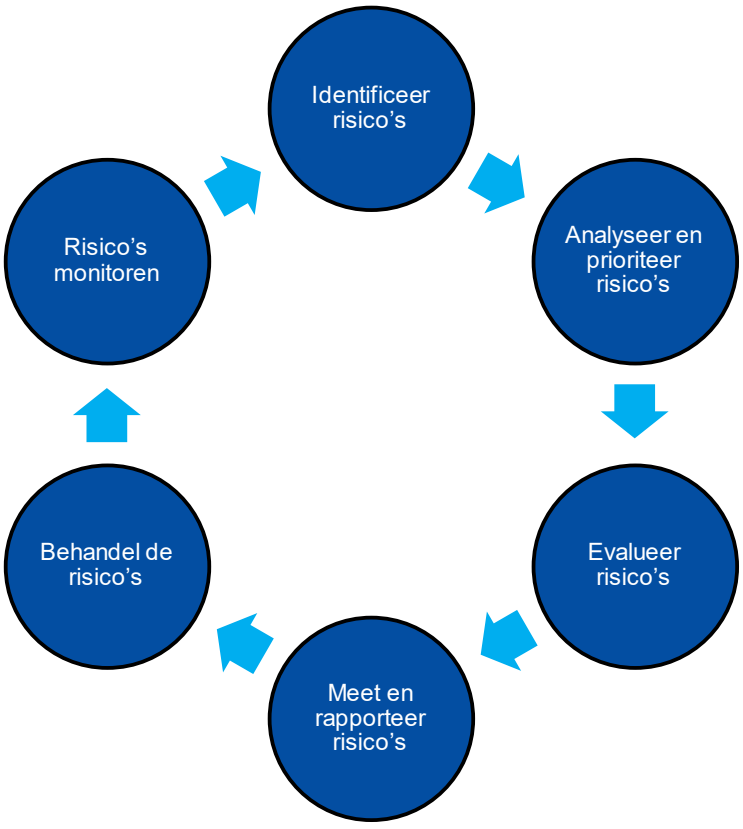
Risico acceptatiecriteria kunnen bijvoorbeeld zijn:

- Alle risico's die een gezondheidsrisico als gevolg hebben zijn niet acceptabel

- Alle risico's die mogelijk imagoschade tot gevolg hebben zijn niet acceptabel

4.4 Een risicobehandelmethode vaststellen

Als het goed is heeft u de methode waarmee u de risico's gaat beoordelen vastgesteld. Nu is het zaak om deze risico's te gaan behandelen. Kortom, u gaat aan de slag om de risico's tot een acceptabel niveau terug te brengen. Hiervoor gaat u allereerst een methode vaststellen. Door het doen van onderzoek kunt u de mogelijkheden om risico's te behandelen in kaart brengen. U kunt hiervoor eigen inzicht en parate kennis inzetten. In de volgende paragraaf beschrijven we 4 manieren om informatie-beveiligingsrisico's te behandelen.



4.4.1 De 4 verschillende manieren om risico's te behandelen

In de basis zijn er vier manieren om risico's te behandelen. Uiteindelijk is het doel dat u de grootte van het risico probeert terug te dringen.

Vragen die u hierbij kunnen helpen zijn bijvoorbeeld:

- Welke acties kan ik doen die minder ingrijpend zijn dan de gevolgen van het risico?
- Hoeveel is het de organisatie waard om zaken rondom dit risico goed te regelen?

Welke methode u gebruikt is mede afhankelijk van het antwoord op deze vragen. Heeft u helder hoe belangrijk de risico's zijn voor uw organisatie? En met name, hoe groot de de gevolgen zijn? Dan kunt u kiezen uit een van de volgende risico behandelmethoden:

1. **Het risico reduceren**
   U kiest ervoor het risico te reduceren. Dit betekent dat u de kans dat het risico zich voordoet gaat verminderen.

2. **Het effect van het risico reduceren**
   U kiest ervoor om het effect van het risico te reduceren. Dit betekent dat u de gevolgen die het risico met zich meebrengt, gaat beperken.

3. **Het risico accepteren**
   U kiest ervoor de gevolgen van het risico te accepteren. Dit betekent in feite dat u niets doet om de gevolgen te beperken. Wanneer het risico zich voordoet, accepteert u dit.

4. **Het risico verzekeren**
   U kiest ervoor de gevolgen van het risico te verleggen, door zaken op voorhand te verzekeren.

Stap 5 - De risico's aanpakken

5. De inhoudelijke beoordeling op de informatiebeveiligingsrisico's

U heeft het meeste voorbereidingswerk gedaan. Nu is het tijd om alles in de praktijk te brengen:

- U gaat eerst de informatiebeveiliging beoordelen op de inhoud.
- Vervolgens gaat u de risico's aanpakken door passende beheersmaatregelen te treffen om te zorgen dat u de risico's ook daadwerkelijk kunt terugdringen.
- Deze output dient als input voor de Verklaring van Toepasselijkheid (ook wel Statement of Applicability). Hierin gaat u alle vastgestelde maatregelen vastleggen.

Het belangrijkste doel in deze fase is dat u op zoek gaat naar de oorzaak van de risico's. Dit is namelijk het startpunt om zaken in te regelen en te voorkomen dat het risico zich voordoet.

5.1 Het uitvoeren van de risico-beoordeling

In de uitvoering van de risicobeoordeling gaat u de risico's daadwerkelijk beoordelen. Dit doet u aan de hand van uw eerder vastgestelde risicobeoordelingsmethode.

Dit is het gedeelte waarin u tot actie komt en u zult ondervinden wat de status is van de organisatie ten opzichte van informatie-beveiliging. Deze stap draait daarnaast ook om samenwerking.

Betrek uw collega's vroeg in het proces. Werknemers weten het beste wat het eigen werk omvat en kunnen u daarom precies vertellen wat er op de werkvloer speelt. Bovendien draagt het bij aan het creëren van draagvlak voor veranderingen.

5.1.1 Hoe voert u de risicobeoordeling uit?

Zoals we al eerder benoemden, is het de bedoeling dat u de organisatie induikt. U gaat bij verschillende afdelingen en in verschillende lagen van de organisatie input ophalen over de status van de organisatie ten opzichte van informatiebeveiliging. Stel uzelf tijdens deze risicobeoordeling bijvoorbeeld de volgende vragen:

- Welke risico's bent u tegen gekomen?
- Hoe waarschijnlijk is het dat de risico's zich voordoen?
- Wat zijn de potentiële consequenties van de risico's, wanneer deze zich voordoen?
- Welke prioriteit krijg het risico?

Maak ook een vergelijking met de risico criteria:

- Is het risico acceptabel of niet?
- Is er een prioritering voor risicobehandeling?
- Hoe belangrijk en urgent is het risico?

5.2 Beheersmaatregelen vaststellen

Om de risico's te kunnen minimaliseren, zijn beheersmaatregelen nodig. Het invoeren van maatregelen kan een hele klus zijn, afhankelijk van hoe ver de organisatie is in het proces.

Een beheersmaatregel kunt u zien als een 'optie' of 'mogelijkheid' die u helpt risico's tot een acceptabel niveau terug te brengen. U bepaalt zelf wat voor u acceptabel is. Het voordeel van beheersmaatregelen is dat het u inzicht geeft in de oorzaken van de risico's. Door het achterhalen van oorzaken, komen de verschillende mogelijkheden tegelijkertijd boven drijven om te voorkomen dat risico's resulteren in problemen.

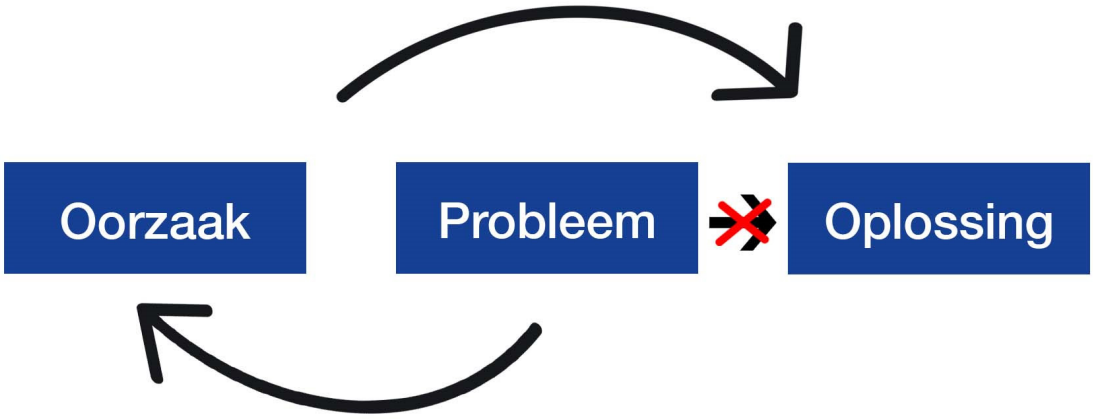
5.2.1 Hoe stelt u een beheersmaatregel vast?

De norm verwacht dat u beheersmaatregelen zelf ontwikkelt of dat u bronnen raadpleegd. Een van die bronnen is Bijlage A uit de NEN 7510 norm. Deze bevat een opsomming van best beschikbare maatregelen en technieken. Stel uit deze lijst vast welke relevant zijn voor uw organisatie en geef hier een argumentatie voor. Gaat u zelf beheersmaatregelen opstellen? Vergelijk deze dan ook met bijlage A. Geef ook een argumentatie voor de beheersmaatregelen die niet van toepassing zijn op uw situatie.

Het *vaststellen* van beheersmaatregelen is één, het daadwerkelijk *toepassen* hiervan in de praktijk is een tweede. Reserveer daarom voldoende ruimte in uw planning voor operationele zaken. Denk bijvoorbeeld aan dossierkasten die via de receptie toegankelijk zijn voor derden wanneer de receptie onbemand is. U stelt vast dat hiervoor extra beveiliging nodig is. Dit betekent dat de ruimte of kasten afsluitbaar moeten worden gemaakt, zodat men de ruimte kan afsluiten bij het verlaten van de ruimte.

Een voorbeeld:
De balie waar u mensen ontvangt bevindt zich in dezelfde ruimte als de wachtruimte. Omdat er gevoelige en persoonlijke gesprekken worden gevoerd aan de balie of aan de telefoon, geeft dit weinig privacy voor uw cliënten. Dit vormt een risico

voor de informatie die besproken wordt. De oorzaak van dit risico is de huidige opstelling van de ruimten. Om dit te voorkomen kunt u besluiten de wachtruimte te scheiden van de balie en de wachtruimte van achtergrondmuziek te voorzien.



5.3 Stel de Verklaring van Toepasselijkheid op

De Verklaring van Toepasselijkheid (engelse term: Statement of applicability, afkorting VvT) is op inhoudelijk gebied in principe een samenvatting van de huidige situatie en van de relevante maatregelen. Waarom?

U stelt hierin namelijk vast welke beheersmaatregelen u al heeft opgesteld, waarom u deze heeft opgesteld en of deze al zijn geïmplementeerd. Wanneer u deze nog niet heeft geïmplementeerd, maakt u hiervoor een actieplan.

In de Verklaring van Toepasselijkheid legt u alle benodigde maatregelen vast, waaronder de maatregelen uit Bijlage A uit de NEN 7510. Maar ook een rechtvaardiging van de maatregelen die niet worden toegepast. U geeft hierin aan of de maatregelen al zijn ingevoerd.

Vaak is de Verklaring van Toepasselijkheid in de vorm van een matrix of tabel weergegeven. U kunt de Verklaring van Toepasselijkheid zien als het laatste puzzelstuk dat de puzzel compleet maakt. Heeft u aanvullende ondersteuning nodig om dit, of een ander onderdeel, invulling te geven? Dan kunt u altijd overwegen om **een adviseur in de arm te nemen**.

Stap 6 - De uitvoering

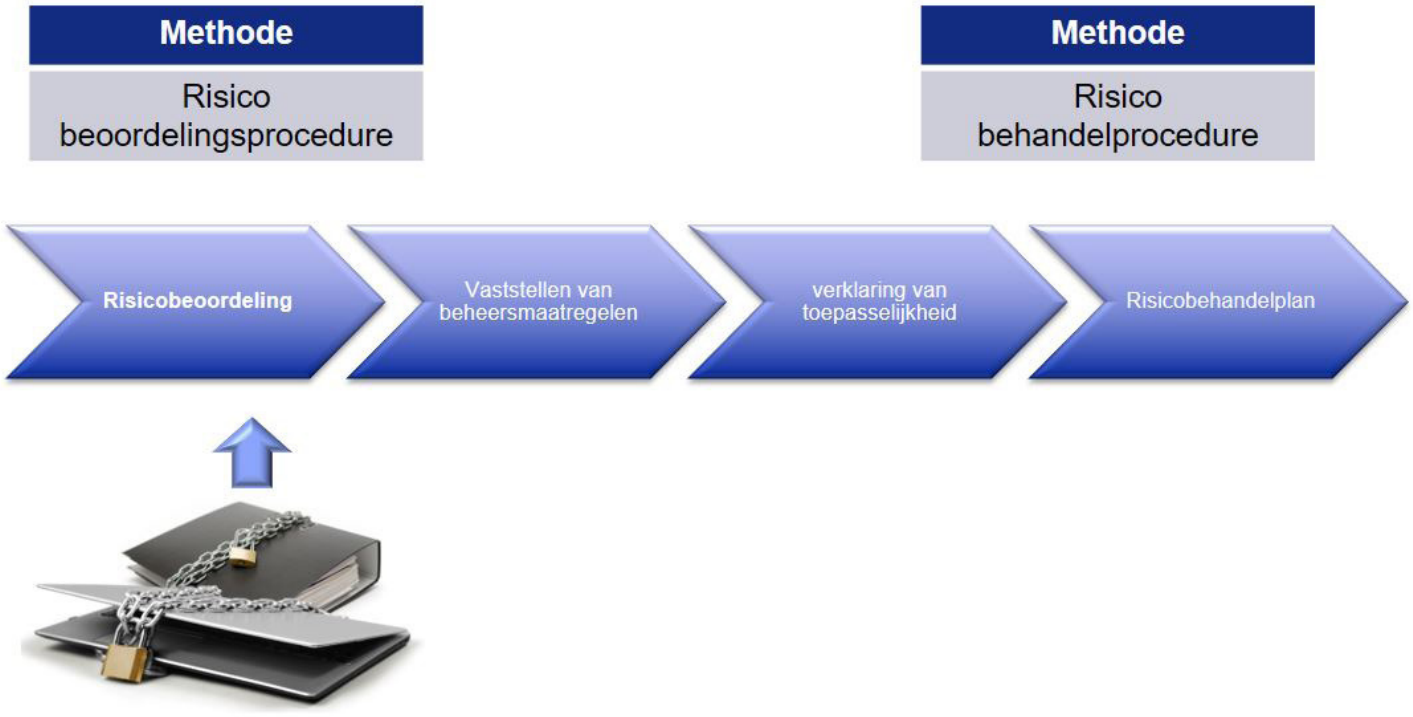
TÜV NORD GROUP

6. De informatiebeveiliging risico's behandelen

Nu u weet welke risico's er zijn vastgesteld en welke maatregelen u hierop gaat treffen, is het tijd om de risico's daadwerkelijk te behandelen.

Hiervoor gaat u eerst een behandelplan opstellen en deze gaat u vervolgens tot uitvoering brengen. Dit hoofdstuk bestaat uit twee stappen:

- Het risicobehandelplan opstellen
- Het risicobehandelplan uitvoeren



6.1 Het risicobehandelplan opstellen

In deze stap gaat u de uitkomst van de Verklaring van Toepasselijkheid daadwerkelijk vastleggen. Wat bedoelen we met de uitkomst?

Hiermee bedoelen we dat u de beheersmaatregelen die u nog niét heeft geïmplementeerd, in het behandelplan gaat opnemen. Dit is belangrijk om de informatiebeveiliging sluitend te krijgen.

Om u te helpen de acties die u gaat uitvoeren scherp te krijgen, kunt u o.a. vragen beantwoorden als:

- Wat ga u daadwerkelijk doen om de risico's te behandelen?
- Wie stelt u aan om de actie(s) te gaan uitvoeren?
- Binnen welke termijn gaat u dit uitvoeren?

6.2 Het risicobehandelplan uitvoeren

In deze stap gaat u de vastgestelde maatregelen tot uitvoering brengen. Hier zult u het meerdendeel van de tijd aan besteden.

Houd rekening met onvoorziene situaties
Komt u tijdens de uitvoering allerlei onvoorziene situaties tegen? Dan kan dit u zomaar meer tijd kosten dan vooraf gepland. Dit is het moment dat u de huidige situatie daadwerkelijk gaat ondervinden. Het is aan te raden hier vroeg in het proces al rekening mee te houden in de tijdsplanning, omdat u hier zo goed als mogelijk op voorbereid wilt zijn.

Leg voldoende vast
Zorg ook in deze stap weer voor voldoende bewijslast om uw verrichtte werk aan te kunnen tonen. Schrijf bijvoorbeeld bij het voltooien van een actie op uw actielijst een korte toelichting op, of houd een meer uitgebreide registratie van informatie bij. Verzamel hierin ook locaties, data en fotomateriaal.

De implementatie van uw systeem is bijna gereed. En nu?

Om de certificering van uw managementsysteem zo spoedig mogelijk rond te krijgen, gaat u nu de plannen concreet maken. In deze afrondende fase is het niet vreemd dat u een aantal vragen heeft, zoals:

- Op welke zaken dien ik scherp te zijn bij het kiezen van een certificatie-instelling?
- Indien ik een certificatie-instelling kies; wat kan ik precies verwachten?
- Hoe wordt een audit vormgegeven en hoe plan ik deze zo efficiënt mogelijk in?

Natuurlijk wilt u het liefst niets aan het toeval overlaten. Een ervaren specialist van TÜV Nederland denkt daarom graag met u mee. Stel direct uw vraag:

Stel uw vraag

Vraag uw certificering aan

Stap 7 - De certificering

TÜV NORD GROUP

7. Het NEN 7510 certificaat behalen

U bent bijna gereed om het certificatietraject voor NEN 7510 in te stappen. U heeft het functioneren van uw eigen systeem beoordeeld aan de hand van interne audits en de directiebeoordeling. De laatste stap is om middels een externe audit uw managementsysteem te laten beoordelen.

Het doel hiervan is dat een externe partij objectief vaststelt dat het managementsysteem binnen uw organisatie voldoet aan de eisen uit de NEN 7510 norm. Heeft de certificerende instelling een positieve uitspraak gedaan? Dan wordt het certificaat uitgereikt en kunt u officeel aantoonbaar maken aan opdrachtgevers en andere belanghebbenden dat u informatie-beveiliging op orde heeft.

7.1 Laat uw certificatietraject soepel verlopen

Het opzetten van een managementsysteem neemt een flink tijdspad met zich mee. Het is daarom aan te bevelen minimaal zes maanden - voordat u de externe audit wilt uitvoeren – te beginnen aan het opzetten van uw managementsysteem. Daarnaast kunt u erover nadenken in het beginstadium contact op te nemen met uw certificerende instelling.

Zij kunnen u ook helpen de planning overzichtelijk te houden en op voorhand rekening te houden met uw gewenste data omtrent proef- en/of externe audits. Door de certificerende instelling vroeg bij het proces te betrekken, kunnen zij u bekend maken met het optimale tijdspad en te nemen stappen om het certificatietraject soepel te laten verlopen.

7.2 Wat is de toegevoegde waarde van een proefaudit?

Een proefaudit is een optioneel onderdeel van certificering voor informatiebeveiliging. Tijdens een proefaudit maakt u kennis met de auditor en wordt de stand van zaken besproken.

De auditor maakt van de huidige stand van zaken van uw organisatie een globale inventarisatie. Welke veranderingen zijn er al doorgevoerd? Waar loopt de organisatie tegenaan? Wat is de mate van implementatie? Een proefaudit helpt uw organisatie potentiële zwaktes gericht aan te pakken voordat u van start gaat met het daadwerkelijke certificatie traject.

7.3 Hoe ziet een NEN 7510 audit eruit?

Wanneer u een NEN 7510 certificaat aanvraagt bij een certificatie instelling zal worden getoetst of uw organisatie aan alle vereisten voldoet. Een auditor zal uw managementsysteem voor informatiebeveiliging toetsen aan de hand van drie stappen:

- Het vooronderzoek
- De externe audit
- De certificering

7.3.1 Het vooronderzoek

De eerste stap in het certificatietraject is het vooronderzoek. Een vooronderzoek wordt uitgevoerd door een certificerende instelling waarvoor u zelf kiest. Tijdens een vooronderzoek komt een externe-auditor kennis met u maken en beoordelen of uw organisatie klaar is voor de externe audit.

In deze fase kijkt de auditor naar uw managementsysteem voor informatiebeveiliging en controleert of alle benodigde onderdelen aanwezig zijn.

U kunt denken aan onderwerpen als: Heeft u een Verklaring van Toepasselijkheid opgesteld? Heeft u de risicoanalyse op de juiste manier uitgevoerd? Zijn de juiste maatregelen gedocumenteerd? Wanneer u alles op orde heeft wordt de audit ingepland.

7.3.2 De externe audit

Tijdens de audit wordt gecontroleerd of het managementsysteem voor informatiebeveiliging goed is geïmplementeerd in uw organisatie. Hierbij wordt niet alleen de documentatie opnieuw gecontroleerd, maar loopt de auditor ook door uw bedrijf heen om te controleren of u aan alle eisen voldoet.

Aan het einde van de audit ontvangt u een rapport. Hierin staat of u wel of niet aan alle NEN 7510 certificeringseisen voldoet. Is dit niet het geval? Dan krijgt u twee maanden de tijd om de benodigde veranderingen door te voeren binnen uw organisatie.

7.3.3 De certificering

Voldoet uw managementsysteem voor informatiebeveiliging wel aan alle NEN 7501 eisen dan krijgt u een positief advies van de auditor. Hierop volgend, ontvangt u binnen enkele weken het auditrapport en het certificaat.

Het NEN 7510 certificaat is drie jaar geldig. Na drie jaar moet u opnieuw op voor certificering. Ook wordt er jaarlijks een controle uitgevoerd om te toetsen of uw informatiebeveiligingssysteem nog voldoet aan alle certificeringseisen. Bent u al gecertificeerd voor NEN 7510? Dan volgt na drie jaar een her-certificering. Hierin moet u opnieuw alle stappen van het certificeringsproces doorlopen.

Certificering: wat zijn de spelregels?

Het liefst wilt u dat u certificatie van uw managementsysteem spoedig en soepel na de invoering kunt laten uitvoeren. Het is dan niet vreemd dat u een aantal vragen heeft, zoals:

- Hoe plan ik belangrijke mijlpalen zo efficiënt mogelijk?
- Wat gebeurt er na de audit (Rapportage - Afwijkingen - Certificatiebeslissing - Certificaat)?
- Wat zijn veel voorkomende valkuilen waar ik op voorbereid moet zijn?

U bent altijd vrij ons vragen te stellen in deze fase, zodat u een weloverwogen beslissing kunt nemen:

Stel uw vraag

Vraag uw certificering aan

Over TÜV Nederland

TÜV NORD GROUP

Wij staan samen sterk voor het bevorderen van de veiligheid, kwaliteit, betrouwbaarheid en leefomgeving voor de maatschappij, organisaties en overheid. Alle onderwerpen die wij toetsen zorgen ervoor dat u verzekerd bent van betrouwbare producten, diensten en leveranciers en u zelf ook de betrouwbaarheid van uw organisatie kunt aantonen.

Kom meer te weten over de oplossingen die we hebben voor **uw branche**. Of bekijk ons aanbod van **certifcaten & keurmerken**, **keuringen** en **training**. Ons hoofddoel is om aantoonbaar te maken dat u aan gestelde eisen voor betrouwbaarheid voldoet. Maar als het spreekwoord “Vreemde ogen dwingen” ergens van toepassing is, is het wel in ons vakgebied.

We identificeren tijdens beoordelingen ook heel feitelijk risico’s en pijnpunten zodat we u ondersteunen in begrip en draagvlak voor verbetering bij belanghebbenden. Raak vertrouwd met onze specialismen certificering, inspectie en keuring, CE-markering en training.