Snel naar NEN7510 met de ISM-methode

Cross-reference en handleiding

Datum: 2 april 2011 Versie: 1.0

Auteur: J. van Bon

Integrated
Service
Management

Snel naar NEN7510 met de ISM-methode!

Informatiebeveiliging in de zorg: een hot item

Zorginstelling moeten, door de komst van o.a. elektronisch patiëntendossiers (EPD's) en zorg op afstand, steeds meer in control zijn van hun informatievoorziening. Als het IT-beheer dan niet adequaat geregeld is het vrijwel onmogelijk dat een instelling voldoet aan de gestelde eisen.

De norm NEN7510 beschrijft waaraan de informatiebeveiliging (IB) van zorginstellingen moet voldoen. Daarbij worden eisen gesteld aan de BIV-criteria (**b**eschikbaarheid, **i**ntegriteit, en **v**ertrouwelijkheid van informatie), en aan de controleerbare inrichting van beveiligingsmaatregelen. Een instelling heeft daarvoor een ISMS, een Information Security Management System, nodig, een systematische inrichting van de beveiliging van informatie. Een ISMS is – zoals het woord al zegt – een managementsysteem, dus een combinatie van de drie soorten productiemiddelen waarmee een organisatie haar prestaties managet: People, Process & Product.

De Inspectie voor de Gezondheidszorg en het College Bescherming Persoonsgegevens stelden in 2008 vast dat geen van de 20 onderzochte ziekenhuizen aan de norm voldeed. De Nederlandse Vereniging van Ziekenhuizen (NVZ) stelde vervolgens dat de meeste instellingen *jaren* nodig hebben om aan alle eisen te voldoen, en heel veel euro's. Om snel een eerste verbetering te kunnen inzetten stelde de NVZ in april 2010 een set van voorlopige normen vast die een (klein) deel van NEN7510 dekken. Alle ziekenhuizen moesten nog in 2010 tegen die voorlopige normen geaudit zijn. De bevindingen van die audit liggen anno 2011 bij de Inspectie, die naar verwachting met een pakket van eisen zal komen.

ISM en het Information Security Management System (ISMS)

IT-beheerorganisaties adopteren steeds vaker een systematische werkwijze volgens de ISM-methode: Integrated Service Management®. Met die systematische werkwijze zijn ze in staat in korte tijd complexe doelen te realiseren, zoals doelen op het gebied van informatiebeveiliging.

Uit de cross-reference van de ISM-methode en NEN7510 blijkt dat ISM praktisch geheel voorziet in het ISMS zoals NEN7510 dat voorschrijft. Dat wil zeggen dat een organisatie die de ISM-methode heeft ingevoerd de specifieke beveiligingstargets uit de norm met behulp van de ISM-methode kan realiseren.

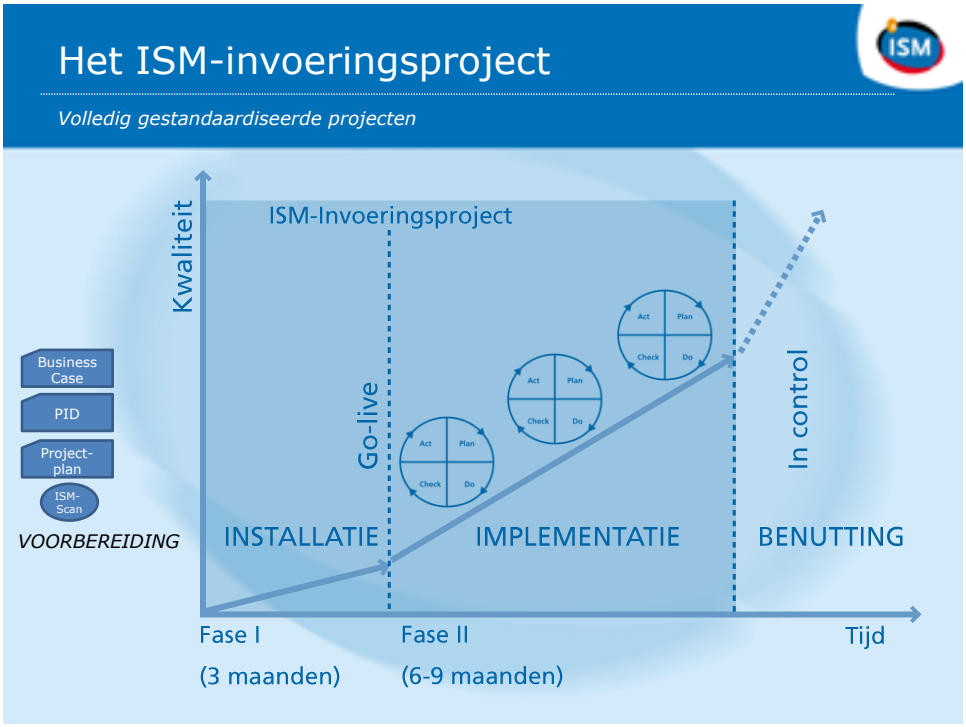
Scope van ISM

De ISM-methode beperkt zich tot de tactische en operationele niveaus van een beheerorganisatie en gaat er vanuit dat er beleid aanwezig is. ISM voorziet dus formeel niet in de (strategische) vaststelling van het informatiebeveiligingsbeleid. Zo'n plan kan echter wel binnen de scope van ISM worden gebracht via het risicomanagementproces QM (Quality Management).

Verder moet worden opgemerkt dat *de realisatie* van enkele componenten van de norm ook formeel buiten de scope van IT-beheer valt, daar waar het gaat om het beheer van mensen (HRM) en middelen (facility management). Ook die componenten kunnen echter vanuit IT-beheer worden aangestuurd, en daarmee binnen de scope van ISM worden gebracht.

Toepassing van de ISM-methode op informatiebeveiliging

In Fase I van de invoering van de ISM-methode wordt vastgelegd hoe de organisatie georganiseerd is, wie welke taken, bevoegdheden en verantwoordelijkheden (TBV) heeft. Deze TBV worden gerelateerd aan de activiteiten in een gestandaardiseerd procesmodel voor dienstverlenende organisaties. De tooling waarmee de organisatie haar activiteiten ondersteunt wordt vervolgens geoptimaliseerd en geïntegreerd met het procesmodel en met de organisatie. De eerste gestandaardiseerde werkwijzen uit het ISM-framework worden in het managementsysteem vastgelegd, en de organisatie wordt voorbereid op het hanteren van het managementsysteem voor een serie verbeterinitiatieven.



In Fase II van een ISM-invoering worden vervolgens enkele verbetercycli doorlopen aan de hand van het ingevoerde managementsysteem. Door deze verbetercycli te richten op informatiebeveiligingstargets kunnen de eisen van NEN7510 stuk voor stuk op de korrel worden genomen, op zo'n manier dat de verbeteringen zeer efficiënt worden doorgevoerd en een blijvend karakter hebben. Niet alleen kunnen de eisen van de norm zo veel sneller worden gerealiseerd, ook de kosten zullen door de efficiënte ISM-aanpak stukken lager uitpakken. Daarmee komt het inrichten van adequate informatiebeveiliging conform NEN7510 voor veel zorginstellingen binnen handbereik.

De speerpunten waar de *voorlopige normen* (NVZ) zich op richten zijn de volgende:

- Informatiebeveiligingsbeleid, -proces en -organisatie
- risicoanalyse
- bewustwording
- fysieke toegang tot systemen en ruimten, virusscanner, firewall en backup
- gegevensuitwisseling en online gegevens
- autorisatie, wachtwoorden en technische achterdeuren
- continuïteitsbeheer
- bedrijfsdocumenten en persoonsgegevens
- incidentmelding

Sommige van deze punten worden geheel door de standaardinrichting van ISM gedekt, andere zijn in een verbetercyclus met de ISM-methode snel en blijvend te bereiken. Daarnaast kan de ISM-methode op elke andere eis uit NEN7510 worden toegepast, waarmee de organisatie meteen klaar is voor de volgende stap: het realiseren van *alle eisen* van NEN7510.
Wie dan nog een stap verder wil kan naar ISO27001 kijken: de oorsprong van de NEN7510-norm.

De cross-reference van ISM en NEN7510

In de cross-referencefiguur op de volgende pagina is afgebeeld hoe de elementen van NEN7510 door de ISM-methode worden gedekt. Met de omlijnde cellen zijn de eisen aangeduid die deels of geheel door de voorlopige NVZ-normen zijn gedekt. De figuur illustreert dat de NVZ-eisen slechts een beperkt deel van de eisen van NEN7510 afdekken. In onderstaande tabel zijn de resultaten van de cross-reference tussen ISM en NEN7510 weergegeven. De onderscheiden relaties zijn met kleuren aangegeven. Deze kleuren komen terug in de cross-reference.

aantal	kwalificatie	waarvan in NVZ
6	standaard geregeld in ISM	2
84	toepassing van ISM-regelgeving op specifiek doel	19
24	technisch kenmerk, onafhankelijk van ISM te regelen	4
114		**25**
5	beleid,realisatie niet binnen ISM maar wel aanstuurbaar vanuit ISM	2
1	HRM, realisatie niet binnen ISM maar wel aanstuurbaar vanuit ISM	1
1	gebruik, realisatie niet binnen ISM maar wel aanstuurbaar vanuit ISM	1
4	facilities, realisatie niet binnen ISM maar wel aanstuurbaar vanuit ISM	4
11		**8**
125		**33**
33	geheel of deels opgenomen in NVZ-normen	33

Overzicht van de cross-reference tussen NEN7510 en ISM

De ISM-methode dekt alle 125 paragrafen van NEN7510, met dien verstande dat van 11 met een roodtint aangeduide paragafen geldt dat de *realisatie* buiten IT-beheer valt maar wel vanuit IT-beheer kan worden *aangestuurd*. Dit betreft:

- 5 paragrafen aangaande het opstellen van **beleidsdocumenten** in het strategische domein
- 1 paragraaf over eisen in het **HRM**-domein
- 1 paragraaf over eisen aan het **gebruik**
- 4 paragrafen over de inrichting van de **technische omgeving** (facilities)

In enkele gevallen refereert een paragraaf mede aan beleid maar is dat niet de hoofdzaak; waar dat het geval is, is dit in het overzicht op de volgende pagina nog in de cel vermeld.

Van deze 125 paragrafen worden 6 belangrijke (groen) al meteen gedekt bij de standaardinvoering van ISM. Dit betreft eisen ten aanzien van **changemanagement, risicomanagement** en **incidentmanagement**, drie van de kernprocessen van ISM. Hiervan zijn 2 paragrafen opgenomen in de NVZ-selectie.

De overige paragrafen vallen uiteen in 84 paragrafen (geel) betreffende **regelgeving** die, door toepassing van de ISM-methode, onder sturing van de processen kan worden ontwikkeld en geborgd (waarvan 19 in de NVZ-selectie), en 24 paragrafen (oker) die steeds uitsluitend een **technische voorziening** betreffen (waarvan 4 in de NVZ-selectie). Beide groepen kunnen geheel worden geregeld door in Fase II van de ISM-invoering een aantal verbetercycli te richten op specifieke beveiligingstargets.

In de ISM-methode worden alle taken, bevoegdheden en verantwoordelijkheden van medewerkers vastgelegd in functies en rollen. Deze organisatorische kenmerken worden vervolgens gepubliceerd in de BPM-tool, en vanuit de intranet-portal ontsloten.
Deze fundamentele eigenschap van ISM dekt een belangrijk deel van de regelgeving-paragrafen. Gestandaardiseerde ISM-procesflows, waarmee in ISM afgesproken werkwijzen worden vastgelegd en ontsloten, dekken een groot deel van de overige paragrafen.

NEN7510 Target	NEN7510 Paragraaf	sub1	sub2	sub3	sub4	sub5	sub6	sub7	sub8	sub9	sub10
5 Beveiligingsbeleid	5.1 Informatiebeveiligingsbeleid	beleid									
6 Organiseren van IB	6.1 Interne organisatie										
	6.2 Externe partijen										
7 Beheer van middelen voor de informatievoorziening	7.1 Verantwoordelijkheid voor de middelen										
	7.2 Classificatie van gegevens										
8 Beveiligingseisen t.a.v. personeel	8.1 Beveiligingseisen bij het aannemen van personeel			HRM							
	8.2 Taakuitvoering		gebruik								
	8.3 Einde van de aanstelling										
9 Fysieke beveiliging en beveiliging van de omgeving	9.1 Beveiligde ruimten	FAC	FAC	FAC	FAC						
	9.2 Beveiliging van apparatuur										
	9.3 Algemene beveiligingsmaatregelen										
10 Operationeel beheer van informatie- en communicatievoorzieningen	10.1 Bedieningsprocedures en verantwoordelijkheden										
	10.2 Uitbesteding										
	10.3 Systeemplanning en -acceptatie										
	10.4 Bescherming tegen kwaadaardige programmatuur										
	10.5 "Back-up"										
	10.6 Netwerkbeheer										
	10.7 Behandeling en beveiliging van media										
	10.8 Uitwisseling van gegevens	beleid				beleid					
11 Toegangsbeveiliging	11.1 Eisen ten aanzien van toegangsbeveiliging	beleid									
	11.2 Identificatie en authenticatie						gebruik				
	11.3 Autorisatie en toegangscontrole	beleid									
	11.4 Toegangsbeveiliging voor netwerken	beleid									
	11.5 Mobiele computers en telewerken	beleid									
12 Aanschaf, ontwikkeling en onderhoud van informatiesystemen	12.1 Beveiligingseisen voor systemen										
	12.2 Beveiliging in toepassingssystemen										
	12.3 Cryptografische beveiliging										
	12.4 Beveiliging van systeembestanden										
	12.5 Beveiliging bij ontwikkel - en ondersteuningsprocessen										
13 Continuïteitsbeheer	13.1 Aspecten van continuïteitsbeheer										
14 Naleving	14.1 Naleving van de wettelijke voorschriften										
	14.2 Beoordeling van de naleving van het beveiligingsbeleid en de technische vereisten										
	14.3 Systeemaudits										
15 Beveiligingsincidenten	15.1 Bewaking										
	15.2 Melden van incidenten en zwakke plekken	FAC									
	15.3 Afhandeling en verbeteringen na incidenten										

Aanwijzingen voor de ondersteuning van de voorlopige VGZ-normen

De NVZ heeft in april 2010 een set normen vastgesteld (kolom 3 in de tabel). In de laatste kolom (blauw) staat steeds vermeld hoe de ISM-methode kan worden gebruikt om deze eisen in de praktijk te realiseren.

Target	Full text van de norm volgens NEN7510	Minimumeis NVZ uit NVZ Toetsingsinstrument Informatiebeveiliging, conform start- en vervolgnormen; letterlijk overgenomen cross-reference	Aanwijzingen voor het toepassen van de ISM-methode
Algemeen: samenhangend stelsel van organisatorische en technische maatregelen			
Algemeen: afweging risico's, mogelijkheden en kosten			
5 Beveiligingsbeleid			
5.1 Informatiebeveiligingsbeleid	Het belang van informatiebeveiliging wordt door de leiding van een zorginstelling tot uiting gebracht in een beleidsdocument. Naast de te bereiken beveiligingsdoelen wordt daarin de weg beschreven waarlangs informatiebeveiliging door de desbetreffende zorginstelling wordt gerealiseerd. Door deze vastlegging en de publicatie ervan, wordt het voor medewerkers van de zorginstelling duidelijk welke inspanning van hen wordt verwacht om informatiebeveiliging gestalte te geven.		
5.1.1 Beleidsdocument voor IB	De leiding van de zorginstelling moet een beleidsdocument opstellen, goedkeuren en op passende wijze uitdragen aan alle medewerkers en andere betrokkenen. Het beleidsdocument moet het omgaan met informatiebeveiliging omschrijven, alsmede de betrokkenheid van de leiding verwoorden. Het beleidsdocument moet aandacht besteden aan: — de betekenis, het doel van de informatiebeveiliging en het belang daarvan voor de organisatie; — het ondubbelzinnig vastleggen van de intenties van de leiding in deze; — de beleidsmaatregelen, uitgangspunten, en gedragsregels ten aanzien van de informatiebeveiliging, met daarbij nadrukkelijk aangegeven welke zaken voor de instelling van wezenlijk belang zijn, zoals: — het nakomen van wettelijke en contractuele verplichtingen; — de vereiste opleiding en training in beveiligingszaken; — het weren van kwaadaardige programmatuur; — het management en de continuïteit van bedrijfsprocessen; — de consequenties van het niet naleven van het beveiligingsbeleid; — de verantwoordelijkheden voor het beheer van de informatiebeveiliging, waaronder het rapporteren van beveiligingsincidenten; — de ondersteunende documentatie.	Er is een risicoanalyse uitgevoerd. Op basis van die risicoanalyse, de norm en de mogelijkheden is een beleidsplan IB opgesteld, met plannen voor de komende drie jaren (inhoud & tijd). Er is een audit IB door een betrouwbare derde (niet eigen accontant of eerdere risicoanalist) uitgevoerd en de rapportage is aan de Inspectie gestuurd.	Definieer een algemeen risico in QM en voer de risicoanalyse uit. Neem het risico-onderzoek op in de risico-kalender Voer een impactanalyse uit van de risico's uit de risicoanalyse, en registreer deze in de ITSM-tool. De afhandeling van het risico vindt plaats volgens het Quality Management proces, waarbij de risico's worden opgenomen op de risicokalender. De voortgang van de risico-afhandeling vindt plaats door procescontrol QM. De planning van de "externe" audit is opgenomen in de risicokalender. Het procesmanagement bewaakt de inpanning en afhandeling van de audit, waaronder het opsturen van het rapport naar de Inspectie. **EXTRA**: • Iedere proceseigenaar hanteert het IB-beleidsdocument als randvoorwaarde bij de inrichting van hun proces. • Neem het document op in de CMDB en breng het onder CHM-toezicht. • Hanteer het IB-beleid in SLM als een

			randvoorwaarde waarin gerefereerd wordt in SLA's. • Neem een toets tegen het IB-beleid op in de ISM-procedure CHM. • Leg risico's voor het niet voldoen aan het IB-beleid vast in QM en handel ze daar af. • Maak bij OPS bekend wat deze richtlijn is, zodat daarop keuzes worden gebaseerd voor de inrichting, het onderhoud, en de bewaking van de IT-infrastructuur. • Neem de categorie 'IB' op in de incident-categorisering en in de managementrapportage • Neem de categorie 'IB' op in QM en in de managementrapportage **CONTROLS**: 1- aanwezigheid document: goedgekeurd IB-beleid, op basis van uitgevoerde risicoanalyse 2- aanwezigheid van het IB-beleidsdocument als een CI in de CMDB 3- optioneel: standaard check op IB-beleid in CHM-procedure 4- optioneel: referentie naar IB-beleid in de beveiligingsparagraaf van een SLA 5- optioneel: beveiligingsincidenten worden als zodanig gecategoriseerd en gerapporteerd 6- optioneel: neem de categorie 'IB' op in QM en rapporteer daarover

Voorbeeld van de uitwerking van de ISM-methode naar een concrete eis uit NEN7510