Aankondiging Webinar NEN 7510 – donderdag 30 september 2021

NEN 7510, certificeren en zelf de regie houden

Veel zorgorganisaties zijn, op een of andere manier, bezig met NEN 7510. Maar hoe kom je daadwerkelijk tot certificering en hoe houd je zelf de regie?

De bedoeling van NEN 7510 is organisaties helpen om zelf hun informatieveiligheidsrisico's te beheersen, en daar zelf bewuste keuzes in te maken. Hoe je dat voor elkaar krijgt, daarover gaan we in gesprek met **Marc Been**, die als CISO gehandicaptenzorginstelling Ipse de Bruggen naar certificering leidde, en **Cees van der Wens**, die vele certificeringsaudits uitvoerde en tegenwoordig als consultant implementatietrajecten ondersteunt.

Onder leiding van **Martine van de Merwe**, bestuurslid van IP-zorg, geven zij een beeld hoe je "NEN 7510" kunt aanpakken. Met volop tips en valkuilen uit hun eigen ervaring.

Over de sprekers

Marc Been (1979) heeft bedrijfskundige informatica gestudeerd aan de HvA. Na lange tijd in internationale omgevingen gewerkt te hebben (bancaire sector, utilities) als consultant is hij sinds 2018 werkzaam binnen de zorgsector. Eerst in de rol als projectmanager implementatie AVG en sinds 2020 als CISO bij stichting Ipse de Bruggen. Een belangrijke mijlpaal voor zowel Marc als stichting Ipse de Bruggen is het behalen van de NEN7510 certificering (geaccrediteerd!) in 2021.

Cees van der Wens (1965) studeerde Industriële Automatisering aan de Hogeschool Utrecht en werkte daarna lange tijd in de technische sector. Vanuit zijn rol als Lead Auditor heeft de auteur tientallen certificatie-audits uitgevoerd bij een breed scala van organisaties. Als consultant heeft hij evenzoveel organisaties geholpen met het verkrijgen van het NEN7510- of ISO27001- certificaat. In 2019 heeft Cees zijn 'Handboek ISO27001' in twee talen gepubliceerd, in 2020 volgde zijn 'Handboek NEN7510' voor Nederlandse zorginstellingen. Sinds 2020 werkt Cees als zelfstandig adviseur/auditor samen met zorginstellingen en het bedrijfsleven.

Verslag Webinar NEN 7510 – donderdag 30 september 2021

Inleiding Peter van der Zwan

Beste mensen,
Allereerst een hartelijk welkom namens Stichting IP-Zorg. In het bijzonder ook voor onze mensen aan tafel die straks met Martine en vast ook met elkaar in gesprek gaan over hun ervaring met certificering voor NEN 7510, elk vanuit een andere rol, Cees van der Wens, jarenlange ervaring als auditor, en Marc Been, CISO bij zorginstelling Ipse De Bruggen die recentelijk in het trotse bezit is gekomen van het certificaat. Jullie stellen je dadelijk nog voor, maar wij zijn natuurlijk erg benieuwd naar jullie ideeën en ervaringen.
Wat we wel alvast kunnen constateren, is dat de markt voor certificering sterkt groeit. Ik las dat in het afgelopen jaar alleen al bij een van de certificerende instanties het aantal vacatures in het afgelopen jaar rond de 1000 lag. Alleen al hieruit blijkt dat organisaties hier steeds vaker voor kiezen. Maar waarom? Als je het goed voor elkaar hebt, wil je dat graag laten weten. En met een NEN 7510 certificaat kun je laten zien dat je informatiebeveiliging binnen de organisatie goed op orde hebt. Maar het kost ook heel veel tijd, geld en energie. En zorginstellingen willen zich toch vooral richten op het leveren van goede zorg? Dat komt vast aan de orde, Marc. Net als de rol van de auditor. Want de ene auditor is de andere niet. Wat is de bewegingsruimte van de auditor? Hoe dwingend kan een auditor zijn? Kan de auditor niet meer adviseren en ondersteunen? Hoe kun je als zorginstelling zelf de regie houden? Zowel als het gaat om het resultaat maar ook om de kosten (denk aan meerwerk). Want als zorginstelling willen we zo veel mogelijk voordeel halen uit certificering en de daarbij horende audits tegen uiteraard zo laag mogelijke kosten. En hoe zorgen we ervoor dat we in 1 keer slagen? Er hoe kan de auditor daarbij helpen.
Dat is wat we vanmiddag hopen te horen. Ik wil het hier graag bij laten. Anders maai ik misschien te veel gras voor de voeten weg. Ik wens u in ieder geval een goede sessie en geef graag het woord aan Martine.

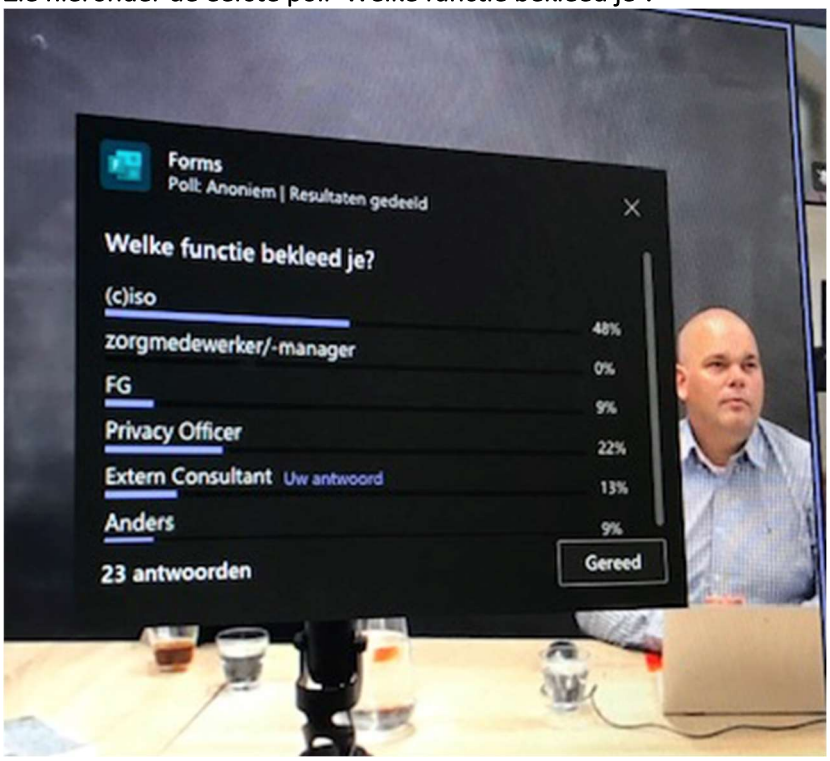
Van links naar rechts: Martine van de Merwe, Cees van der Wens en Marc Been

Martine gaat in gesprek met Marc en Cees.

Martine: Marc, je werkt vanaf 2018 in de zorg en daarvoor in de bancaire wereld. Wat viel je op?
Marc: In de zorg is minder geregeld en het volwassenheidsniveau is lager.

Martine: Cees, je hebt een technische achtergrond, je kent de normen en de manier waarop gecertificeerd moet worden. Je hebt eerst het Handboek ISO 27001 geschreven en daarna het Handboek NEN 7510 dat veel dikker is. Hoe komt dat?
Cees: door het verwerken van feedback, voortschrijvend inzicht en de zorgspecifieke blik. Trouwens, een nieuwe versie van de ISO 27001 zou wellicht ook dikker worden.

Zie hieronder de eerste poll 'Welke functie bekleed je'?



Ter introductie enkele stellingen.
Stelling: Mijn IB thuis verdient ook een NEN 7510 certificaat
Marc: dat gaat me te ver; NEN 7510-certificering is voor organisaties en wat je thuis doet is je eigen verantwoordelijkheid; je moet natuurlijk alert zijn. Ik ben wel extra waakzaam op wat mijn kinderen doen op hun ipads.
Cees: nee. Ik wil niet roomser zijn dan de Paus; bij ons thuis is het af en toe ook wel eens niet goed geregeld en moet ik alle zeilen bijzetten om mijn gegevens goed te beschermen.
Mijn vakgebied is wel aanleiding voor discussies thuis.

Stelling 2: Als ik kan kiezen tussen een middagje golf of het bestuderen van de NEN 7510, wat doe ik dan? Beide kiezen voor een middagje golf; laat je leven niet beheersen door je vakgebied.

Stelling 3: Werken met NEN 7510 is worstelen en vastlopen (citaat uit het handboek van Cees).
Dit wordt bij Ipse herkend. Het vervolgtraject na certificering is worstelen, duwen en trekken. Maar niet opgeven en op zeker moment trek je het vlot.
Cees: dat heeft te maken met het ontstaan van de norm, het is taaie materie. En hoe we ermee omgaan; het samenspel van organisaties, auditoren en RvA.
Hopelijk met als gemeenschappelijk doel: het beheersen van risico's.

Stelling 4: de mens is de zwakste schakel
Cees en Marc beamen dit.
Marc: Het betreft vooral medewerkers die niet direct betrokken zijn bij IB; je moet het komen brengen, ze komen het niet halen. Als je het niet komt brengen blijven ze 'onbewust'.

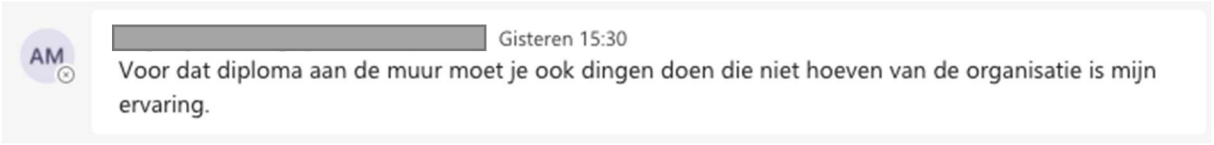
Cees: IB speelt zich grotendeels onzichtbaar af; in een wereld waar iedereen zijn eigen beeld van IB heeft. Zelfs als betrokkenen welwillenden zijn is dat geen garantie dat IB leidt tot het gewenste resultaat.
Martine: ik vind het een vervelende manier om zo naar mensen te kijken. En als er een incident plaatsvindt krijgt vaak iemand de schuld die niet de schuld heeft; omdat in de organisatie zaken niet goed geregeld zijn.

Martine: waarom is IB belangrijk? Waarom doe je het? Een antwoord is zelfs voor IB-ers lastig.
Martine: stel ik ben een patiënt of cliënt en vind al die veiligheidszaken rond privacy belachelijk; hoe reageer je dan?
Cees: er zijn niet zoveel patiënten die dat denken. We zitten in een tijdperk waarin gegevens erg belangrijk zijn en je er ook misbruik van kunt maken. Hoe meer ze van je weten hoe kwetsbaarder je wordt.

Martine: stel ik ben je collega; kun je me uitleggen waarom IB belangrijk is?
Marc: zorgverleners hebben een extra verantwoordelijkheid omdat ze met kwetsbare mensen werken Als vertrouwelijke gegevens op straat komen te liggen dan is het te laat. Naïviteit is niet meer van deze tijd. We hebben te maken met digitale struikrovers
Cees: De NEN 7510 gaat niet alleen over vertrouwelijkheid van persoonsgegevens en datalekken; de norm gaat vooral ook over integriteit, de juistheid van informatie, en beschikbaarheid.

Martine: ik merk in gesprekken met bestuurders dat ze IB belangrijk vinden; maar tegelijk een 'knagend gevoel' hebben en niet weten hoe ze daarmee om moeten gaan. Er zijn altijd wel weer dringende actualiteiten die voorgaan. Hoe kun je die bestuurders helpen?
Cees: ik geef aan dat het niet de bedoeling is alles compleet om te gooien maar dat je verder kunt gaan met wat er al is. Dat je wellicht systematischer te werk kunt gaan.
De norm gaat er wel van uit dat je er welwillend tegenover staat.

Martine: hoe overtuig je de RvB?
Cees: Maak de risico's inzichtelijk door te identificeren en te beoordelen. Rapporteer dat in klare taal. Laat zien wat er kan gebeuren als risico's manifest worden, zodat bestuurders een afweging kunnen maken. Risico's inzichtelijk maken is doorslaggevend. Een argument 'dat hoeft toch niet?' kun je alleen maar pareren met relevante risico's.
Een diploma aan de muur is meegenomen maar kan nooit de echte intentie zijn.



Cees reageert op de chat.
Het veelvuldig 'moeten' in de norm geeft de indruk dat je weinig ruimte krijgt.
Tegelijkertijd heb je wél die ruimte. Als voorbeeld: de inventaris van bedrijfsmiddelen. Van welke bedrijfsmiddelen moet je die maken? Die bedrijfsmiddelen die bijdragen aan het verlagen van je risico's; doe alleen wat dat past bij je risico's.
Cees benadrukt dat in het certificeringsproces de organisatie de regie heeft; dat op basis van 'onze expertise besloten is dat dit voldoende is'. Een goede auditor luistert daarnaar en kan hoogstens vragen of de organisatie hieraan of daaraan heeft gedacht. En wellicht kan een organisatie daar in het vervolgtraject zijn voordeel mee doen.

Martine heeft de gesprekspartners gevraagd een object te laten zien dat een verbintenis heeft met de NEN 7510. Marc heeft uit de kinderkamer thuis een fraaie weegschaal meegenomen. De weegschaal

staat symbool voor het op risico's gebaseerd bezig zijn. Het zoeken naar de balans tussen veilig en gebruikersvriendelijk; tussen informatieveiligheid en wat past bij de business.
Cees: Bij certificering bepaal je zelf de balans tussen acceptabele risico's en de maatregelen. Maar dat is niet onbeperkt; een plafond is het voldoen aan de wettelijke eisen. Het is de taak van de auditor om te beoordelen of het ISMS in staat is om te voldoen aan wettelijke eisen, naast de eisen die de organisatie zelf stelt.

Zie hieronder de tweede poll:

Status NEN7510 in onze organisatie

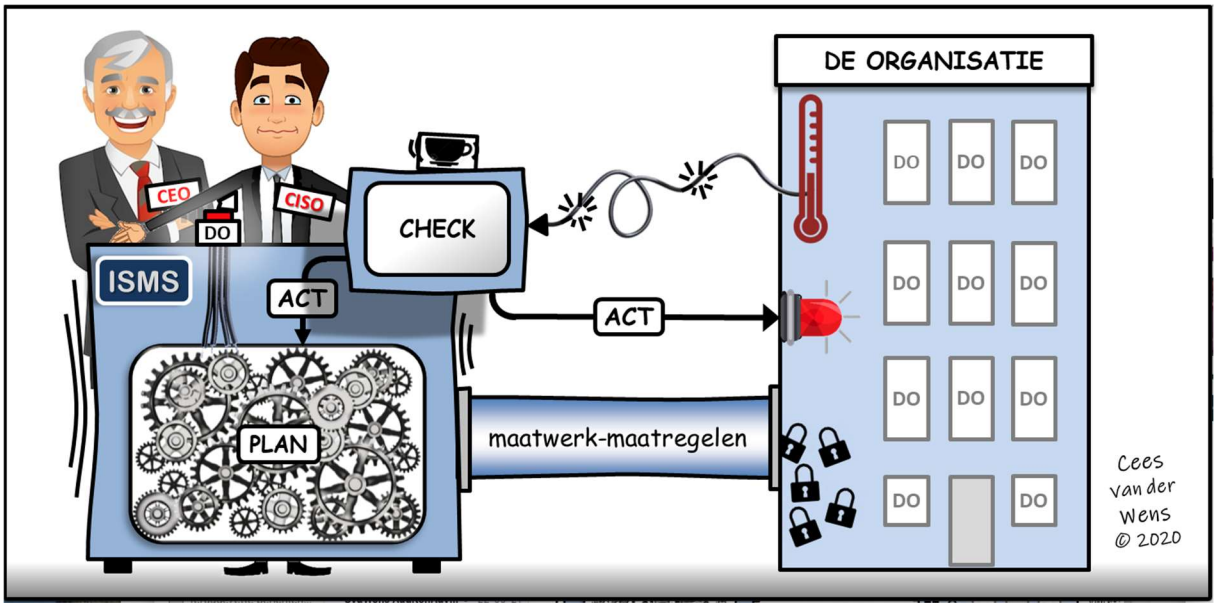
- ○ Gecertificeerd
- ○ We voldoen maar zijn niet gecertificeerd
- ○ Bezig met / Bijna geïmplementeerd
- ○ Net begonnen
- ○ Verdwaald
- ○ Niet mee bezig

Bijgewerkt

Gecertificeerd	13% (3)
We voldoen maar zijn niet gecertificeerd	0% (0)
Bezig met / Bijna geïmplementeerd	30% (7)
Net begonnen	**43% (10)**
Verdwaald	4% (1)
Niet mee bezig	8% (2)

23 reacties

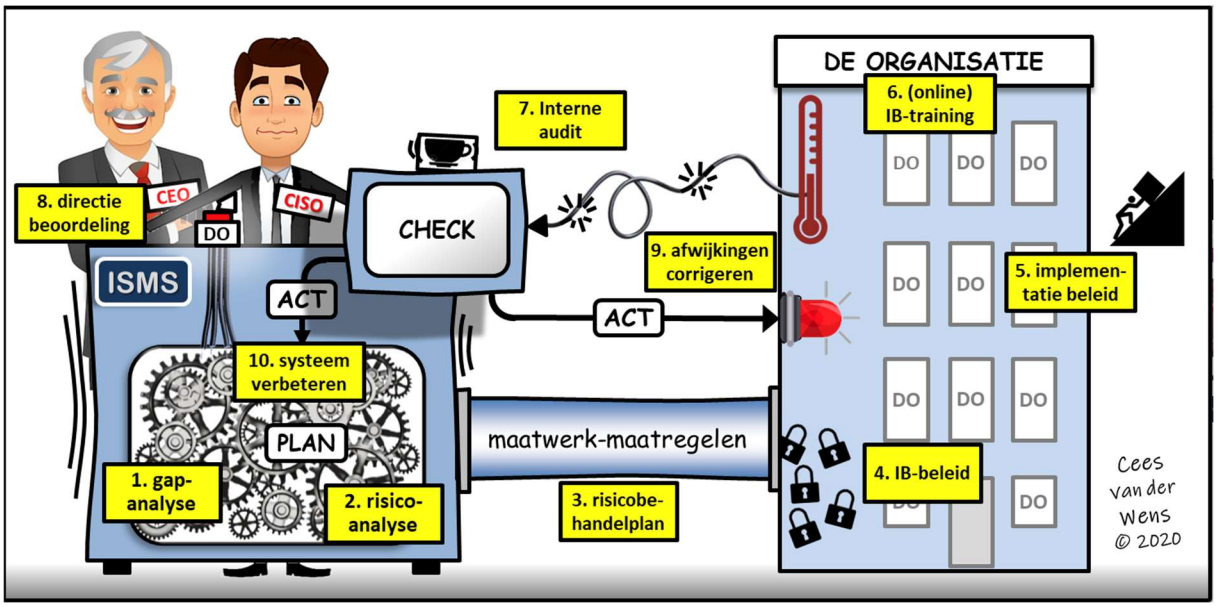
Martine vraagt Cees uit te leggen wat de bedoeling is van de NEN 7510.
Cees laat onderstaand plaatje zien.



Links-onder de NEN 7510-1; het ISMS H4 t/m 10 als machine.

In het Plan vraag je je af: wat zijn de maatregelen die bij ons passen?
In 6.1.3b staat: ga op eigen kracht maatregelen vaststellen.
En in c: ga kijken of in NEN 7510-1 bijlage A maatregelen staan die je kunt toepassen in het kader van je risico's. Ga aan de slag met die maatregelen
Maak de Verklaring van toepasselijkheid; dit dwingt je te verklaren waarom je bepaalde zaken niet toepast. Comply or explain.

Zo 'pomp' de z.g. maatwerk-maatregelen de organisatie in en 'start' de pdca-cyclus.
Je kunt in de act-fase de maatregelen aanpassen maar ook de 'machine' bijstellen.
De maatregelen uit de NEN 7510-2 kun je superbelangrijk maken, maar je kunt ze niet los zien van die 'machine'.



De aanpak van Cees zie je in de geel gemarkeerde stappen. Stap 5, het implementeren van het beleid is het zwaarste traject. Het hele traject duurt, afhankelijk van het ambitieniveau van en aantal maanden tot een aantal jaar.

Hoe was de aanpak bij Ipse de Bruggen?

Marc geeft een toelichting. In 2019 is de IGJ langsgeweest in het kader van het Toetsingskader 'Inzet van e-health door zorgaanbieders'. Daarin staat o.a. dat een organisatie moet voldoen aan de NEN 7510. Bij Ipse de Bruggen waren al wel veel maatregelen getroffen maar was er geen ISMS. Dit moest binnen een jaar worden gerealiseerd. De 'hete adem van de IGJ' was een welkome stimulans.

Wat staat er in de wet over de NEN 7510?

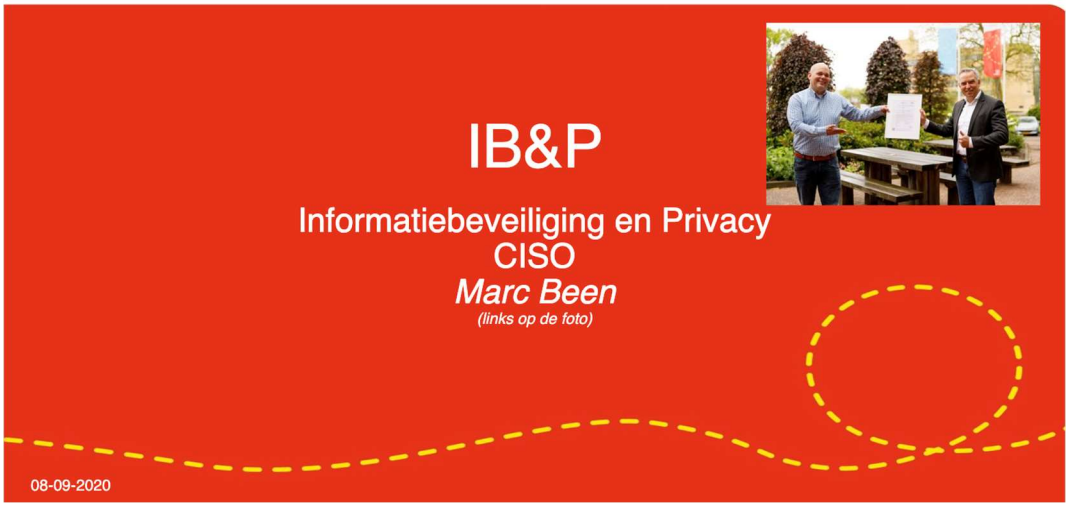
Cees: Bij de 'Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg' hoort het 'Besluit elektronische gegevensverwerking door zorgaanbieders', waarin staat dat een elektronisch uitwisselingssysteem moet voldoen aan de NEN 7510.
Marc: veelzeggend is dat de AP boetes uitdeelt op basis van de NEN 7510; refererend aan de AVG art 32 'gij zult een op uw risico's gebaseerde IB op orde hebben'.

Waarom kiezen voor certificering?

Cees: de onafhankelijkheid van de audit is een pré; de bevindingen en jaarlijkse audits houden de zaak gaande.
Een certificerende instelling komt helpen om te zien of je *op basis van je ISMS* veilig bent.

Bevindingen van de externe auditor kunnen aanleiding zijn voor discussies over je interne audit: heb je deze bevinding zelf ook gedaan bij je interne audit?
Een interne audit kijkt of je maatregelen doeltreffend zijn. Een externe audit kijkt op een ander niveau. Het advies van Cees is dan ook om iemand die bijna dagelijks naar ISMS-en kijkt, te laten beoordelen hoe jouw ISMS verankerd is in de organisatie. Maak gebruik van die ervaring.

Marc & Ipse de Bruggen



Ipse de Bruggen

Wat voor organisatie is Ipse de Bruggen:

- VGZ-organisatie (verstandelijke gehandicapten zorg)
- 5.000+ clienten in Volwassenen Zorg (VZ) en Kind & Jeugd
- 5.500+ medewerkers
- Drie grote landgoederen / 400+ locaties in voornamelijk Zuid-Holland
- Werken met gevoelige informatie van een kwetsbare groep mensen
- In 2021 is Ipse de Bruggen geaccrediteerd NEN7510 gecertificeerd (DigiTrust).

Ipse de Bruggen is in 2021 gecertificeerd door een *geaccrediteerde* organisatie. Certificering is een onbeschermde activiteit en toezicht van de Raad voor Accreditatie (RvA) heeft dan ook een toegevoegde waarde. Belangrijk is bijvoorbeeld dat de RvA als eis stelt dat een certificaat alleen mag worden afgegeven als *alle* primaire processen bij de beoordeling betrokken zijn. Degene die jou certificeert wordt ook zelf geaudit of zij hun processen op orde hebben. Als dat het geval is wordt de certificerende instelling (CI) geaccrediteerd door de RvA.

Deze sheet is besproken in het IB&Privacy team van Ipse de Bruggen.
Steun RvB / Directie is het belangrijkste; de 'druk' vanuit de Inspectie heeft daarbij geholpen.
Ipse de Bruggen heeft gewerkt met standaard risico's; maak het jezelf niet te moeilijk!
Reactie Cees: uitgaan van standaard risico's kan ballast met zich meebrengen. Waarom niet uitgaan van de risico's die voor jou het belangrijkste zijn?
Marc: de belangrijkste risico's waren al gepareerd maar we konden dat niet formeel aantonen.

Als valkuil zien we 'Eigenaar risico' in de sheet.
Het is belangrijk dat iemand in de organisatie zich *eigenaar* van het risico voelt. Marc noemt als voorbeeld een zoneringsplan. Een specialistenteam schrijft dat op, maar uiteindelijk moeten anderen in de organisatie tot actie komen; in dit geval is de risico-eigenaar de facilitaire dienst. In het begin ga je als IB-er veel zelf opstarten, ga je op de stoel zitten van de verschillende risico-eigenaren, maar in de loop van het traject moet je dat overhevelen en dat is in de praktijk lastig.
Cees: betrek de verschillende eigenaren zo vroeg mogelijk bij de risico-inventarisaties; maak ze verantwoordelijk voor uitspraken. Risico-eigenaren moet ook risico's voelen.
Marc: dat is ook veel gebeurd; het beoordelen van risico's in workshops met betrokkenen gaf een positieve dynamiek.

Goed is goed genoeg – niet verzanden in details.
Maar wel continu verbeteren!

Inbreng kennis intern/extern moet in balans zijn; zorg dat kennis van externen binnen je organisatie geborgd wordt.

IB&Privacy zien als geheel; privacy heeft veel raakvlakken met IB.
Marc wil in het ISMS ook de privacy-aspecten opnemen; conform de ISO 27701.
Wellicht later aanvullend op certificeren.

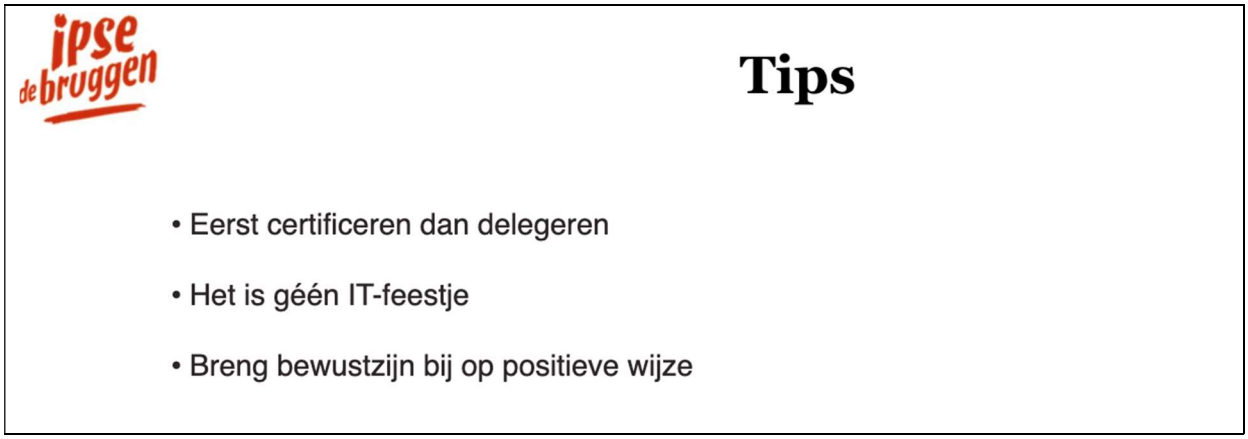
ISMS-Tooling als valkuil.
Marc heeft ervaren dat bij Ipse de Bruggen te snel is begonnen met ISMS-tooling; er was geen overzicht meer en hij is teruggegaan naar Excel. Geeft meer flexibiliteit.
Een tool dwingt je in een bepaald stramien dat vertragend kan werken. Daar staat tegenover dat de tool-aanbieder stelt dat de tool je helpt te structureren.

Ipse de Bruggen is nu wel toe aan tooling om zaken te automatiseren. En het liefst een tool die aansluit bij systemen die er al zijn zoals bijvoorbeeld TOPdesk.

Cees: onderstreept de ervaring van Marc maar ziet ook organisaties waarbij tooling wel heeft gewerkt. Het is maar net hoe je erin staat: wil je aan de hand worden genomen of wil je het zelf ontdekken? Zie chat Dick.
Je kunt ook eerst zelf op pad gaan en daarna de juiste tool erbij zoeken. Let wel op of de risico-beoordeling in de tool tot zijn recht komt.

Koppelen dan wel integreren met andere managementsystemen zoals een kwaliteitsmanagementsysteem en continuïteitssysteem is lastig; IB is op zichzelf al omvangrijk en specifiek.

Hieronder enkele chats die de discussie hebben gevoed.



Hierboven de tips van Marc.
En een tip van Cees: zet IB niet in als dreigmiddel! Benader IB positief.

PF [redacted]
mooie lijfspreuk Marc!

Tot slot: Marc's lijfspreuk 'Goede zorg voor informatie is onderdeel van goede zorg' wordt breed omarmd.

Martine: wat moet je vooral *niet* neerleggen bij een externe adviseur?
Marc: Laat je informeren door iemand die veel kennis meebrengt maar maak je er niet afhankelijk van. Want na het certificaat aan de muur begint het pas. De auto is gebouwd en nu moet je erin gaan rijden.

Object Martine ter illustratie van NEN 7510-implementatie: injectiespuit.
Veel organisaties zien NEN 7510-implementatie als een project dat even moet en dan is het klaar. Het beeld van Martine is dat je het meer moet zien als een infuus; er is voortdurend 'voeding' nodig waarmee de organisatie het zelf draaiend houdt.

Welke rollen moet je voor IB beleggen?
Cees: ga niet de SO en FG verantwoordelijk maken als een politieagent; laat bijvoorbeeld een leidinggevende een medewerker aanspreken op clear desk / clear screen policy.
Denk aan een informatiebeveiligingsmanagementforum (IBMF, NEN 7510-termen); een club mensen die de processen vertegenwoordigen. Ze hebben inhoud beleid gemaakt samen met specialisten. Delegeer de handhaving.
Marc: we hebben een IB-beleid en een IB-Handboek met afspraken over rollen en verantwoordelijkheden per unit. Dat maakt het beleid transparanter en toegankelijker.

S [redacted]
Hoe zou een organisatie van informatiebeveiliging op tactisch en operationeel idealiter eruit moeten zien volgens jullie?

(FG privacy én security officer, ambassadeurs) Wat vraag je aan inzet op tactisch en operationeel niveau binnen de organisatie2

N.a.v. de vraag in de Chat.
Martine: Je kunt heel veel operationeel beleid maken; maar wie gaat dat lezen?
Cees: haal daaruit wat echt relevant is, maak dat via trainingen en dergelijke gefaseerd duidelijk aan betrokkenen. Maar wat belangrijk is, is dat operationeel beleid, hoe het moet gebeuren, gebruikt kan worden als auditcriteria. Terugvallen op afspraken die we in de praktijk doen. Het niet hebben van die regels is geen optie.

Martine: In uitspraken AP worden organisaties afgerekend op dat ze niet doen wat er in hun eigen beleid staat. Het opschrijven van beleid is dus niet vrijblijvend.

Martine: wat is NEN 7510 NIET?
Marc/Cees: geen wondermiddel; je moet het zelf doen!
En geen garantie dat alles met betrekking tot IB dan voor de volle 100% geregeld is.

Hiermee wordt het webinar na anderhalf uur afgesloten, met dank aan de gasten Cees en Marc.