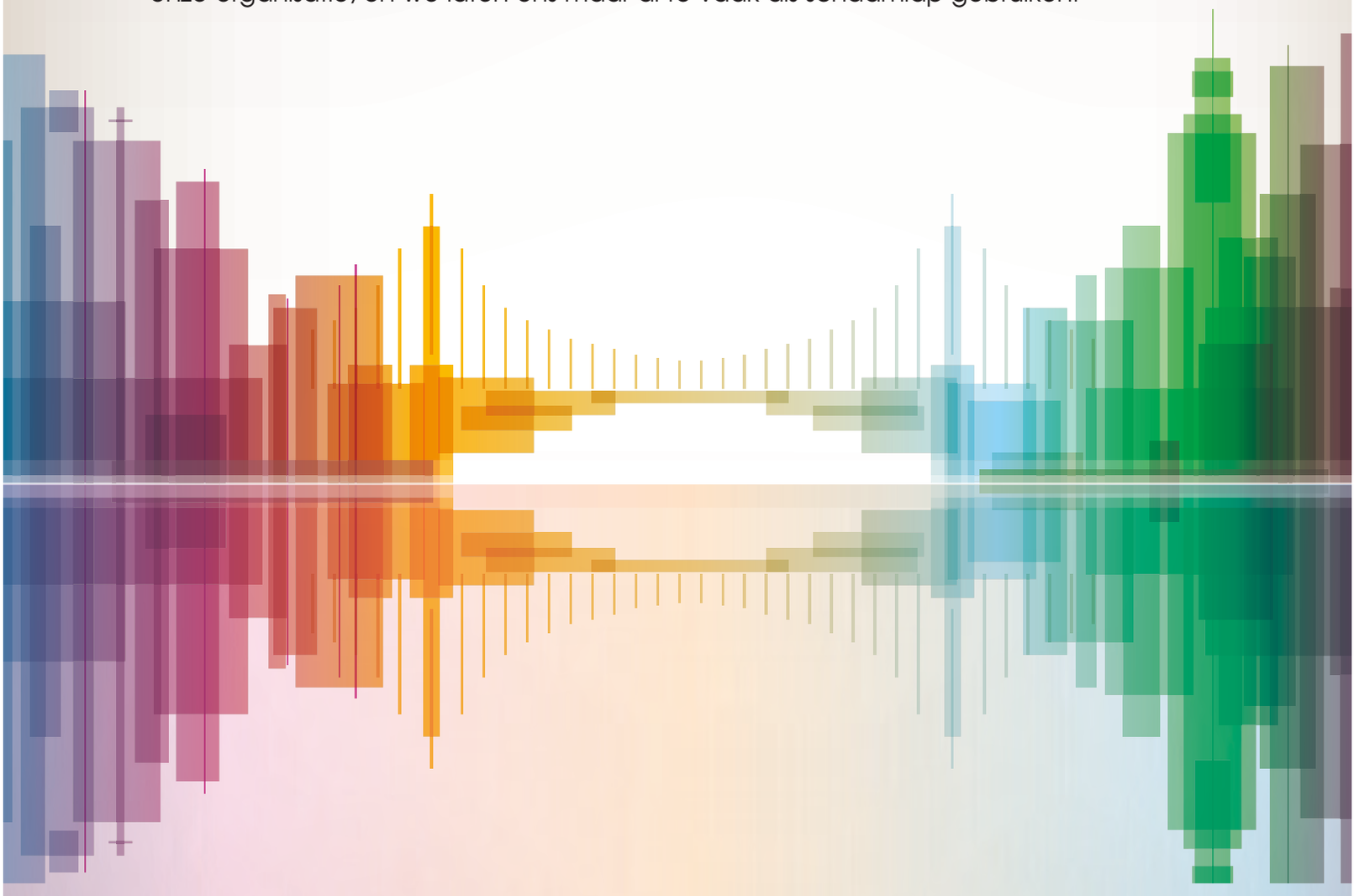
Auteur: André Beerten is sinds 2015 zelfstandig adviseur informatiebeveiliging en ook associate bij Verdonck, Klooster en Associates. Hij werkte eerder bij KPN, Getronics en het Groene Hartziekenhuis. Hij is te bereiken via: andre@octopus-ib.nl of via LinkedIn (1).

Maesbruggen 4

Afgelopen februari, in mijn eerste bijdrage aan dit blad, heb ik de vloer aangeveegd met óns, de ISO's. We bakken er niets van, zo was mijn stelling in het artikel *De falende CISO*. Vóór publicatie van dat artikel heb ik het artikel vaak met vakgenoten besproken en in alle gevallen instemming op mijn diagnose mogen constateren: we zijn niet effectief in het realiseren van control, van passende beheersing van risico's bij onze organisatie, én we laten ons maar al te vaak als schaamlap gebruiken.



Het neersabelen van de hele beroepsgroep is natuurlijk makkelijk, ongenuanceerd. Velen zullen zich minder aangesproken voelen, hopelijk terecht. Maar ik moet ook uitleggen hoe het (volgens mij) wél moet. Daarover gaat de komende reeks bijdragen van mijn hand over het ISMS, eigenaarschap, risico's vinden en het 'Register'. Maar we beginnen met de belangrijkste: **Maesbruggen bouwen**.

De implementatiekloof

Een Maesbrug overspant een van de belangrijkste obstakels die de informatiebeveiliger moet zien te overwinnen: 'de kloof' tussen ivoren toren en werkvloer, tussen beveiligingsopdracht en -realisatie, tussen vragers naar en aanbieders van veiligheid; de **implementatiekloof**. Risicoanalyses en normen leiden tot opdrachten voor beveiliging die ergens in de organisatie moeten worden omgezet -geïmplementeerd - naar effectieve maatregelen.

• *Over de muur*

Zó gaat het vaak: je maakt als adviseur een mooi lijstje met actiehouders bij IT, huisvesting, PZ et cetera. Waaraan je de norm-controls toewijst. Je nodigt jezelf uit op de koffie en je legt uit dat het belangrijk/verstandig is (en dat het moet van de baas) en je keert vervolgens hoopvol terug naar je ivoren toren. De actiehouders zijn nu aan zet, want implementeren is tenslotte niet jóuw, maar hun werk.

• *Vraagtekens*

Na een paar weken/maanden kom je dan terug en vraag je hoe het ermee staat. 10 tegen 1 is het er nog niet van gekomen, waren er andere prioriteiten, zijn ze het vergeten … óf hebben ze nog iets meer uitleg nodig. Want zeg nou zelf: wat is eigenlijk de bedoeling van die vage normteksten?

• *Ondertussen*

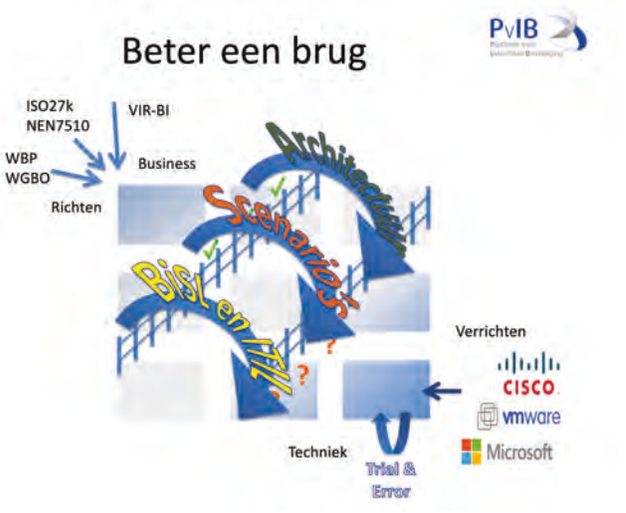
Voor veel bestuurders en toezichthouders begint ook de belangstelling voor informatiebeveiliging toe te nemen, maar dan in de trant van 'waar staan we'? Hoever zijn we al met de implementatie van BIO/NEN/ISO? Wat zeg je dan als (C)ISO wanneer je dit wordt gevraagd? De waarheid is vaak dat we van alles vermoeden, geen zekerheid hebben en het alleen anekdotisch kunnen illustreren. Incidenten verraden intussen dat verbetering mogelijk is.

Merk op dat niet alleen wij het niet kunnen beoordelen, maar ook de actiehouders niet, terwijl het wel hún 'pakkie-an' is: *implementeren en rapporteren*.

Maesbruggen

Wie mij een beetje heeft gevolgd binnen het PvIB weet dat ik sinds 2014 al publiekelijk worstel met dit kloof-probleem. Ik hanteer daarbij al sinds die tijd het 9-vlaksmodel van Professor Rik Maes.

De bruggen die ik probeer te slaan, over de kloof, heten bijgevolg Maesbruggen. Dat heeft onder meer geleid tot drie PvIB-bijeenkomsten met de titels Maesbruggen 1 t/m 3 (2014, '18 en '19).



Figuur 1: Beeld bij Maesbruggen 1.

In die bijeenkomsten hebben we allerlei opties verkend: architectuur kwam voorbij, BiSL + ITIL en bedrijfsbrede scenario's als cultuurkader, Mintzbergs organisatiemodellen, Agile werken, BCM-governance, zelfs een werkmodel voor duidelijker teksten en ook een praktijkcasus. Helaas, geen van al die mogelijkheden leverde een stabiele brug op. Het is gebleven bij genoeglijke avonden met collega's.

> De hamvraag is: Wat ís *implementeren*? Hoe doe je dat en wanneer is het goed genoeg? Als de opdracht aan de actiehouder niet duidelijk is, kan diegene er ook weinig mee.

• *Meetbare MaatregelAanpak - MMA*

In de loop der jaren heb ik mijn hoofd vaak gestoten bij mijn pogingen om het *implementeren* te bevorderen, maar uitein-

delijk heb ik toch een opening gevonden in de vorm van een gemeenschappelijke 'taal'. Die taal is in de kern heel eenvoudig: ik ga in gesprek met de actiehouders aan de hand van tien vragen over de *proceskwaliteit van de implementatie*. Deze taal biedt de actiehouder zowel een werkinstructie alsook een instrument om het resultaat van zijn werk te beoordelen.

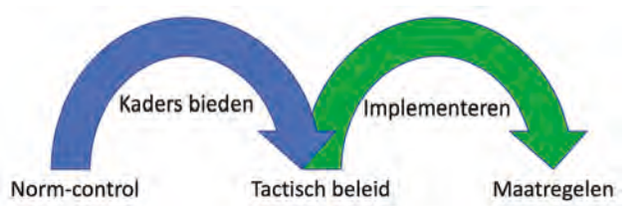
Ik, de ISO, ben alleen gespreksleider en kritisch meedenker. Ik ga niet over de antwoorden en niet over het oordeel of het goed genoeg is. Dat is de verantwoordelijkheid van de eerste lijn, van de actiehouder.

• *Doorvragen naar control*
Het gesprek gaat bij alle vragen over de 'control', de beheersing van het kwaliteitsaspect: hoe beheers je scope, je verantwoordelijkheid, de omgang met risico's, wet en regels et cetera. Krijg ik antwoorden in de trant van 'zo doen we dat' dan reageer ik met 'waarom'? Als men zegt 'dat doet Jantje', dan vraag ik 'is hem daarvoor een opdracht, instructie, tijd toegewezen'? Bij alles volgt de vraag naar documentatie en bij KPI's volgt de vraag: 'weet je het zeker?' en 'hoe ben je tot die keuze gekomen?'.

Steeds ben ik op zoek naar de 'rationale', een goed onderbouwde keuze en ook goed gedocumenteerd. Hoe beter de uitwerking van de control is onderbouwd en hoe beter de maatregelen zijn verankerd, des te volwassener is de implementatie.

Eerst tactisch beleid

De afstand (de kloof) tussen norm en werkvloer is zo groot dat die in twee stappen overbrugd moet worden. Te beginnen met de vertaling van de norm, en in details dus de controls, naar bedrijfseigen keuzes oftewel organisatiekaders. De norm vraagt er in meerdere controls ook om: het komt een keer of vijftien terug als eis, náást het algemene IB-beleid.



Figuur 2: Kaders als eerste stap bij het implementeren.

Hiermee sla je het eerste deel van de Maesbrug, het geeft duidelijkheid over waaraan de implementatie moet voldoen om te passen bij de bedrijfseigen middelen en manier van werken. Tactisch beleid moet liefst verre blijven van het 'hoe', maar zich beperken tot het 'wat'. Kaders dus, waarbinnen je moet blijven en minimumeisen aan de implementatie et cetera.

En dan implementatie

Implementatie is niet zozeer het 'doen' van dingen, maar met name ook het herhaalbare proces dat leidt tot een passende en effectieve maatregel. Dit proces kent meerdere stappen die allemaal uitgevoerd en ook gedocumenteerd moeten worden. Op die manier kom je navolgbaar in control en is je implementatie ook verifieerbaar voor intern- of extern toezicht. De volgende stappen zijn noodzakelijke aspecten van de implementatie.

1. *Bereik:*
   Waarover gáát de control, wat hoort erbij, wat valt erbuiten? Hoe is het vastgelegd waar deze control over gaat? En wie gaat er over de rest van al wat relevant is voor de control, dus meerdere deeleigenaren voor één control? Denk aan meerdere bedrijfslocaties of screening van medewerkers op afdelingen.
2. *Control-eigenaarschap [2]:*
   Naast *Verwerkingseigenaren* (ook wel 'proces-eigenaar' of 'systeem-eigenaar' genoemd) die de **vraagkant** van informatiebeveiliging vertegenwoordigen hebben we eigenaren aan de **aanbodkant** van informatiebeveiliging nodig: *Control-eigenaren*. Ze zijn te herkennen aan het feit dat ze macht en middelen hebben en zich ook verantwoordelijk achten, *liefst organisatiebreed*. Op die manier is 'control' te organiseren: een beperkte groep eigenaren bepaalt en weet hoe het zit. *Deze eigenaren rapporteren ook periodiek over de staat van de implementatie!*
3. *Kennis vereist:*
   Een goed geïmplementeerde control omvat kennis en vaardigheden van mensen en de toepassing van hulpmiddelen, allemaal op de juiste manier ingezet. Dus de mensen met kennis van zaken moeten in actie komen. Niet de CISO in zijn ivoren toren, maar de inhoudelijk deskundige.
4. *Competentie:*
   Hebben de mensen die de control moeten laten werken en gebruiken, de juiste competenties? Hebben ze voldoende scholing en ervaring? Hoe borgen we dat over de tijd?
5. *Samenwerking:*
   Controls worden maatregelen die in samenhang moeten werken, dus is overleg nodig om het functioneren te bewaken, gebreken op te sporen en verbetering door te voeren. Wie overleggen, hoe vaak, wordt er verslag van opgemaakt en worden actiepunten bijgehouden?

6. *Beleids- en risico-input:*
   Om een control zo te ontwerpen dat het 'passend' (3) kan worden genoemd moet de relatie worden gelegd met tactisch beleid, wetten, regels en organisatie-, verwerkings- en maatregelspecifieke risico's. Bij een verschuivend risicobeeld, in algemene zin of voor een specifieke informatieverwerking is dat dubbel van belang. Merk op dat ik drie niveaus van risico-informatie aanwijs, eigenlijk zijn er nog meer. Het tactisch beleid levert heel duidelijke aangrijpingspunten op voor implementatie en KPI's.
7. *Ontwerp:*
   Een maatregel kan alleen goed werken als hij goed ontworpen is. Dat betekent nadenken over preventie, detectie en repressie.
   • Preventie = de kernmaatregel in de control, deze bestrijdt het risico;
   • Detectie = deze maatregel merkt het falen van de preventie op;
   • Repressie = het handelingsperspectief van de eigenaar om de impact van falende preventie te beperken (bijvoorbeeld het 'stekkermandaat' bij het vermoeden van inbraak).

Voorbeeld van het wijzigingsproces:
De gecommuniceerde plicht om het wijzigingsproces geheel te doorlopen, is je preventieve maatregel. Als je vervolgens geen middel hebt om een ongeautoriseerde wijziging (het falen van de preventie) te detecteren, zal dat onopgemerkt gebeuren. Zonder mandaat om de ongeautoriseerde wijziging te stoppen (of terug te draaien) zul je de gevolgen daarvan niet kunnen beperken (geen repressie).

8. *Realisatie:*
   Het is aan de control-eigenaar om de bedachte werking te realiseren in processen, taken en middelen op alle relevante plekken in de scope, conform het ontwerp van de control. Hiervan maakt hij documentatie beschikbaar voor uitvoerders en toezichthouders.
9. *KPI's:*
   Monitoren en meten is alleen zinvol als er betekenisvolle meetpunten (KPI's) zijn gedefinieerd, zowel SMART als relevant voor de werking en effectiviteit. Deze vloeien voort uit het ontwerp en zijn te vinden in de gerealiseerde maatregelen. Relevante en meetbare KPI's zijn verplichte output in de MMA.
10. *Evalueren en verbeteren:*
    Niemand beter dan de maatregelverantwoordelijke en -uitvoerder kan beoordelen of alle bekende (en vermoede) risico's effectief worden bestreden. Samen met de CISO doet hij/zij een analyse van de control-implementatie alsook de effectiviteit van de maatregel. Daar komen onvermijdelijk verbeterpunten naar voren, die in een verbeterplanning thuishoren.

From the horse's mouth

Op basis van de 10 vragen krijgen we informatie 'from the horse's mouth', dus van de bron, van degene die het inzicht heeft en die verantwoordelijkheid draagt voor implementatie. Beter wordt het niet als het gaat om het inzicht in de maatregelen en of deze 'passend' zijn voor de organisatie en haar risico's.

Restrisico's en verbeteracties:
Met de MMA kan restrisico worden ingeschat: immers een control dekt een risico af, een onvolkomen implementatie laat dreigingen bestaan: dat noem ik het restrisico van de control-implementatie.

Rapporteren & bijsturen:
Elk restrisico moet leiden tot een actie: vermijden / verdragen / behandelen of accepteren: daarin kan de control-eigenaar een keuze maken, maar niet zonder afstemming met de 'hogere' risico-eigenaren. De risico-eigenaren: ten eerste de verwerkings-/procesverantwoordelijken en natuurlijk ook de directie kunnen op basis hiervan keuzes maken (de ACT-fase).

Nog meer voordelen

Toezicht:
Ik - de informatiebeveiliger en beheerder van het ISMS - notuleer, reflecteer en adviseer. En als ik zie dat een vraag niet serieus wordt opgepakt, heb ik natuurlijk de plicht om dat te melden. Implementatie die niet serieus wordt opgepakt, waar niet goed wordt geanalyseerd, waar risico's worden genegeerd vormen een risico voor de organisatie en die *moet* ik melden.

3 lines model:
Merk op dat de adviseur in de tweede lijn, de ISO/ CISO/ adviseur informatiebeveiliging, in dit alles de rol heeft van gespreksleider en adviseur, maar dat de ondersteuners in en van de eerste lijn, zoals IT, HR, Facilities, inkoop en anderen, hun rol pakken: zij zorgen voor de implementatie en rapportage. Zij zijn degenen die de opdracht hebben gekregen van de directie, althans dat is de juiste manier.

Audits:
De derde lijn, de formele toezichthouder (intern/extern auditor, rekenkamer et cetera) krijgt met de MMA-documentatie op een presenteerblaadje gestructureerde informatie over (de kwaliteit van) het implementatieproces, de gemaakte keuzes. Hij/zij kan op basis van deze informatie een uitspraak doen die niet voortkomt uit zijn/haar mening, maar uit voorliggende - gecontroleerde - feiten. Het auditproces wordt op die manier zuiverder voor auditor en auditee.

Maesbrug – Meetbare MaatregelAanpak

Alle elementen van een goede control-implementatie heb ik aldus verwerkt in mijn aanpak. Mijn eigen MMA die ik sinds 2017 bij een brede waaier van organisaties in de zorg, lokale, regionale en nationale overheden heb gebruikt.

De gebruikers van de methode zien de voordelen:

- Inzicht door een gesprek: geen meningen meer uit interviews, maar controleerbare feiten aan de hand van een eenvoudige structuur van 10 aspecten van kwaliteit;
- Maatwerk: implementatie die past bij de organisatie die ook uitgaat van wat er al is, wat goed werkt, ook al is het met `papiertjes en postduiven';
- Betrokkenheid: de 'werkvloer' geeft aan eindelijk te snappen wat de norm van hen vraagt. De opdracht is niet meer vaag, de veiligheidsbrengers komen aan het woord;
- Controleerbaarheid: de Control-documentatie (een word-document waarin elk van de 10 aspecten aan bod komt) biedt het perfecte vertrekpunt voor periodieke evaluatie van de Control, zowel voor de Control-eigenaar, voor de informatiebeveiliger als ook voor de derde lijn: de auditor;
- 3 lines: de verhoudingen tussen de rollen worden duidelijker en de informatiebeveiliger komt toe aan zijn kerntaken van advies en ondersteuning.

Natuurlijk zijn er ook nadelen:

- Arbeidsintensief: met name de eerste kennismaking neemt enkele uren per control in beslag, maar daarna wordt het per doorloop makkelijker want de IST is vastgelegd en de SOLL volgt uit de verbeterpunten;
- Gesprekstechniek: niet meer luisteren naar 'zo doen we dat', maar praten over beheersing, over control op de kwaliteitsaspecten. Dat valt, zeker in het begin, niet mee.

De voordelen wegen ruimschoots op tegen de nadelen, zo blijkt in de praktijk, maar het is wel belangrijk de betrokkenen ook op de nadelen voor te bereiden.

De kloof gedicht

Ben je erin geslaagd met tactisch beleid en methodische implementatie (zoals met de MMA) een brug te slaan naar de leveranciers van veiligheid, dan kun je met recht stellen dat je in control bent. Je hebt het gesprek tussen de ivoren toren en de werkvloer op gang gebracht. Zo kun je samenwerken aan continue verbetering, zoals de normen van je vragen.

PvIB-bijeenkomst

Het plan is om op 7 juni de MMA te presenteren in een PvIB AC-bijeenkomst, waarbij ik ook op het gebruik in de praktijk zal ingaan en mogelijk nog wat meer nieuws over de adoptie met jullie kan delen. De belangrijkste toevoeging die ik ga tonen, is hoe je op basis van de methode volwassenheid kunt claimen, en communiceren, die niet meer steunt op checklijsten of vage organisatiebrede concepten.

Wie hier niet op wil wachten en nu al meer wil weten kan me bereiken op andre@octopus-ib.nl of 06-12 72 72 38. Ik deel alle kennis en middelen voor mijn MMA zonder kosten met als enige voorwaarden dat je er niet aan sleutelt zonder mijn instemming en altijd verwijst naar de bron.

Referenties

(1) https://www.linkedin.com/in/andrebeerten/
(2) Ik gebruik liever het woord 'eigenaar' dan verantwoordelijke, het is persoonlijker
(3) Art 32 AVG: '..passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen'