COMPUTABLE

Deze opinie is van een externe deskundige. De inhoud vertegenwoordigt dus niet het redactionele gedachtegoed van Computable.

Zorg en financiele wereld verschillen niet zo veel

24-03-2014 09:15 | DoorJan van Bon | Lees meer artikelen over: ITIL, Cobit, BiSL, ASL | Er zijn 2 reacties op dit artikel | Dit artikel heeft nog geen cijfer (te weinig beoordelingen) | Permalink

Computable Expert

Jan van Bon
directeur
Expert van Computable voor het topic Management

Meer

Zowel in de zorg als in de financiële wereld volgen de toezichthouders in de ict een rule-based benadering. In feite willen ze dat helemaal niet. Ze hebben liever dat hun doelgroep zich zo goed organiseert dat ze iedere toets op kwaliteit kunnen doorstaan. Een rule-based benadering is dan het paard achter de wagen spannen.

Zorginstellingen hebben steeds meer te maken met eisen op het gebied van de informatiebeveiliging. Dat wordt ingevuld met NEN7510, en voor academische ziekenhuizen met ISO27001. In 2010 verordonneerde de Inspectie voor de Gezondheidszorg (IGZ) dat zorginstellingen moesten voldoen aan een subset van enkele tientallen controls, gebaseerd op de set controls van NEN7510. Intussen is NEN7510 in 2011 geupdate, en zijn de controls aangepast.

Geen harde scores

De IGZ eiste bij de toetsing geen harde scores, maar wel dat de betrokken organisatie kon laten zien dat ze planmatig aan een beter score op die controls werkte. Eigenlijk wilde de IGZ dus dat die instellingen hun kwaliteitszorg op een methodische manier verbeterden, zodat ze een volgende toets, tegen een op dat moment geldende set controls, zouden kunnen doorstaan. De toets lijkt in de praktijk echter nog steeds op controls te worden gebaseerd. In het artikel 'Status NEN7510 in de zorg is grote uitdaging' van Christ Ooms wordt gemeld dat NEN7510 op afzienbare termijn zelfs via een Algemene Maatregel van Bestuur de status van wet krijgt....

Deze benadering lijkt sterk op wat er momenteel in de financiële wereld gebeurt: ook daar is voor informatiebeveiliging een steekproef uitgevaardigd met behulp van een (self-)assessment. De toezichthouder is daar De Nederlandse Bank, en de controls zijn in hoofdzaak afkomstig van Cobit en ISO27001. In essentie geldt daar echter hetzelfde: een control-gebaseerde

aanpak ('rule based') leidt niet tot het gewenste resultaat: organisaties zouden zich liever een kwaliteitsaanpak eigen moeten maken die van binnenuit zorgt voor de gewenste borging van in dit geval informatiebeveiliging.

Zorginstellingen zijn intussen in staat om binnen een jaar (CMM) niveau 3 te halen via een gestandaardiseerde aanpak volgens de ISM-methode. Niet meer rule-based, maar door een systematische aanpak van de besturing te volgen, met een stapsgewijze verbetering. Met die methodische aanpak zijn ze in staat de best practices van onder andere ITIL, ASL , BiSL efficiënt toe te passen.

Stip op de horizon

De essentie is dat de weg naar certificering van informatiebeveiliging niet wordt gelopen door te proberen om vanuit de controls van NEN7510 te denken - of dat er nou dertig zijn of 133, het blijft dan namelijk sterke gelijkenis vertonen met het aanleren van een aantal kunstjes. De truc is dat je het moet omkeren: als je de werkwijze van de organisatie in een geïntegreerd managementsysteem onderbrengt en aanstuurt, dan kun je met zo'n managementsysteem naar elke stip op de horizon koersen die je zelf kiest. Dus ook naar (een op dat moment geldende selectie van) de controls van NEN7510, of voor (internationaal opererende) academische ziekenhuizen: ISO27001.

Het grote voordeel van die aanpak is dat je investeert in een efficiënt en effectief systeem door een methodische aanpak te volgen. Dat voorkomt in hoge mate dat er terugvalgedrag optreedt, omdat het systeem in de samenhang en borging voorziet - mits het management goed managet.

De eerste verzekeraars volgen momenteel hetzelfde pad: ze pakken hun managementsysteem van binnenuit aan, en ze halen binnen een jaar een toets tegen een op dat moment geldende set controls. De weg is dezelfde, de stip op de horizon verschilt hooguit.

Banken, verzekeraars, pensioenfondsen, ziekenhuizen, verzorgingstehuizen, zorgklinieken, ze moeten voor een belangrijk deel de omslag naar systematisch geborgd kwaliteitsmanagement nog maken. Gelukkig moeten ze allemaal hetzelfde bereiken en is een zeer groot deel daarvan te ondersteunen met een gestandaardiseerde methodische aanpak. Dat scheelt tijd, geld, en zorgen. Maar het grootste voordeel zit 'm in de eenvoud die je ermee in huis haalt. Als je 'van binnen' goed in elkaar zit, maakt het niet veel meer uit langs welke lat ze je de maat nemen.