

## General IT-control: management en organisatie

# Informatiebeheer en -beveiliging stevig verankeren in de organisatie

Mischa van der Vliet

In een organisatie waarbij een gestructureerd informatiebeleid ontbreekt, is de stabiliteit van de informatievoorziening niet gegarandeerd. Dat heeft als vervelende consequentie dat er verkeerde en daarmee te dure beslissingen genomen kunnen worden, die een grote impact op de organisatie hebben. Om die reden is de general IT-control management en organisatie een 'sleutel-control'.

OM EEN STABIELE en daarmee effectieve, efficiënte, betrouwbare en continue informatievoorziening in te richten én te behouden, is een informatiestrategie c.q. een informatiebeleid binnen een organisatie noodzakelijk. Dit beleid moet niet op zichzelf staan, maar de organisatiedoelen en -strategie on-

dersteunen en vice versa (alignement). In een organisatie waarbij een gestructureerd informatiebeleid ontbreekt (impliciet en expliciet), is de stabiliteit van de informatievoorziening niet gegarandeerd. Beslissingen die een grote impact hebben op de organisatie kunnen als gevolg daarvan iedere keer anders

worden genomen. Voorbeelden hiervan zijn: maatwerk of standaard leveren, zelf doen of uitbesteden, open source of niet, etc. Om systematisch een informatiebeleid op te stellen, maar ook om dit te controleren, kan onder andere gebruik worden gemaakt van de informatieplanningspiramide (zie afbeelding op pagina 25).

### Informatieplanningspiramide

In het kort de belangrijkste onderdelen van de informatieplanningspiramide. De piramide valt uiteen in vier niveaus. De eerste laag, doelen en strategie, heeft betrekking op de organisatiedoelen en strategie. Het informatiebeleid bestaat uit een algemeen beleid, waarin algemene uitgangspunten worden beschreven met vervolgens een nadere

#### Controlelijst informatiebeleid

##### Beleid t.a.v. applicaties

- prioriteitsstelling
- omvang van de informatiesystemen
- modulariteit
- beheersbaarheid van systeemontwikkeling
- maatwerk of bestaande (standaard) software kopen
- onderhoudbaarheid/aanpasbaarheid
- flexibiliteit van systemen
- gebruikersvriendelijkheid
- continuïteit van applicatie
- autorisatiebeheer
- managementinformatie
- documentatie
- eigenaarschap
- open source
- computervirussen
- e-mail
- internet

##### Beleid t.a.v. gegevens

- gemeenschappelijk gegevensgebruik

- (de)concentratie van gegevensopslag
- aggregatie tot stuurgegevens
- gegevensmodellen
- beveiliging, bescherming, privacy
- kwaliteit van gegevens
- beschikbaarheid van de gegevens

##### Beleid t.a.v. technische infrastructuur

- openheid met omgeving
- investeringen
- (mate van) standaardisatie
- uitbreidbaarheid
- monitoring
- PDA's/smartphones/gsm's
- laptop of desktop
- VPN en webmail

##### Beleid t.a.v. organisatie informatievoorziening

- mate van (de)centralisatie van de informatiefunctie
- relatie tussen lijn en informatie- en automatiseringsstaf
- verantwoordelijkheid over informatiesystemen

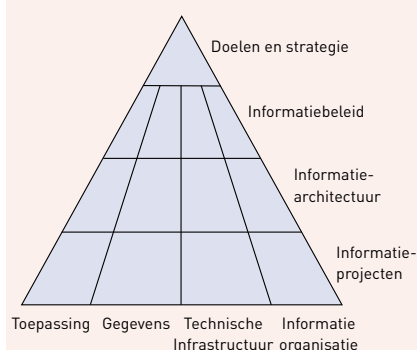
- telewerken/thuiswerken
- beheer van informatiesystemen
- automatiseringspersoneel, inhuur en uitbesteding
- budgetverantwoordelijkheid
- doorbelasting van kosten
- projectmanagement en projectgoedkeuring

##### Beleid t.a.v. informatiebeveiliging

- beveiligingsbeleid
- organisatie van informatiebeveiliging
- beheer van bedrijfsmiddelen
- personele beveiligingseisen
- fysieke beveiliging en beveiliging van de omgeving
- beheer van communicatie en bedieningsprocessen
- toegangsbeveiliging
- verwerving, ontwikkeling en onderhoud van informatiesystemen
- beheer van informatiebeveiligingsincidenten
- bedrijfscontinuïteitsbeheer
- naleving

uitwerking op de gebieden toepassing, gegevens, technische infrastructuur en informatieorganisatie. De architectuurlaag is een beschrijving van de daadwerkelijke inrichting per gebied en als laatste niveau worden op basis van het beleid en de huidige situatie plannen opgesteld om de tekortkomingen op te lossen. De organisatie dient dus een aantal onderwerpen concreet te hebben benoemd (zie kader op pag. 24) in haar informatiebeleid. Uiteraard is de lijst in het kader niet uitputtend, ook moet per organisatie de specifieke situatie worden onderzocht.

#### De informatieplanningspiramide



#### Beveiligingsbeleid van informatie

Naast het informatiebeleid neemt het belang van een informatiebeveiligingsbeleid ook steeds meer toe. Hoe belangrijker de informatie, hoe belangrijker de beveiliging ervan wordt. Een informatiebeveiligingsbeleid richt zich op drie kwaliteitsaspecten, te weten: de integriteit, de beschikbaarheid en de exclusiviteit. Voor dit informatiebeveiligingsbeleid kan bijvoorbeeld ISO27001 of 27002 worden gehanteerd. Op basis van de hoofdstukken van deze ISO-normen kan de audit systematisch worden doorlopen (zie kader).

Een belangrijk onderdeel is een gedegen risicoanalyse die ten grondslag ligt aan het informatiebeveiligingsbeleid. Alleen op die manier kan de auditor vaststellen of de juiste keuzes zijn gemaakt. ISO27002 biedt hiervoor meer ruimte dan 27001. Deze laatste wordt met name bij rekencentra gebruikt en is vrij rigide en dwingend van aard. Ook minder zinvolle maatregelen moeten hierbij worden genomen om aan de vereisen te voldoen. ISO27002 biedt de organisatie daarentegen ruimte om zelf keuzes te maken.

#### Deel I – management en organisatie

Dit is het eerste artikel in een serie over general IT-controls. Controls, die voorwaardenscheppend zijn voor een goede beheersing van de IT-omgeving. In deze bijdrage staat de general IT-control 'management en organisatie' centraal. Als eerste aandacht voor de componenten informatiebeleid en informatiebeveiligingsbeleid van deze IT-control, gevolgd door een controlelijst per component, die als uitgangspunt kan dienen op het moment dat deze control wordt onderzocht.

In een volgende editie van *Accountancy-nieuws* wordt de general IT-control 'wijzigingsbeheer' verder uitgewerkt. Naast een beschrijving van deze control zal een ook hiervoor bruikbare controlelijst worden aangereikt, zodat efficiënt kan worden gecontroleerd. [An](#)

Drs. Mischa van der Vliet RE, IT-auditor bij Auditconnect b.v.

## VAN ACCOUNTANT

## NAAR ADVISEUR



### Gaat u hem daarbij helpen?

Op vrijdag 13 juni verschijnt het themanummer MKB-advies. Adverteerders bellen Gerdien Ruitenbeek (0570) 64 74 52 of mailen [adverterenfiscaal@kluwer.nl](mailto:adverterenfiscaal@kluwer.nl). Reserveren kan tot 6 juni.

**Accountancynieuws**  
SNEL EN COMPLEET GEÏNFORMEERD

2-WEKELIJKS VAKBLAD

ONLINE

EVENTS