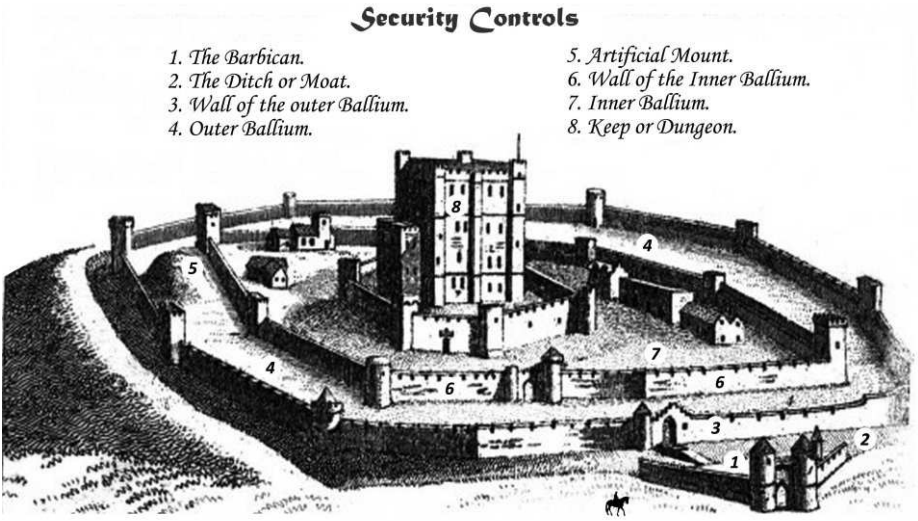
Handboek ISO 27001

Implementeren en auditen van een managementsysteem voor informatiebeveiliging bij het midden- en kleinbedrijf



Uitgeverij Deseo
ISBN 9789402186284
BISAC COM053000
NUR 982
Versie: 20200711
Trefwoord: Informatiebeveiliging

Boekomslag: Rob Westendorp – WSTNDRP grafisch ontwerp & illustratie
Foto auteur: Heleen Rozeveld
Afbeeldingen in het boek: Cees van der Wens
Omslagillustratie: iStock.com/Physicx

Inhoud

Inleiding

Doel van dit boek

Het organiseren van informatiebeveiliging wordt steeds complexer, ook binnen het MKB. Een systematische aanpak van informatiebeveiliging is daarom een noodzaak geworden

Dit handboek is geschreven met als doel MKB-organisaties te helpen bij het inrichten, implementeren, onderhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging volgens de eisen van de norm ISO/IEC 27001. In dit boek vindt u uitleg, voorbeelden en valkuilen met betrekking tot het voldoen aan alle eisen van deze norm.

Tegelijkertijd is dit handboek ook bedoeld om ondersteuning te bieden aan auditoren die moeten onderzoeken of een managementsysteem voor informatiebeveiliging aan alle eisen voldoet en doeltreffend geïmplementeerd is. Dit boek biedt de auditor informatie over alle na te leven eisen, wijst de auditor op veel voorkomende tekortkomingen en bevat specifieke aanwijzingen voor het uitvoeren van ISO/IEC 27001-audits.

De reden dat dit handboek zich richt op het MKB (België: KMO), is vanwege het feit dat een managementsysteem voor informatiebeveiliging daar op een andere wijze moet worden ingericht dan bij een grote organisatie. Een MKB-organisatie moet aan dezelfde eisen voldoen, maar het managementsysteem moet passen bij een bedrijf dat kleiner en wendbaarder is, en dat laatste onder geen beding wil verliezen.

Certificatie

De uitleg in dit handboek houdt voortdurend rekening met de mogelijkheid dat u uw managementsysteem voor informatiebeveiliging uiteindelijk wilt laten certificeren. Speciaal voor dit doel is een apart hoofdstuk opgenomen over de specifieke spelregels en het verloop van een certificatie-audit.

Certificering zou geen doel op zich moeten zijn. Ook een niet-gecertificeerd managementsysteem kan een uitstekend hulpmiddel zijn om informatiebeveiliging op een doeltreffende wijze te organiseren.

Leeswijzer voor dit boek

De nummers en titels van hoofdstuk 4 t/m 10 van dit boek komen overeen met de nummers en titels van hoofdstuk 4 t/m 10 van de norm. Hierdoor kunnen boek en norm gemakkelijk naast elkaar worden gebruikt.

Bij het lezen van de hoofdstukken 4 t/m 10 van dit boek zult u zien dat de norm nauwgezet wordt gevolgd, maar daarvan niet de letterlijke tekst laat zien. De reden hiervoor is dat dit boek geen vervanging is van de norm. Om in detail kennis te nemen van de normteksten zult u een exemplaar van de norm moeten aanschaffen.

De hoofdstukken 4 t/m 10 behandelen elk één of meerdere normelementen. Het in dit boek gebruikte woord *normelement* komt niet uit de norm, het is een door de auteur gehanteerde term om de norm op te delen in logische eenheden. Binnen een normelement staan één of meerdere *eisen* beschreven. Eisen zijn voorwaarden waaraan u moet voldoen om conformiteit met de norm te kunnen claimen.

Om geen extra ruis te introduceren, is in dit boek het woordgebruik bewust zo dicht mogelijk bij dat van de norm gehouden. Waar nodig worden woorden en begrippen uitgelegd. Teksten die beginnen met een ➢-symbool zijn bedoeld als verduidelijking of aanvulling op de hoofdtekst.

De hoofdstukken 4 t/m 10 in dit boek beginnen elk met een schematische weergave van de norm. In het schema zijn de normelementen gemarkeerd die deel uitmaken van het betreffende hoofdstuk. De schema's zijn van de auteur van dit boek, en dus niet afkomstig uit de norm.

Zoals gezegd worden binnen de hoofdstukken 4 t/m 10 van dit boek één of meerdere normelementen besproken. Bij elk normelement komen de volgende vaste onderwerpen aan de orde:

- *Uitleg, voorbeelden en valkuilen*
  Welke eisen staan er in dit normelement? Wat betekenen ze? Wat moet u doen? Wat moet u niet doen?
- *Verplichte documentatie*
  Welke gedocumenteerde informatie eist dit normelement?
- *Aanwijzingen voor het uitvoeren van audits*
  Wat zou een (interne) auditor kunnen onderzoeken met betrekking tot de eisen van dit normelement?

De ‘aanwijzingen voor het uitvoeren van audits’, hebben als doel u te helpen bij het voldoen aan de eisen van normelement 9.2. Bij 9.2 staat dat u met geplande tussenpozen *interne audits* moet (laten) uitvoeren om te bepalen of uw managementsysteem voor informatiebeveiliging doeltreffend is en aan alle eisen voldoet. De aanwijzingen aan het einde van elk normelement bevatten concrete informatie ten behoeve van deze audits.

Dit handboek volgt de norm op de voet, maar waar de norm stopt bij Bijlage-A, gaat dit boek nog een aantal hoofdstukken verder. Deze extra hoofdstukken bevatten praktische tips en aanvullende informatie.

Soms komt u in de tekst van dit boek een blokje met een nummer tegen, bijvoorbeeld: [3]. Het nummer in het blokje verwijst naar een van de bronnen die door de auteur zijn gebruikt en die achter in dit boek bij het hoofdstuk *Bronnen* worden gespecificeerd.

Disclaimer

De uitleg en voorbeelden in dit boek komen voort uit persoonlijke meningen en ervaringen van de auteur en kunnen ter discussie worden gesteld door anderen. De auteur kan niet verantwoordelijk gesteld worden voor eventuele negatieve gevolgen die voortvloeien uit het toepassen van de informatie in dit boek.

1. Over de norm ISO/IEC 27001

HET GEBRUIK VAN DE NORM

De norm ISO/IEC 27001 is een document van ongeveer 30 pagina's dat te koop is via de website van NEN (in België via de website van NBN). De norm is internationaal en is daarom verkrijgbaar in vele talen. De Engelstalige norm bevat de brontekst waarvan alle vertalingen zijn afgeleid.

De norm ISO/IEC 27001 is een uitgave van ISO (International Organization for Standardization) en IEC (International Electrotechnical Commission). ISO/IEC vormt een stelsel dat gespecialiseerd is in wereldwijde normalisatie.

In de praktijk wordt de norm-aanduiding 'ISO/IEC 27001' voor het gemak vaak ingekort tot 'ISO 27001' (zie ook de titel van dit boek). In dit boek is de aanduiding 'ISO/IEC 27001' voor het gemak bijna overal afgekort tot 'de norm'.

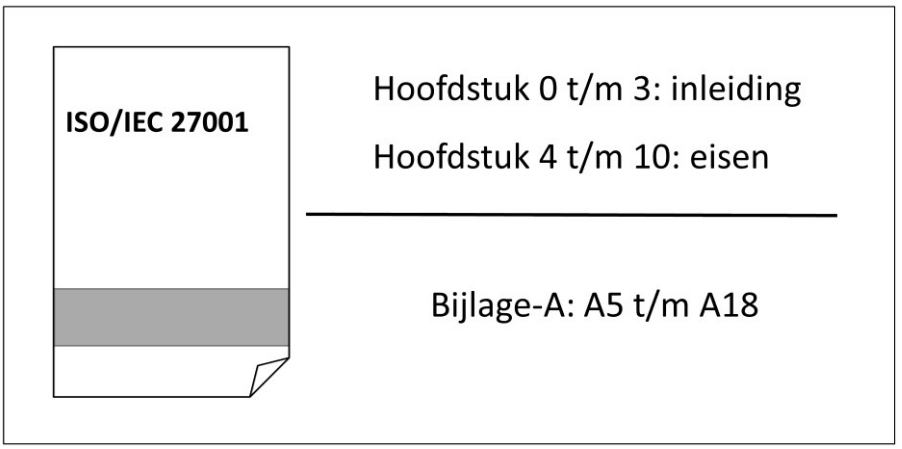
Vooral voor beginners is de norm niet eenvoudig te doorgronden. Hij bevat geen lijstjes met onderwerpen die u kunt afvinken en geeft nauwelijks uitleg over wat u precies moet doen. Het is de bedoeling dat u zelf betekenis geeft aan de norm, een betekenis die past bij uw specifieke activiteiten, verplichtingen, risico's en doelstellingen. Dit boek is bedoeld om u hierbij te helpen.

OPBOUW VAN DE NORM

In de hoofdstukken 0 t/m 3 van de norm vindt u inleidende teksten. Het kan verhelderend zijn om deze teksten te lezen.

In de hoofdstukken 4 t/m 10 van de norm staan de eisen beschreven waaraan u moet voldoen 'om conformiteit met de norm te kunnen claimen', ofwel, om te mogen beweren dat uw managementsysteem voor informatiebeveiliging aan de norm voldoet.

De norm kent ook nog een Bijlage-A. De beheersdoelstellingen en beheersmaatregelen die in deze bijlage staan, zijn rechtsreeks afgeleid van en in overeenstemming met die in document ISO/IEC 27002 [3].



WAT MAG VAN DE NORM? WAT MOET?

In hoofdstuk 1 van de norm kunt u lezen dat uitsluiting van een van de eisen genoemd in de hoofdstukken 4 t/m 10 niet is toegestaan. Kortom, voor elk type organisatie geldt: alle eisen zijn verplicht.

En Bijlage-A van de norm? Moet u alles wat daarin staat ook toepassen en naleven? Dat ligt eraan. In dit boek wordt bij normelement 6.1.3 uitgebreid uitgelegd hoe u moet omgaan met Bijlage-A.

Valkuil 1 'We voldoen aan Bijlage-A, dus aan de norm ISO 27001'

Soms denken organisaties dat ze aan de norm voldoen omdat ze de beheersmaatregelen hebben geïmplementeerd die in Bijlage-A staan. In werkelijkheid voldoet een organisatie pas aan de norm als er ook een managementsysteem voor informatiebeveiliging is geïmplementeerd volgens de eisen in hoofdstuk 4 t/m 10.

WAT BEDOELT DE NORM MET HET WOORD 'ORGANISATIE'?

In hoofdstuk 1 van de norm kunt u lezen dat de eisen in de norm bedoeld zijn voor alle organisaties, ongeacht type, omvang of aard. Wat bedoelt de norm met het woord *organisatie*?

Het begrip *organisatie* omvat, maar is niet beperkt tot: eenmanszaak, bedrijf, vennootschap, firma, onderneming, autoriteit, partnerschap, liefda-

digheidsinstelling of genootschap, of een deel of combinatie daarvan, hetzij als rechtspersoon erkend of niet, publiek of privaat [1].

Merk op dat een *organisatie* geen rechtspersoon (juridische entiteit) hoeft te zijn en dat een managementsysteem voor informatiebeveiliging ook kan worden toegepast bij een eenmanszaak.

WAAROM IS DE TEKST VAN DE NORM ZO VAAG?

In paragraaf 0.1 van de norm kunt u lezen dat de volgorde van de eisen die in de norm worden gepresenteerd, niet de volgorde impliceert waarin deze eisen moeten worden geïmplementeerd, en ook niets zegt over het belang van die eisen. Dat klinkt een beetje als een kookboek waarin staat dat de volgorde van de ingrediënten die in de recepten staan, niets zegt over het belang van die ingrediënten, en ook niets zegt over de volgorde waarin ze tijdens het koken moeten worden gebruikt.

Behalve dat de volgorde van normeisen verwarrend kan overkomen, worden de teksten in de onderwerpen door velen als 'vaag' ervaren. Waarom staat er niet concreet wat u moet doen, zodat u het kunt uitvoeren en van uw lijst kunt schrappen? Waarom moet u het allemaal zelf uitzoeken en bedenken?

De belangrijkste oorzaak van de 'vaagheid' is dat de norm bedoeld is voor alle typen organisaties en de eisen van de norm dus niet al te specifiek kunnen zijn. De norm kan bijvoorbeeld wel eisen dat er een informatiebeveiligingsbeleid moet zijn, maar niet wat er in dat beleid moet staan. Dat hangt namelijk af van wat er aan beleid nodig is binnen uw organisatie. De norm kan ook geen passende beheersmaatregelen voorschrijven, want wat passend is hangt af van uw specifieke informatiebeveiligingsrisico's.

U moet daarom zelf een managementsysteem voor informatiebeveiliging gaan definiëren dat voldoet aan de norm, dat past bij uw activiteiten, verplichtingen, risico's en doelstellingen, en dat geïntegreerd kan worden met uw bedrijfsprocessen en met uw managementstructuur. Dat is nogal wat, en in de praktijk blijkt dit niet altijd eenvoudig. Dit boek is bedoeld om u hierbij te helpen.

Een andere reden waarom de norm soms wat raadselachtig overkomt, is dat ISO/IEC liever geen zaken uitlegt die al in andere ISO/IEC-documenten beschreven staan. Dit boek verwijst soms naar deze documenten (zie ook hoofdstuk *Bronnen* achter in dit boek).

HOOFDSTRUCTUUR (HIGH LEVEL STRUCTURE)

Paragraaf 0.2 van de norm gaat in op de compatibiliteit van de norm met de andere ISO/IEC-managementsysteemnormen. Wat wordt hiermee bedoeld?

De norm ISO/IEC 27001 is niet de enige *managementsysteemnorm*. Andere ISO/IEC-managementsysteemnormen zijn bijvoorbeeld ISO/IEC 9001 (kwaliteit), ISO/IEC 14001 (milieu) en ISO/IEC 22301 (bedrijfscontinuïteit).

De norm ISO/IEC 27001 past de zogenaamde *hoofdstructuur* toe (Engels: High Level Structure), dat wil zeggen dat de norm dezelfde paragraaftitels, identieke tekst, gemeenschappelijke termen en kerndefinities gebruikt als de andere ISO/IEC-managementsysteemnormen. Deze compatibiliteit is nuttig voor organisaties die ervoor kiezen een enkelvoudig managementsysteem uit te voeren dat voldoet aan de eisen van twee of meer managementsysteemnormen.

➢ *Dit boek besteedt geen speciale aandacht aan het combineren van meerdere managementsysteemnormen.*

ISO/IEC 27000

In de hoofdstukken 2 en 3 van de norm wordt u gewezen op het bestaan van document ISO/IEC 27000 (zie ook *Bronnen* [1]). Dit document is te koop via de website van NEN (België: NBN). Hierin staan definities die u kunt gebruiken om meer duidelijkheid te krijgen over de betekenis van bepaalde termen die in de norm worden gebruikt. In dit boek wordt soms verwezen naar dit document.

BIBLIOGRAFIE

Achter in de norm staat onder de titel *Bibliografie* een lijst met documenten opgenomen. Deze documenten bieden aanvullende informatie op de norm ISO/IEC 27001.

Het in de Bibliografie van de norm genoemde document ISO/IEC 27003 bevat, net als dit boek, richtlijnen voor het implementeren van de norm, alleen is de informatie in dit document zeer beperkt. In dit boek wordt regelmatig verwezen naar dit document (zie ook *Bronnen* [4] in dit boek).

2. Informatiebeveiliging

Het begrip *informatiebeveiliging* kan worden opgesplitst in de volgende drie dimensies [1]:

- Het behoud van de *vertrouwelijkheid* van informatie
- Het behoud van de *integriteit* van informatie
- Het behoud van de *beschikbaarheid* van informatie

➢ *De norm spreekt over 'het behoud van', terwijl in de praktijk vaker wordt gesproken over 'het beschermen van' de vertrouwelijkheid, integriteit en beschikbaarheid van informatie.*

BEHOUD VAN DE VERTROUWELIJKHEID VAN INFORMATIE

Als het om informatiebeveiliging gaat, wordt het begrip *vertrouwelijkheid* meestal als eerste genoemd. Bij het behoud van vertrouwelijkheid gaat het erom dat informatie niet beschikbaar of bekend wordt gemaakt aan onbevoegde personen, entiteiten of processen [1]. In plaats van het woord *vertrouwelijkheid* wordt ook wel het woord *exclusiviteit* gebruikt.

Bij vertrouwelijke informatie kan het om persoonsgegevens gaan, maar ook om andere soorten informatie zoals bedrijfsgeheimen of concurrentiegevoelige gegevens. Verlies van vertrouwelijkheid van informatie kan op veel manieren plaatsvinden. Organisaties kunnen vertrouwelijke gegevens van hun klanten zonder toestemming delen met anderen. Een e-mail met vertrouwelijke informatie kan per ongeluk naar de verkeerde persoon worden gestuurd. Personen met kwade bedoelingen kunnen vertrouwelijke gegevens stelen of kopiëren en daar hun voordeel mee doen. Loslippige personen kunnen bewust of per ongeluk vertrouwelijke informatie delen. Een verloren, gestolen of onzorgvuldig afgedankte computer kan een schat aan vertrouwelijke gegevens bevatten.

Valkuil 2 'Informatiebeveiliging gaat over vertrouwelijkheid'

Vaak wordt gedacht dat informatiebeveiliging alleen over het beschermen van de *vertrouwelijkheid* van informatie gaat. Binnen de context van de norm gaat informatiebeveiliging echter ook over de *integriteit* en de *beschikbaarheid* van informatie.

BEHOUD VAN DE INTEGRITEIT VAN INFORMATIE

Met de *integriteit* van informatie wordt de nauwkeurigheid en volledigheid van informatie bedoeld [1]. Het woord *integriteit* leidt nog wel eens tot verwarring omdat het ook buiten de context van informatiebeveiliging bestaat, namelijk in de vorm van een persoonlijke eigenschap (eerlijk, oprecht, niet omkoopbaar). Je zou kunnen zeggen dat integere informatie een eerlijk beeld geeft: nauwkeurig (juist) en volledig (compleet).

Verlies van integriteit van informatie kan bijvoorbeeld optreden door een onjuiste invoer, verwerking of presentatie van gegevens (handmatig of geautomatiseerd). Personen met kwade bedoelingen kunnen de juistheid en compleetheid van informatie opzettelijk aantasten om er beter van te worden of om schade te berokkenen. Iemand kan een verkeerde back-up terugplaatsen, waardoor informatie niet meer klopt of compleet is. Bedenk dat zelfs grote banken af en toe kampen met het probleem van onjuiste saldo's.

BEHOUD VAN DE BESCHIKBAARHEID VAN INFORMATIE

Als het om informatiebeveiliging gaat, wordt het aspect *beschikbaarheid* vaak als laatste genoemd. Niet omdat het beschikbaar zijn van informatie als onbelangrijk wordt beschouwd, maar omdat het niet altijd meteen gekoppeld wordt aan het beveiligen van informatie. Bij het behoud van beschikbaarheid gaat het erom dat informatie toegankelijk en bruikbaar is op verzoek van een bevoegde entiteit [1] (ofwel: de organisatie of persoon die over de informatie wil en mag beschikken).

Verlies van beschikbaarheid van informatie kan tijdelijk of permanent zijn. Een verlies kan veroorzaakt worden door onbedoelde oorzaken zoals foutieve handelingen, technische storingen of natuurrampen. Personen met kwade bedoelingen kunnen informatie vernietigen, ontoegankelijk maken of onleesbaar maken. Informatiesystemen kunnen overbelast raken. Iemand kan een DDoS-aanval opzetten om informatiesystemen opzettelijk te verstoren. Informatiedragers zoals papier, tapes, harde schrijven en usb-sticks kunnen door veroudering hun informatie verliezen. Soms is informatie niet meer beschikbaar omdat een overleden persoon als enige bepaalde wachtwoorden kende.

BIV / BIV-CLASSIFICATIE

Om de drie dimensies van informatiebeveiliging af te korten, wordt in de praktijk vaak de afkorting BIV gebruikt. De volgorde van de letters is daarbij willekeurig gekozen (in het Engels wordt de afkorting CIA gebruikt: Confidentiality, Integrity, Availability).

Informatiesystemen, bedrijfsprocessen en gegevens worden soms geclassificeerd volgens een zogenaamde BIV-classificatie. Het hoogst geclassificeerd systeem kent dan bijvoorbeeld een BIV-klasse van 333, het laagst geclassificeerd systeem de BIV-klasse 111. Op basis van deze classificatie worden dan passende beheersmaatregelen getroffen.

De norm schrijft het gebruikt van een BIV-classificatie niet voor, maar beschrijft in Bijlage-A wel iets wat erop lijkt. Volgens beheersmaatregel A.8.2.1 moet informatie worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking en wijziging. Zie hoofdstuk 'Bijlage-A' in dit boek voor meer informatie over het classificeren van informatie.

OVERIGE ASPECTEN

Informatiebeveiliging kan ook andere eigenschappen betreffen, zoals [1]:

- *Onweerlegbaarheid*. Hiermee wordt het vermogen bedoeld om te bewijzen dat een geclaimde gebeurtenis of actie zich daadwerkelijk heeft voorgedaan. Denk bijvoorbeeld aan het laten plaatsen van een handtekening voor ontvangst bij het afleveren van een postpakket.
- *Authenticiteit*: Hierbij gaat het om de eigenschap dat een entiteit is wat zij claimt te zijn. Denk bijvoorbeeld aan het gebruik van een digitaal certificaat dat zorgt dat de iemand weet dat berichten van een bepaalde verzender afkomstig zijn (bronauthenticiteit).
- *Betrouwbaarheid*. Hiermee wordt de eigenschap bedoeld van consistent beoogd gedrag en consistente resultaten. Denk bijvoorbeeld aan informatie die de ene keer snel, en de andere keer traag op een beeldscherm verschijnt, of waarbij de getoonde informatie per keer kan verschillen, terwijl dat in beide gevallen niet de bedoeling is.

INFORMATIEBEVEILIGING EN DE AVG

Het begrip *informatiebeveiliging* kan betrekking hebben op alle soorten informatie, dus ook op persoonsgegevens. Zodra het over de bescherming van persoonsgegevens gaat, is in Europees verband de GDPR en in Nederland de daarvan afgeleide Algemene Verordening Gegevensbescherming (AVG) van belang. Artikel 32 van de AVG gaat over *Beveiliging van de verwerking*. In dit artikel spreekt de verordening over [10]:

> *het treffen van passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten: (…) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen.*

Zoals u bij het lezen van dit boek zult zien, komt 'het treffen van maatregelen die afgestemd zijn op risico's' en 'het op gezette tijden evalueren van de doeltreffendheid van die maatregelen' exact overeen met de aanpak van de norm ISO/IEC 27001.

➢ *De AVG gaat over veel meer onderwerpen dan Persoonsgegevensbeveiliging. De norm ISO/IEC 27001 dekt dus niet alle AVG-eisen af.*

Artikel 33 van de AVG gaat over een 'melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit'. In Nederland spreken we in dit verband vaak over een *datalek*. In de praktijk wordt vaak gedacht dat een datalek alleen betrekking heeft op het aspect *vertrouwelijkheid*, maar volgens de Autoriteit Persoonsgegevens zijn er drie categorieën datalekken te onderscheiden [11]:

- inbreuk op de vertrouwelijkheid van persoonsgegevens;
- inbreuk op de integriteit van persoonsgegevens;
- inbreuk op de beschikbaarheid van persoonsgegevens.

Zoals u ziet sluiten de definities van de drie verschillende soorten datalekken volledig aan bij de drie eerder besproken dimensies van informatiebeveiliging.

Dit boek gaat niet over de AVG, maar zal daar nu en dan wel naar verwijzen.

3. Managementsysteem

ALGEMEEN

De norm begint met hoofdstuk nul. In paragraaf 0.1 kunt u lezen dat de norm eisen bevat voor een managementsysteem voor informatiebeveiliging. Zoals u in dit boek stap-voor-stap zult zien, is dit een systeem dat een organisatie kan helpen bij het implementeren, uitvoeren, controleren, beoordelen, onderhouden en verbeteren van informatiebeveiliging.

Om een beetje warm te lopen voor het door u in te richten managementsysteem voor informatiebeveiliging, besteedt dit hoofdstuk aandacht aan het doel en de achterliggende gedachte van dit systeem. Specifieke uitleg vindt u vanaf hoofdstuk 4 in dit boek.

ISMS

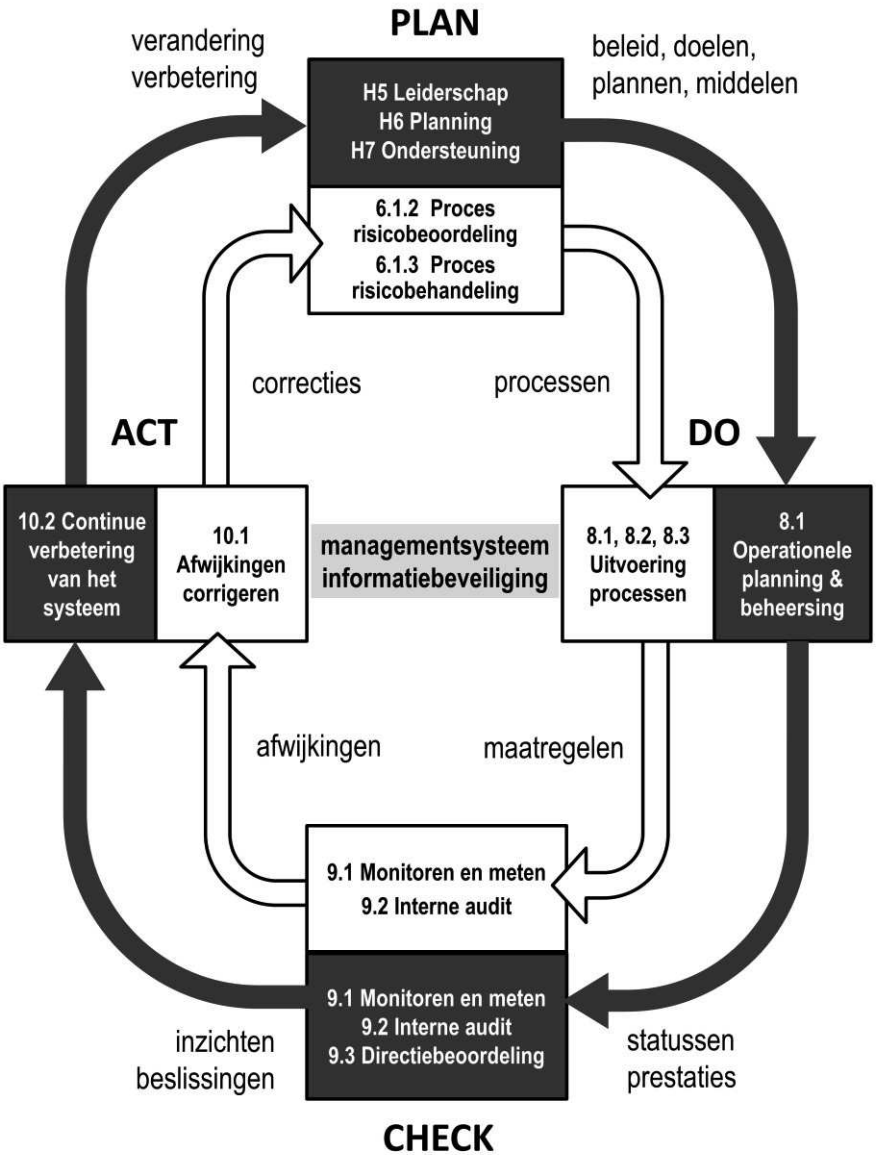
Voor het aanduiden van een managementsysteem voor informatiebeveiliging wordt ook wel de afkorting *ISMS* gebruikt (van het Engelse 'Information Security Management System'). Om verwarring te voorkomen, en om aan te blijven sluiten bij het taalgebruik van de norm, wordt de aanduiding ISMS in dit boek niet gebruikt.

PDCA

Hoewel de norm zelf geen verwijzing maakt naar de kwaliteitscirkel van Deming (een wereldwijd bekend en veel toegepast model voor kwaliteitsverbetering), zijn de onderdelen van het managementsysteem duidelijk te linken aan de Plan-Do-Check-Act-fasen van dit model.

In de afbeelding op de volgende pagina is de norm vertaald naar de cirkel van Deming. De nummers en titels in het getoonde model verwijzen naar de hoofdstukken en paragrafen van de norm, en naar de gelijknamige hoofdstukken en paragrafen van dit boek.

In het model staan twee PDCA-cirkels: een binnen-cirkel (de witte) en een buiten-cirkel (de zwarte).


PLAN
verandering
verbetering
beleid, doelen,
plannen, middelen
H5 Leiderschap
H6 Planning
H7 Ondersteuning
6.1.2 Proces
risicobeoordeling
6.1.3 Proces
risicobehandeling
correcties
processen
ACT
DO
10.2 Continue
verbetering
van het
systeem
10.1
Afwijkingen
corrigeren
managementsysteem
informatiebeveiliging
8.1, 8.2, 8.3
Uitvoering
processen
8.1
Operationele
planning &
beheersing
afwijkingen
maatregelen
9.1 Monitoren en meten
9.2 Interne audit
9.1 Monitoren en meten
9.2 Interne audit
9.3 Directiebeoordeling
inzichten
beslissingen
statussen
prestaties
CHECK

➢ *Het model van het managementsysteem met de twee cirkels is van de auteur van dit boek, en is dus niet afkomstig uit de norm.*

De binnenste PDCA-cirkel van het getoonde model heeft betrekking op het managen van informatiebeveiligingsrisico's. Deze cirkel is bij de meeste organisaties in zekere mate al aanwezig: er zijn ideeën over het omgaan met informatiebeveiligingsrisico's (plan), er worden maatregelen getroffen om die risico's te beheersen (do), er wordt gecontroleerd of de maatregelen het gewenste resultaat opleveren (check) en er wordt actie ondernomen als dit niet het geval is (act).

Helaas blijkt de binnenste cirkel niet altijd even goed te functioneren. Door een gebrek aan discipline, systematiek en ondersteuning kunnen er onzichtbare gevaren in de organisatie sluipen die plotseling toeslaan en grote schade aanrichten. Hiervan zien we dagelijks de gevolgen in de vorm van een verlies van vertrouwelijkheid, integriteit en beschikbaarheid van informatie bij talloze organisaties.

Daarom maakt de norm gebruik van een tweede PDCA-cirkel. Deze buitenste cirkel biedt ondersteuning aan de binnenste cirkel in de vorm van leiderschap en ondersteuning (plan), planning en beheersing (do), een systematische evaluatie van prestaties (check) en een continue verbetering van het systeem als geheel (act).

De omloopsnelheden van de twee PDCA-cirkels kunnen verschillen, maar de buitenste cirkel zoekt regelmatig contact met de binnenste cirkel, voedt hem en bewaakt hem nauwlettend (zoals u in dit boek kunt lezen).

Zodoende biedt invoering van een managementsysteem voor informatiebeveiliging op twee fronten verbetering: de introductie van een formeel proces voor het managen van informatiebeveiligingsrisico's (de binnenste cirkel) en het gebruik van een ondersteunend proces daar omheen (de buitenste cirkel). Het geheel vormt een zeer krachtig systeem dat overal ter wereld wordt toegepast en nog steeds in populariteit groeit.

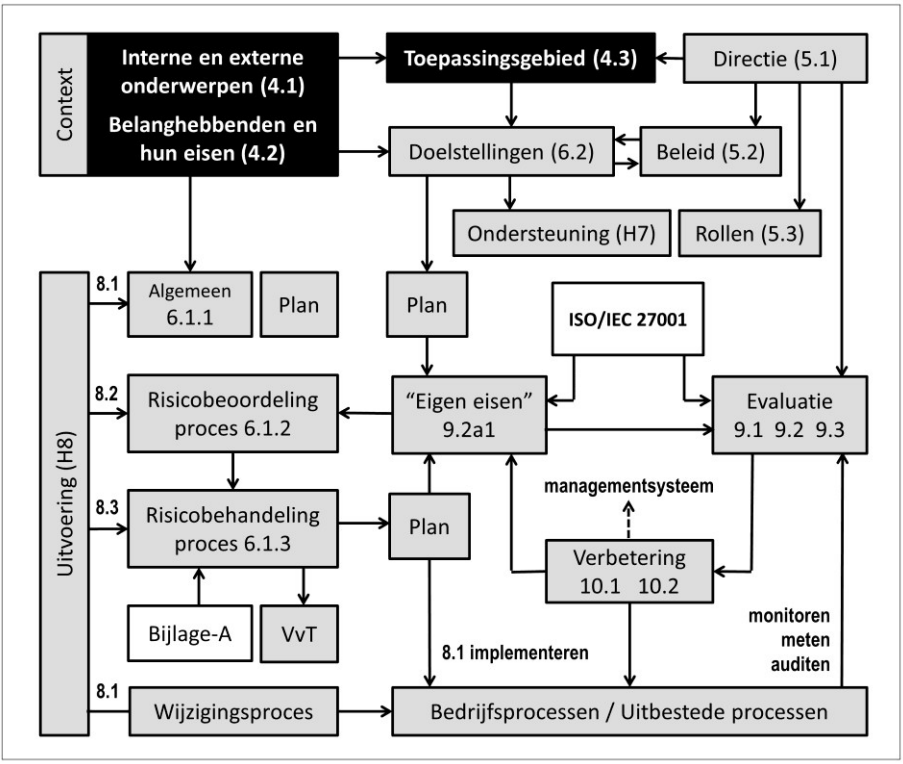
Ten aanzien van het gebruik van de binnenste cirkel is het mogelijk dat u de touwtjes wat strakker moet aantrekken dan u op dit moment doet: alle processen moeten worden gedocumenteerd en volgens een planning worden uitgevoerd. De buitenste cirkel is bij veel organisaties nog onvoldoende aanwezig, of onvoldoende aantoonbaar.

- *Voor wie de kwaliteitscirkel van Deming een handige methode vindt, is in dit boek aan het begin van de hoofdstukken 5 t/m 10 met een PDCA-afbeelding aangegeven bij welke fase van de cirkel het hoofdstuk hoort.*

4. Context

In hoofdstuk 4 van de norm draait het om de volgende vragen:

1) Welke interne en externe factoren zijn relevant voor uw managementsysteem voor informatiebeveiliging?
2) Welke behoeften en verwachtingen van belanghebbenden zijn relevant voor uw managementsysteem voor informatiebeveiliging?
3) Wat is een geschikt toepassingsgebied voor uw managementsysteem voor informatiebeveiliging?
4) Hoe gaat u een managementsysteem voor informatiebeveiliging inrichten, implementeren, onderhouden en continu verbeteren in overeenstemming met de eisen van de norm?



4.1 De organisatie en haar context

INLEIDING

Normelement 4.1 eist dat u alle externe en interne onderwerpen vaststelt:

- die relevant zijn voor uw *doelstelling*;
- die het vermogen van uw organisatie kunnen beïnvloeden om de *beoogde resultaten* van uw managementsysteem voor informatiebeveiliging te behalen.

➢ *De norm spreekt bij 4.1 over 'onderwerpen', de Engelstalige norm, die de brontekst bevat, spreekt over 'issues' (vraagstukken). Omdat het woord 'onderwerpen' vrij neutraal is en het in werkelijkheid om bepalende factoren gaat, wordt in de praktijk vaak over 'factoren' gesproken. Voor een beter begrip spreekt dit boek daarom vanaf hier steeds over 'externe en interne factoren'.*

De door u vast te stellen externe en interne factoren moet u in een later stadium gebruiken tijdens het implementeren van uw managementsysteem voor informatiebeveiliging. U wordt verwacht dit te doen bij:

- het vaststellen van het toepassingsgebied van uw managementsysteem (zie uitleg bij normelement 4.3);
- het vaststellen en behandelen van risico's die voorkomen dat het managementsystemen voor informatiebeveiliging zijn beoogde resultaten behaalt (zie uitleg bij normelement 6.1.1);
- het vaststellen van informatiebeveiligingsdoelstellingen [4] (zie uitleg bij normelement 6.2).

EXTERNE EN INTERNE FACTOREN: BEDRIJFSDOELSTELLING

Het woord *doelstelling* dat bij normelement 4.1 genoemd wordt, gaat over uw bedrijfsdoelstelling met betrekking tot informatiebeveiliging. Bijvoorbeeld: 'het leveren van veilige en betrouwbare diensten en het vertrouwen bieden aan klanten dat risico's adequaat worden beheerst'.

De vraag waar het bij dit normelement om gaat is: welke positieve en negatieve factoren zijn relevant voor het behalen van uw doelstelling?

Voorbeeld

Een organisatie heeft als doelstelling 'veilige en betrouwbare IT-diensten leveren en vertrouwen bieden aan klanten dat risico's adequaat worden beheerst'. Tijdens een brainstorm komen de volgende interne factoren naar voren die relevant zijn voor deze doelstelling:

Sterktes (intern)
Gunstige financiële positie
Gemotiveerd personeel
Nooit ernstige incidenten gehad.
Veel IT-kennis
Goede tools

Zwaktes (intern)
Weinig formele processen en regels
Weinig interne controles
Weinig inzicht in risico's
Laag bewustzijn bij sommige medewerkers.

Om een beter beeld te krijgen van de context, betrekt de organisatie de door haar vastgestelde factoren in een bredere analyse. Hiervoor wordt een zogenaamde *SWOT-analyse* gebruikt (Strength, Weakness, Opportunity, Threat).

	FACTOREN VOOR HET BEHALEN VAN HET BEDRIJFSDOEL	
	POSITIEF	**NEGATIEF**
INTERN	**Sterktes** • Gunstige financiële positie • Gemotiveerd personeel • Nooit ernstige incidenten gehad • Veel IT-kennis • Goede tools	**Zwaktes** • Weinig inzicht in risico's • Weinig formele processen en regels • Weinig interne controles op doeltreffendheid van maatregelen • Laag bewustzijn t.a.v. informatiebeveiliging bij sommige medewerkers.
EXTERN	**Kansen** • Een ISO/IEC 27001-certificaat is een kans om klanten nog meer vertrouwen te bieden.	**Bedreigingen** • Probleem bij leverancier X • Krapte op de arbeidsmarkt • Veranderende wetgeving • Steeds nieuwe vormen cybercrime

➢ *Let op: de norm verplicht u niet om een SWOT-analyse uit te voeren. In principe hoeft u bij normelement 4.1 alleen maar interne en externe factoren vast te stellen.*

INTERNE EN EXTERNE FACTOREN: BEOOGDE RESULTATEN

Zodra het strategische besluit is genomen om binnen een bepaalde tijd een managementsysteem voor informatiebeveiliging te gaan invoeren, komt de volgende vraag naar voren: welke positieve en negatieve factoren beïnvloeden het vermogen van uw organisatie om de beoogde resultaten van uw managementsysteem te behalen'?

Voorbeeld

Dezelfde organisatie als in het vorige voorbeeld organiseert ook een brainstorm over de interne factoren die 'de beoogde resultaten van het managementsysteem' beïnvloeden. De uitkomsten worden in een SWOT-analyse geplaatst.

INTERNE FACTOREN VOOR HET MANAGEMENTSYSTEEM	
POSITIEF	**NEGATIEF**
Sterktes • Betrokkenheid directie • Kleine organisatie, snelle beslissingen • Gemotiveerd personeel • Veel IT-kennis • Goede tools	**Zwaktes** • Beperkte mankracht • Weinig kennis van ISO/IEC 27001 • Weinig kennis van de wet • Laag bewustzijn t.a.v. informatiebeveiliging bij sommige medewerkers. • Documentatie is rommelig
Kansen • Vermindering aantal incidenten • Verbetering bestaande processen • Betere samenwerking met klanten en leveranciers • Beter voldoen aan wettelijke en contractuele eisen	**Bedreigingen** • Project X gaat dit jaar veel mankracht eisen wat ten koste kan gaan van het managementsysteem • Dit jaar gaan drie ervaren medewerkers met pensioen

Het is logisch dat er bij het bepalen van interne en externe factoren soms een overlap is tussen de bedrijfsdoelstelling en de beoogde resultaten van het managementsysteem. De resultaten van het managementsysteem dragen immers bij aan het behalen van uw bedrijfsdoelstelling.

INTERNE FACTOREN VASTSTELLEN

Denk bij het vaststellen van interne factoren bijvoorbeeld aan:

- de omvang van uw organisatie;
- uw bedrijfscultuur;
- de volwassenheid van leiderschap, beleid, processen en procedures;
- uw verplichtingen, doelstellingen en plannen voor de toekomst;
- uw beschikbare middelen zoals kapitaal, mankracht en tijd.

Bij grotere organisaties kunnen andere interne factoren spelen dan bij kleinere.

Voorbeeld

Een organisatie met 150 medewerkers en 3 vestigingen ziet de volgende interne factoren die relevant zijn voor haar doelstelling en die haar vermogen kunnen beïnvloeden om de beoogde resultaten van haar managementsysteem te behalen:

- De directie is tot op heden weinig betrokken bij het onderwerp informatiebeveiliging.
- Besluitvorming kan erg traag zijn.
- Activiteiten en cultuur op de vestigingen zijn zeer verschillend.
- 12 medewerkers beheersen niet de Nederlandse taal.

EXTERNE FACTOREN VASTSTELLEN

Denk bij het vaststellen van externe factoren bijvoorbeeld aan;

- de invloed van de economische situatie en het politieke klimaat;
- wet- en regelgeving op het gebied van informatiebeveiliging;
- technologische ontwikkelingen die buiten uw organisatie spelen;
- ontwikkelingen bij uw leveranciers.

Kenmerkend voor externe factoren is dat u er meestal geen of weinig invloed op kan uitoefenen.

Valkuil 3 Factoren bepaald voor het beoogde toepassingsgebied

Kijk bij het vaststellen van interne en externe factoren nog niet naar het beoogde *toepassingsgebied* van uw managementsysteem (zie uitleg bij normelement 4.3). Het is juist de bedoeling dat u dit *toepassingsgebied* mede op basis van uw interne en externe factoren gaat bepalen.

🕮 VERPLICHTE DOCUMENTATIE

In de eisen van normelement 4.1 wordt nergens gesteld dat er iets gedefinieerd of gedocumenteerd moet worden (woorden die u bij veel andere normelementen wel tegenkomt). Om te kunnen aantonen dat aan de eisen van de norm wordt voldaan, kunt u een gedocumenteerd overzicht maken van uw externe en interne factoren.

☑ AANWIJZINGEN VOOR HET UITVOEREN VAN AUDITS

Met betrekking tot het hiervoor besproken normelement 4.1 zou een auditor kunnen onderzoeken:

- of de organisatie een 'doelstelling' heeft geformuleerd met betrekking tot informatiebeveiliging (dit is geen eis, maar volgens normelement 4.1 wel een noodzakelijke voorwaarde);
- of de organisatie interne en externe factoren heeft vastgesteld die relevant zijn voor haar doelstelling met betrekking tot informatiebeveiliging;
- of de organisatie 'beoogde resultaten' heeft geformuleerd met betrekking tot het managementsysteem voor informatiebeveiliging (dit is geen eis, maar volgens normelement 4.1 wel een noodzakelijke voorwaarde);
- of de organisatie interne en externe factoren heeft vastgesteld die haar vermogen kunnen beïnvloeden om de beoogde resultaten van haar managementsysteem voor informatiebeveiliging te behalen;
- of de organisatie regelmatig onderzoekt of de vastgestelde informatie over interne en externe factoren compleet en actueel is.

4.2 Belanghebbenden

INLEIDING

Normelement 4.2 eist dat u vaststelt welke *belanghebbenden* relevant zijn voor uw managementsysteem voor informatiebeveiliging en welke eisen van deze belanghebbenden relevant zijn voor informatiebeveiliging.

De vastgestelde informatie moet u in een later stadium gebruiken tijdens het implementeren van uw managementsysteem voor informatiebeveiliging. Net als bij de interne en externe factoren (zie normelement 4.1) wordt u verwacht dit te doen bij:

- het vaststellen van het toepassingsgebied van uw managementsysteem (zie uitleg bij normelement 4.3);
- het vaststellen en behandelen van algemene risico's om te zorgen dat het managementsystemen voor informatiebeveiliging zijn beoogde resultaten behaalt (zie uitleg bij normelement 6.1.1);
- het vaststellen van informatiebeveiligingsdoelstellingen [4] (zie uitleg bij normelement 6.2).

BELANGHEBBENDEN: SOORTEN BELANGHEBBENDEN

Wat bedoelt de norm met belanghebbenden? Een belanghebbende is [1]:

- een persoon of organisatie die invloed kan hebben op een beslissing of activiteit van uw organisatie;
- een persoon of organisatie die beïnvloed kan worden door een beslissing of activiteit van uw organisatie;
- een persoon of organisatie die ervaart dat hij wordt beïnvloed (positief of negatief) door een beslissing of activiteit van uw organisatie.

➢ *De Nederlandse norm gebruikt het woord 'belanghebbenden'. De Engelstalige norm (die de brontekst bevat) spreekt over 'interested parties'. In de praktijk wordt in Nederland in plaats van het woord 'belanghebbende' ook wel het woord 'stakeholder' gebruikt. Het onderzoek dat in het kader van normelement 4.2 moet worden uitgevoerd met betrekking tot belanghebbenden en hun eisen, wordt om die reden ook wel een 'stakeholder-analyse' genoemd. Om verwarring*

te voorkomen, en om aan te blijven sluiten bij het taalgebruik van de norm, wordt de aanduiding 'stakeholder' in dit boek niet gebruikt.

De volgende soorten belanghebbenden kunnen onderscheiden worden:

- *Intern*: personen of partijen binnen uw organisatie.
- *Extern*: externe personen of organisaties, zoals klanten, partners, leveranciers en crediteuren.
- *Interface*: partijen die niet betrokken zijn bij de organisatie, maar die een specifiek (legitiem) belang hebben en invloed uitoefenen. Denk aan de overheid, toezichthouders, Kamer van Koophandel, brancheorganisaties, de maatschappij, etc.

Hieronder zijn enkele voorbeelden van belanghebbenden opgenomen die mogelijk invloed hebben op, of invloed ondervinden vanuit uw organisatie.

BELANGHEBBENDEN (INTERN): DIRECTIE

De directie van een organisatie is de eerste relevante belanghebbende voor het managementsysteem voor informatiebeveiliging. De directie heeft er alle belang bij dat de bedrijfsdoelstelling niet in gevaar komt en dat het managementsysteem zijn beoogde resultaten behaalt. Als het aan de norm ligt, dan speelt de directie een zeer belangrijke rol bij informatiebeveiliging (zie uitleg bij de normelementen 5.1, 5.2, 5.3 en 9.3).

BELANGHEBBENDEN (INTERN): PERSONEEL

Ook het personeel is een relevante belanghebbende voor het managementsysteem voor informatiebeveiliging. Personeel dat werkzaamheden verricht onder het gezag van uw organisatie heeft behoefte aan sturing, opleiding en middelen om taken goed uit te voeren. Daarnaast verwacht personeel van de organisatie dat hun eigen persoonsgegevens veilig worden opgeslagen en niet zomaar met iedereen worden gedeeld.

BELANGHEBBENDEN (EXTERN): KLANTEN

Wat verwachten uw klanten op het gebied van informatiebeveiliging? Dat hangt ervan af wat u doet. Ontwikkelt u software? Dan verwachten uw

klanten dat die software goed beveiligd is. Levert u hosting-diensten? Dan eisen uw klanten waarschijnlijk dat uw diensten een bepaalde beschikbaarheidsgraad hebben. Levert u datacenter-diensten? Dan belooft u uw klanten een veilige en stabiele omgeving voor hun IT-apparatuur. Heeft u een drukkerij? Dan mag het drukwerk van uw klanten vast niet door iedereen worden bekeken. Werkt u inhoudelijk met informatie en gebruikt u daarbij persoonsgegevens? Dan moeten die persoonsgegevens overeenkomstig de wet worden beschermd.

Meestal hebben uw klanten goede redenen om eisen op het gebied van informatiebeveiliging te stellen, namelijk dat hun reputatie of zelfs hun voortbestaan op het spel kan komen te staan op het moment dat u onverstandige dingen doet. Een andere mogelijkheid is dat een klant bepaalde contractuele verplichtingen heeft naar zijn eigen opdrachtgevers, en dat hij een deel daarvan moet doorzetten naar u. En als het om het verwerken van persoonsgegevens gaat, is er ook nog de wet.

- *Als het om het verwerken van persoonsgegevens gaat, dan zegt de Algemene Verordening Gegevensbescherming (AVG) bij artikel 28 lid 3 [10]: 'De verwerking door een verwerker wordt geregeld in een overeenkomst of andere rechtshandeling krachtens het Unierecht of het lidstatelijke recht, die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt (…)'.*

Hoe groter de belangen, des te meer uw klanten zullen aandringen op het maken van goede afspraken over informatiebeveiliging. Uiteindelijk zullen afspraken ten aanzien van informatiebeveiliging, direct of indirect, herleidbaar zijn naar het behoud van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie (zie uitleg bij hoofdstuk 1). Steeds vaker eisen organisaties een ISO/IEC 27001-certificaat van hun leveranciers.

BELANGHEBBENDEN (EXTERN): CONSUMENTEN

Mogelijk hebben de activiteiten en beslissingen van uw organisatie rechtstreeks invloed op consumenten die gebruik maken van uw producten of diensten. Consumenten hebben rechten. Zo bent u waarschijnlijk al bekend met het bestaan van wettelijke eisen ten aanzien van de bescherming van persoonsgegevens (een bijzondere vorm van informatie).