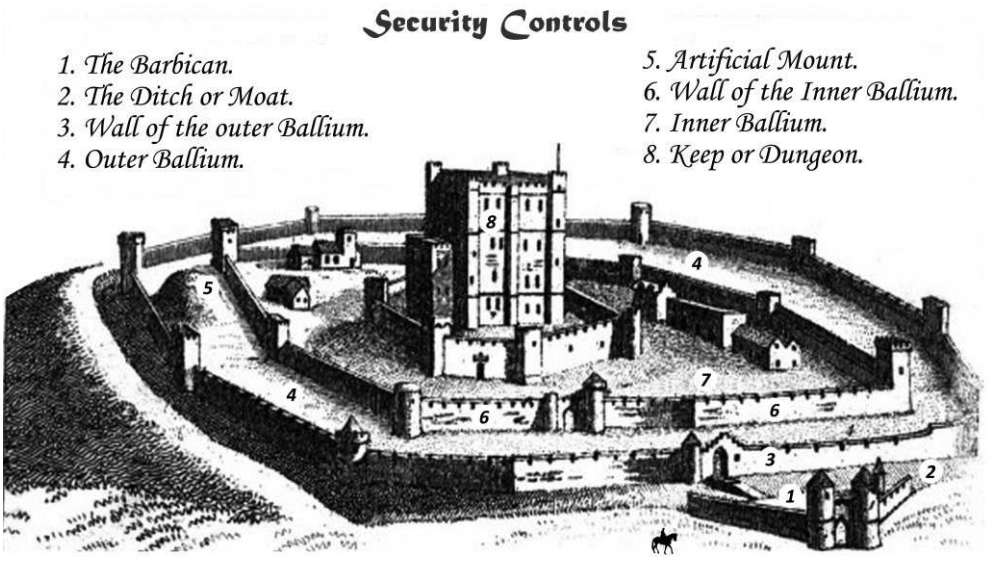
Handboek
ISO 27001 Controls

Het implementeren en auditen van 93 controls
om informatiebeveiligingsrisico's te verlagen



Uitgeverij: Deseo
ISBN 9789464652192
BISAC COM053000
NUR 982
Versie: 20231201
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

Handboek ISO 27001 Controls is een aanvulling op het basisboek *Handboek ISO 27001 ISMS*. In het boek dat voor u ligt, vindt u een samenvatting van het basisboek.

De internationale norm ISO/IEC 27001 bevat eisen voor het opzetten en onderhouden van een managementsysteem voor informatiebeveiliging (ISMS). De norm bevat ook een bijlage met 93 beheersmaatregelen (Engels: controls). Over die 93 beheersmaatregelen gaat dit handboek.

De formulering van de 93 beheersmaatregelen is vaak moeilijk te doorgronden. Het bestuderen van de normteksten en het zoeken naar de betekenis ervan, levert soms meer vragen op dan antwoorden. Waarom zijn de teksten zo algemeen en vaag geformuleerd?

De norm ISO/IEC 27001 is bedoeld *'om toepasselijk te zijn voor alle organisaties, ongeacht type, omvang of aard'*. Dit geldt ook voor de 93 beheersmaatregelen die in de norm worden genoemd: ook die zijn bedoeld voor alle soorten organisaties, in alle landen van de wereld.

De 93 algemeen geformuleerde normteksten krijgen pas betekenis wanneer ze worden toegepast bij het behandelen van de informatiebeveiligingsrisico's die verband houden met de activiteiten, doelstellingen en verplichtingen van uw organisatie.

Dit handboek legt uit waar de beheersmaatregelen van de norm ISO/IEC 27001 over gaan. Zodra u het idee en de speelruimte van een beheersmaatregel begrijpt, kunt u deze implementeren op een manier die past bij uw specifieke risico's.

Handboek ISO 27001 Controls slaat een brug tussen de wereld van ISO/IEC 27001 en de echte wereld. Het boek laat u kennismaken met onderwerpen die mogelijk interessant zijn om verder te onderzoeken. Het boek legt ook verbanden met de AVG.

Daarnaast is dit handboek ook bedoeld voor auditoren die bij een organisatie willen onderzoeken of de beheersmaatregelen doeltreffend en volgens de norm zijn geïmplementeerd. Dit boek bevat voor alle 93 beheersmaatregelen aanwijzingen voor het uitvoeren van audits.

Wees niet bang om aan de slag te gaan. Wees creatief, werk samen en probeer alles zo eenvoudig mogelijk te organiseren. Succes!

Leeswijzer voor dit boek

Bij het lezen van dit handboek is het raadzaam de norm ISO/IEC 27001 bij de hand te houden. Zo kunt u controleren waar bepaalde uitspraken, begrippen en nummers vandaan komen. Eigenlijk kan dit boek niet zonder de norm (die te koop is via de website van NEN).

- *De norm is auteursrechtelijk beschermd en kan niet opgenomen worden in dit boek.*

Lees de norm ISO/IEC 27001 een keer van begin tot einde door, inclusief Bijlage-A. U zult zien dat de nummers van de beheersmaatregelen in Bijlage-A overeenkomen met de nummers van de beheersmaatregelen in de hoofdstukken 5 t/m 8 van dit handboek.

De 93 beheersmaatregelen van de norm staan niet op zichzelf, ze moeten worden gebruikt in samenhang met een 'managementsysteem voor informatiebeveiliging'. Als u geen of weinig ervaring heeft met dit managementsysteem, lees dan eerst de hoofdstukken 1 t/m 4 van dit handboek.

De hoofdstukken 5 t/m 8 in dit handboek niet geschreven om van begin tot einde te lezen. Uiteraard mag u dat doen, maar het oorspronkelijke idee is om deze hoofdstukken te raadplegen wanneer u uitleg of inspiratie nodig heeft bij het implementeren van bepaalde maatregelen.

Omdat vertalingen tot verwarring kunnen leiden, worden in dit handboek regelmatig Engelse bronteksten geciteerd. Bij enkele beheersmaatregelen is een opmerking over de Nederlandse vertaling van de Engelse brontekst opgenomen.

Om geen ruis te introduceren, is in dit handboek 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.

Wanneer een tekst geen ander doel heeft dan het uitleggen van een begrip, dan wordt deze tekst voorafgaan door een titel die begint met het woord 'Begrip'. Voorbeelden in dit boek worden voorafgegaan door het 🕮 -symbool.

Soms komt u in de tekst van dit handboek een blokje met een nummer tegen, bijvoorbeeld: [6]. 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.

Achter in dit boek bevindt zich ook nog een tabel die het verband duidelijk maakt tussen de beheersmaatregelen van vorige versie van de norm en de beheersmaatregelen in de huidige versie.

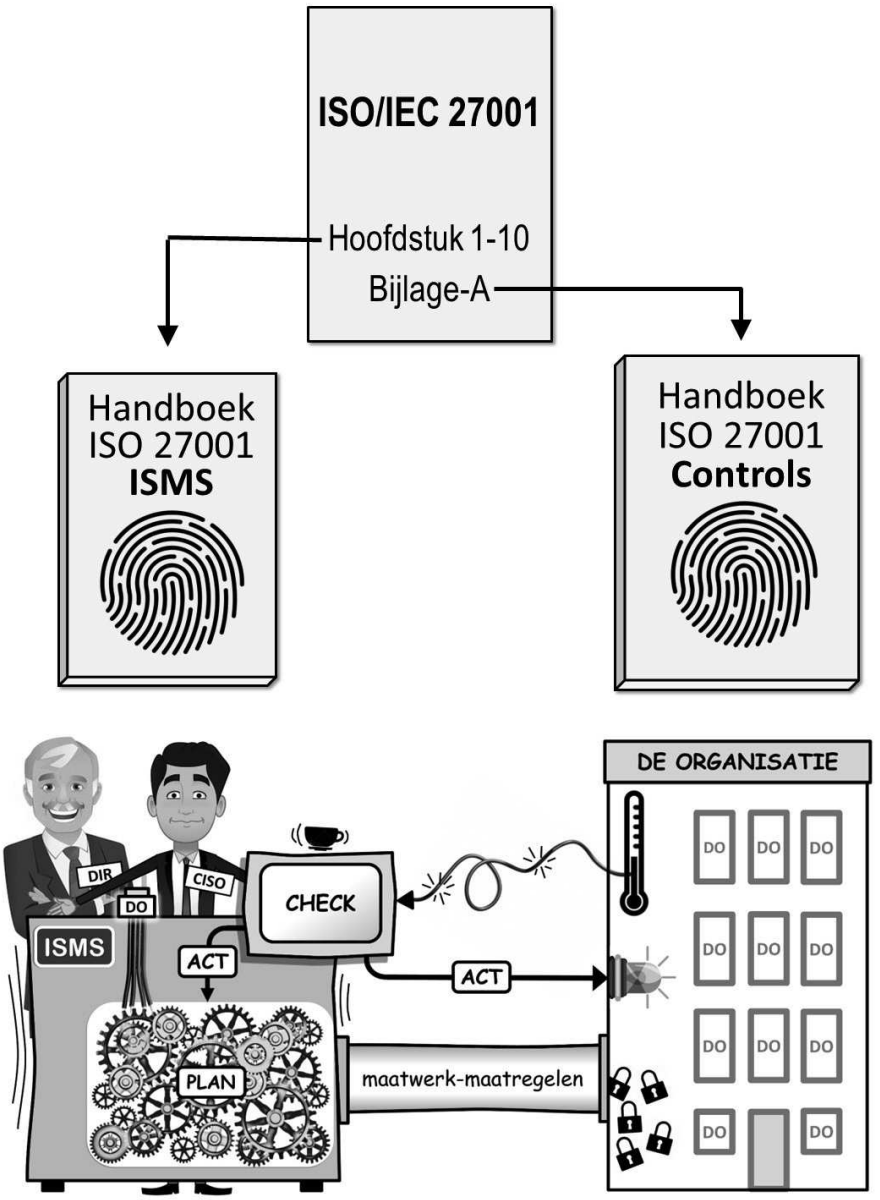
Beheersmaatregelen

Dit *Handboek ISO 27001 Controls* richt zich op de 93 beheersmaatregelen die in Bijlage-A van de norm ISO/IEC 27001 staan. Bij het bespreken van deze beheersmaatregelen komen steeds de volgende onderwerpen aan de orde:

- *Wat vraagt deze beheersmaatregel?*
  Dit onderwerp beschrijft wat uw organisatie moet hebben gerealiseerd om conformiteit met de betreffende beheersmaatregel te mogen claimen.
- *Waar gaat deze maatregel over?*
  Dit onderwerp legt uit waar de betreffende beheersmaatregel (niet) over gaat, verklaart de betekenis van specifieke begrippen en geeft suggesties voor de implementatie.
- *Toepasselijkheid*
  Dit onderwerp beschrijft in algemene bewoordingen het doel waarvoor u de betreffende beheersmaatregel kunt toepassen.
- *Aanwijzingen voor het uitvoeren van audits*
  Dit onderwerp biedt een aantal vragen die een auditor zou kunnen stellen bij het auditen van de betreffende beheersmaatregel.

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 worden gesteld voor eventuele negatieve gevolgen die voortvloeien uit het toepassen van de informatie in dit boek.



Control your risks before they control you

1. Informatiebeveiliging

INFORMATIEBEVEILIGING

De organisatie ISO/IEC splitst het begrip *informatiebeveiliging* op in drie aspecten [1]:

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

Een uitgebreidere definitie zou kunnen zijn:

> *Informatiebeveiliging gaat over het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie binnen een gekozen toepassingsgebied, waaronder persoonsgegevens, in overeenstemming met risico's en verplichtingen*.*

[*] Het naleven van contractuele eisen en wettelijke verplichtingen speelt een belangrijke rol bij het toepassen van de norm ISO/IEC 27001 (zie ook de uitleg bij 5.31 in dit boek).

BEHOUD VAN DE VERTROUWELIJKHEID VAN INFORMATIE

Als het om informatiebeveiliging gaat, denken de meeste mensen op de eerste plaats aan het de *vertrouwelijkheid* van informatie. Bij het behoud van vertrouwelijkheid gaat het erom dat informatie niet beschikbaar of bekend wordt gemaakt aan onbevoegde personen, entiteiten of processen [1].

Bij vertrouwelijke informatie kan het om persoonsgegevens gaan, maar ook om andere soorten informatie, zoals wachtwoorden, bedrijfsgeheimen of concurrentiegevoelige gegevens.

Een verlies van vertrouwelijkheid kan op veel manieren plaatsvinden. Organisaties kunnen gegevens van klanten onrechtmatig delen met derden. 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 per ongeluk vertrouwelijke informatie delen. Een verloren, gestolen of afgedankte computer kan een schat aan vertrouwelijke gegevens bevatten.

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).

Een verlies van integriteit kan op veel manieren plaatsvinden, bijvoorbeeld als gevolg van 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. Na het terugplaatsen van een back-up is bepaalde informatie mogelijk niet meer actueel of compleet.

BEHOUD VAN DE BESCHIKBAARHEID VAN INFORMATIE

Als het over *informatiebeveiliging* gaat, wordt het aspect *beschikbaarheid* vaak als laatste genoemd. Niet omdat het beschikbaar zijn van informatie als onbelangrijk wordt beschouwd, maar omdat het zorgen dat informatie beschikbaar blijft niet altijd wordt gekoppeld aan het beveiligen van informatie. Bij het behoud van beschikbaarheid gaat het erom dat informatie toegankelijk en bruikbaar is op verzoek van degene die over de informatie wil en mag beschikken [1].

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

INFORMATIEBEVEILIGING VERSUS INFORMATIEVEILIGHEID

In plaats van het woord *informatiebeveiliging* wordt in Nederland regelmatig het woord *informatieveiligheid* gebruikt. Een nieuw woord is prima als het minstens even goed is als het oude, maar is dat hier het geval?

Het woord *informatieveiligheid* zegt iets over de over de status van informatie. Die varieert dan ergens tussen 'veilig' en 'niet veilig'. Van informatie die ‘veilig’ is, zou de vertrouwelijkheid in voldoende mate gewaarborgd moeten zijn.

Hier zien we meteen twee verschillen tussen *informatiebeveiliging* en *informatieveiligheid*. Ten eerste gaat informatiebeveiliging over de inspanning die nodig is om tot ‘veilige informatie’ te komen. Ten tweede gaat informatiebeveiliging over meer dan alleen ‘vertrouwelijkheid’.

Op het moment dat een informatiesysteem uitvalt, dan is niet zozeer de veiligheid van informatie in het geding, maar wel de beschikbaarheid van informatie, en daarmee bijvoorbeeld de veiligheid van een ziekenhuispatiënt. Informatiebeveiliging kijkt dus verder.

BIV / BIV-CLASSIFICATIE

Om de drie aspecten van informatiebeveiliging samen te vatten, 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 informatie worden soms geclassificeerd volgens een zogenaamde BIV-classificatie. Het hoogst geclassificeerde systeem kent dan bijvoorbeeld een BIV-klasse van 333, het laagst geclassificeerde systeem de BIV-klasse 111. Op basis van deze classificatie kunnen dan passende beheersmaatregelen worden getroffen.

Beheersmaatregel 5.12 gaat over het classificeren van informatie *in overeenstemming met de informatiebeveiligingsbehoeften van de organisatie op basis van vertrouwelijkheid, integriteit, beschikbaarheid en relevante vereisten van belanghebbenden* (zie 5.12 in dit boek).

2. ISO/IEC 27001- Managementsysteem

DE NORM ISO/IEC 27001

De norm ISO/IEC 27001 is een document van ongeveer 30 pagina's dat te koop is via de website van NEN (België: 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.

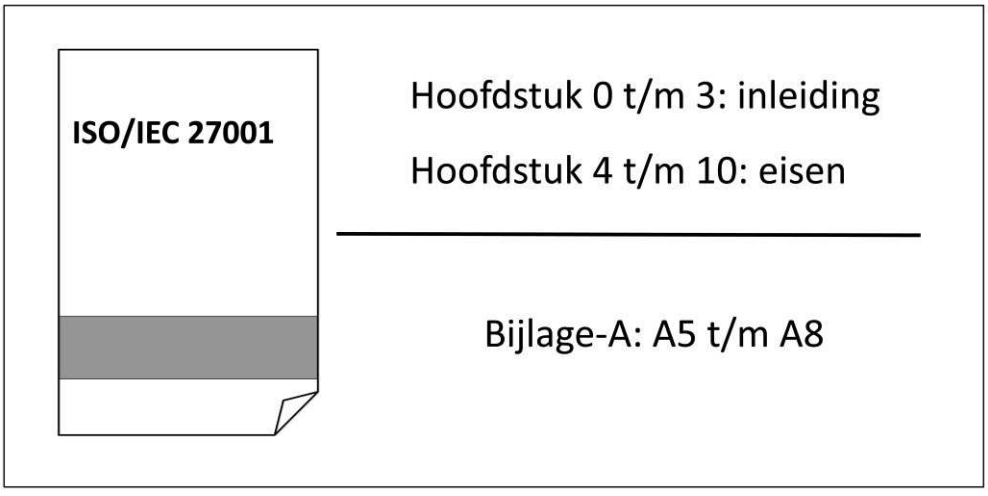
In de praktijk wordt de norm-aanduiding 'ISO/IEC 27001' voor het gemak vaak ingekort tot 'ISO 27001' (zie ook de titel van dit boek).

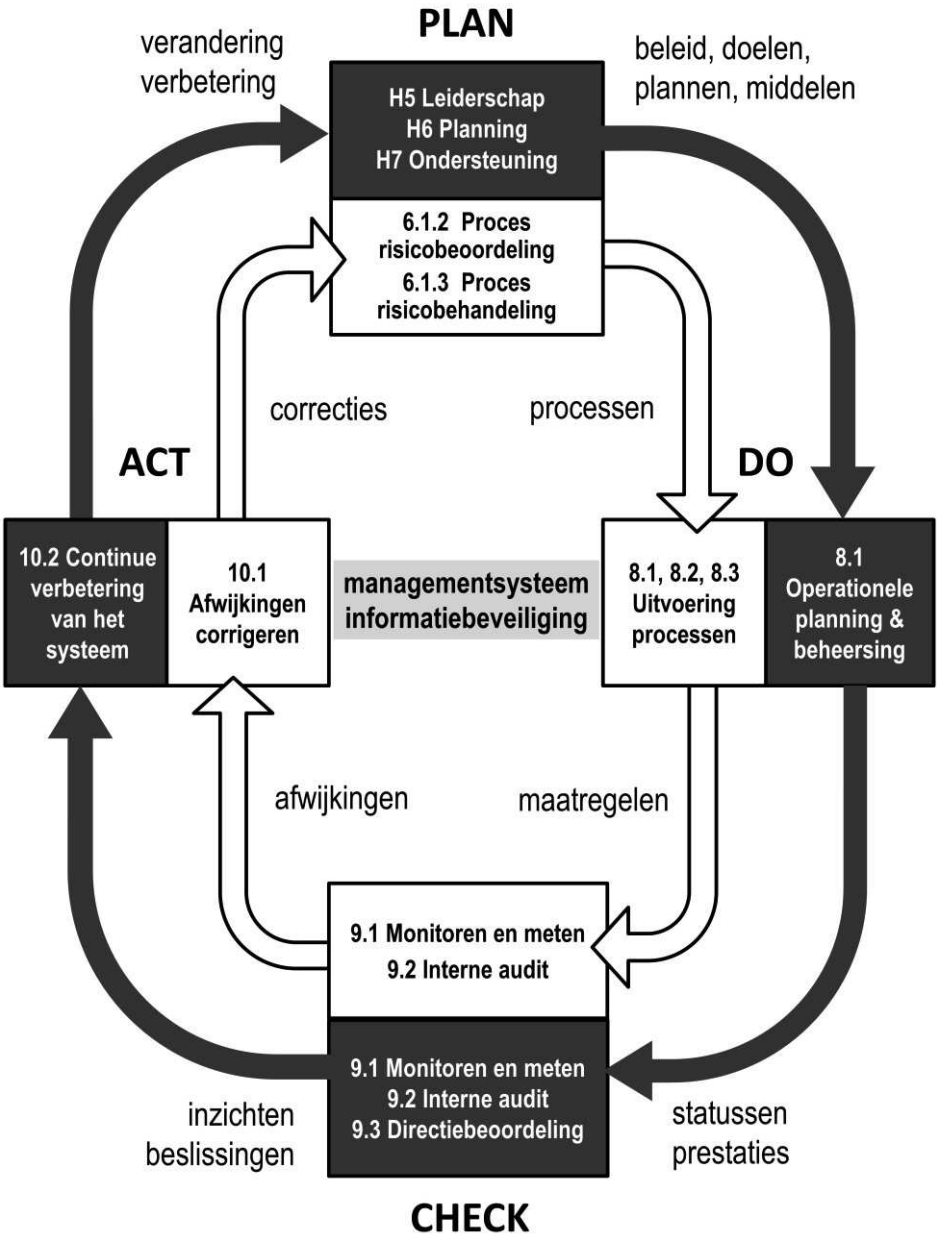
MANAGEMENTSYSTEEM VOOR INFORMATIEBEVEILIGING, ISMS

De norm ISO/IEC 27001:2022 bevat eisen voor het inrichten, implementeren, onderhouden en continu verbeteren van een *managementsysteem voor informatiebeveiliging* (Engels: Information Security Management System, afgekort: ISMS). Dit is een systeem dat uw organisatie kan helpen bij het op orde krijgen van de informatiebeveiliging, en het op orde houden daarvan.

Blader door de norm ISO/IEC 27001. In de hoofdstukken 0 t/m 3 ziet u inleidende teksten staan, het kan verhelderend zijn om deze te lezen. In de hoofdstukken 4 t/m 10 van de norm staan de eisen beschreven waaraan u volgens de norm moet voldoen 'om conformiteit met de norm te kunnen claimen', ofwel, om te mogen beweren dat uw managementsysteem voor informatiebeveiliging aan de norm voldoet.

In het eerste hoofdstuk van de norm ISO/IEC 27001:2022 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.




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

Hoewel de norm ISO/IEC 27001:2022 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 vorige pagina is de inhoud van de norm ISO/IEC 27001 vertaald naar de cirkel van Deming. De afbeelding toont twee PDCA-cirkels: een binnen-cirkel (de witte) en een buiten-cirkel (de zwarte). De nummers en titels verwijzen naar de hoofdstukken en paragrafen van de norm, en naar de hoofdstukken en paragrafen van dit boek.

- *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 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.

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.

HET BELANG VAN HET MANAGEMENTSYSTEEM

Hoe belangrijk is het *managementsysteem* binnen de norm ISO/IEC 27001? Antwoord: de hele norm draait om het *managementsysteem*. Ter illustratie: een ISO/IEC 27001-certificaat doet geen uitspraak over uw informatiebeveiliging, alleen over uw *managementsysteem voor informatiebeveiliging*.

Let op:

Een certificatie-instelling zal met geplande tussenpozen controleren of een gecertificeerd managementsysteem aan de eisen voldoet, en of dit systeem doeltreffend is geïmplementeerd en onderhouden. De wijze waarop de certificatie-instelling dat doet (documentenonderzoek, interviews, observeren, fysieke inspectie, systeemonderzoek), wekt soms de indruk dat er een volledig beveiligingsonderzoek wordt uitgevoerd. Dit is niet het geval.

Wanneer een certificatie-instelling een audit uitvoert, dan is dit niet om te onderzoeken of uw informatiebeveiliging 'op orde is', maar om te onderzoeken of uw *managementsysteem voor informatiebeveiliging* 'op orde is'. Met andere woorden: of u zelf, met behulp van uw managementsysteem, in staat bent te zorgen dat uw informatiebeveiliging 'op orde' is en blijft.

Een typisch vraag van een certificatie-instelling die een afwijking vindt, is: 'had u deze afwijking zelf ook al ontdekt?' Dit is een terechte vraag, want een belangrijk onderdeel binnen uw managementsysteem is het uitvoeren van interne controles. Met deze controles dient uw organisatie zelf afwijkingen aan het licht te brengen (zie ISMS-normelement 9.1 en 9.2 in de norm).

Indien u de vraag van de certificatie-instelling met 'ja' kunt beantwoorden, dan zal dit de certificatie-instelling sterken in de overtuiging dat uw managementsysteem doeltreffend werkt. Is het antwoord 'nee', dan kan de certificatie-instelling bijvoorbeeld aanvullend onderzoek doen naar de wijze waarop u interne audits uitvoert (of laat uitvoeren).

Zodoende kan de certificatie-instelling uw organisatie helpen om uw managementsysteem te verbeteren. Het continu verbeteren van uw managementsysteem zou moeten leiden tot een continue verbetering van uw informatiebeveiliging (zie ISMS-normelement 10.1 in de norm).

Een ISO/IEC 27001-certificaat van een certificatie-instelling mag niet beweren dat een organisatie haar informatiebeveiliging 'op orde heeft' (of iets dergelijks). Het certificaat mag alleen een uitspraak doen over het managementsysteem voor informatiebeveiliging. In Nederland ziet de Raad van Accreditatie (RvA) hierop toe.

➢ *Meer informatie over het inrichten, implementeren, onderhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging, met inbegrip van de benodigde processen en hun interacties, vindt u in 'Handboek ISO 27001 ISMS' [26]*

3. ISO/IEC 27001- Bijlage-A

INHOUD VAN BIJLAGE-A

Neem de norm ISO/IEC 27001:2022 erbij en ga naar Bijlage-A. In deze bijlage ziet u 93 beheersmaatregelen staan die u kunt toepassen om informatiebeveiligingsrisico's te behandelen.

Voor het implementeren van een managementsysteem voor informatiebeveiliging had Bijlage-A in principe uit de norm gelaten kunnen worden. De bijlage is alleen maar in de norm opgenomen zodat u, na het kiezen van eigen maatregelen, kunt *verifiëren dat er geen noodzakelijke beheersmaatregelen zijn weggelaten* (zie ISMS-normelement 6.1.3).

De norm wil voorkomen dat u iets over het hoofd ziet en heeft daarom 93 veelgebruikte beheersmaatregelen in een bijlage geplaatst. De organisatie ISO/IEC beschrijft de 93 beheersmaatregelen in Bijlage-A als [6]:

> *Een generieke mix van organisatorische, mensgerichte, fysieke en technologische beheersmaatregelen voor informatiebeveiliging die zijn ontleend aan internationaal erkende 'best practices'.*

Lees nu de tekst die direct onder de titel 'Bijlage-A' staat. Deze begint met de opmerking dat de beheersmaatregelen van Bijlage-A 'rechtstreeks zijn afgeleid van en in overeenstemming zijn met die in de norm ISO/IEC 27002:2022'.

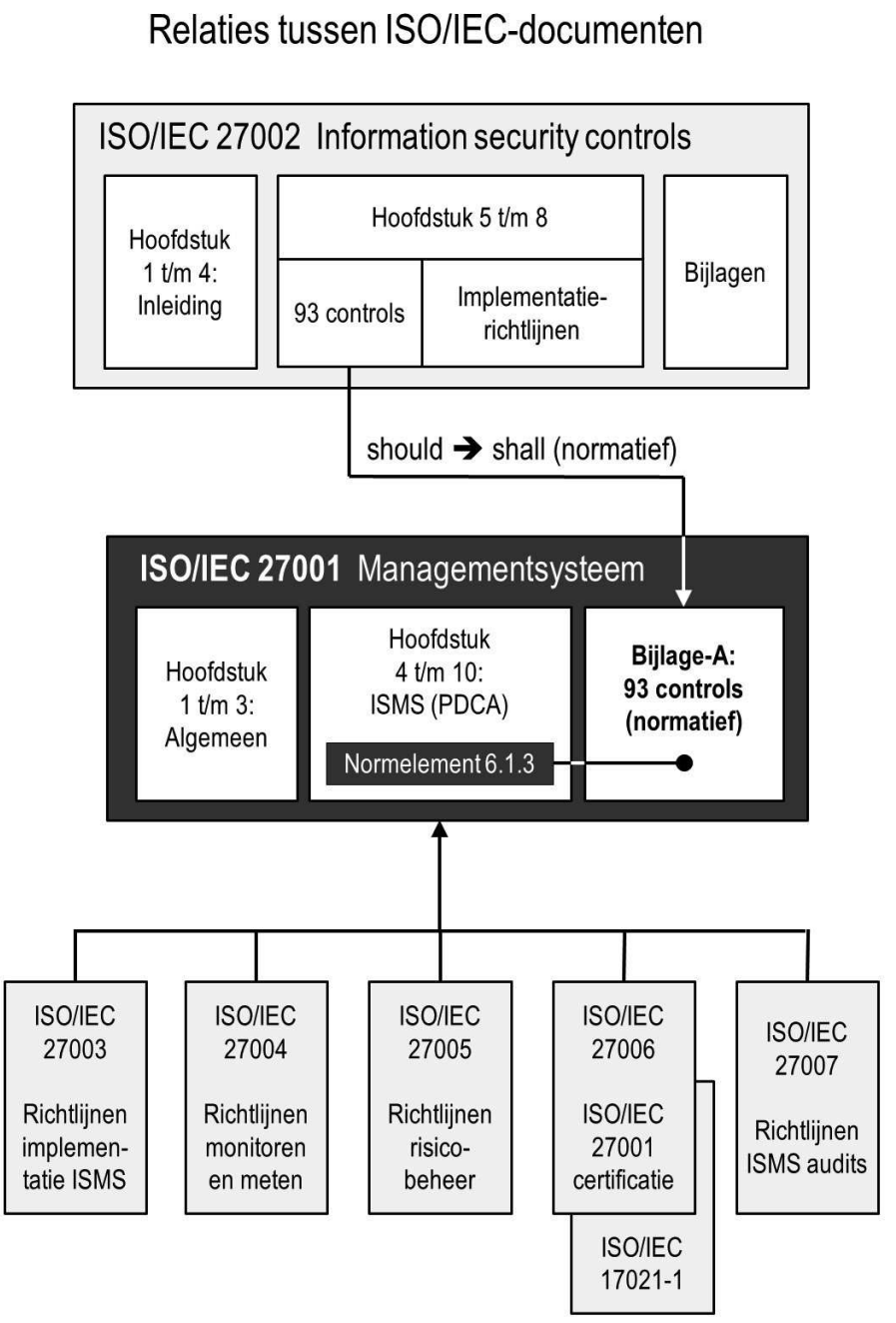
De reden dat de nummering van de beheersmaatregelen in Bijlage-A van de norm ISO/IEC 27001 bij 5 begint en niet bij 1, is simpelweg omdat deze beheersmaatregelen uit de norm ISO/IEC 27002 komen, en daarin vanaf hoofdstuk 5 worden behandeld. Zie de afbeelding hiernaast met een overzicht van de relaties tussen de verschillende ISO/IEC-documenten.

Tussen de 93 beheersmaatregelen die in de norm ISO/IEC 27002 staan en de 93 beheersmaatregelen die in Bijlage-A van de norm ISO/IEC 27001 staan, is er wel een belangrijk verschil. Bij alle beheersmaatregelen die in de norm ISO/IEC 27001 staan, is het vrijblijvende BEHOREN TE (Engels: should) vervangen door het dwingende MOETEN (Engels: shall). Het volgende voorbeeld laat dit verschil zien:

Voorbeeld

ISO/IEC 27002-8.15: Logging	ISO/IEC 27001-A.8.15: Logging
Logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, **BEHOREN TE** worden geproduceerd, beschermd, opgeslagen en geanalyseerd.	Logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, **MOETEN** worden geproduceerd, beschermd, opgeslagen en geanalyseerd.

Door de beheersmaatregelen *normatief* te maken, dwingt de norm ISO/IEC 27001 u om een uitspraak te doen over de vraag welke beheersmaatregelen van Bijlage-A voor uw organisatie wel of niet van toepassing zijn. U moet deze uitspraak vastleggen in een formeel document: de *Verklaring van Toepasselijkheid*. Daarover straks meer, eerst nog even iets anders.


Relaties tussen ISO/IEC-documenten
ISO/IEC 27002 Information security controls
Hoofdstuk 1 t/m 4: Inleiding
Hoofdstuk 5 t/m 8
93 controls
Implementatie-richtlijnen
Bijlagen
should ➔ shall (normatief)
ISO/IEC 27001 Managementsysteem
Hoofdstuk 1 t/m 3: Algemeen
Hoofdstuk 4 t/m 10: ISMS (PDCA)
Normelement 6.1.3
Bijlage-A: 93 controls (normatief)
ISO/IEC 27003 Richtlijnen implementatie ISMS
ISO/IEC 27004 Richtlijnen monitoren en meten
ISO/IEC 27005 Richtlijnen risico-beheer
ISO/IEC 27006 ISO/IEC 27001 certificatie
ISO/IEC 17021-1
ISO/IEC 27007 Richtlijnen ISMS audits

SAMENHANG TUSSEN BEHEERSMAATREGELEN EN RISICO'S

Pak de norm ISO/IEC 27001 er weer bij en lees nog een keer de korte tekst die onder de titel 'Bijlage-A' staat. In het laatste deel van deze tekst staat dat alle beheersmaatregelen van Bijlage-A *moeten worden gebruikt in samenhang met 6.1.3*. Wat wordt hiermee bedoeld?

Ga in de norm naar ISMS-normelement 6.1.3. Zoals u ziet gaat dit normelement over het *behandelen van informatiebeveiligingsrisico's*. De 93 beheersmaatregelen van Bijlage-A zijn dus allemaal bedoeld voor het behandelen van uw informatiebeveiligingsrisico's. Met andere woorden: er moet een logische *samenhang* zijn tussen uw risico's en het gebruik van de beheersmaatregelen in Bijlage-A.

De verplichte *samenhang* tussen beheersmaatregelen en risico's werpt de volgende vraag op: betekent een lijst met 93 beheersmaatregelen dat u minimaal 93 informatiebeveiligingsrisico's moet hebben geïdentificeerd? Nee, dit is niet het geval. Vaak kunnen er voor de behandeling van één risico namelijk meerdere beheersmaatregelen tegelijk worden ingezet.

Voorbeeld

Een organisatie wil het risico verlagen dat ransomware de beschikbaarheid van informatie aantast. Het risico wordt behandeld met de volgende beheersmaatregelen: bewustwording, opleiding en training (6.3), beheersmaatregelen tegen malware (8.7) en back-up van informatie (8.13).

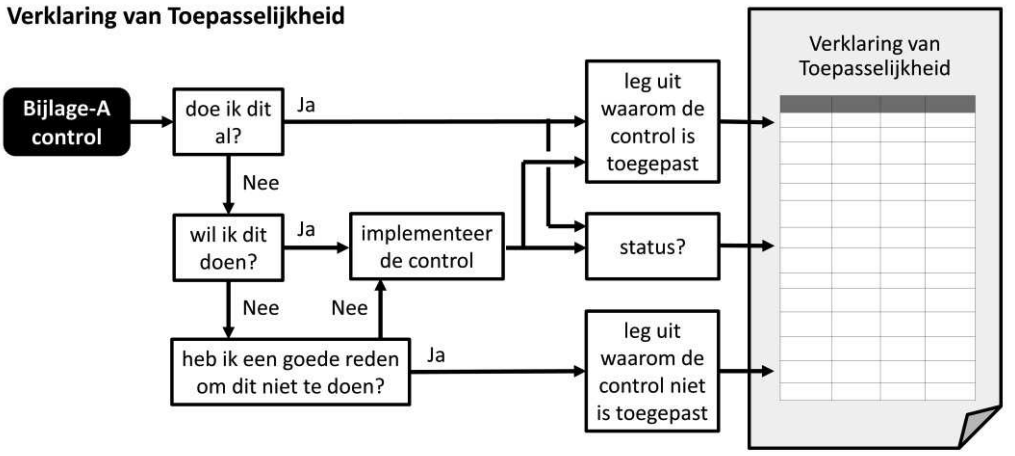
Net zo goed kunnen meerdere risico's soms profiteren van één en dezelfde beheersmaatregel. Zo kan bijvoorbeeld de beheersmaatregel 'bewustwording, opleiding en training' (6.3) vaak worden ingezet voor het behandelen van meerdere risico's. Kortom: er is geen één-op-één-relatie tussen risico's en beheersmaatregelen.

Moet u alle beheersmaatregelen toepassen? Nee, dat hoeft niet. Indien u een Bijlage-A-beheersmaatregel niet kunt toepassen voor het behandelen van uw risico's, dan mag u deze beheersmaatregel *uitsluiten* in uw 'Verklaring van Toepasselijkheid'.

VERKLARING VAN TOEPASSELIJKHEID (VVT)

ISMS-normelement 6.1.3 eist dat u een *Verklaring van Toepasselijkheid* opstelt (VvT) opstelt. Dat is een document dat de volgende informatie moet bevatten:

- **De benodigde beheersmaatregelen**. Geef in uw VvT een opsomming van de 93 beheersmaatregelen van Bijlage-A, alsmede een beschrijving van eventuele andere beheersmaatregelen die u hebt toegepast.
- **De rechtvaardiging voor het opnemen ervan**. Geef in uw VvT bij elke toepaste beheersmaatregel een korte verklaring *waarom* u deze hebt toegepast.
- **Of de benodigde beheersmaatregelen wel of niet geïmplementeerd zijn**. Maak in uw VvT bij elke toegepaste beheersmaatregel duidelijk of deze op dit moment wel of niet is *geïmplementeerd*.
- **De rechtvaardiging voor het uitsluiten van de in Bijlage-A genoemde beheersmaatregelen**. Geef in uw VvT bij elke Bijlage-A-beheersmaatregel die u *niet* heeft toegepast een korte verklaring waarom dit het geval is.



Voorbeeld

Organisatie ABC heeft de volgende Verklaring van Toepasselijkheid opgesteld:

ABC | Verklaring van Toepasselijkheid | Versie: 12 november 2023					
Nr.	**Titel**	**Beheersmaatregel**	**Geïmplementeerd?**	**Reden toepassing**	**Reden uitsluiting**
A.5.1	**Beleidsregels voor informatiebeveiliging**	Informatiebeveiligingsbeleid en onderwerpspecifieke beleidsregels moeten worden gedefinieerd, goedgekeurd door het management, gepubliceerd, gecommuniceerd aan en erkend door relevant personeel en relevante belanghebbenden en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, te worden beoordeeld.	Ja	Risico #01 Risico #08 Risico #09	X
A.5.2	**Rollen en verantwoordelijkheden**	Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.	Ja	Risico #03 Risico #44	X
Etc.					

Om zeker te zijn dat de norm ISO/IEC 27001 op de juiste wijze wordt toegepast, heeft de organisatie ISO/IEC een ondersteunend document gepubliceerd: de norm ISO/IEC 27003 [8]. In deze norm staat het volgende over het uitsluiten van beheersmaatregelen:

> *Elke beheersmaatregel die in Bijlage-A staat en die niet bijdraagt aan het wijzigen van een risico, behoort te worden uitgesloten, en de uitsluiting moet worden gemotiveerd met een rechtvaardiging.*

Uit de rechtvaardig voor het uitsluiten van een beheersmaatregel zou dus moeten blijken waarom de maatregel niet kan bijdragen aan het wijzigen van uw informatiebeveiligingsrisico's.

➢ *Meer informatie over het opstellen en gebruik van een Verklaring van Toepasselijkheid vindt u in het eerder door de auteur gepubliceerde 'Handboek ISO27001' [26].*

HET GEDEELTELIJK TOEPASSEN VAN BEHEERSMAATREGELEN

De ondersteunende norm ISO/IEC 27003 (richtlijnen voor ISMS-implementatie) zegt het volgende over het *gedeeltelijk toepassen* van een beheersmaatregel van Bijlage-A [8]:

> *De rechtvaardiging voor het gedeeltelijk toepassen van een beheersmaatregel is afhankelijk van het effect van de beheersmaatregel op het wijzigen van een informatiebeveiligingsrisico. In de Verklaring van Toepasselijkheid volstaat een rechtvaardiging die verwijst naar de resultaten van de risicobeoordeling en de resultaten van het risicobehandelplan.*

Dit handboek bespreekt bij de uitleg van beheersmaatregel 8.26 een voorbeeld van het gedeeltelijk toepassen van een beheersmaatregel. Deze beheersmaatregel gaat zowel over het *ontwikkelen* van toepassingen als over het *aanschaffen* van door leveranciers ontwikkelde toepassingen. Indien uw organisatie wel toepassingen *aanschaft*, maar geen toepassingen *ontwikkelt*, dan kunt u dit uitleggen in uw Verklaring van Toepasselijkheid

BEHEERSMAATREGELEN BIJ LEVERANCIERS

ISMS-normelement 4.3 gaat over het vaststellen van een toepassingsgebied (Engels: scope) voor uw managementsysteem voor informatiebeveiliging. Met het bepalen van het toepassingsgebied, wordt duidelijk welke processen, mensen, gebouwen, systemen, etc. relevant zijn voor uw managementsysteem.

Zodra duidelijk is welke processen er binnen het toepassingsgebied van uw managementsysteem vallen, kunt u een onderscheid maken tussen processen die u volledig zelf uitvoert en processen die u (gedeeltelijk) laat uitvoeren door een externe organisatie. De organisatie ISO/IEC zegt hierover het volgende [1]:

> *Een externe organisatie valt buiten het toepassingsgebied van uw managementsysteem, hoewel het uitbestede proces er wel binnen valt.*

Dat een uitbesteed proces binnen het toepassingsgebied van uw managementsysteem voor informatiebeveiliging valt, betekent uw organisatie eindverantwoordelijk blijft voor dat proces, inclusief de beheersmaatregelen die nodig zijn voor het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van uw informatie.

Voorbeeld

> Organisatie ABC bestaat uit vier medewerkers die een webapplicatie hebben ontwikkeld. Vanwege kostenbesparing is besloten om geen kantoorpand te huren. De vier medewerkers werken vanuit huis, of op een willekeurige andere locatie. De webapplicatie wordt als SaaS via het IT-platform van een provider aangeboden aan klanten.
>
> Organisatie ABC heeft geen kantoor met een stroomvoorziening, maar ABC is wel afhankelijk van een betrouwbare stroomvoorziening van de cloud provider. De organisatie heeft daarom beheersmaatregel 7.11 (nutsvoorzieningen) van toepassing verklaard. ABC stelt vast dat de provider over een adequate en geteste noodstroomvoorziening beschikt.

Het is de verantwoordelijkheid van uw organisatie om leveranciers te kiezen die passende beheersmaatregelen hebben geïmplementeerd, om voor passende overeenkomsten te zorgen (zie 5.20) en toe te zien op de naleving daarvan (zie 5.22).

EXTRA BEHEERSMAATREGELEN

Behalve de 93 beheersmaatregelen van Bijlage-A van de norm ISO/IEC 27001, mag u ook 'eigen beheersmaatregelen' toevoegen aan uw Verklaring van Toepasselijkheid. De norm ISO/IEC 27007 (met richtlijnen voor het uitvoeren van ISMS-audits) zegt hierover [10]:

> *De voor risicobehandeling noodzakelijke beheersmaatregelen kunnen Bijlage-A-beheersmaatregelen zijn, maar dit is niet verplicht. Het kunnen ook beheersmaatregelen zijn die overgenomen zijn uit andere standaarden of andere bronnen, of ze kunnen speciaal ontworpen zijn door de organisatie.*

Voeg dus gerust 'eigen beheersmaatregelen' toe aan uw Verklaring van Toepasselijkheid. Let in dat geval wel op in hoeverre uw eigen beheersmaatregelen *overlappen* met de 93 Bijlage-A-beheersmaatregelen. De norm ISO/IEC 27007 zegt hierover [10]:

> *In sommige gevallen gebruikt een organisatie een beheersingsmaatregel die een variant is van een Bijlage-A-beheersmaatregel. De reden voor uitsluiting van de Bijlage-A-beheersmaatregel is dan dat deze is vervangen door een variant van de beheersmaatregel.*

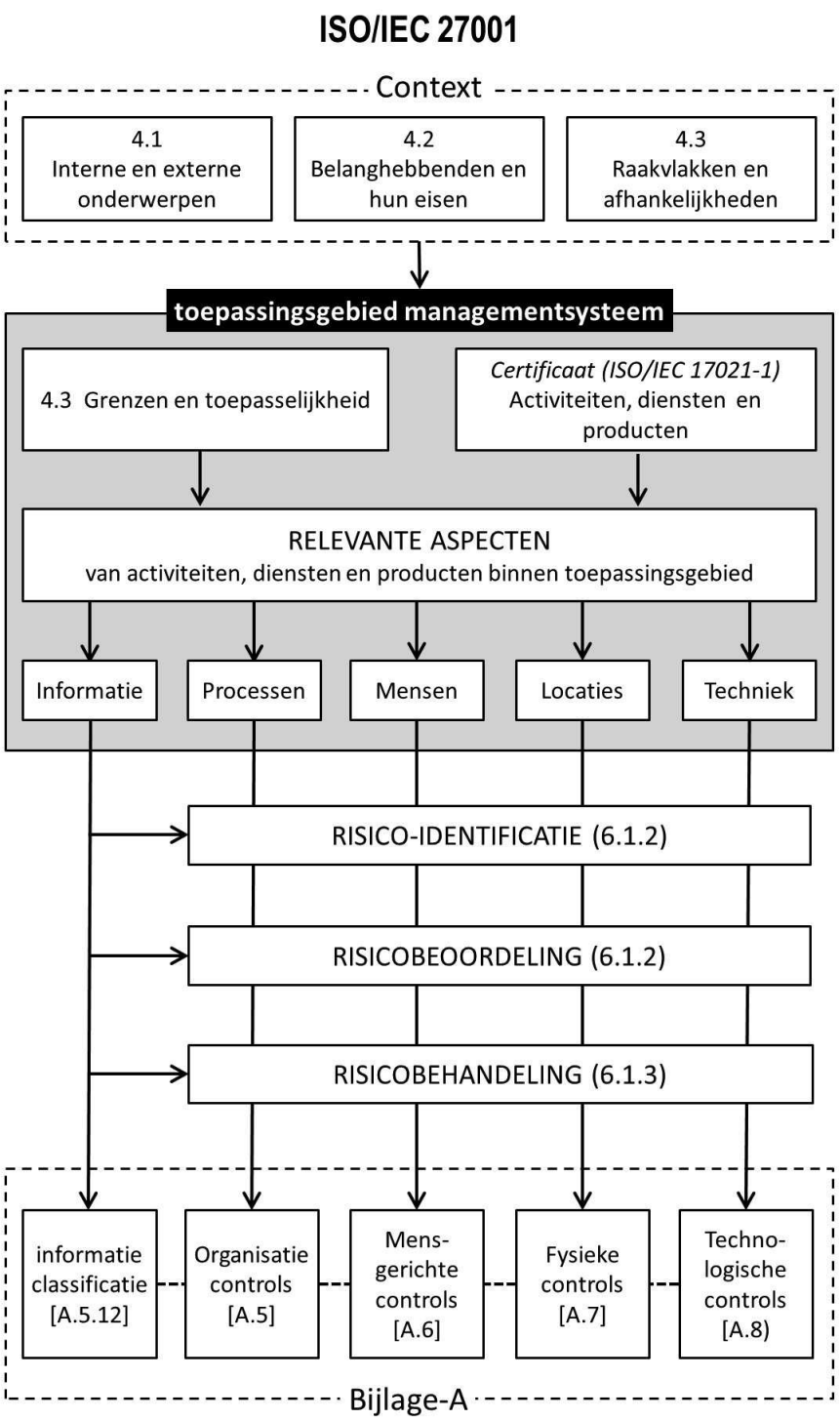
Dus als u in het kader van risicobehandeling een eigen variant van een bestaande Bijlage-A-beheersmaatregel hebt geïmplementeerd, dan mag u de Bijlage-A-beheersmaatregel uitsluiten in de Verklaring van Toepasselijkheid, maar dan wel met de rechtvaardiging dat deze is vervangen door een eigen variant van deze beheersmaatregel.

Mogelijk is uw eigen beheersmaatregel gelijkwaardig aan, of een uitbreiding op een Bijlage-A-beheersmaatregel. De norm ISO/IEC 27007 zegt hierover [10]:

> *De variant van de organisatie kan een Bijlage-A-beheersmaatregel omvatten. De Bijlage-A-beheersmaatregel zou in dat geval niet moeten worden uitgesloten.*

Met andere woorden: het is niet logisch om een Bijlage A-beheersmaatregel uit te sluiten, terwijl deze volledig besloten ligt in uw eigen beheersmaatregel.

De meeste organisaties maken alleen gebruik van de 93 beheersmaatregelen van Bijlage-A, omdat deze meestal prima bruikbaar zijn voor het behandelen van informatiebeveiligingsrisico's.


ISO/IEC 27001
Context
4.1
Interne en externe onderwerpen
4.2
Belanghebbenden en hun eisen
4.3
Raakvlakken en afhankelijkheden
toepassingsgebied managementsysteem
4.3 Grenzen en toepasselijkheid
Certificaat (ISO/IEC 17021-1)
Activiteiten, diensten en producten
RELEVANTE ASPECTEN
van activiteiten, diensten en producten binnen toepassingsgebied
Informatie
Processen
Mensen
Locaties
Techniek
RISICO-IDENTIFICATIE (6.1.2)
RISICOBEOORDELING (6.1.2)
RISICOBEHANDELING (6.1.3)
informatie classificatie [A.5.12]
Organisatie controls [A.5]
Mens-gerichte controls [A.6]
Fysieke controls [A.7]
Techno-logische controls [A.8)
Bijlage-A

4. Beheersmaatregelen

WAT IS EEN BEHEERSMAATREGEL?

De organisatie ISO/IEC definieert een *beheersmaatregel* (Engels: control) als volgt [6]:

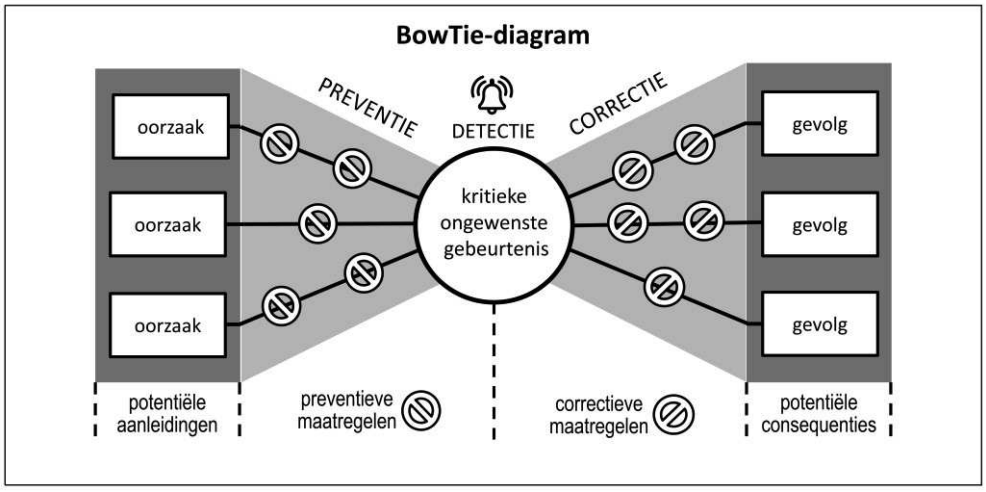
> *Elke vorm van proces, beleid, voorziening, werkwijze, of andere omstandigheid of maatregel, waarmee het risico in stand wordt gehouden en/of wordt gewijzigd.*

Met het *in stand houden van een risico* wordt bedoeld: zorgen dat het risico niet groter kan worden dan het nu is (fixeren). Het *wijzigen van een risico* gaat bijna altijd over het verkleinen van een risico, wat ook bekend staat als het 'mitigeren' (verzachten) van een risico.

De organisatie ISO/IEC maakt onderscheid tussen drie *typen* beheersmaatregelen. Dit wordt duidelijk als we kijken naar het onderstaande BowTie-diagram. Het diagram is vernoemd naar de vorm ervan, die lijkt op een vlinderdas. In het centrum van het diagram bevindt zich een kritieke, ongewenste gebeurtenis die plaatsvindt als de controle over een proces verloren gaat.

Aan de linkerzijde in het diagram bevinden zich *oorzaken* (bedreigingen) die aanleiding kunnen geven tot het optreden van de ongewenste gebeurtenis. Tussen elke oorzaak en de gebeurtenis kunnen soms één of meerdere *preventieve* beheersmaatregelen worden geplaatst om de kans te verkleinen dat de gebeurtenis zich voordoet. Denk bijvoorbeeld aan het gebruik van anti-malware software om problemen met malware op systemen te voorkomen (zie 8.7).

Aan de rechterzijde in het diagram bevinden zich de *gevolgen* die zouden kunnen optreden als de ongewenste gebeurtenis ondanks alle preventieve maatregelen toch heeft plaatsgevonden. Tussen de gebeurtenis en een gevolg kunnen soms één of meerdere *correctieve* beheersmaatregelen worden geplaatst om de impact van de gebeurtenis te verkleinen. Denk bijvoorbeeld aan maatregelen die u in staat stellen om een back-up van informatie terug te zetten (zie 8.13).



Naast *preventieve* en *correctieve* beheersmaatregelen zijn er ook beheersmaatregelen die zich richten op *detectie*. Detectieve beheersmaatregelen zijn bedoeld om gegevens te verzamelen die op zichzelf of in hun samenhang duiden op een relevante gebeurtenis (event). Denk bijvoorbeeld aan het gebruik van een 'intrusion detection system' dat een kwaadaardige digitale inbraak detecteert (zie 8.16).

Sommige beheersmaatregelen zijn uitsluitend preventief, correctief of detectief, maar er zijn ook beheersmaatregelen die meerdere functies tegelijk kunnen vervullen. Zo zou een beheersmaatregel tegen malware (zie 8.7) zowel preventief, correctief als detectief kunnen worden ingezet. Verder kan opgemerkt worden dat er binnen de set van 93 beheersmaatregelen relatief weinig correctieve maatregelen zijn. Het zwaartepunt ligt bij preventie en detectie.

➢ *Zoals gezegd zijn alle 93 beheersmaatregelen van Bijlage-A rechtstreeks afgeleid van en in overeenstemming met die in de norm ISO/IEC 27002 [6]. In deze laatste norm is bij elk van de 93 beheersmaatregelen een set met specifieke 'attributen' opgenomen, waaronder het attribuut 'type beheersmaatregel' dat duidelijk maakt of een beheersmaatregel als preventief, correctief en/of detectief bedoeld is.*

BEHEERSMAATREGELEN: ONTWERPEN

Ga in de norm ISO/IEC 27001 naar Bijlage-A. Zoals u ziet zijn de 93 beheersmaatregelen in deze bijlage verdeeld over vier groepen: organisatorische (37 stuks), mensgerichte (8 stuks), fysieke (14 stuks) en technologische beheersmaatregelen (34 stuks).

De beheersmaatregelen van Bijlage-A zijn zeer algemeen geformuleerd. In de beschrijving van de maatregelen staat wel 'wat' u moet doen, maar niet 'hoe' u dit moet doen. Dit doet de norm bewust: u moet de beheersmaatregelen van Bijlage-A namelijk vertalen naar beheersmaatregelen die passen bij uw informatiebeveiligingsrisico's. Hoe pakt u dat aan?

Het woordje 'moet' dat in alle beheersmaatregelen van Bijlage-A staat, lijkt tegen te spreken dat beheersmaatregelen vertaald mogen worden naar specifieke eigen beheersmaatregelen. Maar ook als u letterlijk doet wat een beheersmaatregel eist, is er nog steeds veel ruimte om deze beheersmaatregel op uw eigen manier toe te passen. Kijk maar:

Voorbeeld

Indien u besluit om beheersmaatregel 8.15 toe te passen, dan MOET u, in overeenstemming met de eis van de beheersmaatregel, zorgen dat logbestanden die activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen registreren, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.

Maar u mag zelf bepalen WELKE activiteiten, uitzonderingen, fouten en andere gebeurtenissen relevant zijn, HOE u uw logbestanden beschermt, WAAR u uw logbestanden opslaat, HOE VAAK u uw logbestanden analyseert en HOE u de analyse uitvoert.

Bij het vertalen van een algemeen geformuleerde beheersmaatregel naar een specifieke eigen beheersmaatregel, kijkt u dus eerst naar het dwingende gedeelte van de eis. Daarna onderzoekt u hoeveel vrijheid er over blijft om de beheersmaatregel te implementeren op een manier die past bij uw risico's. Zo werkt het voor alle beheersmaatregelen.

De aard en de hoogte van het risico dat samenhangt met de beheersmaatregel, bepaalt uiteindelijk hoe uw *eigen beheersmaatregel* eruit moet zien. Houd daarbij ook rekening met eventuele andere beheersmaatregelen die al zijn geïmplementeerd en die het risico al hebben verlaagd.

BEHEERSMAATREGELEN: IMPLEMENTEREN

Prima dat het onderwerp 'informatiebeveiliging' volop aandacht heeft gekregen bij uw laatste project (zie control 5.8), maar hoe heeft u geregeld dat dit bij uw volgende projecten weer gebeurt?

Heel goed dat u onlangs informatie heeft verwijderd die niet langer nodig was (zie control 8.10), maar hoe heeft u geregeld dat het tijdig verwijderen van informatie in de toekomst weer plaatsvindt?

Het *implementeren van beheersmaatregelen* betekent: het implementeren van beleidsregels, processen en procedures die zorgen dat risico's blijvend worden verlaagd. Op die manier wordt *beheersing* (Engels: control) verkregen.

Voorbeeld

Organisatie ABC gebruikt applicatie X om gevoelige informatie te verwerken. ABC heeft beheersmaatregel A.5.18 (toegangsrechten) toegepast, die zegt dat toegangsrechten moeten worden beoordeeld.

Nadat ABC heeft bepaald welke toegangsrechten van medewerkers relevant zijn om te beoordelen op juistheid, is de vraag hoe ze moeten worden beoordeeld, wanneer, hoe vaak en door wie.

ABC besluit om elk kwartaal op basis van een steekproef een beoordeling van toekende toegangsrechten uit te voeren tegen de autorisatiematrix van applicatie X en tegen gegevens in het HR-systeem.

De beheerder van applicatie X dient de beoordeling uit te voeren. De terugkerende taak is vastgelegd in een operationele planning. De resultaten moeten worden gerapporteerd aan de security officer.

Voor het plannen, implementeren en beheersen van een proces kunt u soms gebruik maken van andere beheersmaatregelen.

Voorbeeld

Een organisatie vindt het belangrijk dat medewerkers hun computerschermen vergrendelen wanneer ze hun werkplek verlaten en dat dit op een passende wijze wordt afgedwongen (control 7.7).

Het vergrendelen van computerschermen komt aan de orde in de opleiding van alle nieuwe medewerkers (control 6.3) en ook in de gedragscode met regels voor het aanvaardbaar gebruik van bedrijfsmiddelen (control 5.10).

Van leidinggevenden wordt verwacht dat ze de naleving van de gedragscode handhaven (control 5.36). Deze verantwoordelijkheid is gedefinieerd en toegewezen (control 5.2).

In de bovenstaande voorbeelden zijn er 'processen om te voldoen aan de eisen' gepland, geïmplementeerd en beheerst. Op dezelfde manier kunt u processen inrichten voor andere beheersmaatregelen.

➢ *De uitdaging bij het implementeren van beheersmaatregelen is om ze zodanig te integreren in uw manier van werken dat ze uw bedrijfsprocessen niet al te veel belasten of verstoren.*

BEHEERSMAATREGELEN: VORM

Indien een beheersmaatregel een bepaalde vorm voorschrijft, dan zal deze maatregel in die vorm moeten worden geïmplementeerd. Dus als u een *beleid* moet definiëren, dan moet u zorgen dat er een gedocumenteerd *beleid* komt. Als u een *procedure* moet definiëren, dan moet u zorgen voor een gedocumenteerde *procedure*.

Bestudeer de 93 beheersmaatregelen van Bijlage-A en merk op dat slechts bij een klein deel daarvan vermeld wordt in welke vorm ze geïmplementeerd moeten worden (beleid, proces, procedure, plan, etc.). Dit betekent dat u in de meeste gevallen zelf een keuze moet maken voor een geschikte vorm.

Veel organisaties vertalen de beheersmaatregelen van Bijlage-A die niet voorschrijven in welke vorm ze moeten worden geïmplementeerd, naar gedocumenteerde beleidsregels. Zo kunt u bijvoorbeeld beleid opstellen voor het screenen van kandidaten voor een positie binnen uw organisatie (zie 6.1), ondanks dat er bij beheersmaatregel 6.1 geen 'beleid' wordt geëist.

BEHEERSMAATREGELEN: PRIORITEREN

Waar moet u beginnen bij het implementeren van beheersmaatregelen?

ISMS-normelement 6.1.2 zegt dat u de *geanalyseerde risico's moet prioriteren voor risicobehandeling* [4]. Begin daarom met het implementeren van beheersmaatregelen voor het behandelen van risico die het meest belangrijk en urgent zijn, en eindig met het implementeren van beheersmaatregelen voor het behandelen van risico's die het minst belangrijk en urgent zijn. Wijzig uw prioritering als risico's tussentijds veranderen.

BEHEERSMAATREGELEN: DOCUMENTEREN

Wat moet u documenteren bij het implementeren van beheersmaatregelen?

De 93 beheersmaatregelen van Bijlage-A vragen zelden expliciet om documentatie. Bij het vertalen van de algemeen geformuleerde beheersmaatregelen naar eigen beleid, regels en normen, mag u in veel gevallen dus zelf bepalen wat u wel en niet documenteert.

Een belangrijk voordeel van gedocumenteerde regels en procedures is dat ze gemakkelijk kunnen worden gecommuniceerd aan nieuwe collega's, vervangers of opvolgers. Gedocumenteerde informatie maakt een snelle overdracht van interne afspraken mogelijk en voorkomt dat ze steeds weer opnieuw moeten worden 'uitgevonden'.

Een ander belangrijk voordeel van het documenteren van regels en procedures is dat ze kunnen worden gebruikt bij het uitvoeren van audits.

BEHEERSMAATREGELEN: INTERNE AUDITS

ISMS-normelement 9.2 gaat over het uitvoeren van *interne audits* en zegt [4]:

> *De organisatie moet de auditcriteria voor, en de reikwijdte van, elke audit definiëren.*

Van personen die interne audits uitvoeren, wordt geen persoonlijke mening verwacht, maar een objectieve beoordeling. Hoe kan een auditor zonder gedocumenteerde regels, processen en procedures objectief vaststellen of het maken van back-ups 'goed' plaatsvindt? Of dat toegangsrechten 'terecht' zijn toegewezen? Of dat logbestanden 'correct' worden geanalyseerd?

Zonder duidelijke auditcriteria van uw organisatie kan een auditor niets anders dan terugvallen op zijn 'persoonlijke auditcriteria' (mening). Wat vind ik hier persoonlijk van? Wat zou ik zelf hebben gedaan? Hoe heb ik andere organisaties dit zien doen? Dit botst met de norm, want die zegt:

> *Selecteer auditoren en voer audits zodanig uit dat de objectiviteit en de onpartijdigheid van het auditproces worden bewerkstelligd.*

Alleen een auditor die over auditcriteria beschikt, kan overeenkomstig ISMS-normelement 9.2 een objectieve interne audit uitvoeren om informatie te krijgen of uw managementsysteem voor informatiebeveiliging overeenkomt met uw *eigen eisen* en met de *eisen van de norm*, en om vast te stellen of uw managementsysteem doeltreffend is geïmplementeerd en onderhouden.

BEHEERSMAATREGELEN: CERTIFICATIEAUDITS

De regels voor certificatie van een ISO/IEC27001-managementsysteem zijn beschreven in de norm ISO/IEC 17021-1 [11] en in de aanvullende norm ISO/IEC 27006 [9]. Organisaties die hun managementsysteem willen laten certificeren, hoeven deze regels niet te kennen, maar het is wel handig om het volgende te weten.

De initiële certificatie-audit van een ISO/IEC 27001-managementsysteem moet altijd in twee delen plaatsvinden: 'fase 1' en 'fase 2'. De eerste fase is een vooronderzoek dat (deels) op locatie plaatsvindt. Hierbij beoordeelt de certificatie-instelling (CI) of de mate van invoering van het managementsysteem aangeeft dat u gereed bent voor fase 2.

Tijdens de tweede fase van de initiële certificatie-audit, maar ook tijdens controle- en hercertificatieaudits, moet de CI de implementatie van uw managementsysteem voor informatiebeveiliging verifiëren, inclusief de door u toegepaste beheersmaatregelen van Bijlage-A. Over het auditen van de beheersmaatregelen van Bijlage-A zeggen de regels voor certificering het volgende [9]:

> *De implementatie van de beheersmaatregelen die door de klant als noodzakelijk werden bepaald voor het ISMS (volgens de Verklaring van Toepasselijkheid), moet worden beoordeeld tijdens fase 2 van de initiële audit, en tijdens controle-audits of hercertificatieaudits.*
>
> *De auditinformatie die de certificatie-instelling verzamelt, moet voldoende zijn om een conclusie te trekken over of de beheersmaatregelen effectief zijn. Hoe een beheersmaatregel naar verwachting zal presteren, kan bijvoorbeeld gespecificeerd zijn in beleidsregels of procedures van de klant.*

Tijdens een certificatie-audit moet een auditor dus niet alleen beoordelen of de implementatie van uw beheersmaatregelen voldoet aan de eisen van de norm ISO/IEC 27001, maar ook of ze 'presteren' volgens uw *beleidsregels en procedures*.

De opdracht aan elke auditor die een certificatie-audit uitvoert luidt [11] [9]:

- *Het vaststellen van overeenstemming van het managementsysteem van de klant, of delen daarvan, met de auditcriteria [11].*
- *Het vaststellen van het vermogen van het managementsysteem om te bewerkstelligen dat de klant voldoet aan de eisen uit van toepassing zijnde wet- en regelgeving en contractuele eisen [11].*
- *Het vaststellen van de doeltreffendheid van het managementsysteem om te bewerkstelligen dat de klant in redelijke mate mag verwachten zijn gespecificeerde doelstellingen te bereiken [11].*
- *Indien van toepassing, het identificeren van gebieden waar verbetering van het managementsysteem mogelijk is [11].*
- *Het vaststellen van de effectiviteit van het managementsysteem om ervoor zorgen dat de klant, op basis van de risicobeoordeling, toepasselijke beheersmaatregelen heeft geïmplementeerd en de vastgestelde informatiebeveiligingsdoelstellingen heeft bereikt [9].*

Er spelen veel meer regels bij het certificeren van een managementsysteem voor informatiebeveiliging, maar binnen de context van dit boek zijn vooral de genoemde regels van belang.

BEHEERSMAATREGELEN: ISO/IEC 27002

Zoals uitgelegd in hoofdstuk 3 van dit boek zijn alle 93 beheersmaatregelen in Bijlage-A van de norm ISO/IEC 27001:2022 rechtstreeks afgeleid van die in de norm ISO/IEC 27002:2022 [6].

Behalve de 93 beheersmaatregelen biedt de norm ISO/IEC 27002:2022 bij elke beheersmaatregel een set met informatieve 'attributen', informatie over het doel van de beheersmaatregel, en een richtlijn voor de implementatie ervan. Schaf deze norm aan, bestudeer alle informatie en doe er uw voordeel mee.

Bij het implementeren van de beheersmaatregelen van Bijlage-A bent u niet verplicht om de implementatierichtlijnen op te volgen, maar ze verdienen zeker aandacht. Bij het definiëren van de 93 beheersmaatregelen had de organisatie ISO/IEC namelijk bepaalde ideeën voor ogen, en de richtlijnen verschaffen daarover waardevolle informatie. Wijk niet te veel af van het idee dat achter een beheersmaatregel schuilgaat, anders mist u mogelijk de essentie.

➢ *Dit boek verwijst regelmatig naar de implementatierichtlijnen van de norm ISO/IEC 27002. Een verwijzing is niet bedoeld om te vertellen wat u moet doen, maar om aan de hand van de richtlijn uit te leggen waar een beheersmaatregel over gaat. Uiteindelijk kunt u een implementatie realiseren die past bij uw eigen risicocontext.*

5. Organisatorische maatregelen

5.1 Beleidsregels voor informatiebeveiliging

Policies for information security

■ Wat vraagt deze beheersmaatregel?

Om conformiteit met beheersmaatregel 5.1 te mogen claimen, moet uw organisatie het volgende hebben gerealiseerd [4]:

- Er is een informatiebeveiligingsbeleid gedefinieerd.
- Er zijn onderwerpspecifieke beleidsregels gedefinieerd.
- Beleid en beleidsregels zijn goedgekeurd door het management.
- Beleid en beleidsregels zijn gepubliceerd.
- Beleid en beleidsregels worden gecommuniceerd aan relevant personeel.
- Beleid en beleidsregels worden gecommuniceerd aan relevante belanghebbenden.
- Beleid en beleidsregels worden erkend door personeel en belanghebbenden.
- Beleid en beleidsregels worden met geplande tussenpozen beoordeeld.
- Beleid en beleidsregels worden beoordeeld na significante wijzigingen.

■ Waar gaat deze beheersmaatregel over?

◆ INFORMATIEBEVEILIGINGSBELEID (STRATEGISCH)

Beheersmaatregel 5.1 maakt onderscheid tussen *informatiebeveiligingsbeleid* en *onderwerpspecifieke beleidsregels*. Wat is informatiebeveiligingsbeleid? De implementatierichtlijn voor het implementeren van een managementsysteem voor informatiebeveiliging zegt [8]:

> *Het informatiebeveiligingsbeleid beschrijft het strategische belang van het ISMS voor de organisatie en is beschikbaar als gedocumenteerde informatie. Het beleid stuurt informatiebeveiligingsactiviteiten in de organisatie aan.*

Beleid gaat volgens de organisatie ISO/IEC over de intenties en richting van een organisatie, zoals formeel kenbaar gemaakt door haar topmanagement [6]. Dit betekent dat uw *informatiebeveiligingsbeleid* een beleid is dat gaat over de strategische intenties en richting met betrekking tot uw informatiebeveiliging en het managen daarvan.

Uw informatiebeveiligingsbeleid, ook wel het *strategisch beleid* genoemd, hoeft niet specifiek te zijn. Het bevat doorgaans algemene principes die de strategische doelstellingen, risico's en verplichtingen van de organisatie weerspiegelen. Uw strategisch beleid dient als basis voor *onderwerpspecifieke beleidsregels* (zoals we later zullen zien).

Voorbeeld

Het management van een organisatie heeft een strategisch informatiebeveiligingsbeleid van twee pagina's gemaakt met daarin de volgende informatie:

- Definities van begrippen zoals informatie, informatiebeveiliging, bedrijfsmiddelen, etc.

- Uitleg over het managementsysteem van de organisatie (zie hoofdstuk 2 in dit boek).
- Een kader voor het vaststellen van *informatiebeveiligingsdoelstellingen**. Wat wil de organisatie in algemene zin bereiken met het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie? Welk belang hecht de organisatie aan het naleven van wettelijke verplichtingen in verband met informatiebeveiliging?
- Een *verbintenis** om te voldoen aan van toepassing zijnde eisen in verband met informatiebeveiliging, en een *verbintenis** tot continue verbetering van het managementsysteem voor informatiebeveiliging.
- Informatie over *rollen* met speciale verantwoordelijkheden bij informatiebeveiliging (zie ook 5.2) en informatie over *verantwoordelijkheden* van medewerkers die geen speciale rol hebben bij informatiebeveiliging, maar daar wel invloed op hebben.
- De eis van het management dat medewerkers in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie werken (zie ook 5.4).
- Een verwijzing naar de *disciplinaire procedure* van de organisatie (zie ook 6.4).
- De eis dat waargenomen of vermeende *zwakke plekken* in de informatiebeveiliging gemeld moeten worden (zie ook 6.8).

[*] Let op dat uw strategisch informatiebeveiligingsbeleid ook moet voldoen aan de eisen van ISMS-normelement 5.2 (zie de norm).

Let op:

Vermijd in uw informatiebeveiligingsbeleid alleen maar duidelijk te maken wat uw organisatie wil *voorkomen*. Probeer vooral ook duidelijk te maken wat uw organisatie wil *bereiken* (zie ISMS-normelement 6.2: informatiebeveiligingsdoelstellingen). Hierdoor ontstaat duidelijkheid over de intentie en richting die uw organisatie nodig heeft voor het vaststellen van onderwerpspecifiek beleid en de daaruit voortvloeiende regels, maatregelen, processen, en procedures.

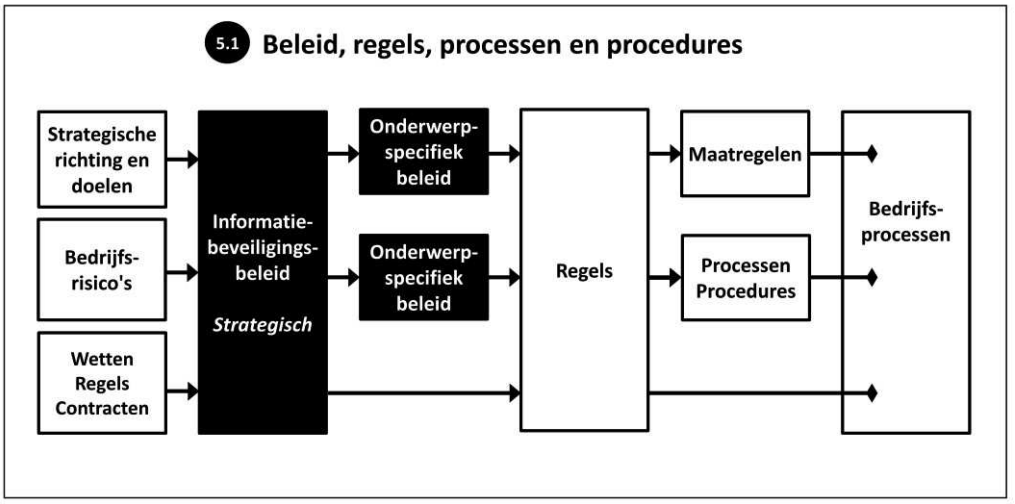
◆ ONDERWERPSPECIFIEKE BELEIDSREGELS

Beheersmaatregel 5.1 gaat ook over het definiëren van *onderwerpspecifieke beleidsregels*. De organisatie ISO/IEC definieert *onderwerpspecifiek beleid* als volgt [6]:

> *Onderwerpspecifiek beleid gaat over intentie en richting met betrekking tot een specifiek onderwerp, zoals formeel uitgedrukt door het juiste managementniveau.*
>
> *Onderwerpspecifiek beleid kan worden gebruikt voor het formeel uitdrukken van regels, richtlijnen of organisatienormen.*

De implementatierichtlijn van beheersmaatregel 5.1 legt uit dat er een hiërarchisch verband is tussen het informatiebeveiligingsbeleid en onderwerpspecifieke beleidsregels [6]:

> *Op een lager niveau behoort het informatiebeveiligingsbeleid te worden ondersteund door onderwerpspecifieke beleidsregels (…).*
>
> *Onderwerpspecifieke beleidsregels behoren te worden afgestemd op het informatiebeveiligingsbeleid van de organisatie en dit aan te vullen.*



Meestal kiest het topmanagement er niet voor om betrokken te worden bij het definiëren van onderwerpspecifieke beleidsregels. Die beleidsregels zijn vaak te specifiek en worden om die reden doorgaans opgesteld door specialisten.

Van alle 93 beheersmaatregelen in Bijlage-A van de norm ISO/IEC 27001 eisen alleen beheersmaatregelen 8.3 en 8.13 *onderwerpspecifiek beleid,* maar uw organisatie mag zoveel onderwerpspecifiek beleid definiëren als nodig is.

Bij beheersmaatregel 6.1 (screening) wordt het woord 'beleid' niet genoemd, maar niets staat u in de weg om een onderwerpspecifiek beleid voor *screening* te definiëren. Hetzelfde geldt voor beheersmaatregel 8.24 (cryptografie). Ook hier wordt het woord 'beleid' niet genoemd, maar ook hier staat u niets in de weg om een onderwerpspecifiek beleid voor *het gebruik van cryptografie* te definiëren.

Kortom: maak zoveel onderwerpspecifiek beleid als nodig is. De implementatierichtlijn van beheersmaatregel 5.1 noemt een lange lijst met voorbeelden van beheersmaatregelen waarbij geen onderwerpspecifiek beleid wordt gevraagd, maar wel zou kunnen worden gemaakt [6].

GDPR (EU), AVG (NL): Gegevensbeschermingsbeleid

De AVG [17] zegt bij artikel 24:

Wanneer zulks in verhouding staat tot de verwerkingsactiviteiten, omvatten de in lid 1 bedoelde maatregelen een passend gegevensbeschermingsbeleid dat door de verwerkingsverantwoordelijke wordt uitgevoerd.

De AVG stelt geen specifieke eisen aan de inhoud van een *gegevensbeschermingsbeleid*. Indien uw organisatie een *informatiebeveiligingsbeleid* heeft gedefinieerd dat beleidsregels bevat, of dat naar beleidsregels verwijst, voor de bescherming van de beschikbaarheid, integriteit en vertrouwelijkheid van *persoonsgegevens*, dan vormt uw informatiebeveiligingsbeleid minstens al een deel van uw *gegevensbeschermingsbeleid*.

REGELS

In de norm staan diverse beheersmaatregelen die gaan over *regels* (bijv. 5.15). De organisatie ISO/IEC zegt het volgende over *regels* [6]:

> *Regels: Principes of instructies die de verwachtingen van de organisatie weergeven over wat er moet gebeuren, wat is toegestaan of niet is toegestaan.*
>
> *Regels kunnen formeel worden uitgedrukt in beleid, en in andere soorten documenten.*

De organisatie ISO/IEC onderscheidt daarmee twee soorten regels:

- **Principes**. Een *principe* geeft wel informatie over wat er gerealiseerd moet worden, maar niet hoe dit gerealiseerd moet worden. Bijvoorbeeld: wachtwoorden moeten beveiligd worden gecommuniceerd.
- **Instructies**. Een *instructie* is concreet over wat er gerealiseerd moet worden. Bijvoorbeeld: na drie keer een verkeerd wachtwoord te hebben ingevoerd, moet het account tien minuten worden geblokkeerd.

PROCESSEN EN PROCEDURES

In Bijlage-A van de norm ISO/IEC 27001 staan ook enkele beheersmaatregelen die verwijzen naar *processen en procedures*.

Een *proces* is een ordening van activiteiten met een input en een output, en met een duidelijk begin en einde. Denk bijvoorbeeld aan een proces voor het afhandelen van informatiebeveiligingsincidenten (zie 5.24). Een *procedure* is een reeks instructies die in een bepaalde volgorde moet worden uitgevoerd. Denk bijvoorbeeld aan een procedure die gevolgd moet worden bij het verstrekken, wijzigen en intrekken van toegangsrechten (zie 5.18).

◆ GOEDKEURING, COMMUNICATIE, ERKENNING EN BEOORDELING

DOCUMENTEREN BELEID

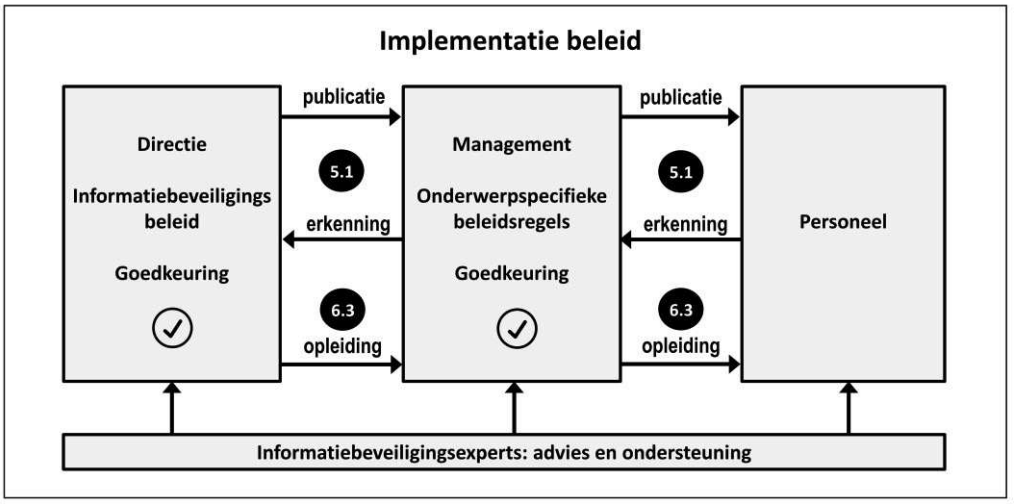
Hoeveel vrijheid heeft u bij het documenteren van uw strategisch informatiebeveiligingsbeleid en onderwerpspecifiek beleidsregels? De implementatierichtlijn van 5.1 zegt [6]:

> *De organisatie kan voor deze beleidsdocumenten formaten en namen vaststellen die aan de behoeften van de organisatie voldoen.*
>
> *In bepaalde organisaties kunnen het informatiebeveiligingsbeleid en het onderwerpspecifieke beleid in één en hetzelfde document worden opgenomen.*

Beleid kan dus in meerdere documenten worden vastgelegd, of in één document, en beleidsdocumenten hoeven dus niet de naam ‘beleid’ te dragen.

GOEDKEUREN BELEID

Beheersmaatregel 5.1 noemt ook het *goedkeuren* van beleid. Hierover zegt de implementatierichtlijn [6]:



> *Informatiebeveiligingsbeleid behoort te worden goedgekeurd door het topmanagement. Onderwerpspecifiek beleid behoort te worden goedgekeurd door het passende managementniveau.*

Merk op dat deze richtlijn niet alleen duidelijk maakt wie welk beleid behoort goed te keuren, maar ook dat het strategisch informatiebeveiligingsbeleid op een hoger niveau ligt dan onderwerpspecifieke beleidsregels.

COMMUNICATIE BELEIDSREGELS AAN PERSONEEL

Beheersmaatregel 5.1 zegt dat de beleidsregels moeten worden gecommuniceerd aan relevant *personeel*. De organisatie ISO/IEC definieert het begrip *personeel* als volgt [6]:

> *Personeel betreft personen die onder leiding van de organisatie werk verrichten. Het begrip personeel omvat de leden van de organisatie, zoals het bestuursorgaan, de directie, medewerkers, tijdelijke medewerkers, contractanten en vrijwilligers.*

In de praktijk is de inhoud van het strategisch informatiebeveiligingsbeleid soms zo algemeen dat besloten wordt om het alleen leidinggevenden van de organisatie te communiceren. Beheersmaatregel 5.1 biedt hier ruimte voor door te zeggen dat beleid moet worden gecommuniceerd aan relevant personeel.

Hetzelfde geldt voor onderwerpspecifieke beleidsregels. Hoe interessant zijn bijvoorbeeld beleidsregels voor veilig coderen (zie 8.28) voor medewerkers van de financiële afdeling? Uw organisatie mag zelf bepalen welke beleidsregels aan welk deel van het personeel worden gecommuniceerd.

➢ *Vaak worden alle beleidsregels via het intranet gecommuniceerd aan het voltallige personeel, en bepalen werknemers zelf welke informatie relevant is.*

COMMUNICATIE BELEIDSREGELS AAN ANDERE BELANGHEBBENDEN

Beheersmaatregel 5.1 zegt ook dat uw beleidsregels moeten worden gecommuniceerd aan relevante *belanghebbenden* (Engels: interested parties / stakeholders). De organisatie ISO/IEC definieert het begrip *belanghebbenden* als volgt [6]:

> *Een belanghebbende is een persoon of organisatie die invloed kan hebben op een beslissing of activiteit van uw organisatie, of die beïnvloed kan worden door een beslissing of activiteit van uw organisatie, of die ervaart dat hij wordt beïnvloed door een beslissing of activiteit van uw organisatie.*

U mag zelf beoordelen welke belanghebbenden, anders dan uw medewerkers, *relevant* zijn voor het communiceren van uw beleidsregels. Denk bijvoorbeeld aan het delen van uw beleid met een leverancier. In de praktijk worden beleidsregels meestal alleen aan medewerkers gecommuniceerd.

ERKENNEN BELEIDSREGELS

Beheersmaatregel 5.1 noemt ook het *erkennen* van beleidsregels door *personeel* en relevante *belanghebbenden*. Met andere woorden: uw mag er niet vanuit gaan dat gecommuniceerde beleidsregels automatisch begrepen en geaccepteerd zijn door de doelgroep.

In plaats van alleen maar beleid te communiceren, zal uw organisatie een vorm van bevestiging van de doelgroep moeten terugkrijgen. Hieruit moet blijken dat de beleidsregels begrepen en geaccepteerd zijn. In de praktijk wordt dit vaak geregeld door vanuit de arbeidsovereenkomst te verwijzen naar het informatiebeveiligingsbeleid (zie 6.2).

PERIODIEKE BEOORDELING BELEIDSREGELS

Beheersmaatregel 5.1 noemt ook het *met geplande tussenpozen beoordelen van uw beleidsregels*. Het doel hiervan is [6]:

> *De voortdurende geschiktheid, toereikendheid, doeltreffendheid van de sturing en ondersteuning door het management bewerkstelligen, overeenkomstig de bedrijfseisen, wet- en regelgeving, statutaire en contractuele eisen.*

Sluiten uw strategisch beleid en specifieke beleidsregels nog steeds aan bij uw informatiebeveiligingsrisico's? Sluiten ze nog steeds in voldoende mate aan bij uw strategische richting, doelen en verplichtingen? De implementatierichtlijn van 5.1 voegt daaraan toe [6]:

> *Bij de beoordeling behoort rekening gehouden te worden met de resultaten van management reviews (ISMS-normelement 9.3) en audits (ISMS-normelement 9.2).*

Beheersmaatregel 5.1 spreekt over *geplande tussenpozen*. Tip: Neem de beoordeling van beleid en beleidsregels op in uw operationele planning (ISMS-normelement 8.1).

BELEIDSREGELS AANPASSEN NA EEN SIGNIFICANTE WIJZIGING

Beheersmaatregel 5.1 noemt ook het *beoordelen van beleidsregels na een significante wijziging*. Zijn uw beleidsregels nog steeds passend als uw risico's plotseling sterk wijzigen? Of als er een

reorganisatie van rollen en verantwoordelijkheden plaatsvindt? Of als uw organisatie fuseert met een andere organisatie? Of als uw organisatie zich afsplitst van een grotere organisatie?

SCHOLING EN BIJSCHOLING IN BELEIDSREGELS

Personen die onder leiding van de organisatie werk verrichten, hebben mogelijk een opleiding nodig om bepaalde beleidsregels te begrijpen. Ook is er mogelijk bijscholing nodig als bepaalde beleidsregels gewijzigd zijn. Hiervoor kunt u beheersmaatregel 6.3 gebruiken: *Bewustwording van, opleiding en training in informatiebeveiliging*.

NALEVING VAN BELEIDSREGELS, REGELS EN NORMEN

Het beschikken over beleidsregels is niet genoeg om informatiebeveiligingsrisico's te kunnen verlagen. Het verlagen van risico's kan alleen plaatsvinden als uw beleidsregels worden nageleefd. Daarom moet de naleving van het informatiebeveiligingsbeleid, het onderwerpspecifiek beleid, de regels en de normen van de organisatie regelmatig worden beoordeeld (zie 5.36).

BELEIDSREGELS ALS AUDITCRITERIA

Zelfs als beleidsregels niet of nauwelijks door medewerkers geraadpleegd worden, kunnen ze toch belangrijk zijn. Beleidsregels kunnen namelijk als criteria worden gebruikt bij audits.

Voorbeeld

Een organisatie laat een auditor zien welke gebruikers toegang hebben tot een informatiesysteem dat gevoelige gegevens verwerkt. Vervolgens wordt de auditor gevraagd een oordeel te geven over de ingestelde toegangsrechten. De auditor constateert dat er geen beleidsregels zijn die bepalen welke gebruiker toegang mag krijgen tot het betreffende systeem. De auditor weigert zijn persoonlijke mening in het auditrapport te zetten en geeft aan de beoordeling niet te kunnen uitvoeren bij gebrek aan auditcriteria.

➢ *Zie ook de uitleg in hoofdstuk 4 van dit boek.*

■ Toepasselijkheid

Om de toepasselijkheid van beheersmaatregel 5.1 te bepalen, moet uw organisatie de kans beoordelen dat er informatiebeveiligingsincidenten optreden doordat medewerkers te veel vrijheid krijgen (of te weinig aansturing krijgen) bij het werken met informatie.

■ Aanwijzingen voor het uitvoeren van audits

Bij deze beheersmaatregel zou een auditor het volgende kunnen onderzoeken:

IMPLEMENTATIE: STRATEGISCH BELEID

- Heeft de organisatie strategisch informatiebeveiligingsbeleid vastgesteld?
- Op welke wijze sluit dit strategisch beleid aan bij de strategische richting van de organisatie (zie ISMS-normelement 5.1a: leiderschap en betrokkenheid)?

- Bevat het strategisch beleid informatiebeveiligingsdoelstellingen, of een kader voor informatiebeveiligingsdoelstellingen (zie ISMS-normelement 5.2)?
- Is het strategisch beleid goedgekeurd door het topmanagement?
- Is het strategisch beleid beschikbaar voor en erkend door relevant personeel en relevante belanghebbenden? Overweeg het afnemen van interviews om dit te controleren.

IMPLEMENTATIE: ONDERWERPSPECIFIEKE BELEIDSREGELS

- Welke documenten en/of teksten bevatten onderwerpspecifieke beleidsregels?
- Zijn alle documenten en/of teksten die onderwerpspecifieke beleidsregels bevatten, goedgekeurd door een passend managementniveau?
- Zijn documenten en/of teksten die onderwerpspecifieke beleidsregels bevatten, beschikbaar voor en erkend door relevant personeel en relevante externe partijen?
- Zijn relevant personeel en relevante belanghebbenden op de hoogte van onderwerpspecifiek informatiebeveiligingsbeleid? Overweeg het afnemen van interviews om dit te controleren.

BEHEERSING

- Hoe heeft de organisatie gewaarborgd dat het *strategisch informatiebeveiligingsbeleid* met geplande tussenpozen wordt beoordeeld?
- Hoe heeft de organisatie gewaarborgd dat *onderwerpspecifieke beleidsregels* met geplande tussenpozen worden beoordeeld?
- Hoe heeft de organisatie gewaarborgd dat beleidsregels worden beoordeeld na een *significante wijziging*? Wat verstaat de organisatie onder een *significante wijziging*?

CONCLUSIE

- Bepaal op basis van de resultaten van het uitgevoerde onderzoek of deze beheersmaatregel doeltreffend, volgens de eisen van de norm, en volgens de eigen eisen van de organisatie is geïmplementeerd (zie ISMS-normelement 9.2.1).

5.2 Rollen en verantwoordelijkheden bij informatiebeveiliging

Information security roles and responsibilities

■ Wat vraagt deze beheersmaatregel?

Om conformiteit met beheersmaatregel 5.2 te mogen claimen, moet uw organisatie het volgende hebben gerealiseerd [4]:

- *Rollen* bij informatiebeveiliging zijn gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.
- *Verantwoordelijkheden* bij informatiebeveiliging zijn gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.

■ Waar gaat deze beheersmaatregel over?

◆ ROLLEN BIJ INFORMATIEBEVEILIGING

Medewerkers krijgen doorgaans een *functie* waarvan de inhoud beschreven wordt in een functieomschrijving. Beheersmaatregel 5.2 gaat niet over *functies*, maar over *rollen*. Een essentieel verschil is dat *functies* een afspiegeling zijn van mensen die worden georganiseerd, terwijl *rollen* een afspiegeling zijn van werkzaamheden die worden georganiseerd.

In de praktijk vervullen mensen vanuit hun *functie* soms meerdere *rollen*. Iemand met de functie 'IT manager' zou ook de rollen 'Security Officer' en 'change manager' kunnen vervullen. In een grotere organisatie zou de 'Security Officer' een aparte functie kunnen zijn, die op zijn beurt weer uit meerdere rollen kan bestaan.

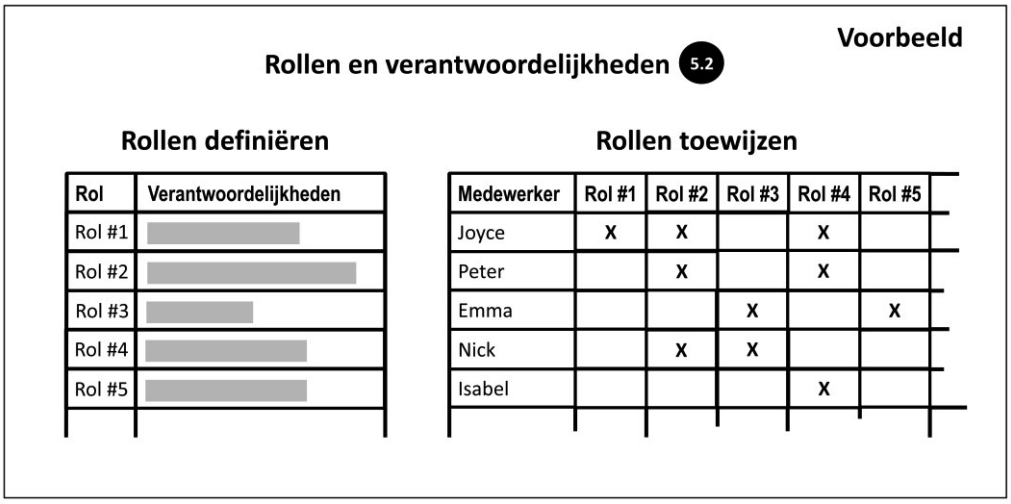
INFORMATIEBEVEILIGINGSEXPERTS

Binnen organisaties kunnen diverse informatiebeveiligingsexperts werkzaam zijn. Denk bijvoorbeeld aan (Chief/Concern) (Information) Security Officer (CISO, ISO, SO), Technical Information Security Officer (TISO), Informatiemanager (IM), Data Protection Officer (DPO), Privacy Officer (PO), Privacy & Security Officer (PSO) en Compliance Officer (CO).

De norm ISO/IEC 27001 kent dit soort rollen niet en stelt er dus ook geen eisen aan. U moet ze zelf definiëren door er taken, verantwoordelijkheden en bevoegdheden aan te verbinden. Beheersmaatregel 5.2 zegt dat rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd 'in overeenstemming met de behoeften van de organisatie'. Let daarbij ook op een veilige scheiding van uitvoerende en controlerende taken (zie 5.3).

SECURITY OFFICER

Veel organisaties hebben een *security officer* aangesteld (of een vergelijkbare rol). Zoals gezegd kent de norm ISO/IEC 27001 de rol van deze functionaris niet. Dit betekent dat organisaties met



een security officer zelf taken, verantwoordelijkheden en bevoegdheden aan deze rol moeten toewijzen.

In de praktijk gebeurt het regelmatig dat de security officer veel verantwoordelijkheden krijgt, waaronder het opstellen van beleid en procedures, en het toezicht op de naleving daarvan. Het gevolg van die aanpak kan zijn dat alle klachten, problemen en lastige vragen bij de security officer terecht komen.

Om te voorkomen dat een security officer overbelast raakt en verantwoordelijkheden moet dragen die niet bij de rol thuishoren, kan het helpen om het management van de organisatie in hoge mate zelf verantwoordelijk te maken voor het opstellen van beleid, regels en procedures, en het toezien op de naleving daarvan (zie ook de uitleg bij 5.9).

Bij die aanpak kan de rol van de security officer grotendeels beperkt blijven tot het gevraagd en ongevraagd advies geven aan het management, en tot het beheren van het managementsysteem voor informatiebeveiliging (zie de uitleg in hoofdstuk 2 van dit boek). Dit kan overigens nog steeds een pittige taak zijn.

FUNCTIONARIS GEGEVENSBESCHERMING

EU-organisaties die persoonsgegevens verwerken, zijn in bepaalde situaties verplicht een functionaris voor gegevensbescherming (FG) aan te stellen (Engels: Data Protection Officer, DPO). Raadpleeg de AVG voor meer informatie en details.

GDPR (EU), AVG (NL): Functionaris Gegevensbescherming

AVG artikel 37 zegt:

De functionaris voor gegevensbescherming wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de in artikel 39 bedoelde taken te vervullen.

De functionaris voor gegevensbescherming kan een personeelslid van de verwerkingsverantwoordelijke of de verwerker zijn, of kan de taken op grond van een dienstverleningsovereenkomst verrichten.

De verwerkingsverantwoordelijke of de verwerker maakt de contactgegevens van de functionaris voor gegevensbescherming bekend en deelt die mee aan de toezichthoudende autoriteit.

De FG heeft volgens artikel 39 een informerende en adviserende taak, ziet toe op de naleving van de AVG, adviseert over en ziet toe op het uitvoeren van DPIA's (zie 5.8) en werkt samen met de toezichthoudende autoriteit (zie 5.34).

Tip: de Nederlandse Autoriteit Persoonsgegevens heeft concrete uitgangspunten opgesteld over de informatiepositie van de FG, de middelen die de FG nodig heeft, en de toegang van de FG tot het bestuur van de organisatie [18].

INFORMATIEMANAGER

Grotere organisatie werken soms met een *informatiemanager*. Deze functionaris is doorgaans verantwoordelijk voor het vertalen van informatiebehoeften die ontstaan vanuit werk- en bedrijfsprocessen. Een informatiemanager vertegenwoordigt de gebruikersorganisatie als afnemer van de informatievoorziening en functioneert als opdrachtgever voor de IT-afdeling (of een externe provider). De informatiemanager maakt in de regel geen onderdeel uit van de IT-afdeling.

TOP MANAGEMENT EN MANAGEMENT

Zie de uitleg in dit boek bij beheersmaatregel 5.4: Managementverantwoordelijkheden.

◆ VERANTWOORDELIJKHEDEN BIJ INFORMATIEBEVEILIGING

VERANTWOORDELIJKHEDEN TOEWIJZEN

Een *verantwoordelijkheid* kan omschreven worden als de verplichting om ervoor te zorgen dat iets goed verloopt. Iemand met een verantwoordelijkheid kan worden aangesproken op het resultaat van een aan hem of haar toegewezen taak.

Auditoren die door een organisatie worden gevraagd om een ISO27001-audit te komen uitvoeren, krijgen regelmatig de vraag: 'wie wil je spreken tijdens de audit?' Vanuit de auditor gezien is dit een vreemde vraag, omdat alle rollen en verantwoordelijkheden bij informatiebeveiliging gedefinieerd en toegewezen zouden moeten zijn.

Zorg dat rolbeschrijvingen duidelijk en specifiek zijn over verantwoordelijkheden bij informatiebeveiliging, en dat voor iedereen duidelijk is aan wie rollen zijn toegewezen.

Mogelijk mogen medewerkers aan wie verantwoordelijkheden inzake informatiebeveiliging zijn toegewezen, beveiligingstaken aan anderen delegeren. In dat geval behoren zij te zorgen dat de gedelegeerde taken tijdig, correct en doeltreffend worden uitgevoerd.

Het definiëren en toewijzen van rollen en verantwoordelijkheden is ook noodzakelijk om als organisatie te kunnen bepalen welke toegangsrechten aan rollen moeten worden toegekend, ervan

uitgaande dat medewerkers niet meer rechten hoeven te krijgen dan nodig voor het uitoefenen van hun rol (zie ook 5.15).

Let op:

Je zou kunnen stellen dat *alle medewerkers* van uw organisatie een verantwoordelijkheid hebben bij informatiebeveiliging. Dit mag waar zijn, toch gaat het bij beheersmaatregel 5.2 vooral om het toewijzen van *specifieke rollen* bij informatiebeveiliging.

Voor medewerkers die geen specifieke rol hebben bij informatiebeveiliging, is het van belang dat ze regelmatig een passende bewustwording van, opleiding, training en bijscholing in informatiebeveiliging krijgen, voor zover relevant voor hun functie (zie 6.3). Ook is belangrijk dat ze zich houden aan algemene gedragsregels, zoals de regels voor het aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen (zie 5.10).

CONTROL OWNERS (EIGENAREN VAN BEHEERSMAATREGELEN)

Beheersmaatregel 5.2 zegt dat rollen en verantwoordelijkheden bij informatiebeveiliging moeten passen bij de behoefte van de organisatie. Veel organisaties komen erachter dat ze behoefte hebben aan *control owners*. Maar laten we eerst beginnen met *risicoeigenaren*.

ISMS-normelement 6.1.2 eist dat er voor elk geïdentificeerd risico een risicoeigenaar wordt aangesteld. De organisatie ISO/IEC hanteert de volgende definitie van een risicoeigenaar [1]:

> *Een risicoeigenaar is de persoon of entiteit met de verantwoordelijkheid en bevoegdheid om een risico te beheersen.*

Voor het beheersen van een risico kunnen één of meer beheersmaatregelen worden geïmplementeerd (Engels: controls). Zoals uitgelegd in hoofdstuk 4 is een control elke vorm van proces, beleid, voorziening, werkwijze, of andere omstandigheid of maatregel, waarmee het risico kan worden beheerst. Volgens ISMS-normelement 6.1.3 moet een eigenaar van een risico akkoord gaan met het plan om het risico met de geselecteerde controls te behandelen.

Nadat een control is geïmplementeerd, zal iemand moeten zorgen dat de control effectief blijft. Worden toegangsrechten nog steeds op tijd ingetrokken? Vindt het screenen van kandidaten voor een positie binnen de organisatie nog steeds plaats volgens de regels? Worden leveranciers nog steeds regelmatig beoordeeld? Indien de effectiviteit van een control afneemt, kan een risico onaanvaardbaar hoog worden, en kunnen er incidenten optreden.

Een control owner is een persoon of entiteit met de verantwoordelijkheid en bevoegdheid om te zorgen dat een control effectief blijft. Meestal worden leidinggevenden aangesteld als control owners. Indien gewenst kunnen zij bepaalde taken delegeren, maar ze blijven verantwoordelijk.

Het werken met control owners is niet verplicht, maar in veel opzichten een logische stap, en daarom het overwegen waard. Gaat u met control owners werken? Zorg dan dat duidelijke verantwoordelijkheden worden gedefinieerd, en dat ze aan geschikte personen worden toegewezen.

Het werken met control owners vereenvoudigd ook het monitoren en auditen van controls (zie ISMS-normelement 9.1 en 9.2).

➢ *In dit handboek zijn bij alle 93 beheersmaatregelen auditvragen opgenomen. Een van de terugkerende vragen is of de benodigde rollen en verantwoordelijkheden zijn gedefinieerd en toewezen voor het implementeren en onderhouden van de beheersmaatregel. Elke onduidelijkheid hierover kan de doeltreffendheid van de beheermaatregelen sterk verminderen. In die zin is beheersmaatregel 5.2 een van de belangrijkste beheersmaatregelen bij het implementeren van een managementsysteem voor informatiebeveiliging.*

INFORMATIEBEVEILIGINGSMANAGEMENTFORUM (IBMF)

Verantwoordelijkheden bij informatiebeveiliging kunnen niet alleen worden toegewezen aan personen, maar ook aan teams.

Voorbeeld

De security officer (SO) van een organisatie met meerdere vestigingen rapporteert rechtstreeks aan het top management. De SO werkt samen met de volgende personen die een belangrijke rol spelen bij informatiebeveiliging: hoofd HR, hoofd facilitaire zaken, hoofd inkoop, hoofd ICT, een ICT-specialist, privacy officer, compliance officer en informatiemanager.

Vanwege de omvang van de organisatie en het belang van samenwerking, besluit de SO om met de genoemde personen een informatiebeveiligingsmanagementforum (IBMF) op te richten. Het forum komt maandelijks bij elkaar en rapporteert als geheel aan het top management.

Onder leiding van de SO richt het forum zich onder andere op het bespreken van incidenten, de voortgang van beveiligingsinitiatieven, de uitkomsten van audits, het monitoren van geplande ISMS-acties en het bewaken van ISMS-KPI's.

➢ *Nederlandse organisaties die met de NEN 7510 werken, zullen in dit voorbeeld het 'informatiebeveiligingsmanagementforum (IBMF)' herkennen dat in deze norm wordt genoemd.*

■ Toepasselijkheid

Om de toepasselijkheid van beheersmaatregel 5.2 te bepalen, moet uw organisatie de kans beoordelen dat er informatiebeveiligingsincidenten optreden doordat noodzakelijke acties niet, niet goed, of niet op tijd worden uitgevoerd, door onduidelijkheden over verantwoordelijkheden.

Indien u een beveiligingstaak (gedeeltelijk) laat uitvoeren door een externe partij, dan blijft u eindverantwoordelijk voor deze activiteit. Zorg indien nodig voor passende afspraken (zie 5.20) en voor het monitoren van de naleving daarvan (zie 5.22).

■ Aanwijzingen voor het uitvoeren van audits

Bij deze beheersmaatregel zou een auditor het volgende kunnen onderzoeken:

TOEPASSING

- Waarom heeft de organisatie deze beheersmaatregel toegepast? Overweeg het raadplegen van de rechtvaardiging in de Verklaring van Toepasselijkheid.

- Deze beheersmaatregel gaat over *rollen en verantwoordelijkheden bij informatiebeveiliging*. Welke rollen en verantwoordelijkheden zijn op dit moment belangrijk voor de organisatie?

IMPLEMENTATIE

- Heeft de organisatie rollen voor informatiebeveiliging gedefinieerd en toegewezen? Heeft de organisatie verantwoordelijkheden bij informatiebeveiliging aan deze rollen verbonden?
- Zijn de rollen en verantwoordelijkheden zodanig gedefinieerd en toegewezen dat er geen onduidelijkheid kan bestaan over de vraag wie het geïmplementeerde managementsysteem en de geïmplementeerde beheersmaatregelen moeten onderhouden?
- Zijn mensen en teams zich in voldoende mate bewust van de aan hen toegewezen verantwoordelijkheden, taken en bevoegdheden bij informatiebeveiliging? Overweeg het afnemen van enkele interviews om dit verder te onderzoeken.

BEHEERSING

- Hoe heeft de organisatie gewaarborgd dat alle noodzakelijke rollen bij informatiebeveiliging vervuld blijven? Denk aan een medewerker die de organisatie verlaat, of een reorganisatie van rollen en verantwoordelijkheden. Zijn alle benodigde rollen op dit moment vervuld?

CONCLUSIE

- Bepaal op basis van de resultaten van het uitgevoerde onderzoek of deze beheersmaatregel doeltreffend, volgens de eisen van de norm, en volgens de eigen eisen van de organisatie is geïmplementeerd (zie ISMS-normelement 9.2.1).

5.3 Functiescheiding

Segregation of duties

■ Wat vraagt deze beheersmaatregel?

Om conformiteit met beheersmaatregel 5.3 te mogen claimen, moet uw organisatie het volgende hebben gerealiseerd [4]:

- Conflicterende taken en verantwoordelijkheden zijn gescheiden.

■ Waar gaat deze beheersmaatregel over?

BEGRIP: FUNCTIESCHEIDING

Functiescheiding (Engels: Segregation of duties, SoD) is een interne beheersmaatregel die is bedoeld om fouten en fraude te voorkomen door ervoor te zorgen dat minimaal twee personen verantwoordelijk zijn voor de afzonderlijke onderdelen van een functie. De implementatierichtlijn zegt over het doel van deze beheersmaatregel [6]:

> *Het risico op fraude, fouten en het omzeilen van beheersmaatregelen voor informatiebeveiliging verminderen.*

Hoewel iedereen er van overtuigd is dat functiescheiding belangrijk is, zijn er vaak allerlei organisatorische en praktische bezwaren die functiescheiding lastig maken.

FUNCTIESCHEIDING BIJ INFORMATIEBEVEILIGING

Bij het definiëren en toewijzen van rollen en verantwoordelijkheden die relevant zijn voor uw informatiebeveiliging (zie 5.2) kan een risico optreden. Op basis van het toegewezen takenpakket zou een medewerker een verzameling rechten en bevoegdheden kunnen ontvangen die deze persoon een onverantwoorde hoeveelheid macht en mogelijkheden verschaft.

Functiescheiding in IT-functies

Functiescheiding is vooral bekend in de financiële wereld. Daar gaat het bijvoorbeeld om het voorkomen van een situatie waarbij iemand als administrateur (controlerend) procuratie heeft (beschikking tot betalen) en tevens fungeert als kassier (bewarend). Of waarbij de kassier ondergeschikt is aan de administrateur.

Het concept van functiescheiding werd relevanter voor IT-organisaties toen regelgevende mandaten zoals de Gramm-Leach-Bliley Act (GLBA, 1999) en Sarbanes-Oxley (SOX, 2002) werden ingevoerd. Dit dwong IT-organisaties om meer nadruk te leggen op functiescheiding in IT-functies.

Binnen de context van informatiebeveiliging is functiescheiding vooral van belang om het risico op fraude, (onontdekte) fouten, sabotage, programmeerinefficiënties en andere soortgelijke risico's

te verkleinen. U dient deze risico's te onderzoeken, en waar nodig taken en verantwoordelijkheden anders te verdelen om een betere functiescheiding te krijgen. Hier zijn enkele voorbeelden van situaties waarbij scheiding van taken van belang kan zijn in een organisatie:

Financiële autorisatie: De persoon die verantwoordelijk is voor het goedkeuren van financiële transacties moet gescheiden zijn van degene die verantwoordelijk is voor het uitvoeren van deze transacties, zelfs binnen geautomatiseerde systemen.

IT-taken versus business-taken: De meest basale scheiding is een scheiding tussen de taken van IT en de taken van de business. Van gebruikersafdelingen wordt verwacht dat ze eisen stellen aan systemen en applicaties, en dat ze een kwaliteitsborgingsfunctie bieden tijdens de testfase. Het grootste deel van de IT-functie zou echter gescheiden moeten worden van de business. Dit betekent dat de business niet haar eigen beveiligingstaken, programmeertaken en andere kritieke IT-taken uitvoert. Door kritieke IT-taken te combineren met gebruikersafdelingen, vergroot u het risico op fouten, fraude en sabotage.

Toegangsbeheer: Het proces van gebruikersauthenticatie moet gescheiden zijn van het proces van het toekennen van toegangsrechten. De persoon die verantwoordelijk is voor het aanmaken van gebruikersaccounts moet niet ook de bevoegdheid hebben om toegangsrechten toe te kennen.

Ontwikkeling en productie: Het team dat verantwoordelijk is voor het ontwikkelen van software moet gescheiden zijn van het team dat verantwoordelijk is voor het implementeren en onderhouden van de productieomgeving. Dit minimaliseert het risico van ongeautoriseerde wijzigingen in de operationele omgeving.

Audit en compliance: Degene die verantwoordelijk is voor het uitvoeren van interne audits moet niet direct betrokken zijn bij de processen die worden onderzocht. Dit waarborgt objectiviteit en voorkomt belangenconflicten.

Back-up en herstel: Voorbeeld: Het beheer van back-ups moet worden gescheiden van het beheer van de productiegegevens. Dit voorkomt manipulatie van back-ups en verhoogt de betrouwbaarheid van het herstelproces.

Incident response: Het team dat belast is met het identificeren en mitigeren van beveiligingsincidenten moet onafhankelijk zijn van de teams die verantwoordelijk zijn voor het dagelijkse beheer van systemen. Dit minimaliseert de kans op verdoezeling van incidenten.

Change management: Het proces van het indienen en goedkeuren van wijzigingsverzoeken moet gescheiden zijn van de daadwerkelijke implementatie van veranderingen. Dit voorkomt ongeautoriseerde of onbedoelde wijzigingen.

Databasebeheerder: De databasebeheerder (Engels: database administrator, DBA) is een kritieke functie die een hoog niveau van functiescheiding vereist. De DBA weet (bijna) alles van de gegevens, de databasestructuur en het databasebeheersysteem. Deze beheerder heeft dus het inherente vermogen om toegang te krijgen tot alles, alles te wijzigen en alles te verwijderen. Vanwege het risiconiveau kiezen veel organisaties ervoor om DBA's te scheiden van alles, behalve van wat ze nodig hebben om hun taken uit te voeren, zoals het ontwerpen van databases, het beheren van de database als technologie, het bewaken van het databasegebruik en de prestaties.