Baseline Informatie-beveiliging Overheid (BIO)

gebaseerd op de ISO 27002:2022

Barry Derksen
Nico Kaag

Van Haren PUBLISHING

Certified BIO Professional

Baseline Informatiebeveiliging Overheid (BIO) gebaseerd op de ISO 27002:2022

Andere uitgaven bij Van Haren Publishing

Van Haren Publishing (VHP) is gespecialiseerd in uitgaven over Best Practices, methodes en standaarden op het gebied van de volgende domeinen:

- IT en IT-management;
- Enterprise-architectuur;
- Projectmanagement;
- Businessmanagement.

Deze uitgaven zijn beschikbaar in meerdere talen en maken deel uit van toonaangevende series, zoals *Best Practice, The Open Group series, Project management* en *PM series.*

Van Haren Publishing is tevens de uitgever voor toonaangevende instellingen en bedrijven, onder andere: Agile Consortium, ASL BiSL Foundation, CA, Centre Henri Tudor, CM Partners, Gaming Works, IACCM, IAOP, IPMA-NL, ITSqc, NAF, KNVI, PMI-NL, PON, The Open Group, The SOX Institute.

Onderwerpen per domein zijn:

IT en IT-management
ABC of ICT
ASL®
CMMI®
COBIT®
e-CF
ISM
ISO/IEC 20000
ISO/IEC 27001/27002
ISPL
IT4IT®
IT-CMF™
IT Service CMM
ITIL®
MOF
MSF
SABSA
SAF
SIAM™
TRIM
VeriSM
XLA®

Enterprise-architectuur
ArchiMate®
BIAN
GEA®
Novius Architectuur Methode
TOGAF®

Projectmanagement
A4-Projectmanagement
DSDM/Atern
ICB / NCB
ISO 21500
MINCE®
M_o_R®
MSP®
P3O®
PMBOK® Guide
Praxis®
PRINCE2®

Businessmanagement
BABOK® Guide
BiSL® en BiSL® Next
BRMBOK™
BTF
CATS CM®
DID®
EFQM
eSCM
FSM
IACCM
ISA-95
ISO 9000/9001
OBM
OPBOK
SixSigma
SOX
SqEME®

Voor een compleet overzicht van alle uitgaven, ga naar onze website: www.vanharen.net

Baseline Informatiebeveiliging Overheid (BIO) gebaseerd op de ISO 27002:2022

Barry Derksen
Nico Kaag

Van Haren PUBLISHING

Colofon

Titel:	Baseline Informatiebeveiliging Overheid (BIO) gebaseerd op de ISO 27002:2022
Auteurs:	Barry Derksen, Nico Kaag
Uitgever:	Van Haren Publishing, 's-Hertogenbosch, www.vanharen.net
ISBN Hard copy:	978 94 018 1045 6
ISBN eBook (pdf):	978 94 018 1046 3
ISBN ePub:	978 94 018 1047 0
Uitgave:	Eerste druk, eerste oplage, juli 2023
Lay-out en dtp:	Coco Bookmedia, Amersfoort

Voorwoord Ronald Verbeek

Of we nu kijken naar overheidsprocessen en -diensten, productieketens of dienstverlening in het bedrijfsleven, of de persoonlijke contacten die we onderhouden, het is evident dat digitale technologie en connectiviteit is doorgedrongen in vrijwel alle aspecten van onze werkomgeving en sociale leven. Dat brengt naast gemak, economische kansen en grote hoeveelheden data, ook risico's met zich mee.

We zijn zó afhankelijk geworden van digitale technologie en de daarin verwerkte data, dat er bijna geen alternatieven zijn als een keer de server uitvalt, de clouddienst niet bereikbaar is of de data door kwaadwillende is versleuteld. Dan ligt alles stil. Nog vervelender kan het zijn als onze processen plaatsvinden met – moedwillig of per ongeluk - vervormde data en als gevolg daarvan ten onrechte beslag wordt gelegd op vermogen, of een verkeerde medische handeling wordt uitgevoerd. Bovendien is het terecht komen van informatie op verkeerde plaatsen over het algemeen ook niet wenselijk, mogelijk zelfs gevaarlijk of strafbaar. Bij het lekken van financiële gegevens bijvoorbeeld.

Daarbij komt dat, vanwege de verwevenheid en complexiteit van digitale systemen enerzijds en de professionalisering van cybercriminelen en de toenemende dreiging van statelijke actoren anderzijds, de risico's toenemen. Kortom, het is van het grootste belang voor elke organisatie om aandacht te hebben voor de 3-eenheid van informatiebeveiliging: beschikbaarheid, integriteit en vertrouwelijkheid.

In de maatschappij en in de politiek is er bovendien een toenemende verwachting dat de beschikbaarheid, integriteit en vertrouwelijkheid van informatie(systemen) actief aandacht krijgen. Aandacht in de vorm van goede preventieve maatregelen, een verantwoord niveau van investeringen en het monitoren en melden van incidenten. De verantwoordelijkheid hiervoor wordt steeds vaker belegd bij bestuurders. Dat is in mijn ogen op zichzelf een goede zaak.

Maar hoe weet je dan als bestuurder wat noodzakelijk en wenselijk is in het specifieke geval van jouw organisatie? En hoe weet je als informatiebeveiliger dat je jouw bestuurder voldoende informatie geeft om de goede afwegingen te kunnen

maken? Een informatiebeveiligingsstandaard geeft dan houvast. Met de nieuwe versie van de Baseline Informatiebeveiliging Overheid (BIO), wordt zo'n geactualiseerde standaard gezet, inclusief een minimale norm.

In dit boek wordt de BIO uitgebreid toegelicht en wordt achtergrondinformatie gegeven over standaarden, normen en ontwikkelingen in de technologie. Het geeft inzicht en context. Dat maakt het gesprek tussen verantwoordelijke bestuurder en informatiebeveiliger gemakkelijker. Voer dat gesprek en beveilig jouw informatie(systemen)!

Ronald Verbeek
Directeur CIO Platform Nederland

Inhoudsopgave

Inleiding

Informatiebeveiliging, best belangrijk!

Dit boek maakt onderdeel uit van het BIO trainingsmateriaal. Het boek is verplichte literatuur voor de het BIO examen[1].
Wij leven in een bijzondere tijd. In een periode waar techneuten de markt bepalen, zijn van de tien grootste bedrijven ter wereld er maar liefst acht IT-bedrijven die groot zijn gemaakt door de 'techies' van deze wereld. Hierbij kan worden gedacht aan Elon Musk (Tesla), Mark Zuckerberg (Meta) en de eerdere Steve Jobs (Apple) en Bill Gates (Microsoft).
Maar met de komst van nieuwe technologische mogelijkheden die deze bedrijven en vele anderen bieden (denk ook aan ChatGPT (OpenAI.com) groeien ook de risico's. Voor elke nieuwe functionaliteit of mogelijkheid is ook een misbruik case te bedenken of een cyber bedreiging. Daarnaast genereren de nieuwe stukken software ook weer nieuwe vulnerabilities (zwakheden) die worden misbruikt door hackers of anderen.

Dit kan fysiek zijn, denk bijvoorbeeld aan het moment dat zelfrijdende auto's volledig zelfrijdend zijn. Een terrorist kan de auto dan gebruiken als zelfrijdende bom. Dichterbij zijn echter de vragen van politiek internationale aard zoals het gebruik van TikTok of de dagelijkse binnenkomende zwakheden in de software (altijd updaten (patchen)) of de aangeklikte phishing link door een medewerker. Informatiebeveiliging is dus best belangrijk.

Dit boek gaat over informatiebeveiliging en maakt hierbij gebruik van de *Baseline Informatiebeveiliging Overheid* (BIO) welke gebaseerd is op de internationale standaard ISO27001:2022. In de eerste twee delen van dit boek wordt hier verder op ingegaan. In het derde deel wordt ingegaan op de ontwikkelingen en trends die effect hebben en gaan hebben op informatiebeveiliging, immers vooruitzien is regeren.

1 Voor meer informatie: https://www.vanharen.store/cbp-certified-bio-professional-baseline-informatiebeveiliging-overheid-exam#filter_format=5721

Dit boek geeft in elk geval voldoende handvatten om de eigen (overheid)organisatie veiliger te maken en om vooruit te zien en te regeren.

Veel leesplezier!

DEEL I KENNISMAKING MET BIO

1. INTRODUCTIE BASELINE INFORMATIEBEVEILIGING OVERHEID

1.1 INLEIDING

In oktober 2022 is de nieuwe informatiebeveiligingsstandaard ISO27001:2022 *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* uitgekomen zoals vastgesteld door de International Standard Organisation. De voorgaande versie (ISO27001:2017) was de basis voor de Baseline Informatiebeveiliging Overheid (BIO) zoals vastgesteld door de Ministerraad voor de Rijksoverheid in december 2018. Tijd dus om ook de BIO te voorzien van de meest recente inzichten gebruik makend van zowel de nieuwe ISO-standaard als ook de ontwikkelingen in de markt. Dit boek gaat in op de BIO die is gebaseerd op de ISO27001:2022 en op de ISO27002:2022.

De BIO vormt het kader voor informatiebeveiliging binnen de overheid. Dit betreft niet alleen het rijk maar ook gemeenten, provincies en andere overheidslagen. Door het gebruik van de BIO als het normenkader voor de gehele overheid is er duidelijkheid over de vereiste of benodigde basisinformatiebeveiliging bij de overheid zelf als ook bij leveranciers, afnemers en andere stakeholders. Het hebben van deze uniforme standaarden in informatiebeveiliging zorgt voor een lastenverlichting, betere vergelijkbaarheid, lagere onderhoudskosten en voor betere afstemming bij overheidsketens. In dit boek gaan wij in op de standaarden in informatiebeveiliging op basis van de BIO.

De BIO is gebaseerd op de ISO27001 (alsook de standaard ISO27002); deze ISO-standaarden zijn geplaatst op de lijst waarbij geldt 'pas toe of leg uit'[2]. Daarbij wordt ook ingegaan op de verhouding van de BIO met de ISO-standaarden. Afwijkend is dat de BIO specifieke beheersmaatregelen kent waarbij overheidsmaatregelen nader worden ingevuld. Dat het niet alleen bij maatregelen binnen de overheid zelf blijft blijkt ook uit de in 2022 uitgekomen Cyber Resilience Act[3] (CRA) van de

2 https://www.forumstandaardisatie.nl/open-standaarden/nen-isoiec-27002
3 https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

Europese Unie. Op basis van deze voorstellen voor regulering van informatiebeveiliging zullen leveranciers aan een aantal standaarden moeten voldoen. Daarbij zal 'security by design' (beveiliging al vanaf ontwerp) de standaard zijn wat voordelen biedt voor zowel overheden als burgers als anderen. De auteurs zijn voorstander van deze regelgeving. In dit boek zullen wij ook nader ingaan op de CRA en wat dit bijvoorbeeld betekent voor nieuwe ontwikkelmethoden als Scrum en agile.

In dit eerste deel van dit boek wordt de achtergrond van informatiebeveiliging in het algemeen en de BIO in het bijzonder weergegeven. Eerst behandelen we de internationale standaard (ISO27001:2022) en daarbij vooral het managementsysteem. Vervolgens gaan we in op de beheersmaatregelen van ISO (ISO27002:2022). Gebaseerd daarop kijken wij naar de belangrijkste verschuivingen die de nieuwe versie van de internationale standaard heeft voor de BIO. Daarna wordt dieper ingegaan op de BIO.

1.2 INFORMATIEBEVEILIGINGSKADERS EN UITGANGSPUNTEN OVERHEID

In de *Staatscourant van het Koninkrijk der Nederlanden*[4] is op 11 februari 2020 het geactualiseerde kader over informatiebeveiliging gepubliceerd. Hierbij zijn de beveiligingsniveaus niet veranderd. In de *Staatscourant* staat dat de BIO is:

- een gemeenschappelijk (normen)kader, gebaseerd op de internationale standaarden ISO27001 en ISO27002 voor de beveiliging van informatie(systemen) van de overheid.
- Een concretisering van een aantal standaarden naar concrete maatregelen die verplicht door alle bestuurslagen moeten worden nageleefd.

De verwachting is dat de implementatie van de BIO een eigen verantwoordelijkheid is van de diverse overheidsorganisaties zelf.

Een belangrijk uitgangspunt is het risico-gebaseerd denken. De overheid past risicomanagement toe om zo de juiste keuzes te maken voor maatregelen en het realiseren van de juiste mate van beveiliging. Dit betekent dat overheidsorganisaties eveneens dienen te bepalen welke mate van risico is geaccepteerd. Daarnaast is het in de meeste gevallen zo dat een hogere mate van beveiliging een hogere mate van kosten met zich meebrengt. Met de overheidsdoelstelling is het dan ook van belang om niet iets met een waarde van tien cent met een euro te beveiligen aangezien dat ten koste gaat van de maatschappelijke of overheidsdoelstelling. In deel III wordt nader ingegaan op risicomanagement en risico frameworks.

4 https://zoek.officielebekendmakingen.nl/stcrt-2020-7857.html

Een tweede belangrijke uitgangspunt is het realiseren, implementeren en onderhouden van een informatiebeveiligingsmanagementsysteem. Dit is een strategische keuze voor een overheidsorganisatie. Het realiseren van een Information Security Management System (ISMS) is in de eerste versie van de BIO bekend als het inrichten van een PDCA-cyclus (Plan-Do-Check-Act). Een nadere specificatie bestaat voor de rijksoverheid in de algemene voorschriften[5] voor de beveiliging van informatiesystemen.
Een ISMS is gericht op het vorm geven aan de informatiekenmerken Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) door het toepassen van een risicomanagementproces. Door het toepassen hiervan kan aan de (keten)partners van de overheid het vertrouwen worden geboden dat risico's afdoende worden beheerd.
Een ISMS dient integraal onderdeel te zijn van de processen binnen een overheidsorganisatie en haar bestuurlijke structuur. Informatiebeveiliging moet daarmee onderdeel zijn van het ontwerp van de (overheids)processen, informatiesystemen en de beheersmaatregelen.

Ten derde is het management verantwoordelijk voor de beveiliging van de informatie(systemen) wat in lijn met het ISMS een reguliere (tenminste jaarlijks) management-review vereist. Hiermee bevestigt het management of bestuur de eindverantwoordelijkheid. Daarnaast bevestigt dit het cyclische karakter van het ISMS, alsook van de PDCA-cyclus.

Het operationeel management stelt de betrouwbaarheidseisen vast voor de (informatie)systemen. Dit doet zij aan de hand van een expliciete risicoafweging. Hierbij wordt een ruime definitie voor een (informatie)systeem gehanteerd[6]:
"Een informatiesysteem is een samenhangend geheel van gegevensverzamelingen, de daarbij behorende personen, processen en programmatuur als ook de voor het (informatie)systeem getroffen voorzieningen als opslag, verwerking en communicatie."

Als vierde uitgangspunt van de BIO wordt uitgegaan van drie Basis Beveiligings-Niveaus (BBN's). Elk niveau kent een aantal verplichte overheidsmaatregelen en de daarbij behorende verantwoording en toezicht. Deze drie niveaus (BBN1, BBN2 en BBN3) worden in paragraaf 6.6 tot en met 6.8 nader toegelicht.

Voordat we ingaan op de BIO behandelen wij eerst kort de nieuwe versies van de ISO-standaarden ISO27001:2022 en ISO27002:2022 waarop de BIO is gebaseerd. Daarnaast gaan wij kort in op het NIST Cyber Security Framework, het informatiebeveiligingsframework van het National Institute for Standards and Technology uit de

5 https://wetten.overheid.nl/BWBR0022141/2007-07-01
6 https://www.noraonline.nl/wiki/Informatiesysteem

Verenigde Staten. Dit is relevant omdat in Europees verband deze geregeld wordt gehanteerd zoals door de Europese Centrale Bank. Zo heeft De Nederlandsche Bank een informatiebeveiligingsbeleid opgesteld in lijn met de internationale standaarden zoals de ISO27001/2 en het NIST CSF[7].

7 https://www.dnb.nl/media/oabls2bx/good-practice-ib-2019-2020-nl.pdf

2. ISO27001:2022 – HET MANAGEMENTSYSTEEM

2.1 INLEIDING EN GESCHIEDENIS

De ISO27001:2022 is alweer de derde versie van de ISO-standaard en vervangt daarmee de eerdere versie die dateert uit 2013. Kern van de ISO27001 is het ISMS (Information Security Management System). De ISO27001 kent vereisten voor het realiseren, implementeren en onderhouden van het ISMS.
De nieuwe versie kent een aantal veranderingen ten opzichte van de vorige versie; de belangrijkste zijn:

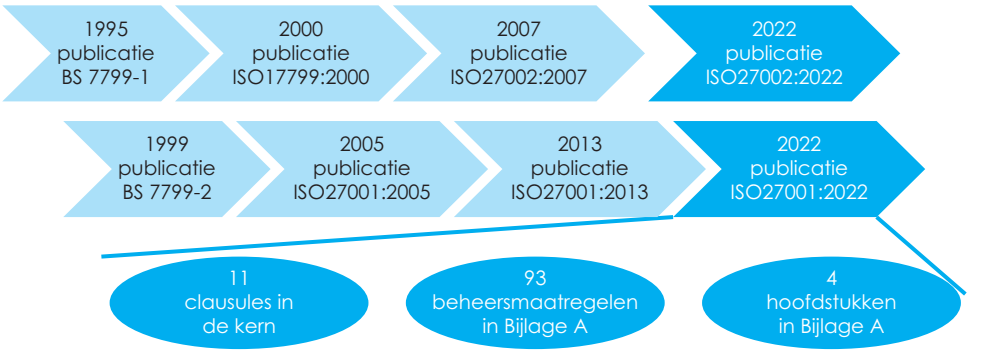
- In de kern van de ISO27001 is een beperkt aantal wijzigingen in de diverse clausules doorgevoerd.
- Het aantal beheersmaatregelen is teruggebracht van 114 tot 93.
- Er worden 11 nieuwe beheersmaatregelen gedefinieerd. Er zijn overigens geen beheersmaatregelen verwijderd, maar zijn er diverse samengevoegd.
- De beheersmaatregelen zijn onderverdeeld in vier hoofdstukken, dit waren in de vorige versie 14 hoofdstukken.

De voorgeschiedenis en belangrijkste wijzigingen van de ISO27001/2 worden in figuur 1 visueel weergegeven.

Bedrijven die de ISO27001/2 hanteren dienen uiterlijk 31 oktober 2025 de transitie naar de nieuwe versie (versie 2022) te hebben afgerond. Tot 31 oktober 2023 kunnen organisaties nog gecertificeerd worden aan de hand van de 2013-versie.

De tekst van de verplichte clausules 4 tot en met 10 is beperkt gewijzigd. Een van de belangrijkste redenen van de wijzigingen is een grotere overeenkomst realiseren met de ISO 9001 en de andere managemenstandaarden van ISO. Meer gedetailleerd bestaan de wijzigingen in de ISO 27001:2022 uit:

- In punt 4.2 (Inzicht in de behoeften en verwachtingen van belanghebbenden) is punt c) toegevoegd, dat een analyse vereist van de vraag welke van de vereisten van de belanghebbende partijen via het ISMS moet worden aangepakt.



	Nieuwe vereisten in ISO27001
4.2c	Vereisten van stakeholders worden geadresseerd via het IBMS
6.3	Planning van veranderingen
8.1	Bepalen criteria voor processen en implementeren beheersmaatregelen hiervoor
9.3.2c	Management review - veranderingen in benodigdheden en vereisten van stakeholders.

	Wijzigingen in Bijlage A
Groot	11 nieuwe beheersmaatregelen
Middel	57 samengevoegde en 1 gesplitste beheersmaatregel
Klein	23 beheersmaatregelen herbenoemd
Geen verandering	35 beheersmaatregelen zijn niet veranderd

Figuur 1 Veranderingen in de ISO27001/2:2022 ten opzichte van de 2013-versie samengevat

- In paragraaf 4.4 (Informatiebeveiligingsbeheersysteem) is een zin toegevoegd die een planning vereist voor processen en hun interacties als onderdeel van het ISMS.
- In paragraaf 5.3 (Organisatorische rollen, verantwoordelijkheden en autoriteiten) is een zin toegevoegd om te verduidelijken dat communicatie van rollen intern binnen de organisatie plaatsvindt.
- In paragraaf 6.2 (Informatiebeveiligingsdoelstellingen en planning om deze te bereiken) is punt d) toegevoegd dat vereist dat doelstellingen worden gemonitord.
- Clausule 6.3 (Planning van wijzigingen) werd toegevoegd, die vereist dat elke wijziging in het ISMS op een geplande manier moet worden uitgevoerd.
- In paragraaf 7.4 (Communicatie) werd punt e) geschrapt, waarvoor het instellen van communicatieprocessen noodzakelijk was.
- In punt 8.1 (Operationele planning en controle) zijn nieuwe eisen toegevoegd voor het vaststellen van criteria voor beveiligingsprocessen en voor het implementeren van processen volgens die criteria. In dezelfde clausule werd de verplichting om plannen uit te voeren om doelstellingen te bereiken geschrapt.
- In punt 9.3 (Management evaluatie/review) is het nieuwe item 9.3.2 c) toegevoegd dat verduidelijkt dat input van belanghebbenden moet gaan over hun behoeften en verwachtingen, en dat deze relevant is voor het ISMS.
- In artikel 10 (Verbetering) zijn de lidparagrafen van plaats veranderd, dus de eerste is Voortdurende verbetering (10.1) en de tweede is Non-conformiteit en corrigerende actie (10.2), terwijl de tekst van die clausules niet is gewijzigd.

Een belangrijk verschil tussen de ISO27001 en de BIO is dat de BIO vooral over de beheersmaatregelen gaat zoals die worden weergegeven in de Bijlage A van de ISO27001. De Bijlage A van de ISO27001 kent de nadere uitwerking van de beheersmaatregelen in de ISO27002. Een ander belangrijk verschil dat de BIO aanvullende maatregelen vereist welke overheidsgericht zijn. Wij willen het belang van een ISMS benadrukken. Het hebben van een ISMS is van cruciaal belang om informatiebeveiliging blijvend te besturen, beheersen en continu te verbeteren. In paragraaf 2.2 zal daarom ook worden ingegaan op de inrichting van een ISMS, rekening houdend met de BIO.

2.2 INFORMATION SECURITY MANAGEMENT SYSTEM

Als eerder aangegeven is een ISMS een cruciaal element van goede (informatie) beveiliging. Daarom wordt in deze paragraaf ingegaan op de betekenis van een ISMS, de redenen voor toepassing en de relatie met de PDCA-cyclus. Een ISMS dient volgens ons integraal onderdeel te zijn van de processen binnen een overheidsorganisatie en de bestuurlijke structuur. Informatiebeveiliging moet daarmee onderdeel zijn van het ontwerp van de (overheids-) processen, informatiesystemen en de beheersmaatregelen. Het woord 'systeem' refereert in dit verband dus nadrukkelijk naar een managementinstrument om de (informatie) beveiliging te realiseren, beheren en besturen.

Een ISMS is gericht op het vorm geven aan de informatiekenmerken Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) door het toepassen van een risicomanagementproces. Door het toepassen hiervan kan aan de (keten)partners van de overheid het vertrouwen worden geboden dat risico's afdoende worden beheerd.

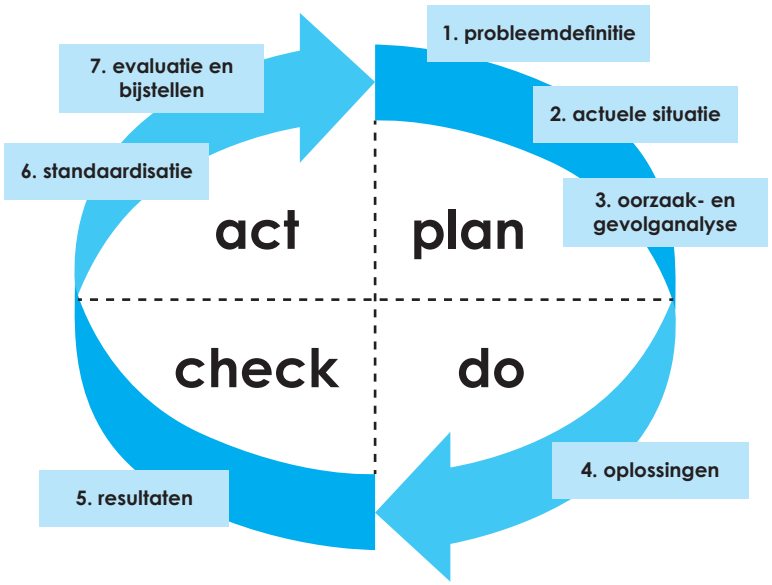
Bij een goed ingericht ISMS is risicomanagement een belangrijk uitgangspunt. Een ISMS wordt dan ook gehanteerd om:

- Overzicht, structuur en een beheermechanisme voor informatiebeveiliging te behouden.
- Sturing te geven aan de PDCA-cyclus en de planning daarvan.
- Continue verbetering over (informatie) beveiliging te realiseren.
- Aansluiting met wetgeving en normenkaders eenvoudiger te realiseren.
- Effectiviteit en efficiency te realiseren voor informatiebeveiliging.

Een belangrijk kenmerk van een ISMS is de PDCA-cyclus voor continue verbetering. Om die reden wordt de PDCA-cyclus hierna nader toegelicht.

2.3 PLAN-DO-CHECK-ACT

De PDCA-cyclus is een methode gericht op het continu verbeteren. In het kader van het adagium 'trends komen en gaan maar goede concepten blijven bestaan' verdient de PDCA-cyclus een lofzang. De PDCA-cyclus staat ook bekend als de Deming-cirkel welke in de jaren '50 van de 20ste eeuw is ontwikkeld door de Amerikaan dr. W.E. Deming[8].



Figuur 2 PDCA-cyclus[9] (bron: T.W. den Hoed[10])

Kenmerkend aan de PDCA-cyclus is dat er geen einde is. Na de besluitvorming van 'Act' wordt er opnieuw gepland. Hiermee ontstaat de continue verbetercyclus. In de eerste fase vindt de plan-fase plaats. Daarbij wordt een probleemdefinitie weergegeven, een analyse uitgevoerd op de actuele situatie, gevolgd door een oorzaak- en gevolganalyse. Voor deze eerste drie stappen zijn diverse additionele technieken beschikbaar vanuit de theorie van kwaliteitsmanagement zoals bijvoorbeeld het Ishikawa visgraatdiagram[11] voor oorzaak- en gevolganalyse.

In de tweede fase, de Do-fase, worden de oplossingen geïmplementeerd om in de derde fase, de Check-fase te controleren of het in de Plan- en Do fasen beoogde effect is gerealiseerd. In de vierde fase, de Act-fase, kunnen de afwijkingen van het

8 *Deming, W. Edwards (1986).* Out of the crisis. *Cambridge, MA: Massachusetts Institute of Technology, Center for Advanced Engineering Study. p 88 ISBN 978-0911379013.*
9 Bron: https://managementmodellensite.nl/pdca-cyclus/
10 Bron: T.W. den Hoed, *Handboek Managementmodellen, een praktisch overzicht van de meest gebruikte modellen.*, 15 november 2013
11 Ishikawa, Kaoru (1976). *Guide to Quality Control.* Asian Productivity Organization. ISBN 92-833-1036-5.

beoogde effect worden aangepast. Vervolgens wordt weer opnieuw de Plan-fase gestart.

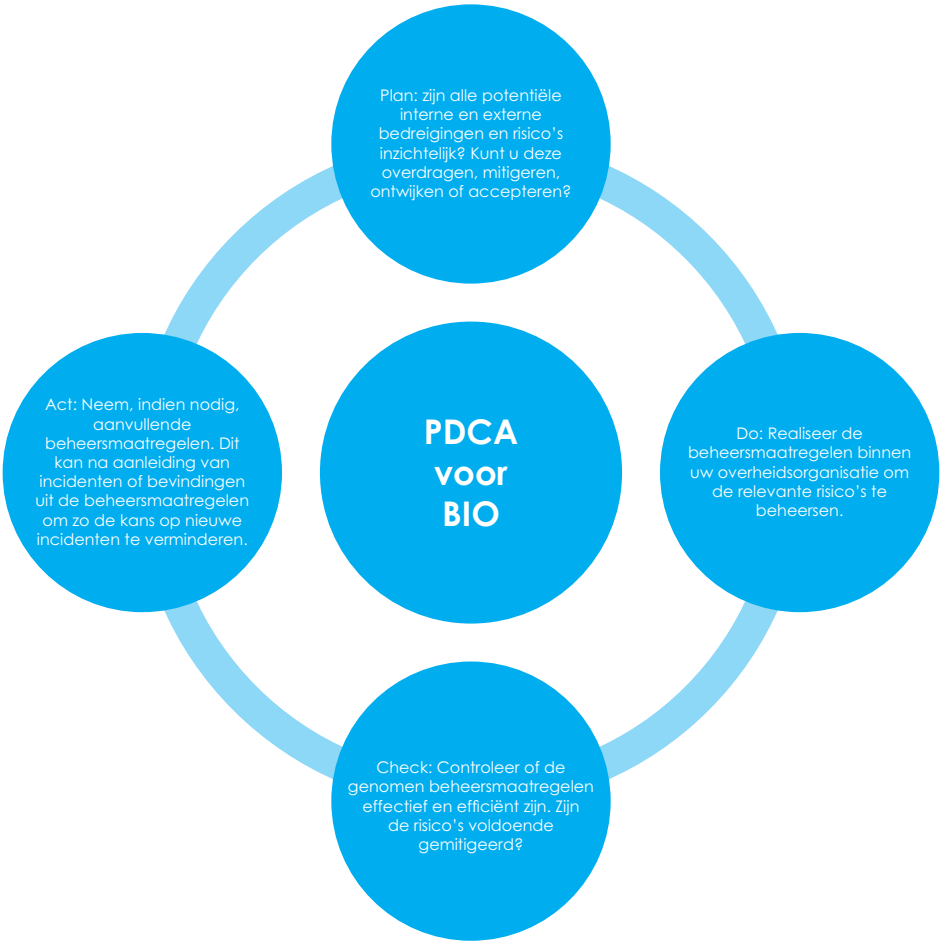
Deming beoogde met de PDCA-cyclus de continue verbetering een resultante te laten zijn van teamwork en wetenschap en geeft daarmee aan dat kwaliteit (in dit geval van informatiebeveiliging) een zaak is van iedereen. Maar het management dient hier wel richting aan te geven.
De visie van Deming komt nadrukkelijk naar voren in de volgende veertien punten (bron: www.managementmodellensite.nl):

1. Zorg voor continuïteit in de doelstelling en wees standvastig in het verbeteren van product en dienst.
2. Accepteer de nieuwe filosofie; we kunnen niet langer doorgaan met algemeen geaccepteerde (lage) niveaus van vertraging, fouten, verkeerde materialen en slecht vakmanschap.
3. Wees niet langer afhankelijk van massale inspecties, maar maak gebruik van statistische procesbeheersing.
4. Beëindig het zakendoen op basis van een prijskaartje, maar ga uit van een combinatie van zinvolle kwaliteitscriteria en de prijs.
5. Werk onophoudelijk aan verbetering van het proces.
6. Introduceer moderne methoden voor 'training on the job'.
7. Introduceer leiderschap, dat gericht is op het helpen van mensen om hun werk (nog) beter te doen.
8. Verdrijf de angst zodat iedereen effectief en in toenemende mate productief zijn werk kan doen.
9. Verwijder de muren tussen afdelingen.
10. Zie af van het gebruik van getalsmatige slogans, posters en doelstellingen waarin op een nieuw niveau van presteren wordt aangedrongen zonder dat daartoe de methoden worden aangereikt.
11. Elimineer werknormen waarin getalsmatige quota worden aangegeven.
12. Verwijder de barrières die werknemers en managers die per uur werken (als freelancer of zzp'er) ervan weerhouden trots te zijn op hun vakmanschap.
13. Moedig leren aan. Stel opleidingsplannen en -programma's op.
14. Creëer een structuur aan de top van de organisatie waardoor elke dag wordt gewerkt aan de bevordering van de bovengemelde dertien punten.

Als de PDCA-cyclus vertaald wordt naar (informatie) beveiliging dan ontstaat figuur 3.

2.4 ISMS ALS ONDERDEEL VAN RISICOMANAGEMENT

Het ISMS is een cruciaal onderdeel van goede informatiebeveiliging maar is ook onderdeel van een groter geheel. Voor een overheidsorganisatie is er naast de

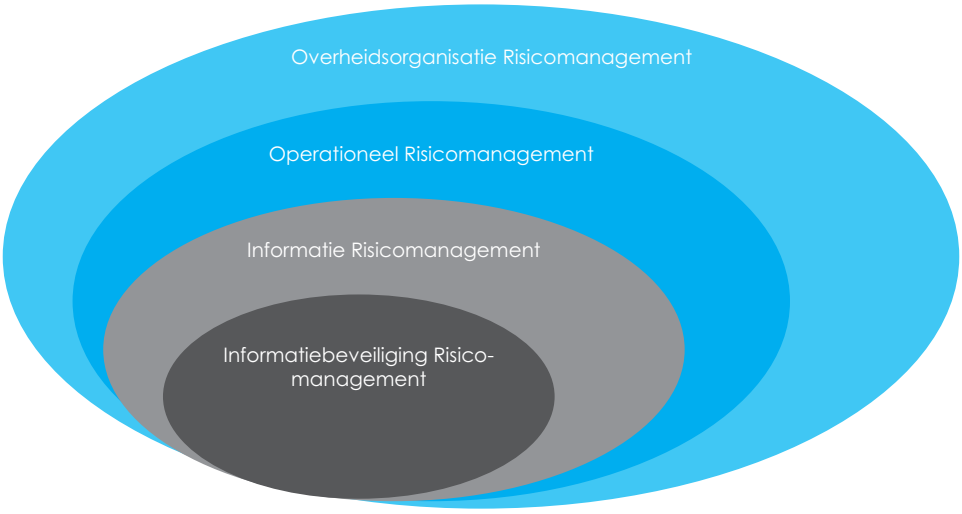


Figuur 3 PDCA-cyclus voor BIO

risico voor informatie en informatiesystemen een breder risico-perspectief van toepassing. Dat is in figuur 4 grafisch weergegeven.

De overheidsorganisatie Risicomanagement betreft het identificeren, analyseren, reageren en bewaken van risico's met betrekking tot de interne en externe omgeving die een overheidsorganisatie kan raken. Dit kunnen bijvoorbeeld de risico's van vergrijzing van de burgers in een gemeente betreffen (bijvoorbeeld het risico dat de vergrijzende bevolking van de burger niet het gewenste niveau van ondersteuning kan worden geboden). Bij de overheidsorganisatie Risicomanagement kan worden gedacht aan risico-types als: financiële risico's, operationele risico's, omgevingsrisico's (bijv. overstroming) en andere vormen van risico. Bekende risico-frameworks

en -standaarden op overheidsorganisatie-breed niveau zijn de COSO ERM[12] en de ISO31000[13].



Figuur 4 Informatiebeveiliging risicomanagement als onderdeel van de overheidsorganisatie Risicomanagement

Een deelverzameling van de overheidsorganisatie Risicomanagement wordt gevormd door Operationeel Risicomanagement, zoals is weergegeven in figuur 4. De risicoprincipes zijn hetzelfde, het bereik van Operationeel Risicomanagement is echter gericht op de overheidsorganisatie zelf en is vaak gericht op de operationele processen van de overheidsorganisatie als ook het menselijke karakter (zowel bescherming als bijvoorbeeld fraude).

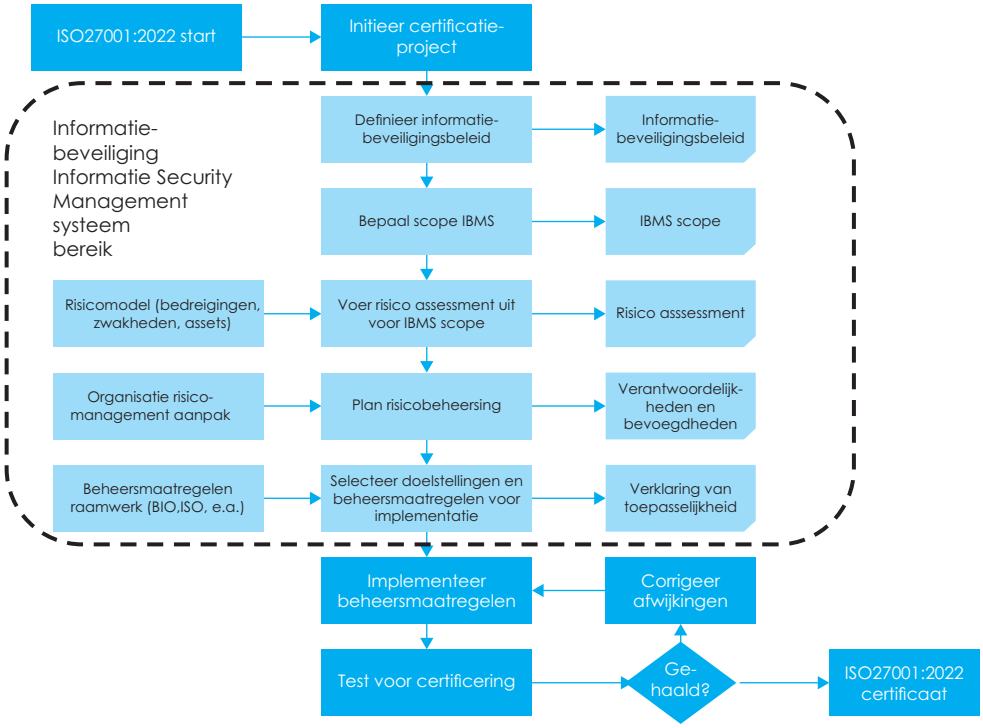
Binnen Operationeel Risicomanagement valt ook de deelverzameling Informatie Risicomanagement. Informatie is een belangrijk aspect van de operationele processen binnen een overheidsorganisatie. Echter naast informatiebeveiliging-risico's bestaat ook het risico van verkeerd gebruik van (op zichzelf juiste) informatie. Dit betreft eerder een informatie-risico dan een informatiebeveiliging-risico.

Voor een goed risicomanagement bij een overheidsorganisatie is het van belang onderscheid te maken in de diverse risicosoorten zoals hiervoor beschreven. De genomen beheersmaatregelen kunnen echter diverse vormen van risico's ondersteunen. Daarom is het zoeken van aansluiting tussen de diverse risicogebieden en -experts van belang.

12 https://www.coso.org/sitepages/guidance-on-enterprise-risk-management.aspx?web=1
13 https://www.iso.org/iso-31000-risk-management.html

Een overheidsorganisatie kan niet op basis van de BIO gecertificeerd worden. Medewerkers kunnen wel gecertificeerd worden als Certified BIO Professional[14] . Echter als de BIO (gebaseerd op de ISO27001:2022) is geïmplementeerd dan kan de overheidsorganisatie wel aanvullen met een ISO-certificering. In dat geval voldoet de overheidsorganisatie aan de BIO en heeft zij een ISO27001:2022-certificering welke gehanteerd kan worden bijvoorbeeld in relatie tot de (keten-)partners. Diverse overheidsorganisaties vereisen ook van toeleveranciers de ISO27001:2022-certificering.

Als een overheidsorganisatie voor een 27001:2022-certificering wil opgaan dan is het ISMS een kernelement. In figuur 5 wordt op geconsolideerde wijze weergegeven wat van het ISMS gerealiseerd dient te zijn. De elementen binnen de stippellijn vormen de benodigde activiteiten en producten om een ISMS gerealiseerd te hebben. De activiteiten van zowel binnen als buiten de stippellijn geven aan wat benodigd is voor de ISO27001:2022-certificering.



Figuur 5 Bereik en producten voor het ISMS

Als wordt uitgegaan van de wens tot ISO27001:2022-certificering dan is het inrichten van een certificatie-project te adviseren, maar we adviseren om ook voor

14 https://www.vhls.global/certification/cbp-certified-bio-professional-baseline-informatiebeveiliging-overheid/

BIO-realisatie een project in te richten. Een belangrijke reden hiertoe is dat meerdere onderdelen van de overheidsorganisatie betrokken zullen zijn zoals de secretaris/algemeen directeur en de afdelingen facility management, personeelszaken, IT en diverse anderen.

De eerste stap binnen het domein van ISMS is het definiëren van het informatiebeveiligingsbeleid. Doelstelling hiervan is het geven van directieaansturing van en -steun voor (informatie)beveiliging welke aansluiten op de bedrijfseisen, relevante wet- en regelgeving en bij de bredere risicodomeinen zoals operationele risico's, omgevingsrisico's en anderen (zie figuur 4). In het informatiebeveiligingsbeleid staan beleidsregels die goedgekeurd zijn door de directie, gepubliceerd zijn en bekend zijn bij de medewerkers en indien van toepassing ook bij relevante externe partijen. Daarnaast kunnen sommige beleidsregels ondernemingsraad-gevoelig zijn, denk hierbij aan regels waarbij mails van medewerkers worden getoetst op AVG-vereisten. Dit gebeurt bijvoorbeeld met een beheersmaatregel als Data Loss Protection (DLP, wat nader wordt toegelicht in hoofdstuk 13).

In stap 2 wordt het bereik van het ISMS bepaald. Binnen de BIO is een BBN (Basis Beveiliging Niveau) van toepassing welke bepaalt welke beheersmaatregelen en risico-mitigerende maatregelen van toepassing zijn. Als de overheidsorganisatie ook een ISO27001:2022-certificering wenst dan is Bijlage A van de ISO27001:2022 van toepassing. Een ander onderdeel van het bereik (in geval van ISO27001:2022-certificering) is het bepalen welke onderdelen van de organisatie binnen het bereik vallen, denk hierbij aan personeelsveiligheid, fysieke veiligheid of anderen. Er zijn organisaties die alleen de IT-organisatie certificeren. Het bereik van de ISO27001:2022-certificering en de verklaring van toepasselijkheid zijn in de praktijk dan ook belangrijke punten om te controleren als een overheidsorganisatie wenst uit te gaan van bijvoorbeeld een leverancier met een ISO27001:2022-certificaat. Wij adviseren om altijd het bereik van het ISMS en de verklaring van toepasselijkheid te controleren op aansluiting op de diensten die uw organisatie afneemt.

De elementen van stap 3, risico assessment, worden uitvoerig behandeld in deel II van dit boek. Het resultaat van deze stap is een risico assessment op de ISMS-scope.

In stap 4 wordt gepland voor risicobeheersing. Daarbij is het van belang om eigenaarschap, verantwoordelijkheden en bevoegdheden te bepalen. De impact hiervan kan zeer groot zijn. Bedenk bijvoorbeeld wie het besluit mag nemen om de servers met primaire overheidsapplicaties los te koppelen van het (inter)net in geval van een grote ransomware aanval. Het hoeft geen betoog dat dit een serieuze verantwoordelijkheid betreft.

Stap 5 gaat over het selecteren van de doelstellingen en de beheersmaatregelen voor implementatie. Afhankelijk van het BBN zal een aantal beheersmaatregelen

vereist zijn voor overheidsorganisaties. Een belangrijk resultaat van deze vijfde stap is de verklaring van toepasselijkheid.

In de PDCA-cyclus is stap 6 het implementeren van de beheersmaatregelen als aangegeven in de verklaring van toepasselijkheid.
Als de overheidsorganisatie ook de ISO27001:2022-certificering wenst te behalen dan is een test voor certificering (een beoordeling of de certificering wordt behaald) van belang, bij voorkeur door een certificerende organisatie. Als de test succesvol is dan kan het ISO-certificaat worden aangevraagd. Zo niet, dan volgen correcties op de geïmplementeerde beheersmaatregelen. Zie hoofdstuk 3 voor de aan de ISO27001:2022 gerelateerde beheersmaatregelen.

Samengevat kan worden gesteld dat voldoen aan de BIO-vereisten en de ISO27001:2022-certificering een overheidsorganisatie helpt in de continue verbetercyclus welke wordt nagestreefd in zowel de BIO als de ISO27001:2022.