Onderzoek Impact 2021 versie ISO27002 op de BIO

ONDERZOEK IMPACT 2021 VERSIE ISO27002 OP DE BIO

Joep Janssen, Willem Vos, Ed Baltussen

datum	**22-11-2021**
status	Definitief
versie	1.0
projectnummer	20218715
Interne toets	Steven Debets

MANAGEMENTSAMENVATTING

Aanleiding en opdracht

De ISO 27002 normen zijn voor het laatst inhoudelijk aangepast in 2013 en in 2018 is besloten deze normen te herzien. De introductie van de nieuwe versie van de ISO 27002 staat voor begin 2022 gepland. Uit de consultatieversie valt op te maken dat een aantal wijzigingen zijn uitgevoerd op structuur en inhoud:

- Het gebruik van kenmerken bij controls, zodat controls op diverse perspectieven geordend en beoordeeld kunnen worden. Als gevolg hiervan is ook de uitwerking van de controls aangepast.
- Het aantal thema's is teruggebracht van 14 naar 4 gebieden (mensen, fysieke objecten, technologie en organisatie)
- Er zijn nu minder controls gedefinieerd, 96 t.o.v. 110, maar 24 controls bestaan uit samenvoegingen van oude controls en er zijn 13 nieuwe controls toegevoegd.

VKA heeft in opdracht van BZK een onderzoek uitgevoerd naar de impact van de komende ISO 27002 wijzingen op de huidige BIO en de verdere implementaties daarvan .
De huidige BIO is gebaseerd op controls uit de ISO 27002. De gevraagde impactanalyse geeft, behalve de impact op de BIO, ook de mogelijke consequenties weer van deze wijzigingen voor de verschillende bestuurslagen binnen de overheid.

Conclusies

Bestuurslagen geven aan dat ze alle aanpassingen en nieuwe controls van ISO 27002 zinvol achten voor de BIO. Daarom dient de BIO gekoppeld te blijven aan de nieuwe ISO 27002 en kan deze volledig gebruikt worden voor een nieuwe versie van de BIO.

Indien besloten wordt dat de BIO de nieuwe ISO 27002 volgt, dan dient een traject ingezet te worden om wijzigingen door te voeren in de BIO.

Kern IBO heeft aangegeven dat geen nieuwe overheidsmaatregelen worden toegevoegd aan de nieuwe BIO. Daarmee is de impact op dat punt gering voor de bestuurslagen.

Het invoeren van de overige controls vindt bij de overheidsorganisaties conform de BIO plaats op basis van een risicoafweging en is onderdeel van het reguliere proces van beoordeling van risico's en maatregelen binnen de organisatie. Afhankelijk van de situatie van de organisatie en de uitgevoerde risicoafweging kan de impact op de organisaties van de nieuwe controls meer of minder zijn.

De impact van een aangepaste BIO voor de vier bestuurslagen in termen van werklast, kosten en doorlooptijd zijn binnen het bestek van deze opdracht niet exact kwantitatief te duiden. Het

niveau van implementatie van de BIO wisselt sterk in de bestuurslagen en is niet in algemene zin per bestuurslaag aan te geven.

Uit de reacties die VKA ontvangen heeft blijkt de impact te variëren van klein tot groot. Indien de 13 nieuwe controls volledig doorgevoerd moeten worden in de organisatie als gevolg van de risicoanalyse: een werklast van een tot twee manjaar. De doorlooptijd varieert van enkele weken tot 5 jaar, afhankelijk van de (reguliere) onderhoudscyclus dat organisaties aanhouden voor het aanpassen van BIO controls.

De BIO gaat uit van risicomanagement als integraal startpunt voor de implementatie van maatregelen. In de praktijk zien we twee benaderingen bij overheidsorganisaties:

1. Een compliance based benadering waarbij de focus gelegd wordt op de implementatie van overheidsmaatregelen. Als de overheidsmaatregelen niet of zeer beperkt wijzigen bij de nieuwe BIO versie, zullen deze organisaties weinig impact van de nieuwe versie ondervinden.
2. Een risicogebaseerde benadering, waarbij de focus ligt de analyse van bedreigingen en risico's en vervolgens op het toepassen van de controls. Bij implementatie van de nieuwe BIO versie zullen deze organisaties afhankelijk van de bedreigingen en risico's de nieuwe controls waar nodig inpassen.

De respondenten van de bestuurslagen geven hierbij aan dat de beschreven risicobenadering in de BIO niet aansluit op de eigen praktijk en context. Men zoekt naar een strategische risicobenadering, waarbij de BIO één van de invalshoeken is naast andere beveiligingsstandaarden.

INHOUDSOPGAVE

1 INLEIDING

1.1 Opdrachtomschrijving

BZK heeft VKA verzocht een onderzoek te doen naar de impact van de komende ISO 27002 wijzingen op de huidige BIO[1] en de verdere implementaties daarvan. De BIO is gebaseerd op controls uit de ISO 27002, en wil daarmee in lijn blijven. De gevraagde impactanalyse geeft, behalve de impact op de BIO, ook de mogelijke consequenties weer van deze wijzigingen voor de verschillende bestuurslagen binnen de overheid.

De BIO is van toepassing voor de gehele overheid en vanaf 2019 van toepassing verklaard. De BIO is inmiddels breed ingevoerd en er bestaan veel hulpmiddelen en documentatie om de invoering en de operationele processen te ondersteunen. Hoewel de BIO een overheidsbreed normenkader is, zal de implementatie ervan in de vier bestuurslagen van de overheid deels verschillend zijn. Gemeenten, waterschappen, provincies en Rijksoverheid kennen iedere hun eigen specifiek karakter, doelstellingen, werkprocessen, risicoprofiel en organisatievorm. Daarmee is, naar verwachting, ook de impact van deze verandering bij de vier bestuurslagen verschillend. En daarmee een belangrijk onderwerp van dit onderzoek.

De formele opdrachtgever is mr. drs. D.P.E.M. Dèsirée Geerts, afdelingshoofd Informatiesamenleving van het ministerie van BZK. Het Kern-IBO vormt de stuurgroep en de werkgroep BIO vormt de klankbordgroep voor het onderzoek. De deelnemers van de werkgroep BIO en Kern-IBO dienen als contactpersoon naar de betrokken organisaties en domein vertegenwoordigers van de bestuurslagen.

1.2 Aanleiding en achtergrond van de opdracht

De ISO 27002 normen zijn voor het laatst inhoudelijk aangepast in 2013 en in 2018 is besloten deze normen te herzien. De introductie van de nieuwe versie van de ISO 27002 staat voor begin 2022 gepland. Uit de consultatieversie valt op te maken dat een aantal wijzigingen zijn uitgevoerd op structuur en inhoud:

- Het gebruik van kenmerken bij controls, zodat controls op diverse perspectieven geordend en beoordeeld kunnen worden. Als gevolg hiervan is ook de uitwerking van de controls aangepast.
- Het aantal thema's is teruggebracht van 14 naar 4 gebieden (mensen, fysieke objecten, technologie en organisatie)

[1] Baseline Informatiebeveiliging Overheid. De BIO is in 2019 geïntroduceerd als de baseline voor de informatiebeveiliging voor de overheid. DE BIO is gestructureerd volgens de NEN-ISO/IEC 27001:2017, bijlage A en NEN-ISO/IEC27002:2017. De ISO 27002 beschrijft de per aandachtsgebied mogelijke controls voor de informatiebeveiliging en omvat de 'best practices' voor informatiebeveiliging. De BIO voegt hier nog de verplichte 'overheidsmaatregelen' aan toe.

- Er zijn nu minder controls gedefinieerd, 96 t.o.v. 110, maar 24 controls bestaan uit samenvoegingen van oude controls en er zijn 13 nieuwe controls toegevoegd.

In de twee jaar dat de BIO nu bestaat hebben overheidsorganisaties de BIO ingevoerd, (beveiligings-)processen ingericht, documentatie samengesteld en ISMS'en[2] ingericht om te voldoen aan de eisen. Daarnaast hebben organisaties als IBD[3] HWH[4], IPO[5] en CIP[6] de overheidsorganisaties ondersteund met documentatie en hulpmiddelen, zoals zelfevaluaties, handreikingen, sjablonen en toelichting op specifieke controls en overheidsmaatregelen uit de BIO. Er is veel werk verzet om de BIO in te voeren en te ondersteunen en dat maakt het belangrijk om in te schatten wat er mogelijk wijzigt aan deze instrumenten en wat daarvan de inspanning is.

1.3 Doel van de opdracht

Doel van de opdracht is een rapportage op te stellen voor de werkgroep BIO en kern-IBO, die inzicht geeft in de impact van de wijzigingen in ISO27002 voor wat betreft:

- De huidige samenstelling, inhoud en praktijk van de BIO.
- De centraal beschikbare hulpmiddelen en handreikingen van IBD, HWH, IPO en CIP.
- De impact en ondersteuning die nodig is voor de implementatie voor de vier bestuurslagen.
- De impact op lopende certificeringstrajecten van leveranciers.
- De contractering van leveranciers in relatie tot de inkoopvoorwaarden van de bestuurslagen.

1.4 Deelvragen van de opdracht

BZK heeft in haar opdrachtformulering een keuze gemaakt voor de onderwerpen die in de impactanalyse betrokken moeten worden, namelijk:

1. Welke impact heeft de nieuwe NEN-ISO-27002 op de inhoud en samenstelling van de huidige BIO? Impact als gevolg van:
   a. De hernummering/herindeling van de ISO-27002-controls.
   b. Het samenvoegen van een aantal ISO-controls.
   c. De uitbreiding van een aantal ISO-controls.
   d. Het aanpassen van formuleringen van ISO-controls.
   e. Het aanpassen van formuleringen van ISO-maatregelen t.o.v. de bestaande overheidsmaatregelen in de BIO.
   f. Het uitbreiden van ISO-controls.
   g. Het uitbreiden of schrappen van Overheidsmaatregelen o.b.v. van de nieuwe en geredigeerde implementatie richtlijnen.

[2] ISMS Information Security Management System

[3] IBD Informatiebeveiligingsdienst, onderdeel van VNG

[4] HWH Het Waterschapshuis

[5] IPO Interprovinciaal overleg

[6] Centrum Informatiebeveiliging en Privacybescherming, publiek-private netwerkorganisatie

2. Welke aanpassingen willen betrokkenen doorvoeren in de huidige BIO?
   a. op het gebied van controls (inclusief de nieuwe aandachtsgebieden die de NEN-ISO-27002 onderkent) en
   b. op gebied van de overheidsmaatregelen
3. Wat is de geschatte werklast voor aanpassing en de doorlooptijd van de BIO?
4. Wat is impact van het al dan niet volledig aanpassen van de BIO aan de NEN-ISO-27002 voor:
   a. reeds afgesloten dan wel af te sluiten contracten;
   b. ISO-27001 certificeringstrajecten?
5. Wat is de impact van een aangepaste BIO op de organisaties binnen de 4 bestuurslagen en op de organisaties waarmee de overheid samenwerkt? Met een focus op kosten, werklast, doorlooptijden, etc.
6. Binnen welke termijn kan de aangepaste BIO van kracht zijn?
7. Wat is de impact op aanpassingen in de ondersteunende BIO-producten?
   a. Best practices;
   b. Tools zoals ISMS-en en inkoophulpmiddelen?

Het onderzoek naar de impact biedt ook een mogelijkheid om eerste inzichten op te halen over een toekomstige evaluatie van de BIO. Deze inzichten zijn niet het primaire object van de impactanalyse. De inzichten geven wij alleen in beschrijvende zin weer in bijlage A. we. Het gaat dan om inzichten als:

- Ideeën over de aanpak van de evaluatie van de BIO.
- Onderwerpen die kunnen worden geëvalueerd.
- Eerste beelden of vooruitblikken op de resultaten van zo'n evaluatie.

1.5 Reikwijdte en diepgang van de opdracht

Dit onderzoek inventariseert de verwachtte impact van wijzigingen in de BIO en de impact daarvan op de bestuurslagen op hoofdlijnen:

- VKA baseert zich daarbij op de ISO 27002 consultatieversie[7] om de impact te bepalen op de huidige BIO, versie 1.04.
- VKA verzamelt informatie over de impact bij de bestuurslagen Rijksoverheid, provincies, waterschappen en gemeenten.
  - Voor de bestuurslagen provincies, waterschappen en gemeenten worden de vragen over impact gesteld via de representatieve overlegvormen en zo beantwoord.
  - Voor de Rijksoverheid interviewen we een aantal representatieve organisaties over de impact van een nieuwe BIO en vormen ons zo een beeld.
- VKA vraagt, naast kwalitatieve informatie, de bestuurslagen specifiek een uitspraak te doen naar impact in termen van doorlooptijd, manjaren werk en out of pocket kosten.
- Voor de impact op centraal beschikbare hulpmiddelen en handreikingen voor de BIO heeft VKA interviews gehouden met CIP en IBD.

1.6 Onderzoekaanpak

Het onderzoek heeft bestaan uit drie fasen, namelijk voorbereiding, de analyse van de nieuwe ISO 27002 en de huidige BIO, het uitvragen van de impact bij de bestuurslagen en het samenstellen en

[7] Officieel versie ISO/IECCD27002:2019(E)

afstemmen van de rapportage. Hieronder worden alle specifieke stappen en resultaten kort toegelicht.

Fase	Activiteit	Resultaten
Voorbereiding	Kick-Off	Afgestemde onderzoekopzet
		Afgestemde lijst te interviewen personen en organisaties
		Object onderzoek vastgesteld
		Documentstudie
	Voorbereiding onderzoek	Ingeplande interviews
Uitvoering	Verschillenanalyse ISO 27002 en BIO	Factsheet voor geïnterviewden
	Interviews afnemen • Rijksoverheid, CIP, IBD, VNG Uitvraag via • Contactpersoon Waterschap • Contactpersoon Provincies	10 interviews Aanvullende documentatie bestuderen en antwoorden op de vragen uit de Factsheet verwerken
	Aanvullende documentstudie	Conceptrapportage opgesteld
	Uitwerken rapportage	Conceptrapportage afgestemd, inclusief verbetervoorstellen opdrachtgever
	Afstemmen concept rapportage	Definitieve rapportage opgeleverd
Afronding	Definitieve rapportage	Presentatie resultaten onderzoek
	Afronding onderzoek	22-11-2021

1.7 Leeswijzer

In dit rapport bespreken we in hoofdstuk 2 eerst de inhoudelijke wijzigingen van de ISO 27002 en welke impact die hebben voor een nieuwe versie van de BIO. Deze wijzigingen zijn verwerkt in een factsheet, die vervolgens is gedeeld en besproken met de bestuurslagen. De resultaten daarvan zijn opgenomen in hoofdstuk 3. Vervolgens zijn de andere onderzoeksvragen naar impact uitgewerkt, namelijk de impact op bestaande contractering en certificeringsprojecten, in hoofdstuk 4. In hoofdstuk 5 vindt u de conclusies en aanbevelingen van ons onderzoek.

2 ISO 27002 EN BIO, FEITELIJKE WIJZIGINGEN ISO 27002

Dit hoofdstuk behandelt de eerste onderzoeksvraag, zijnde:

1. Welke impact heeft de nieuwe NEN-ISO-27002 op de inhoud en samenstelling van de huidige BIO? Impact als gevolg van:
   a. De hernummering/herindeling van de ISO-27002-controls.
   b. Het samenvoegen van een aantal ISO-controls.
   c. De uitbreiding van een aantal ISO-controls.
   d. Het aanpassen van formuleringen van ISO-controls.
   e. Het aanpassen van formuleringen van ISO-controls t.o.v. de bestaande overheidsmaatregelen in de BIO.
   f. Het uitbreiden van ISO-controls.
   g. Het uitbreiden of schrappen van Overheidsmaatregelen o.b.v. van de nieuwe en geredigeerde implementatie richtlijnen.

2.1 Beschrijving ISO 27002

De ISO 27002 is een 'best practice' aan controls voor informatiebeveiliging. De ISO 27002 is een nadere uitwerking van de ISO 27001, en kan organisaties ondersteunen gedurende de implementatie van een Information Security Management System (ISMS).

2.2 Beschrijving BIO

De Baseline Informatiebeveiliging Overheid (BIO) is het gemeenschappelijke normenkader voor informatiebeveiliging waar alle lagen van de overheid (Rijksdienst, provincies, waterschappen en gemeentes) aan moeten voldoen. De BIO beveelt daarnaast aan om 'de BIO te verankeren in de taakomschrijving van de overige overheidsorganisaties en organisaties waarmee de overheid publiek-privaat samenwerkt en private samenwerkingen waarbij de overheid de enige aandeelhouder is'.[8]

De BIO is inhoudelijk gebaseerd op de ISO 27002 en volgt een gelijke indeling. Aanvullend op de ISO 27002 zijn de verplichte overheidsmaatregelen, die voortvloeien uit a) wet- en regelgeving, b) van fundamentele aard zijn voor betrouwbare informatievoorzieningen/of c) van belang zijn voor ketenbeveiliging.

2.3 Ondersteuning voor de BIO in NL context (IBD, CIP)

In Nederland zijn twee overheidsorganisaties die bekend zijn voor ondersteuning bij de implementatie van de BIO, zijnde de Informatie beveiligingsdienst (IBD) en het Centrum Informatiebeveiliging en Privacybescherming (CIP).

De IBD, als onderdeel van de Vereniging van Nederlandse Gemeenten (VNG), biedt gemeenten kennisproducten waarmee zij de BIO kunnen implementeren. Daarnaast draagt de IBD bij aan

[8] Baseline Informatiebeveiliging Overheid v1.0.4zv, p. 9

kennisdeling tussen gemeenten onderling en met andere bestuurslagen en leveranciers. De IBD geeft aan dat een nieuwe ISO 27002 weinig impact zal hebben op de ondersteunende producten. Het onderhoud van deze producten is volgens de IBD immers onderdeel van de normale procesgang.

Het CIP biedt evenals de IBD uitwerkingen en handreikingen om de BIO te implementeren in BIO Thema-uitwerkingen. Het primaire doel van het CIP is informatie-uitwisseling en kennisdeling tussen verschillende overheidsorganisaties. In tegenstelling tot de IBD geeft het CIP aan dat de nieuwe ISO 27002 grote impact zal hebben op de ondersteunende producten van het CIP, aangezien deze allemaal aangepast dienen te worden doordat de nieuwe ISO 27002 verschilt op structuur én inhoud.

2.4 Samenvatting wijzigingen

In de nieuwe versie van de ISO 27002 zijn wijzigingen uitgevoerd op structuur en inhoud. Het aantal thema's is teruggebracht van 14 naar 4 gebieden (mensen, fysieke objecten, technologie en organisatie). In de ISO zijn nu minder controls gedefinieerd, 96 ten opzichte van 110, maar 24 controls bestaan uit samenvoegingen van oude controls en er zijn 13 nieuwe controls toegevoegd.

In de nieuwe ISO 27002 bevat elke control attributen, waarmee controls op verschillend perspectief geordend en beoordeeld kunnen worden. Elke control heeft vier typen attributen, zijnde:

a) Control types (#Preventive, #Detective, #Corrective)
b) Information security properties (#Confidentiality, #Integrity, #Availability)
c) Cybersecurity concepts (#Identify, #Protect, #Detect, #Respond, #Recover)
d) Operational capabilities, waar generieke onderwerpen van de control vermeld worden.

De attributen hebben als doel dat organisaties de controls kunnen filteren, sorteren of anders kunnen weergeven voor verschillende doelgroepen. In de Annex A van de nieuwe ISO 27002 staat een voorbeeld hoe organisaties gebruik kunnen maken van attributen.

2.5 Impact wijzigingen ISO 27002 op BIO

Indien besloten wordt dat de wijzigingen in de ISO 27002 zullen leiden tot wijzigingen in de BIO, dan zal het noodzakelijk zijn om de wijzigingen zoals in voorgaande paragrafen uiteengezet over te nemen. Naast het wijzigen van de indelingen het aanpassen van de controls zal ook nagegaan moeten worden welke overheidsmaatregelen herzien moeten worden, dan wel nieuwe overheidsmaatregelen gedefinieerd moeten worden. Geschrapte controls uit de oude ISO 27002 zullen bij het aanpassen van de BIO verdwijnen, tenzij ook deze omgevormd worden tot overheidsmaatregelen in de BIO.

2.6 Nieuwe controls

In de nieuwe ISO 27002 zijn 13 nieuwe controls opgenomen. Deze nieuwe controls zijn vooral van technische aard om de ISO beter aan te laten sluiten op een moderne IT-omgeving. Hieronder vallen bijvoorbeeld informatiebeveiliging bij het gebruik van clouddiensten, data masking en data leakage prevention.

Daarnaast besteedt de nieuwe ISO 27002 meer aandacht aan monitoring, zowel van de IT als de monitoring van fysieke omgevingen.

In bijlage C is een lijst opgenomen van de 13 nieuwe controls.

2.7 Vergelijking tussen beide ISO versies

We hebben globaal vastgesteld of er in de teksten van de nieuwe ISO versie geen/weinig of meerdere wijzigingen zijn opgetreden ten opzichte van de oude 2013 versie. De individuele controls zijn niet specifiek onderzocht.

Een voorbeeld van een control waar meerdere wijzigingen in zijn opgetreden is 14.1.1 (Information security requirements analysis and specification) uit de oude ISO, nu 5.8 (Information security in project management) in de nieuwe ISO. Ter vergelijking de beide teksten van de control:

> 14.1.1 Information security requirements analysis and specification
> Control
> The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems.
>
> 5.8 Information security in project management
> Control
> Information security should be integrated into the organization's project management method(s).

Hier is een uitbreiding te zien in de scope van de control in de nieuwe ISO om informatiebeveiliging niet alleen mee te nemen in de eisen voor nieuwe of bestaande informatiesystemen, maar als integraal onderdeel van de projectmanagementmethodiek(en).

Als een control in de nieuwe ISO hooguit verplaatst of samengevoegd wordt, of enkele niet-inhoudelijke tekstuele wijzigingen bevat, is geconcludeerd dat de control geen/weinig wijzigingen bevat.

ISO:2013	Meerdere wijzigingen	Geen/weinig wijzigingen	Totaal		% Meerdere	% geen/weinig
H5	0	2	2		0	100
H6	1	6	7		14,3	85,7
H7	0	6	6		0	100
H8	1	9	10		10	90
H9	6	8	14		42,9	57,1
H10	0	2	2		0	100
H11	2	13	15		13,3	86,7
H12	0	14	14		0	100
H13	4	3	7		57,1	42,9
H14	9	4	13		69,2	30,8
H15	2	3	5		40	60
H16	3	4	7		42,9	57,1
H17	1	3	4		25	75
H18	0	8	8		0	100
Totaal:	29	85	114	**Gemiddeld:**	22,4	77,5

Op basis van onze analyse verwachten we dat de meeste wijzigingen, geordend naar impact, optreden in:

- Hoofdstuk 14 'Acquisitie, ontwikkeling en onderhoud van informatiesystemen'
- Hoofdstuk 13 'Communicatiebeveiliging'
- Hoofdstuk 9 'Toegangsbeveiliging' en 16 'Beheer van informatiebeveiligingsincidenten'

In 22% van de gevallen blijken dezelfde controls in de nieuwe versie meerdere wijzigingen te bevatten.

2.8 Vergelijking tussen de nieuwe ISO en de bestaande BIO overheidsmaatregelen

Het Kern-IBO heeft aangegeven dat het inhoudelijke aanpassingen van overheidsmaatregelen pas bij de in 2023 geplande evaluatie van de BIO aan de orde zijn. De wijzigingen in de ISO27002 kunnen eventueel wel leiden tot het splitsen of samenvoegen van overheidsmaatregelen of in een incidenteel geval tot het laten vervallen van overheidsmaatregelen. Het beoogde beveiligingsniveau zal echter niet veranderen door de komst van de nieuwe ISO. VKA heeft de bestaande BIO overheidsmaatregelen vergeleken met de teksten van de vergelijkbare nieuwe 27002 controls. Het betrof een globale analyse, de individuele controls zijn niet diep inhoudelijk vergeleken met de BIO overheidsmaatregelen. Met behulp van deze aanpak hebben wij een beperkt aantal controls uit de nieuwe ISO 27002 gevonden die afwijken van de formulering of inhoud van de bestaande BIO overheidsmaatregelen.

Een voorbeeld van zo'n gewijzigde control uit de nieuwe ISO is 5.17 (Authentication information), voorheen o.a. 9.4.3 (Password management system), met bijbehorende overheidsmaatregel '9.4.3.1. De overheidsmaatregel geeft o.a. aan dat de complexiteitseis van een wachtwoord vervalt na een wachtwoordlengte van 20 posities.' Control 5.17 stelt nu:

l) when passwords are used as authentication information, good quality passwords should be selected, which:
1) are not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers and dates of birth etc.;
2) are not based on dictionary words or combinations thereof;
3) include alphanumerical and special characters;
4) have a minimum length;

[…]

Password management system

When password is used as authentication information, the password management system should:

[…]

q) enforce a choice of strong passwords (see l));

Uit deze subheaders binnen control 5.17 kan men opmaken dat de complexiteitseis niet zou moeten vervallen na een wachtwoordlengte van 20 posities.

BIO	Meerdere wijzigingen	Geen/weinig wijzigingen	Totaal		% Meerdere	% geen/weinig
H5	0	2	2		0	100
H6	0	9	9		0	100
H7	1	5	6		16,7	83,3
H8	0	9	9		0	100
H9	6	17	23		26,1	73,9
H10	1	3	4		25	75
H11	1	9	10		10	90
H12	3	21	24		12,5	87,5
H13	0	9	9		0	100
H14	2	6	8		25	75
H15	0	11	11		0	100
H16	3	9	12		25	75
H17	0	3	3		0	100
H18	0	8	8		0	100
Totaal:	17	121	138	**Gemiddeld:**	10	90

Op basis van onze analyse verwachten we dat de meeste wijzigingen, geordend naar impact, optreden in:

- Hoofdstuk 9 'Toegangsbeveiliging'
- Hoofdstuk 10 'Cryptografie' en 14 'Acquisitie, ontwikkeling en onderhoud' van informatiesystemen en 16 'Beheer van informatiebeveiligingsincidenten'

Het effect van de nieuwe ISO 27002 op de bestaande overheidsmaatregelen lijkt beperkt te zijn. Slechts 10% kent meerdere wijzigingen.

2.9 Het uitbreiden of schrappen van BIO overheidsmaatregelen

Zoals aangegeven heeft het Kern-IBO heeft aangegeven dat het inhoudelijke aanpassingen van overheidsmaatregelen pas bij de in 2023 geplande evaluatie van de BIO aan de orde zijn. De wijzigingen in de ISO27002 kunnen wel leiden tot het splitsen of samenvoegen van overheidsmaatregelen of in een incidenteel geval tot het laten vervallen van overheidsmaatregelen; het beoogde beveiligingsniveau zal echter niet veranderen door de komst van de nieuwe ISO.

3 BESCHRIJVING IMPACT BESTUURSLAGEN OVERHEID

3.1 Inleiding

De beschrijving van de impact op de bestuurslagen behandelt de onderzoeksvragen 2 , 3, 5, 6 en 7b. Specifiek:

2. Welke aanpassingen willen betrokkenen doorvoeren in de huidige BIO?
   a. op het gebied van controls (inclusief de nieuwe aandachtsgebieden die de NEN-ISO-27002 onderkent) en
   b. op gebied van de overheidsmaatregelen
3. Wat is de geschatte werklast voor aanpassing en de doorlooptijd van de BIO?

5. Wat is de impact van een aangepaste BIO op de organisaties binnen de 4 bestuurslagen en op de organisaties waarmee de overheid samenwerkt? Met een focus op kosten, werklast, doorlooptijden, etc.
6. Binnen welke termijn kan de aangepaste BIO van kracht zijn?
7. Wat is de impact op aanpassingen in de ondersteunende BIO-producten?
   b. Tools zoals ISMS-en en inkoophulpmiddelen?

3.2 Kader voor het bepalen van impact

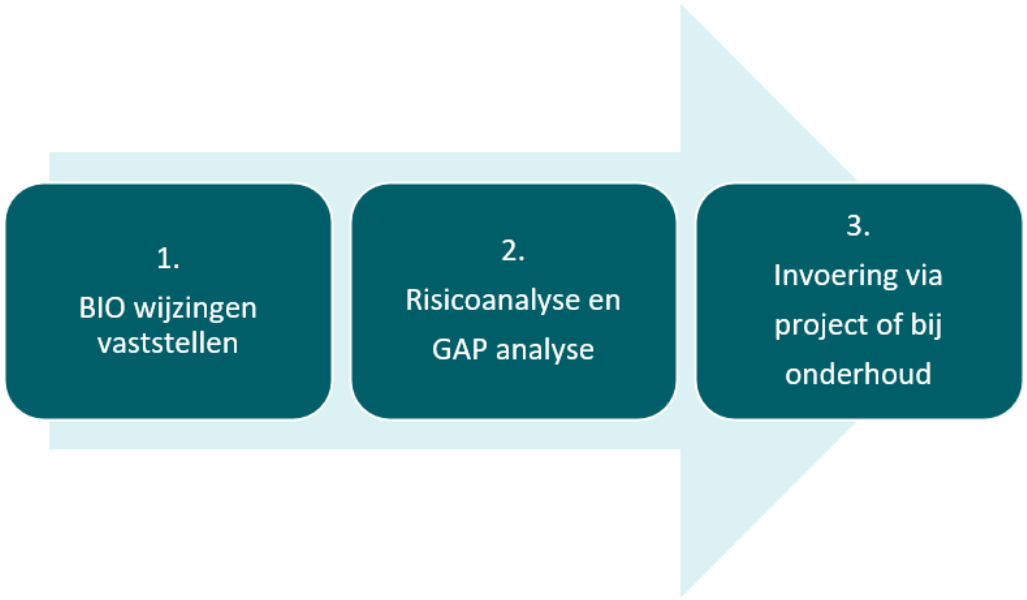
Gedurende dit onderzoek is duidelijk geworden de vraag naar impact, zoals bedoeld met de vragen 3, 5, 6 en 7b, een nader inkadering behoeft. Daarmee kunnen de vragen en ook de gegeven antwoorden in dit onderzoek beter begrepen worden.

De impact voor de bestuurslagen is volgens onderstaande gedachtenlijn geanalyseerd.

1. De wijzigingen voor de BIO, en met name de overheidsmaatregelen worden beschreven en ter kennis gebracht. Dit omvat dan de nieuwe, gewijzigde en vervallen (overheids-)maatregelen. Hier spelen twee belangrijke uitgangspunten een rol:
   a. De Kern-IBO heeft aangegeven dat het beoogde beveiligingsniveau dat met de overheidsmaatregelen gerealiseerd wordt niet gewijzigd gaat worden. Daarnaast blijkt uit onze analyse in paragraaf 2.8 dat een beperkt aantal wijzigingen mogelijk zijn.
   b. De nieuwe ISO27002 benoemt een aantal nieuwe aspecten en invalshoeken. Los van de aanpassing van de BIO is het voor organisaties van belang om aan de slag te gaan met deze vernieuwing en deze risicogericht toe te passen.
2. De organisatie voert in overeenstemming met de BIO een risicoanalyse uit en stelt vast of dit leidt tot specifieke wijzigingen in de maatregelen. Het kan immers zijn dat de organisatie een aantal van de nieuwe ISO controls al geïmplementeerd heeft, vanuit eerdere risicoanalyses. Daarna voert de organisatie een GAP analyse uit en stelt zo vast welke aanpassingen noodzakelijk zijn.
3. Als de organisatie de aanpassingen in beeld heeft, zal ze de keuze maken hoe deze maatregelen in te voeren in de organisatie. Dat kan op twee manieren:

a. Als apart project. De wijzigingen worden als totaalpakket ingepland en uitgerold in de organisatie. De prioriteit van het project, de omvang van de wijzigingen en de projectresources bepalen de start en doorlooptijd van de implementatie. Dit kan en zal per organisatie verschillen. Gelijke projecten kunnen verschillen in doorlooptijd.
b. Als onderdeel van de reguliere onderhoudscyclus. De wijzigingen worden als deelpakketten behandeld in de verschillende (vaak meerjarige) onderhoudscycli die de organisatie hanteert voor het aanpassen van processen, informatiesystemen en infrastructuur. In deze optie bepalen de voorbereidingstijd en de onderhoudscycli de totale doorlooptijd van de invoering. Een onderhoudscyclus kan soms meerdere jaren zijn (bijvoorbeeld eens in de drie-vier jaren aanpassen van het beveiligingsbeleid). Dat wil nog niet zeggen dat een control op basis van een risicoafweging al niet eerder ingepast en opgeleverd kan worden. Een control kan ook in het begin van zo'n cyclus al geïmplementeerd worden.

Schematisch:



De eerste stap wordt uitgevoerd door de Werkgroep BIO en bekrachtigd in Kern IBO. De tweede en derde stap wordt uitgevoerd door de individuele organisaties binnen de bestuurslagen. De uitvoerde interviews, uitgezette vragenlijsten en analyse in dit hoofdstuk behandelen de verzamelde inzichten van de tweede en derde stap in het schema. We zullen waar mogelijk benadrukken hoe een bestuurslaag denkt de invoering af te handelen.

3.3 Rijksoverheid

De Rijksoverheid omvat een groot aantal organisaties die landelijk beleid maken en/of landelijke taken uitvoeren. De Rijksoverheid omvat ongeveer 1200 organisaties[9] die opereren in verschillende context. De context die onzes inziens relevant is voor deze analyse, is:

- Beleidsdepartementen, die opereren in Nederlandse dan wel internationale context.
- Uitvoeringsorganisaties, die vooral opereren in Nederlandse context. Daarbinnen zijn twee vormen te onderscheiden:
    - Uitvoeringsorganisaties die vallen onder de verantwoordelijkheid van een departement.
    - Zelfstandige bestuursorganen (ZBO's). Zij zijn een zelfstandig rechtspersoon en niet verplicht de BIO te implementeren.

In ons onderzoek hebben we met CISO's van meerdere beleidsdepartementen gesproken. Voor wat betreft de uitvoeringsorganisaties hebben we gesproken met de Belastingdienst en RDW. Deze interviews geven onzes inziens een representatief beeld van de grotere organisaties binnen de Rijksoverheid.

Het algemene beeld is dat de Rijksoverheid zich wil houden aan de afspraken om met de BIO te werken en de BIO toepast en onderhoudt. Meerdere keren is in de interviews wel aangegeven dat er een spanningsveld is tussen het toepassen van de BIO (overheids)maatregelen en de maatregelen die genomen (moeten) worden vanuit de specifieke internationale context van de Rijksorganisatie en dat zij daarbij hun eigen risicoafweging maken. Zo geven ministeries van Algemene Zaken, Defensie en Buitenlandse Zaken aan verplicht te zijn om ook te voldoen aan de specifieke informatiebeveiligingseisen in Europees en NATO verband. Denk hierbij aan de beveiliging van bijzondere informatie met een hoge vertrouwelijkheid.

Naast de BIO is ook behoefte aan andere informatiebeveiligingsstandaarden. Als onderwerpen worden benoemd: de beveiliging van applicaties & websites, de implementatie van 'application controls', de beveiliging van 'supply chains', de beveiliging van ketens en -afhankelijkheden (NATO/EU verband), en de beveiliging van medewerkers tegen fysieke bedreigingen en compromittering, en de aanpak voor statelijke actoren.

Onder de premisse dat de overheidsmaatregelen niet zullen wijzigen als gevolg van de nieuwe ISO 27001, zullen Rijksdiensten vooralsnog de nieuwe controls toepassen als die nodig blijken uit de risicoafweging. Omdat de implementatie dan afhangt van de risicoanalyse en de al genomen maatregelen, zal ieder traject per rijksdienst anders zijn. De Belastingdienst en een drietal departementen geven aan de mogelijke wijzigingen van de BIO (overheids)maatregelen op te nemen in hun onderhoudscyclus. Voor de departementen kent deze een cyclus van 3-5 jaar. De voorbereiding op het onderhoud zal extra werklast meebrengen en wordt ingeschat op 1 manjaar

[9] https://www.werkenvoornederland.nl/over-de-rijksoverheid/wat-is-de-rijksoverheid

of, bij het andere departement, op 2 manjaar. Een departement zal die capaciteit inhuren en schat de kosten daarvan in op euro 150K.

In het kort de samenvatting van de onderzoeksvragen voor de Rijksoverheid:

2. Welke aanpassingen willen betrokkenen doorvoeren in de huidige BIO?
   Alle.
3. Wat is de geschatte werklast voor aanpassing en de doorlooptijd van de BIO?
   De rijksdiensten geven aan de nieuwe BIO op te nemen in hun onderhoudscyclus. Drie departementen en de Belastingdienst geven expliciet aan. De werklast is voor de voorbereidingen en bedraagt een tot twee manjaar (obv 2 interviews).

5. Wat is de impact van een aangepaste BIO op de organisaties binnen de 4 bestuurslagen en op de organisaties waarmee de overheid samenwerkt? Met een focus op kosten, werklast, doorlooptijden, etc.
   Dit is voor de Rijksoverheid in algemene zin niet aan te geven. We schatten in dat de invoering meerdere jaren zal duren omdat de invoering veelal gekoppeld wordt aan de meerjarige onderhoudscyclus. De werklast en kosten zitten vooral in de voorbereidingen van de wijzigingen. Die worden voor zover gegeven ingeschat op een of twee manjaar. De kosten van een extern manjaar worden ingeschat op 150K.
6. Binnen welke termijn kan de aangepaste BIO van kracht zijn?
   Gemiddeld genomen na de onderhoudscyclus, die, voor zover aangegeven, maximaal 3-5 jaar duurt.
7. Wat is de impact op aanpassingen in de ondersteunende BIO-producten?
   b. Tools zoals ISMS-en en inkoophulpmiddelen?
   Het Ministerie van Algemene Zaken geeft aan dat de voorbereidingen van 1 jaar en werklast van 1 manjaar vooral bestaat uit het aanpassen van de specifieke hulpmiddelen die zij gebruikt voor de implementatie van de BIO.

3.4 Provincies

De inventarisaties voor de provincies zijn uitgevoerd met een vragenlijst. Van de twaalf provincies hebben vijf gereageerd. De resultaten van deze vijf beschouwen we als representatief.

Uit de beantwoording van de interview vragen komen de volgende punten naar voren:

- De provincies volgen hun eigen ontwikkeling in het implementeren van informatiebeveiliging en passen meerdere standaarden toe. Expliciet worden ISO27001/2 genoemd, naast andere standaarden voor procesautomatisering en informatiebeveiliging zoals Forum voor Standaardisatie, NIST, CSIR (RWS), CSA (Cloud), en auditnormen (DigiD).
- Op dit moment kunnen de provincies niet inschatten wat de impact van een gewijzigde BIO is op hun situatie. Enkele provincies geven aan dat men onderhanden is met de implementatie van informatiebeveiliging en de wijzigingen te zijner tijd worden geanalyseerd en ingepast. Er is één inschatting gegeven van de werklast (‘enkele weken’) en twee voor doorlooptijd (‘kwartaal’, ‘6-12 maanden’). Er zijn geen andere inschattingen gegeven over tijdsduur, werklast of kosten.

- De provincies geven aan dat er geen of slechts beperkte ondersteunende tooling aanwezig is ('dashboards', 'monitoring tools'). De impact voor provincies van een gewijzigde BIO op deze tooling lijkt daarom beperkt.
- Op de vraag naar de impact op leveranciers zijn zeer verschillende antwoorden gegeven. Veelal kan men de vraag (nog) niet beantwoorden of wordt 'nvt' ingevuld. Een antwoord geeft aan dat haar leverancier de ISO normen volgen en daarom meebewegen met de nieuwe wijzigingen, een ander antwoord geeft aan dat er eigenlijk per contract zou moeten worden bepaald wat er precies over het voldoen van de BIO is afgesproken ('check huidige contracten').

In het kort de samenvatting van de onderzoeksvragen voor de provincies:

2. Welke aanpassingen willen betrokkenen doorvoeren in de huidige BIO?
   Alle voor zover die passen in de context van de provincies.
3. Wat is de geschatte werklast voor aanpassing en de doorlooptijd van de BIO?
   Die is voor de provincies niet aan te geven. Er is een antwoord gegeven van 'enkele weken'. De gegeven inschattingen van doorlooptijden variëren van enkele weken tot 12 maanden.

5. Wat is de impact van een aangepaste BIO op de organisaties binnen de 4 bestuurslagen en op de organisaties waarmee de overheid samenwerkt? Met een focus op kosten, werklast, doorlooptijden, etc.
   Die is voor de provincies niet eensluidend aan te geven. Kosten en werklast worden niet benoemd, de inschattingen van doorlooptijden variëren van enkele weken tot 12 maanden.
6. Binnen welke termijn kan de aangepaste BIO van kracht zijn?
   Die is voor de provincies niet duidelijk aan te geven.
7. Wat is de impact op aanpassingen in de ondersteunende BIO-producten?
   b. Tools zoals ISMS-en en inkoophulpmiddelen?
      Provincies geven aan over weinig ondersteunende tooling te beschikken. De impact van een gewijzigde BIO lijkt dan ook beperkt.

3.5 Waterschappen

VKA heeft voor de impactanalyse van de waterschappen kunnen steunen op een coördinator die namens VKA de onderzoeksvragen heeft gesteld. Uit zijn verslag komt het volgende beeld van de impact naar voren.

Nederland kent 21 waterschappen. De BIO is kaderstellend voor de waterschappen voor het organiseren en toepassen van een voldoende niveau van informatiebeveiliging. De waterschappen hebben zich gecommitteerd om in 2024 de BIO controls te adresseren op basis van het BIO volwassenheidsmodel van het CIP. De waterschappen geven aan dat naast de BIO ook de IEC62443 wordt gehanteerd voor procesautomatisering. Uitgangspunt voor de waterschappen is aantoonbare 'digitale weerbaarheid'. Waterschappen gebruiken voornamelijk ISMS tooling als ondersteuning voor de BIO. Dit varieert van eigen excellijsten tot gespecialiseerde software.

Omdat nog veel waterschappen onderhanden zijn met de invoering van de BIO valt aan te nemen dat, gemiddeld gezien, geen hogere kosten verwacht worden. Omdat de meeste aanpassingen

van technische aard zijn, valt te verwachten dat de kostenstijgingen niet onverwacht groot zullen zijn en veelal opgevangen kunnen worden in bestaande life-cycle investeringen. Waterschappen die de BIO al volledig hebben ingevoerd verwachten een implementatieduur van 1 jaar.

Voor wat betreft de impact werklast van de waterschappen valt geen eensluidend beeld te schetsen. De veranderingen zijn nog onvoldoende bekend. De benodigde resources voor het doorvoeren van de maatregelen zullen sterk verschillen per waterschap. Wetende dat het merendeel van de waterschappen (~80%) nog druk bezig is met het implementeren van de BIO, valt te verwachten dat de aanpassingen voor het merendeel opgevangen kunnen worden binnen de bestaande planningen.

De impact voor de leveranciers van de waterschappen wordt als klein ingeschat. De meeste wijzigingen zijn technisch van aard. Het kan voorkomen dat bestaande contracten opgebroken moeten worden. Dit is geheel afhankelijk van de tijd die waterschappen zich gunnen om de vernieuwde maatregelen door te voeren. Veelal zal prioriteit gegeven worden aan het uitdienen van bestaande contracten. Door de 'groei' van de BIO bestaat het risico dat bestaande leveranciers niet kunnen voldoen aan de gestelde eisen. Een klein risico bestaat dat afscheid genomen dient te worden van bestaande leveranciers.

In het kort de samenvatting van de onderzoeksvragen voor de waterschappen:

2. Welke aanpassingen willen betrokkenen doorvoeren in de huidige BIO?
   De BIO is het kader voor informatiebeveiliging. Ze wordt toegepast waar nodig en aangevuld met andere normkaders, zoals CSIR. Bij de implementatie staat weerbaarheid centraal.
3. Wat is de geschatte werklast voor aanpassing en de doorlooptijd van de BIO?
   Deze varieert per waterschap. In algemene zin: hoe meer er nog gedaan moet worden aan de BIO hoe makkelijker de wijzigingen ingepast kunnen worden in het lopende traject. Een apart traject kan nodig zijn voor waterschappen die al ver zijn de BIO implementatie. De looptijd daarvan wordt ingeschat op een jaar.

5. Wat is de impact van een aangepaste BIO op de organisaties binnen de 4 bestuurslagen en op de organisaties waarmee de overheid samenwerkt? Met een focus op kosten, werklast, doorlooptijden, etc.
   Deze varieert per waterschap. Waterschappen die verder zijn met de invoering van de BIO verwachten een apart traject te moeten uitvoeren met een doorlooptijd van een jaar. Waterschappen die minder ver zijn met de implementatie (80%)hebben meer mogelijkheden om de wijzigingen te integreren in het lopende traject (project). Daardoor valt de impact op de werklast mee. De impact op kosten wordt laag ingeschat, omdat deze vooral technisch van aard zijn en worden opgevangen door de reguliere life cycle investeringen.
6. Binnen welke termijn kan de aangepaste BIO van kracht zijn?
   Dit is voor de waterschappen goed in te schatten. Men ziet de implementatie van de huidige BIO als een continu proces dat gepland is in 2024 gereed te zijn. Voor waterschappen die al gereed zijn met de BIO, zou een traject van een jaar nodig zijn. Als de beschrijving van de BIO wijzigingen, de risicoanalyses en de GAP analyse op tijd gereed zijn, namelijk voor eind 2023, dan kan een jaar later de implementatie afgerond zijn. En past dat geheel binnen de planning van 2024.
7. Wat is de impact op aanpassingen in de ondersteunende BIO-producten?

b. Tools zoals ISMS-en en inkoophulpmiddelen?
Waterschappen gebruiken vooral ISMS tooling voor de BIO. Deze variëren van Excels tot gespecialiseerde software. Een impact is niet aangegeven. Voor de gespecialiseerde software zal de leverancier hoogstwaarschijnlijk de aanpassingen verzorgen en is de impact relatief laag.

3.6 Gemeenten

Voor de impactanalyse van de gemeenten heeft VKA gesproken met VNG en niet met individuele gemeenten. De reden hiervoor is dat het niet mogelijk lijkt om met een beperkt aantal interviews een getrouw beeld op te bouwen over de impact van een gewijzigde BIO op gemeenten.

De VNG onderkent dat de 352 gemeenten ieder hun eigen ontwikkeling op het vlak van informatieveiligheid doormaken. Dat gemeenten verschillen in grootte en daarmee ook verschillen in mogelijkheden om de BIO in te voeren. Toch is de opgave voor iedere gemeente hetzelfde. Gemeente die al verder zijn met de invoering van de BIO hebben voordeel en zullen de nieuwe eisen als gevolg van de nieuwe ISO 27002 makkelijker implementeren.

Binnen de VNG voorziet de IBD (Informatiebeveiligingsdienst) de gemeenten van informatie en handreikingen om de BIO te implementeren. Daarnaast is de Agenda Digitale Veiligheid[10] opgesteld om gemeenten te ondersteunen bij het voorkomen en oplossen van cyberincidenten. In zogenaamde actielijnen zijn de onderwerpen verder uitgewerkt, zoals het risicogedreven werken. De IBD biedt hiervoor ook hulpmiddelen aan.

Het Bestuursbureau VNG heeft met de gemeenten de koers ingezet om informatieveiligheid op orde te krijgen, te verbeteren en onderhouden (resolutie ALV feb 2021). Met als basisniveau de BIO overheidsmaatregelen. Onderdeel daarvan is het periodiek onderhouden van de structuur en inhoud ervan. Daarmee is de impact van een nieuwe onderliggende standaard als ISO 27002 onderdeel van het proces dat al uitgevoerd moet worden. En daarmee is de impact voor gemeenten 'op papier' dus nul.

In het kort de samenvatting van de onderzoeksvragen voor de gemeenten:

2. Welke aanpassingen willen betrokkenen doorvoeren in de huidige BIO?
De BIO is het basisniveau voor informatiebeveiliging. Dit betekent dat de overheids-maatregelen volledig en verplicht worden ingevoerd, inclusief onderhoud daarvan. De nieuwe versie van ISO 27002 is een vorm van dit onderhoud.
3. Wat is de geschatte werklast voor aanpassing en de doorlooptijd van de BIO?
Deze varieert per gemeente. Hoe verder de gemeente is met de invoering van de BIO, hoe kleiner de werklast zal zijn.

5. Wat is de impact van een aangepaste BIO op de organisaties binnen de 4 bestuurslagen en op de organisaties waarmee de overheid samenwerkt? Met een focus op kosten, werklast,

[10] https://vng.nl/publicaties/agenda-digitale-veiligheid-2020-2024

doorlooptijden, etc.
Deze varieert per gemeente. Hoe verder de gemeente is met de invoering van de BIO, hoe kleiner de werklast zal zijn. Er is geen specifieke uitspraak te doen over kosten, werklast of doorlooptijd, omdat het onderdeel is van bestaand, deels al ingericht, onderhoud.

6. Binnen welke termijn kan de aangepaste BIO van kracht zijn?
   Dit is voor gemeenten niet direct in te schatten. De implementatie van de BIO is een continu proces.
7. Wat is de impact op aanpassingen in de ondersteunende BIO-producten?
   b. Tools zoals ISMS-en en inkoophulpmiddelen?
      Dit is niet verder aangeven door de VNG, zie hiervoor de inventarisatie van de IBD, paragraaf 2.3.

3.7 Naschrift VKA

Wat opvalt is dat VNG en waterschappen een ander beeld geven dan provincies en Rijk. Wij hebben hier geen nader onderzoek naar verricht. Wel is ons beeld dat bij gemeenten en waterschappen de invoering van informatiebeveiliging centraal gecoördineerd plaats vindt en dat bij provincies en het Rijk dit meer een zaak is van de individuele organisaties. In welke mate dat van invloed is op het beeld kunnen wij niet aangeven.

4 BESCHRIJVING IMPACT LEVERANCIERS

4.1 Inleiding

De beschrijving van de impact op leveranciers betreft de uitwerking van de vierde onderzoeksvraag, zijnde:

4. Wat is impact van het al dan niet volledig aanpassen van de BIO aan de NEN-ISO-27002 voor:
    a. reeds afgesloten dan wel af te sluiten contracten;
    b. ISO-27001 certificeringstrajecten?

4.2 Impact gewijzigde BIO op bestaande contracten

Ten behoeve van het onderzoek naar de impact van een gewijzigde BIO op bestaande en nieuwe contracten is gekeken naar de verschillende algemene inkoopvoorwaarden die gebruikt worden binnen de overheid. De verschillende bestuurslagen maken gebruik van gezamenlijke algemene inkoopvoorwaarden. Dit betreft voor het Rijk:

- de Algemene Rijksinkoopvoorwaarden voor het verstrekken van opdrachten tot het verrichten van diensten (ARVODI-2018, hierna: ARVODI); en
- de Algemene Rijksinkoopvoorwaarden bij IT-overeenkomsten (ARBIT-2018, hierna: ARBIT).

Voor de provincies betreft dit:

- de Algemene Inkoopvoorwaarden Provincies 2018 voor leveringen en diensten.

Voor de waterschappen betreft dit:

- de Algemene Waterschapsinkoopvoorwaarden ICT;
- de Algemene Waterschapsinkoopvoorwaarden voor leveringen (AWIV-2018, hierna: AWIV); en
- de Algemene Waterschapsinkoopvoorwaarden voor het verstrekken van opdrachten tot het verrichten van diensten 2018 (AWVODI-2018, hierna; AWVODI).

Voor de gemeenten betreft dit:

- de Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT); en
- de Gemeentelijke ICT Kwaliteitsnormen.

Deze algemene voorwaarden maken geen vermelding van de BIO, maar verwijzen naar 'het in acht nemen van beveiligingsprocedures' van de opdrachtgever (art. 15 ARVODI, art. 19 Algemene waterschapsinkoopvoorwaarden). In contracten die gebruik maken van deze algemene voorwaarden moet men in de onderliggende documentatie onderzoeken welke specifieke afspraken gemaakt zijn voor beveiliging en compliance aan de BIO.

De inkoopvoorwaarden van de provincies maken geen vermelding van beveiliging. Wel is de opdrachtnemer conform art. 4(5) Algemene Inkoopvoorwaarden Provincies 2018 verplicht om "alle van toepassing zijnde wettelijke eisen en overige overheidsvoorschriften" na te leven.

Informatiebeveiligingseisen dienen daarom nog altijd vastgesteld en overeengekomen te worden tussen de provincie en de leverancier ex. 15.1.2 BIO.

In alle bovengenoemde situaties is het echter alleen verplicht om te voldoen aan beveiligingsprocedures en vastgestelde informatiebeveiligingseisen. Compliance aan een gewijzigde BIO is hier niet inherent onderdeel van, tenzij dit zo is overeengekomen. Als dit niet het geval is zal de impact van een gewijzigde BIO nihil zijn.

Een uitzondering hierop is de situatie voor de gemeenten. In de Gemeentelijke ICT kwaliteitsnormen is in 4.3 opgenomen dat "de ICT prestatie dient de functionele en technische mogelijkheden te hebben zodat de Opdrachtgever kan voldoen aan de Baseline Informatiebeveiliging Overheid (BIO)." Afhankelijk van de aard van de ICT prestatie kan een gewijzigde BIO grote impact hebben op dergelijke contracten door de inzichten die de nieuwe BIO kan bieden op de specifieke terreinen van de nieuwe controls. Belangrijk is het om hierbij op te noemen dat art. 25(1) jo. 25(2) GIBIT de mogelijkheid bieden om een andere norm voor informatiebeveiliging overeen te komen dan de BIO. Als de gemeenten met hun leveranciers overeengekomen zijn dat bijvoorbeeld een ISO27001 certificaat volstaat zal een gewijzigde BIO geen problemen veroorzaken – het certificaat blijft immers geldig voor een termijn van drie jaar, ook na wijziging van de norm.

Indien de overheidsorganisatie met een leverancier overeengekomen is dat de leverancier dient te voldoen aan alle controls van een actuele versie van de BIO kan het voorkomen dat het contract mogelijk opgebroken moet worden. Hierbij zullen opdrachtgever en opdrachtnemer gezamenlijk moeten afspreken welke hersteltermijn de opdrachtnemer krijgt om diens product wederom compliant aan de BIO te laten zijn, of dat het contract daadwerkelijk opengebroken moet worden. Dit moet geschieden al naar gelang redelijkheid en billijkheid, oftewel in casu de vraag of de instandhouding van het contract dusdanig zware gevolgen heeft voor de overheidsinstantie dat dit niet meer redelijkerwijs verwacht kan worden.

4.3 Impact gewijzigde BIO op nieuwe contracten

Bij het opstellen van nieuwe contracten gelden in feite dezelfde regels als bij bestaande contracten. Het is echter een stuk gemakkelijker om bij nieuwe contracten concrete afspraken nog te maken over de beveiligingsprocedures en daarbij rekening te houden met de gewijzigde BIO.

Zeker voor gemeenten, waarbij compliance aan de BIO verplicht is tenzij een andere norm voor informatiebeveiliging is overeengekomen, biedt dit een uitkomst om bij het sluiten van nieuwe contracten rekening te houden met het feit dat ook leveranciers tijd nodig zullen hebben om compliant te zijn met de gewijzigde BIO.

Leveranciers maken echter vooral gebruik van ISO27001-certificeringen. Na de 'transitieperiode' zullen zij, om een certificering te behouden, uiterlijk drie jaar na invoering van de nieuwe ISO een

hercertificering volgens de nieuwe ISO 27001 moeten halen. Hiermee blijven zij ook compliant aan een gewijzigde BIO.

De impact van een gewijzigde BIO op nieuwe contracten kan dan ook als minimaal beschouwd worden, voornamelijk aangezien onder de huidige algemene voorwaarden opdrachtgever en -nemer gezamenlijk overeen kunnen komen welke norm voor informatiebeveiliging zij willen hanteren.

4.4 Impact gewijzigde BIO op certificeringstrajecten bij leveranciers

In 2013 is de vorige versie van ISO 27001 en ISO 27002 verschenen. Voor de Nederlandse context zijn deze ISO normen vertaald naar de NEN-ISO/IEC 27001:2017 en NEN-ISO/IEC 27002:2017. Dit zijn 1:1 vertalingen van de 2013 normen.

In 2018 heeft de International Organization for Standardization (ISO) geconstateerd dat ISO 27002 van 2013 herzien moest worden. Naar verwachting zal de nieuwe versie volgend jaar, 2022, ook in het Nederlands worden gepubliceerd. Omdat de controls uit ISO 27002 ook in ISO 27001 (Annex A) worden gebruikt, zal ook deze norm ook worden herzien.

De herziening van ISO 27001 heeft ook impact op de gerelateerde normen, zoals ISO 27017, ISO 27018, ISO 27701, ISO 27799/NEN 7510, en uiteraard de BIO, want zij steunen grotendeels op de Annex A. Het is niet de verwachting dat deze normen meteen zullen worden herzien, omdat ze hun eigen startdatum en ontwikkeling kennen. Zo duurde het van 2013 tot 2017 alvorens NEN 7510 werd herzien. En ISO 27701 is een relatief jonge norm uit 2019 waardoor het nog zeker tot 2024 duurt alvorens hier een beslissing over wordt genomen.

Wat betekent de wijziging van de ISO 27002 nu voor de leveranciers van de overheid? Hier zijn twee groepen te onderscheiden: leveranciers die al gecertificeerd zijn en leveranciers die nog niet zijn gecertificeerd.

4.4.1 Nog niet ISO 27001 gecertificeerd

Zodra de nieuwe ISO 27002 verschijnt zal ook een overgangsperiode worden vastgesteld. Die periode is vermoedelijk twee of drie jaar. Leveranciers kunnen tijdens de overgangsperiode nog certificeren tegen de voorafgaande versie van ISO 27001. Dit is met name interessant voor leveranciers die al ver zijn met de implementatie van de 2013 variant van ISO 27001.

4.4.2 Wel ISO 27001 gecertificeerd

Leveranciers die wel beschikken over een bestaand certificaat van ISO 27001, kunnen dat verlengen tijdens overgangsperiode. Pas op het moment van de hercertificering, na drie jaar, zal de toetsing verplicht gaan plaatsvinden volgens de 2022-variant. Dit betekent dat leveranciers, technisch gezien, twee tot drie jaar de tijd hebben om zich aan te passen aan de nieuwe eisen.

Praktisch gezien zullen de Certificerende Instellingen (CI) hun klanten al snel vragen om een plan van aanpak voor te bereiden en dat plan ook toetsen. Daarmee wordt voorkomen dat leveranciers te laat starten met hun aanpassingen.

4.4.3 Consequenties voor de bestuurslagen

Voor de overheden die gebruiken maken van ISO 27001 gecertificeerde leveranciers betekent dat met de duale periode een fase van twee tot drie jaar in werking treedt. Dat is uiteraard afhankelijk van gestelde overgangsperiode. Tijdens de duale periode zijn er twee certificeringen van ISO 27001 geldig. Ook kan in specifieke gevallen de Verklaring van Toepasselijkheid de nieuwe nummering zal bevatten van ISO 27001, terwijl de specifieke controls uit de gerelateerde norm, denk aan NEN 7510, nog de oude nummering volgen.

Na de duale periode zijn alle certificeringen vernieuwd en volgens de nieuwe ISO 27001. Daarbij heeft de leverancier keuzevrijheid om zelf de specifieke maatregelen te bepalen. Mochten bestuurslagen tijdens die periode al specifieke eisen willen stellen aan maatregelen van leveranciers, of de deadline willen verkorten, dan leidt dit tot contractaanpassingen. En treden dan scenario's in werking zoals beschreven onder paragraaf 4.2 en 4.3.

5 CONCLUSIES EN AANBEVELINGEN

5.1 Onderzoeksvragen

Dit onderzoek geeft een antwoord op de vraag wat de impact is van de komende ISO 27002 wijzingen op de huidige BIO en de verdere implementaties daarvan. In onderstaande paragrafen lichten wij onze conclusies op de verschillende onderzoeksvragen toe en geven we onze aanbevelingen.

5.1.1 Impact nieuwe ISO 27002 op BIO

Indien besloten wordt dat de BIO de nieuwe ISO 27002 volgt, dan zal dit leiden tot wijzigingen in de BIO. De BIO zal opnieuw ingedeeld moeten worden. Bestuurslagen geven aan dat ze alle nieuwe controls zinvol achten, daarom kan de nieuwe ISO 27002 volledig gebruikt worden voor de nieuwe versie van de BIO.
Kern IBO heeft aangegeven dat geen nieuwe overheidsmaatregelen worden toegevoegd aan de nieuwe BIO. Daarmee is de impact op dat punt gering voor de bestuurslagen.
Het invoeren van de overige controls vindt conform de BIO plaats op basis van een risicoafweging en is onderdeel van het reguliere proces van beoordeling van risico's en maatregelen binnen de organisatie. Afhankelijk van de situatie van de organisatie en de uitgevoerde risicoafweging kan de impact van de nieuwe controls meer of minder zijn.

Advies
Start het traject voor het aanpassen van de BIO op korte termijn op. Met behulp van de nieuwe BIO versie kan ook beter aan de bestuurslagen uitgelegd worden wat de exacte wijzigingen zijn. Benadruk daarbij dat de invoering van controls altijd gebaseerd is en een risicoafweging. Benadruk dat de controls altijd op basis van een risicoafweging vertaald moeten worden naar concrete maatregel. Daarvoor kunnen de implementatierichtlijnen als inspiratie worden gebruikt. De overheidsmaatregelen blijven verplicht en zijn onvervreemdbaar.

5.1.2 Welke aanpassingen willen betrokkenen doorvoeren in de huidige BIO?

Alle 13 nieuwe ISO controls worden als zinvol en van toegevoegde waarde beschouwd. De bestuurslagen zijn bereid om deze aanpassingen in te voeren wanneer deze volgen uit de eigen risicoanalyses.

Advies
Neem in de nieuwe BIO alle (nieuwe) maatregelen over uit de nieuwe versie van de ISO 27002.

5.1.3 Geschatte werklast voor aanpassing en de doorlooptijd van de BIO

Deze vraag overlapt sterk met de vraag uit paragraaf 5.1.5. Die voegt als extra nog de kosten toe. We behandelen daarom beide vragen onder paragraaf 5.1.5.

5.1.4 Impact aanpassen BIO aan ISO 27002 voor contracten en certificeringen

CONTRACTEN

In alle binnen de bestuurslagen gehanteerde algemene voorwaarden is het alleen verplicht om te voldoen aan beveiligingsprocedures en vastgestelde informatiebeveiligingseisen. Compliance aan een gewijzigde BIO is hier niet expliciet in vermeld, tenzij dit apart wordt overeengekomen. Een uitzondering hierop zijn de gemeentelijke inkoopvoorwaarden, waar tenzij anders overeengekomen, de ICT prestatie de functionele en technische mogelijkheden dient te hebben zodat de Opdrachtgever kan voldoen aan de Baseline Informatiebeveiliging Overheid (BIO)." Gezien de mogelijkheid tot het anders overeenkomen dan bovenstaande is de impact van de nieuwe BIO bij het toepassen van de algemene voorwaarden nihil.

Als een overheidsorganisatie met een leverancier overeengekomen is dat de leverancier compliant dient te zijn aan een actuele versie van de BIO kan het voorkomen dat het contract mogelijk opgebroken moet worden. Hierbij zullen opdrachtgever en opdrachtnemer gezamenlijk moeten afspreken welke hersteltermijn de opdrachtnemer krijgt om wederom compliant aan de BIO te zijn, of dat het contract daadwerkelijk opengebroken moet worden. Hierbij geldt het algemene principe van redelijkheid en billijkheid, in casu de vraag of de instandhouding van het contract dusdanig zware gevolgen heeft voor de overheidsinstantie dat dit niet meer redelijkerwijs verwacht kan worden.

Bij het opstellen van nieuwe contracten gelden in feite dezelfde regels als bij bestaande contracten. Het is echter een stuk gemakkelijker om bij nieuwe contracten concrete afspraken nog te maken over de beveiligingsprocedures en daarbij rekening te houden met de gewijzigde BIO.

De impact van een gewijzigde BIO op nieuwe contracten kan dan ook als minimaal beschouwd worden, omdat onder de huidige algemene voorwaarden opdrachtgever en -nemer gezamenlijk overeen kunnen komen welke norm voor informatiebeveiliging zij willen hanteren.

<u>Advies</u>

Bij het toepassen van de algemene voorwaarden zal er weinig impact zijn op bestaande contracten zijn door wijzigingen in de BIO. Kern IBO geeft aan geen nieuwe overheidsmaatregelen te introduceren. Daarnaast is die impact alleen van toepassing als compliance aan de BIO expliciet is afgesproken is in het contract. Bepaald dan per contract de impact. Bij nieuwe contracten kan bepaald worden of compliancy aan de BIO is eis wordt gesteld.

CERTIFICERINGEN

Voor de overheden die gebruiken maken van ISO 27001 gecertificeerde leveranciers betekent de wijziging van ISO 27002 dat de duale periode van twee tot drie jaar in werking treedt. Tijdens de duale periode zijn beide certificeringen van ISO 27001, die van 2013 en 2022, geldig. De duale periode is uiteraard afhankelijk van de dan ingestelde overgangsperiode. Na de duale periode zijn alle certificeringen vernieuwd en volgens de nieuwe ISO 27001:2022. Daarbij heeft de leverancier

keuzevrijheid om zelf de specifieke maatregelen te bepalen. Mochten bestuurslagen tijdens die periode al specifieke eisen willen stellen aan maatregelen van leveranciers, of de deadline willen verkorten, dan leidt dit tot contractaanpassingen.

Advies

In het algemeen zal er weinig impact zijn op bestaande en lopende ISO certificeringen bij leveranciers. Na de duale periode zijn alle certificeringen vernieuwd. We adviseren om de duur van de overgangsperiode af te wachten en alleen extra eisen te stellen, of kortere deadlines te eisen, als dat echt vanuit de risicoanalyse van de organisatie nodig is.

5.1.5 Impact van een aangepaste BIO op de organisaties binnen de 4 bestuurslagen

De impact van een aangepaste BIO in termen van werklast, kosten en doorlooptijd zijn binnen het bestek van deze opdracht niet exact kwantitatief te duiden voor de bestuurslagen. Het niveau van implementatie van de BIO wisselt sterk in de bestuurslagen en is niet in algemene zin per bestuurslaag aan te geven.

Uit de reacties die wij ontvangen hebben blijkt de impact te variëren van klein tot groot. Indien de 13 nieuwe controls volledig doorgevoerd moeten worden in de organisatie als gevolg van de risicoanalyse: een werklast van een tot twee manjaar met een doorlooptijd: enkele weken tot 5 jaar, afhankelijk van de onderhoudscyclus dat organisaties aanhouden voor het aanpassen van de controls. Belangrijk is hier onderscheid te maken tussen organisaties die voorne mens zijn de wijzigingen in projectvorm uit te voeren en de organisaties die de wijzigingen uitvoeren als onderdeel van de lopende onderhoudscyclus. Die cycli zijn lang: 3-5 jaar, en vertegenwoordigen niet de daadwerkelijke (snelste) implementatietermijn. Er zijn nu nog geen nauwkeurige schattingen per bestuurslaag aan te geven. De inschatting hangt sterk af van de situatie van een specifieke organisatie.

De BIO gaat uit van risicomanagement als integraal startpunt voor de implementatie van maatregelen. In de praktijk zien we twee benaderingen bij overheidsorganisaties:

3. Een compliance based benadering waarbij de focus gelegd wordt op de implementatie van overheidsmaatregelen. Als de overheidsmaatregelen niet of zeer beperkt wijzigen bij de nieuwe BIO versie, zullen deze organisaties weinig impact van de nieuwe versie ondervinden.
4. Een risicogebaseerde benadering, waarbij de focus ligt de analyse van bedreigingen en risico's en vervolgens op het toepassen van de controls. Bij implementatie van de nieuwe BIO versie zullen deze organisaties afhankelijk van de bedreigingen en risico's de nieuwe controls waar nodig inpassen.

Nota bene: ons onderzoek is niet gericht geweest op het vaststellen van welke benadering de bestuurslagen hanteren, we kunnen daar geen uitspraak over doen.

Advies

Het is van belang expliciet te maken voor welke maatregelen de compliance based benadering geldt en voor welke maatregelen de risicobenadering.

5.1.6 Termijn waar binnen de aangepaste BIO van kracht kan zijn

In de vorige paragraaf is aangegeven dat er verschillende beelden zijn bij de inschatting van de totale doorlooptijd van de invoering van de gewijzigde BIO. Als we het stappenplan volgen voor de implementatie van de nieuwe BIO, dan zou de eerste stap, namelijk de wijzigingen in kaart brengen, naar schatting een half jaar in beslag nemen. Daarna kunnen (representatieve) organisaties op basis hiervan hun risicoanalyses en GAP analyses uitvoeren. Afhankelijk van de aanpak, project of onderhoud, kan al een inschatting gegeven worden van de totale doorlooptijd. In het geval van departementen zijn die onderhoudstermijnen lang (3-5 jaar). Als we inschatten dat de GAP analyse in 6 maanden kunnen worden uitgevoerd, dan zou de termijn liggen tussen 1 en 6 jaar, als maximum. De waterschappen geven het meest concreet een einddatum aan: eind 2024 is de BIO ingevoerd, inclusief de nieuwe wijzigingen.

Advies

Op basis van onze inschatting moet het mogelijk zijn om binnen een jaar een duidelijker beeld te krijgen van de tijdslijnen. Dan zouden een aantal risico- en GAP analyses binnen de bestuurslagen afgerond kunnen zijn. We adviseren kern IBO dit traject in gang te zetten.

5.1.7 Impact nieuwe ISO 27002 op aanpassingen in de ondersteunende BIO-producten

ONDERSTEUNENDE TOOLING EN BEST PRACTICES VAN IBD EN CIP

IBD en CIP bieden beiden kennisproducten voor de implementatie van de BIO. De impact van een gewijzigde BIO wordt anders ingeschat. Waar de IBD de wijzigingen ziet als onderdeel de lopende onderhoudscyclus en als het ware absorbeert, verwacht CIP juist grote inspanning te moeten leveren om de wijzigingen door te voeren.

Advies

Draag zorg voor uitwisseling van kennis en ervaring tussen IBD en CIP, zodat bestuurslagen op een vergelijkbare wijze ondersteund kunnen worden.

ONDERSTEUNENDE TOOLING BINNEN BESTUURSLAGEN, ZOALS ISMS-EN EN INKOOPHULPMIDDELEN

Over het algemeen wordt binnen de bestuurslagen beperkt gebruik gemaakt van eigen tooling. Het ministerie van Algemene Zaken geeft, als enige, heel duidelijk aan uitgebreid gebruik te maken van eigen hulpmiddelen en analysetools. Als het gaat om specialistisch ingekochte software door bestuurslagen, verwachten wij dat de leverancier de gewijzigde BIO zal overnemen en de organisaties helpen met de overgang.

Advies

In algemene zin schatten we de impact als laag in voor de ondersteunende tooling van de bestuurslagen.

A Bijlage: Inzichten voor de evaluatie

De opdrachtgever heeft de onderzoekers verzocht om de beelden die tijdens de interviews over de BIO naar voren en die relevant kunnen zijn voor de evaluatie van de BIO apart te noteren.

Onderstaand geven wij deze beelden weer.

De implementatie van de BIO steunt op het uitvoeren van risicomanagement. Respondenten geven aan dat de beschreven risicobenadering in de BIO niet aansluit op de eigen praktijk en context. Men zoekt naar een strategische risicobenadering, waarbij de BIO één van de invalshoeken is naast andere beveiligingsstandaarden.

Respondenten geven aan dat naast de BIO ook behoefte is aan andere normkaders. Zo wordt aangegeven dat de BIO zich vooral richt op kantoorautomatisering en minder op procesautomatisering (ICS/SCADA). Daarnaast is er behoefte aan invulling van thema's als 'application controls' of 'de beveiliging van web sites'.

De BIO biedt nu (vooral) een tactisch handelingsperspectief op informatiebeveiliging. Respondenten geven aan ook op zoek te zijn naar het handelingsperspectief voor de bestuurstafel. Door meer aandacht te besteden aan risicomanagement op strategisch niveau, wordt informatiebeveiliging ook meer een zaak van het bestuur.

De IBD heeft een duidelijke rol op zich genomen voor het beheren van de BIO standaard voor gemeenten. Voor de andere bestuurslagen bestaan dergelijke centrale beheersorganisaties niet. Andere bestuurslagen kijken wel naar de ondersteuning door het CIP.

ZBO's hoeven niet te voldoen aan BIO overheidsmaatregelen. Een aantal ZBO's maakt wel gebruik van de BIO om een vergelijkbaar beveiligingskader te hanteren als de overige overheidsinstanties waar zij gegevens mee uitwisselen. Een aantal ZBO's speelt echter wel een grote rol bij de kwaliteitsborging en de beveiliging van (persoons-)data, zoals de basisregistraties[1]. Nagagaan zou kunnen worden om ZBO's nauwer te betrekken bij de implementatie van de BIO.

[1] https://www.digitaleoverheid.nl/dossiers/basisregistraties/

B Bijlage: Lijst geïnterviewden

Organisatie	Geïnterviewde(n) Expertisegebied/Functie
Belastingdienst	Inge Wertwijn Architect Security en kwaliteit
Drents Overijsselse Delta	Rob de Lange Informatieadviseur/CISO
Ministerie van Algemene Zaken	Frederik van der Burg CISO en DPO
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	Bart Pieters CIO Rijk Senior adviseur informatiebeveiliging
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	Erik van der Zeeuw Adviseur informatieveiligheid Kerndepartement en uitvoeringsorganisaties
Ministerie van Buitenlandse Zaken	Edwin Haaring CISO
Ministerie van Defensie	René Visser CISO
Ministerie van Sociale Zaken en Werkgelegenheid	Freddie Muller CISO
Provincie Drenthe	David van der Meer Coördinator informatiebeveiliging
Provincie Flevoland	Hilko Batterink CISO
Provincie Groningen	Michel Wekema CISO
Provincie Noord-Holland	Pieter de Ruiter CISO
Provincie Overijssel	Dirk Jan Muntendam CISO
Provincie Utrecht	Casper Schutte CISO
RDW (ZBO - Ministerie van Infrastructuur en Waterstaat)	Gert Maneschijn CSO Hans Borsboom
Vereniging Nederlandse Gemeenten	Kato Vierbergen Programmamanager Agenda Digitale Veiligheid
Vereniging Nederlandse Gemeenten	Kees Hintzbergen Senior adviseur informatiebeveiliging
Waterschappen	Inventarisatie namens de waterschappen Rob de Lange Waterschap Drents Overijsselse Delta CISO

C Bijlage Nieuwe ISO 27002 controls

Code	Omschrijving
5.7	Threat Intelligence
5.23	Information security for use of cloud services
5.30	ICT readiness for business continuity
7.4	Physical security monitoring
8.9	Configuration management
8.10	Information deletion
8.11	Data masking
8.12	Data leakage prevention
8.13	Information protection using digital rights technologies
8.17	Monitoring activities
8.21	Vulnerability disclosure and handling in delivering ICT products and services
8.24	Web filtering
8.30	Secure coding

D Wijzigingen ISO 27002:2018 versus 2021

ISO /IEC 27002 (E) control identifier	ISO IEC 27002:2013 control identifier	Control name
5.1	5.1.1, 5.1.2	Policies for information security
5.2	6.1.1	Information security roles and responsibilities
5.3	6.1.2	Segregation of duties
5.4	7.2.1	Management responsibilities
5.5	6.1.3	Contact with authorities
5.6	6.1.4	Contact with special interest groups
5.7	New	Threat Intelligence
5.8	6.1.5, 14.1.1	Information security in project management
5.9	8.1.1, 8.1.2	Inventory of information and associated assets
5.10	8.1.3, 8.2.3	Use of information and associated assets
5.11	8.1.4	Return of assets
5.12	8.2.1	Classification of information
5.13	8.2.2	Labelling of information
5.14	13.2.1, 13.2.2, 13.2.3	Information transfer
5.15	9.1.1, 9.1.2	Information transfer
5.16	9.2.1	Identity management
5.17	9.2.4, 9.3.1, 9.4.3	Authentication information
5.18	9.2.2, 9.2.5, 9.2.6	Access rights
5.19	15.1.1	Information security in supplier relationships
5.20	15.1.2	Addressing information security within supplier agreements
5.21	15.1.3	Managing information security in the ICT supply chain
5.22	15.2.1, 15.2.2	Monitoring, review and change management of supplier services
5.23	New	Information security for use of cloud services
5.24	16.1.1	Information security incidents responsibilities and procedures
5.25	16.1.4	Assessment and decision on information security events
5.26	16.1.5	Response to information security incidents
5.27	16.1.6	Learning from information security incidents
5.28	16.1.7	Collection of evidence

5.29	17.1.1, 17.1.2, 17.1.3	Information security during disruption
5.30	New	ICT readiness for business continuity
5.31	18.1.1, 18.1.5	Identification of legal, statutory, regulatory and contractual requirements
5.32	18.1.2	Intellectual property rights
5.33	18.1.3	Protection of records
5.34	18.1.4	Privacy and protection of personally identifiable information
5.35	18.2.1	Independent review of information security
5.36	18.2.2, 18.2.3	Compliance with information security policies and standards
5.37	12.1.1	Documented operating procedures
6.1	7.1.1	Screening
6.2	7.1.2	Terms and conditions of employment
6.3	7.2.2	Information security awareness, education and training
6.4	7.2.3	Disciplinary process
6.5	7.3.1	Responsibilities after termination or change of employment responsibilities
6.6	13.2.4	Confidentiality or non-disclosure agreements
6.7	6.2.2	Remote working
6.8	16.1.2, 16.1.3	Information security event reporting
7.1	11.1.1	Physical security perimeter
7.2	11.1.2, 11.1.6	Physical entry controls
7.3	11.1.3	Securing offices, rooms and facilities
7.4	New	Physical security monitoring
7.5	11.1.4	Protection against physical and environmental threats
7.6	11.1.5	Working in secure areas
7.7	11.2.9	Clear desk and clear screen
7.8	11.2.1	Equipment siting and protection
7.9	11.2.6	Security of assets off-premises
7.10	8.3.1, 8.3.2, 8.3.3	Storage media
7.11	11.2.2	Supporting utilities
7.12	11.2.3	Cabling security
7.13	11.2.4	Equipment maintenance
7.14	11.2.7	Secure disposal or re-use of equipment
8.1	6.2.1, 11.2.8	Endpoint devices
8.2	9.2.3	Privileged access rights
8.3	9.4.1	Information access restriction
8.4	9.4.5	Access control to source code
8.5	9.4.2	Secure authentication
8.6	12.1.3	Capacity management

8.7	12.2.1	Malware protection
8.8	12.6.1, 18.2.3	Management of technical vulnerabilities
8.9	New	Configuration management
8.10	New	Information deletion
8.11	New	Data masking
8.12	New	Data leakage prevention
8.13	New	Information protection using digital rights technologies
8.14	12.3.1	Information backup
8.15	17.2.1	Redundancy of information processing facilities
8.16	12.4.1, 12.4.2, 12.4.3	Logging
8.17	New	Monitoring activities
8.18	12.4.4	Clock synchronization
8.19	9.4.4	Use of privileged utility programs
8.20	12.5.1, 12.6.2	Installation of software on operational systems
8.21	New	Vulnerability disclosure and handling in delivering ICT products and services
8.22	13.1.1	Network controls
8.23	13.1.2	Security of network services
8.24	New	Web filtering
8.25	13.1.3	Segregation in networks
8.26	10.1.1, 10.1.2	Use of cryptography
8.27	14.2.1	Secure development lifecycle
8.28	14.1.2, 14.1.3	Application security requirement
8.29	14.2.5	Secure system architecture and engineering principles
8.30	New	Secure coding
8.31	14.2.8, 14.2.9	Secure testing in development and acceptance
8.32	14.2.7	Outsourced development
8.33	12.1.4, 14.2.6	Separation of development, test and production environments
8.34	12.1.2, 14.2.2, 14.2.3, 14.2.4	Change management
8.35	14.3.1	Protection of test information
8.36	12.7.1	Protection of information systems during audit and testing