Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

de colleges van burgemeester & wethouders, de gedeputeerden van de provincies, de dijkgraven van de waterschappen, de directeuren van de uitvoeringsorganisaties

P.S.

INGEKOMEN 30 APR. 2019

Directoraat-Generaal OverheidsOrganisatie
Directie Informatiesamenleving en Overheid

Turfmarkt 147
2511 DP
Postbus 20011
2500 EA Den Haag

Datum
16 april 2019

Kenmerk
2019-0000184156

circulaire

Onderwerp	Toepassen van de Baseline Informatiebeveiliging Overheid in het digitale verkeer met het Rijk
Doelstelling	Informatie
Juridische grondslag	MR besluit
Relaties met andere circulaires	
Ingangsdatum	1 januari 2020
Geldig tot	

Geacht college, geacht bestuur,

Met deze circulaire informeer ik u over het normenkader inzake informatiebeveiliging.

De Ministerraad van 14 december 2018 heeft de Baseline Informatiebeveiliging Overheid (BIO) vastgesteld voor het Rijk en in het interbestuurlijk verkeer met het Rijk. De BIO is:

- een gemeenschappelijk normenkader, gebaseerd op de internationale norm ISO 27001/2 voor de beveiliging van de informatie(systemen) van de overheid;
- een afgeleide van de huidige BIR2017, die al in werking is voor het Rijk;
- een concretisering van een aantal normen tot verplichte overheidsmaatregelen.

Iedere overheidslaag heeft besloten de bestaande eigen baseline informatiebeveiliging te vervangen door de BIO. Het gevolg van bovengenoemde besluiten is dat alle overheidsorganisaties hun bestaande sectorale baselines zullen vervangen door de BIO. De BIO vervangt voor de gemeenten, waterschappen, provincies en het Rijk respectievelijk de BIG, BIWA, IBI en de BIR2017[1].

Om te voorkomen dat het Rijk in de informatie-uitwisseling met andere bestuurslagen andere normen gaat eisen, heeft de Ministerraad besloten om de

[1] BIG staat voor Baseline Informatiebeveiliging Gemeenten, BIWA voor Baseline Informatiebeveiliging Waterschappen, IBI voor Interprovinciale Baseline Informatiebeveiliging en BIR voor Baseline Informatiebeveiliging Rijksdienst.

BIO te hanteren in de informatie-uitwisseling tussen het Rijk en **alle** bestuurslagen.

Achtergrond
Cybersecurity heeft verscherpte aandacht vanuit de Tweede Kamer. In de Nederlandse Cybersecurity Agenda van de minister J&V is opgenomen dat (citaat) "het verder uniformeren en harmoniseren van normenkaders op informatiebeveiliging, waaronder de totstandkoming en implementatie van een Baseline Informatiebeveiliging Overheid (BIO) onder verantwoordelijkheid van BZK verder vorm krijgt".

De BIO is het gezamenlijke product van en is afgestemd met Rijk, provincies, gemeenten en waterschappen. Een interbestuurlijke werkgroep Normatiek, waarin alle bestuurslagen vertegenwoordigd zijn, heeft de BIO de afgelopen jaren ontwikkeld en per mei 2018 afgerond na consultatie bij professionele gemeenschappen in de verschillende overheidslagen.

Ondersteuning
Implementatie van de BIO is en blijft de eigen verantwoordelijkheid van overheidsorganisaties. Om hen daarbij te ondersteunen heeft het Ministerie van BZK een ondersteuningsprogramma ingericht bij het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) om overheidsorganisaties te ondersteunen bij het implementeren van de BIO in hun organisatie. Dit programma is afgestemd met alle bestuurslagen en is aanvullend op wat bestuurslagen zelf al ondernemen om de implementatie vorm te geven.

Het ondersteuningsprogramma geeft een impuls aan implementatie van de BIO. Het is gericht op een nadere verankering van de BIO (en daarmee informatieveiligheid) door ondersteunen van beheer en onderhoud, inhoudelijke verdieping op informatieveiligheid, ontwikkeling van hulpinstrumenten, het vergroten van bewustzijn (gerichtheid op veiligheid door toepassen van de baseline) en het bevorderen van kennis en kunde onder de betrokkenen. Het ondersteuningsprogramma loopt in 2019 en 2020.

Overheidsorganisaties die gebruik willen maken van het ondersteuningsprogramma kunnen terecht op https://www.bio-overheid.nl. Ik moedig u aan om van de diensten van het ondersteuningsprogramma gebruik te maken.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

drs. R.W. Knops

BIO Versie 1

De Baseline Informatiebeveiliging Overheid (BIO) is geheel gestructureerd volgens NEN-ISO/IEC 27001:2017, bijlage A en NEN-ISO/IEC 27002:2017. Het Forum Standaardisatie heeft deze normen opgenomen in de 'pas toe-of-leg uit'- lijst met verplichte standaarden voor de publieke sector, volgens het comply or explain principe. Dit betekent dat de overheid deze normen toepast tenzij er expliciet geformuleerde redenen zijn om dat niet te doen.

De BIO beschrijft de invulling van de NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017 voor de overheid. Met klem vermeldt zij dat de BIO deze normen niet vervangt.

In de BIO hebben specifieke overheidsmaatregelen de tekstkleur groen. NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017 beschrijven details voor implementatie (implementatierichtlijnen) en eisen voor de procesinrichting (o.a. het ISMS uit NEN-ISO/IEC 27001:2017). Die documenten geven dus de details voor de toepassing, die niet in de BIO zijn beschreven en die nodig blijven voor een goede implementatie van de BIO.

Het gebruik van de NEN-ISO/IEC normen 27001 en 27002 in de BIO is auteursrechtelijk beschermd.

Het gebruik van teksten uit deze normen in de BIO geschiedt met toestemming van het Nederlands Normalisatie Instituut. Voor meer informatie over de NEN en het gebruik van hun producten zie: www.nen.nl

Wijzigingshistorie:

VERSIE	DATUM	OPMERKINGEN
0.1	11-6-2017	Aanpassingen van BIR 2017 versie 0.6
0.2	11-7-2017	Omschrijven naar ISO 27001 aanpak (hoofdstuk 4), samenvoegen hoofdstuk 3 en 4, ISO 27001 aanpak in hoofdstuk 4, tekstuele aanpassing controls (must/should)
0.3		Verschillende opmerkingen verwerkt
0.4	10-10-2017	Diverse opmerkingen verwerkt van leden, splitsen baseline in 2 delen, analoog aan de BIR2017
0.5	20-10-2017	Hoofdstuk 4 toegevoegd in deel 2 om ISMS te borgen als control / maatregel
0.6	20-02-2018	Verder aanscherping als gevolg van review commentaar, maken apart addendum voor specifieke Rijks zaken
0.7	02-05-2018	Aanpassing als gevolg van commentaar BZK, 3 delen samengevoegd, alignment met de BIR2017 bewerkstelligd, totale herziening BIO, ISMS-deel als gevolg van commentaar laten vervallen
0.8	21-05-2018	Verdere aanpassingen als gevolg van commentaar en opmerkingen door gemeenten, waterschappen en provincies
0.9	25-05-2018	Verdere aanpassingen als gevolg van commentaar en verspreiding concept onder leden werkgroep Normatiek
1.0	01-06-2018	Laatste wijzigingen en commentaar NCSC en BZK verwerkt
1.01	11-10-2018	Wijzigingen uit de community, opmerkingen Forum Standaardisatie en kleine typo's aangepast, copyright NEN toegevoegd
1.02	01-11-2018	Aanwijzing NEN, jaartal ISO veranderd van 2013 naar 2017, inhoudelijk geen wijzigingen, de 2017 versie is ontstaan als gevolg van een Europees besluit.
1.03	13-03-2019	Aangepaste passage over gebruik van de NEN-ISO/IEC 27001:2017 en NEN-ISO/IEC 27002:2017. Deze passage en de wijzigingshistorie verplaatst van pagina 4 naar pagina 2.

Voorwoord

Informatiebeveiliging vormt een belangrijk kwaliteitsaspect van de informatievoorziening van de overheid. Het beveiligen van informatie is echter geen eenmalige zaak, maar een proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen. Het doorlopen van dit proces is een verantwoordelijkheid van het lijnmanagement. Om te voorkomen dat informatie en informatiesystemen te licht of te zwaar worden beveiligd, vormt risicomanagement een belangrijk onderdeel in dit proces.

De eerste stap in het beveiligingsproces is het maken van een risicoafweging. Daarbij wordt een inschatting gemaakt van mogelijke schade als informatiesystemen (tijdelijk) niet beschikbaar zijn, de informatie niet integer is en/of deze informatie in verkeerde handen valt. Ook wordt een inschatting gemaakt van de dreigingen waartegen beschermd moet worden. De inschatting van mogelijke schade en dreigingen leidt tot beveiligingseisen om het risico te beperken. Om deze eisen af te dekken worden passende maatregelen getroffen of wordt het (rest)risico geaccepteerd.

De Baseline Informatiebeveiliging Overheid (BIO) helpt het lijnmanagement bij het nemen van haar verantwoordelijkheid ten aanzien van informatiebeveiliging. Het ingewikkelde proces van risicomanagement wordt met de BIO vereenvoudigd. In de BIO zijn namelijk op basis van de generieke schades en dreigingen voor de overheid standaard basisbeveiligingsniveaus (BBN's) gedefinieerd met bijbehorende beveiligingseisen die moeten worden ingevuld. Per informatiesysteem bepaalt het lijnmanagement het BBN; de BIO biedt daarvoor een zogenaamde BBN-toets.

In de BIO staat per BBN beschreven aan welke controls uit de ISO 27002 (Code voor Informatiebeveiliging) moet worden voldaan. Bij alle controls dient, op basis van een individuele risicoafweging, bepaald te worden hoe aan de beveiligingsdoelstelling van de control voldaan kan worden. Daarbij zijn de controls, waar van toepassing, gedeeltelijk uitgewerkt in verplichte, concrete overheidsmaatregelen. De controls zijn toebedeeld aan rollen, waarmee de verdeling over verantwoordelijken makkelijker is. Zo kan ook de dienstenleverancier die de expertise heeft, bepalen met welke concrete maatregelen hij de control in vult.

Ten slotte moet verantwoording worden afgelegd over de risicoafweging en over de effectieve invulling van de controls. Deze verantwoording is onderdeel van de bestuurlijke verantwoording over de beveiliging van informatiesystemen. De wijze en mate van detail van de verantwoording hangt af van het BBN. Des te hoger het BBN, des te meer detail nodig is in verband met de hogere potentiële impact. Dienstenleveranciers leggen verantwoording af aan hun (gedeelde) opdrachtgever en er wordt verantwoording afgelegd aan de ketenpartners met wie afspraken over de beveiliging van informatie zijn gemaakt. De opdrachtgever ziet erop toe dat de afgenomen diensten in overeenstemming met de gestelde eisen beveiligd zijn; de afnemers van de diensten mogen hierop vertrouwen en worden door de opdrachtgever geïnformeerd over uitzonderingssituaties.

De BIO biedt hiermee de basis om te zorgen dat de beveiliging van informatie(systemen) bij alle bedrijfsonderdelen van de overheid bevorderd wordt. Deze bedrijfsonderdelen kunnen erop vertrouwen dat gegevens die worden verstuurd naar of worden ontvangen van andere onderdelen van de overheid in lijn met wet- en regelgeving passend beveiligd zijn. Waar naleving (nog) niet volledig mogelijk is, dienen de bedrijfsonderdelen via een 'explain' de eventuele risico's inzichtelijk te maken aan hun ketenpartners.

De BIO is opgedeeld in twee delen waarbij het eerste deel de achtergrond weergeeft en het tweede deel het daadwerkelijk uit te voeren kader omvat.

Inhoudsopgave

Wijzigingshistorie: 2

Voorwoord 3

DEEL 1 Achtergrond BIO 7

1. Informatiebeveiliging bij de overheid 9
   - 1.1 Inleiding 9
   - 1.2 Informatiebeveiligingskaders en uitgangspunten overheid 9
   - 1.3 ISO 27002 10
   - 1.4 Evaluatie en bijstelling 11
   - 1.5 Forum Standaardisatie 11
2. Opzet van de BIO 13
   - 2.1 Opzet BBN's 13
   - 2.2 Controls 13
   - 2.3 Implementatierichtlijnen 13
   - 2.4 Overheidsmaatregelen 14
   - 2.5 Addendum 14
   - 2.6 Operationalisering in handreikingen 14
   - 2.7 Rollen 14
3. Basisbeveiligingsniveaus 17
   - 3.1 BBN1 17
   - 3.2 BBN2 17
   - 3.3 BBN3 18
4. Verantwoording over de BIO 19
   - 4.1 Verantwoordelijkheid afhankelijk van basisbeveiligingsniveau 19
   - 4.2 Explains op overheidsmaatregelen 19
   - 4.3 Ketensamenwerking 20
   - 4.4 Dienstenleveranciers 20

DEEL 2 Kader BIO 23

Inleiding 24

BBN-toets 25

Controls en overheidsmaatregelen 26

5. Informatiebeveiligingsbeleid 27
   - 5.1 Aansturing door de directie van de informatiebeveiliging 27
6. Organiseren van informatiebeveiliging 29
   - 6.1 Interne organisatie 29
   - 6.2 Mobiele apparatuur en telewerken 30
7. Veilig personeel 31
   - 7.1 Voorafgaand aan het dienstverband 31
   - 7.2 Tijdens het dienstverband 31
   - 7.3 Beëindiging en wijziging van dienstverband 32
8. Beheer van bedrijfsmiddelen 33
   - 8.1 Verantwoordelijkheid voor bedrijfsmiddelen 33
   - 8.2 Informatieclassificatie 34
   - 8.3 Behandelen van media 35
9. Toegangsbeveiliging 37
   - 9.1 Bedrijfseisen voor toegangsbeveiliging 37
   - 9.2 Beheer van toegangsrechten van gebruikers 37
   - 9.3 Verantwoordelijkheden van gebruikers 39
   - 9.4 Toegangsbeveiliging van systeem en toepassing 39
10. Cryptografie 41
    - 10.1 Cryptografische beheersmaatregelen 41
11. Fysieke beveiliging en beveiliging van de omgeving 43
    - 11.1 Beveiligde gebieden 43
    - 11.2 Apparatuur 44
12. Beveiliging bedrijfsvoering 47
    - 12.1 Bedieningsprocedures en verantwoordelijkheden 47
    - 12.2 Bescherming tegen malware 48
    - 12.3 Back-up 49
    - 12.4 Verslaglegging en monitoren 50
    - 12.5 Beheersing van operationele software 51
    - 12.6 Beheer van technische kwetsbaarheden 51
    - 12.7 Overwegingen betreffende audits van informatiesystemen 51
13. Communicatiebeveiliging 53
    - 13.1 Beheer van netwerkbeveiliging 53
    - 13.2 Informatietransport 54
14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen 55
    - 14.1 Beveiligingseisen voor informatiesystemen 55
    - 14.2 Beveiliging in ontwikkelings- en ondersteunende processen 56
    - 14.3 Testgegevens 57
15. Leveranciersrelaties 59
    - 15.1 Informatiebeveiliging in leveranciersrelaties 59
    - 15.2 Beheer van dienstverlening van leveranciers 61
16. Beheer van informatie-beveiligingsincidenten 63
    - 16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen 63
17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer 65
    - 17.1 Informatiebeveiligingscontinuïteit 65
    - 17.2 Redundante componenten 66
18. Naleving 67
    - 18.1 Naleving van wettelijke en contractuele eisen 67
    - 18.2 Informatiebeveiligingsbeoordelingen 68

Bijlage 1: Wet- en regelgeving 69

Bijlage 2: Basisbeveiligingsniveaus 70

DEEL 3 Addendum BIO 73

Inleiding Addendum 74

5. Informatiebeveiligingsbeleid 75
   5.1 Aansturing door de directie van de informatiebeveiliging 75

6. Organiseren van informatiebeveiliging 75
   6.1 Interne organisatie 75

7. Veilig personeel 76
   7.1 Voorafgaand aan het dienstverband 76
   7.2 Tijdens het dienstverband 76

8. Beheer van bedrijfsmiddelen 76
   8.1 Verantwoordelijkheid voor bedrijfsmiddelen 76
   8.3 Behandelen van media 76

11. Fysieke beveiliging en beveiliging van de omgeving 77
   11.1 Beveiligde gebieden 77

14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen 77
   14.1 Beveiligingseisen voor informatiesystemen 77

15. Leveranciersrelaties 78
   15.1 Informatiebeveiliging in leveranciersrelaties 78

16. Beheer van informatiebeveiligingsincidenten 78
   16.1 Beheer van informatiebeveiligings-incidenten en -verbeteringen 78

Deel 1

Achtergrond BIO

1

Informatiebeveiliging bij de overheid

1.1 Inleiding

Informatiebeveiliging is het proces van vaststellen van de vereiste beveiliging van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen[1].

De BIO beoogt de beveiliging van informatie(systemen) bij alle bedrijfsonderdelen van de overheid te bevorderen, zodat deze bedrijfsonderdelen erop kunnen vertrouwen dat gegevens die worden verstuurd naar of worden ontvangen van andere onderdelen van de overheid, in lijn met wet- en regelgeving, passend beveiligd zijn.

De BIO beoogt zo de beveiliging van informatie(systemen) bij alle bestuurslagen en bestuursorganen van de overheid te bevorderen, zodat alle onderdelen erop kunnen vertrouwen dat onderling uitgewisselde gegevens, in lijn met wet- en regelgeving, passend beveiligd zijn. Het doel is continuïteit in de bedrijfsprocessen door waarborgen van juiste en tijdige informatie. Daarmee is de BIO ook van toepassing op besturings- en meetprocessen voor zover deze binnen een bestuursorgaan gebruikt worden.

De BIO is van toepassing op de overheid. In verband hiermee is de BIO van toepassing op de volgende bestuursorganen:

- Rijksdienst
- Provincies
- Waterschappen
- Gemeentes

Daarnaast wordt aanbevolen 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.

1.2 Informatiebeveiligingskaders en uitgangspunten overheid

De overheid past risicomanagement toe om tot de juiste beveiliging van informatie en informatiesystemen te komen binnen de context van de bedrijfsdoelstellingen. Risicomanagement is het inzichtelijk en systematisch inventariseren, beoordelen en – door het treffen van maatregelen – beheersbaar maken van risico's en kansen, die het bereiken van de doelstellingen van de organisatie bedreigen dan wel bevorderen, op een zodanige wijze dat verantwoording kan worden afgelegd over de gemaakte keuzes[2].

1) Artikel 1 sub a Voorschrift Informatiebeveiliging Rijksdienst 2007, *Stcrt.* 2007, 122/11.

2) Artikel 5 lid 2 BVR en Artikel 1 sub d BVR.

De insteek van risicomanagement in het kader van de BIO is dat er cyclisch en methodisch vanuit een PDCA-cyclus wordt omgegaan met informatiebeveiliging. De overheidslagen kiezen als basis voor deze procesmatige inrichting van risicomanagement en het inrichten van de PDCA-cyclus voor de NEN/ISO 27001:2017[3]. Voor de rijksoverheid vindt nadere specificatie plaats in de algemene voorschriften voor de beveiliging van informatiesystemen: het Beveiligingsvoorschrift Rijksdienst[4] (BVR), het Voorschrift Informatiebeveiliging Rijksdienst[5] (VIR) en het Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie[6] (VIR-BI)

Voor de BIO geldt (op basis van deze documenten van NEN/ISO 27001 en BVR, VIR en VIR-BI) kort samengevat het volgende.

- Een ruime definitie voor een informatiesysteem, namelijk "een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.[7]
- Het lijnmanagement is verantwoordelijk voor de beveiliging van informatie(systemen);
- Informatiebeveiliging is een cyclisch proces is, volgens de Plan-Do-Check-Act cyclus[8];
- Deze Plan-Do-Check-Act cyclus maakt het lijnmanagement verantwoordelijk voor het treffen van maatregelen op basis van risicomanagement;
- De Secretaris/algemeen directeur van een organisatie is eindverantwoordelijk[9] voor deze beveiliging en voor de inrichting en werking van de beveiligingsorganisatie[10];
- Het lijnmanagement stelt op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesystemen vast[11];
- Op basis van de betrouwbaarheidseisen kiest, implementeert en draagt het lijnmanagement de maatregelen uit[12].

De BIO is allereerst een gemeenschappelijk normenkader voor de beveiliging van de informatie(systemen) van de overheid. Daarnaast concretiseert de BIO een aantal normen tot verplichte overheidsmaatregelen:

- op grond van wet- en regelgeving[13];
- vanwege de gemeenschappelijk veiligheid van informatieketens;
- omdat deze fundamenteel zijn voor een betrouwbare c.q. professionele informatievoorziening.

De Baseline Informatiebeveiliging Overheid BIO is gebaseerd op de ISO 27002 standaard[14].

1.3 ISO 27002

De ISO 27002 'Code voor informatiebeveiliging' geeft richtlijnen en principes voor het initiëren, het implementeren, het onderhouden en het verbeteren van informatiebeveiliging binnen een organisatie. Deze standaard is een "best practice" om informatiebeveiligingsrisico's aan te pakken met betrekking tot vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening. De standaard kan gezien worden als een nadere specificatie van de ISO 27001 standaard[15]. De ISO 27002 kan dienen als een praktische richtlijn voor het ontwerpen van veiligheidsstandaarden binnen een organisatie en als effectieve methode voor het bereiken van deze veiligheid.

3) De NEN/ISO 31000 aanpak wordt gezien als een goed alternatief voor de 27001.
4) Beveiligingsvoorschrift Rijksdienst 2013, *Stcrt.* 2013, 15496.
5) Voorschrift Informatiebeveiliging Rijksdienst 2007, *Stcrt.* 2007, 122/11.
6) Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie 2013, *Stcrt.* 2013, 15497.
7) Artikel 1 sub b VIR.
8) Artikel 4 VIR, ISO 6.1 en 9.1
9) In sommige organisaties heet de eindverantwoordelijke bestuursvoorzitter of directeur en moet de term Secretaris/algemeen directeur als "directeur" of "bestuursvoorzitter" worden gelezen.
10) Artikel 5 lid 2 BVR en Artikel 4 lid 1 BVR.
11) Artikel 4 sub a en sub b VIR, ISO 27001 6.1 en 6.2.
12) Artikel 4 sub a en sub b VIR, ISO 27001 6.1 en 6.2.
13) Zie voor nadere detaillering: Bijlage 1: Wet- en regelgeving.
14) NEN-ISO/IEC 27002:2017. (dit is de 27002:2013 met geconsolideerde correctiebladen C1 en C2).
15) De NEN-ISO/IEC 27001-standaard bevat eisen waar het managementsysteem voor informatiebeveiliging aan dient te voldoen. Het is deze norm waartegen wordt ge-audit bij certificering. Deze standaard specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's van een organisatie.

De ISO bestaat uit 114 controls; de term 'control' wordt in de ISO vertaald als een beheersmaatregel[16]. De BIO volgt de opbouw van de ISO 27002 en haar controls. De controls zijn in de BIO letterlijk[17] overgenomen. Dit vergemakkelijkt afstemming met externe partners of leveranciers. Daarnaast vult de BIO enkele bepalingen uit het VIR inzake PDCA-cyclus en verantwoordelijkheden op een generieke wijze in[18].

1.4 Evaluatie en bijstelling

Door de snelle ontwikkelingen van de techniek verouderen maatregelensets voor informatiebeveiliging snel. De BIO is daarom zoveel als mogelijk op een abstractieniveau geschreven waarbij dergelijke wijzigingen en ontwikkelingen een zo klein mogelijke impact hebben op de maatregelen.[19] De BIO beschrijft het wat en niet het hoe. Desondanks kunnen wijzigingen noodzakelijk zijn bij bijvoorbeeld aanpassingen van onderliggende wet- en regelgeving, nieuwe of juist verouderde handreikingen of nieuwe dreigingen en kwetsbaarheden.

Dit document wordt daarom regelmatig in zijn geheel geëvalueerd en indien nodig bijgesteld. Daarnaast wordt specifiek bezien of er wijzigingen en aanvullingen in de maatregelen en de (operationele) handreikingen nodig of gewenst zijn om hiermee de praktische toepasbaarheid te vergroten. Besluiten hierover worden via de bestaande informatiebeveiligingsgremia genomen en door de beheerder van de BIO verwerkt[20].

1.5 Forum Standaardisatie

De overheid volgt de standaarden die op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie[21] (hierna Forum) staan. De BIO is gebaseerd op de NEN-ISO/IEC 27002:2017 en vanuit de BIO wordt verwezen naar de NEN-ISO/IEC 27001:2017, beide standaarden staan op de 'pas toe of leg uit'-lijst[22] van het Forum. Ook een aantal technische maatregelen uit de BIO staan op de 'pas toe of leg uit'-lijst of op de 'open standaarden'-lijst[23] van het Forum. Deze technische invullingen zijn niet allemaal uitgewerkt in deze BIO. Er is voor gekozen alleen aan te geven of de maatregel ingevuld wordt door een verplichte of open standaard van het Forum. Hierdoor wordt de BIO minder onderhoudsgevoelig.

16) De Nederlandse versie van ISO27002 spreekt van beheersmaatregelen. Er zijn echter ook implementatiemaatregelen. Om het onderscheid daartussen makkelijker te maken, hanteert de BIO de Engelse term, namelijk 'controls'. Het gebruik van deze term sluit aan bij de informatiebeveiligingspraktijk.
17) In tegenstelling tot de verschillende oude baselines, zijn de controls dus niet tekstueel aangepast.
18) Met name artikel 4 sub a en sub b van het VIR.
19) Ook de ISO is vanuit dit principe opgesteld.
20) Daartoe is in het OBDO een procedure overeengekomen.
21) Zie ook de website van het Forum Standaardisatie op https://www.forumstandaardisatie.nl
22) Zie ook: https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht
23) Zie ook: https://www.forumstandaardisatie.nl/open-standaarden/lijst/aanbevolen

2

Opzet van de BIO

2.1 Opzet BBN's

Om risicomanagement hanteerbaar en efficiënt te houden, kiest de BIO voor een diepgang van de uitwerking van het risicomanagement die proportioneel is aan de te beschermen belangen in combinatie met relevante dreigingen. Daarom onderscheidt de BIO drie basisbeveiligingsniveau's (BBN). Voor BBN1 ligt de nadruk op 'wat mag minimaal verwacht worden?'. Voor BBN2 ligt de nadruk op de bescherming van de meest voorkomende categorieën informatie volgens het principe 'valt de maatregel onder goed huisvaderschap; toont deze beveiliging de betrouwbare overheid?'. BBN3[24] is van toepassing op gerubriceerde informatie Departementaal Vertrouwelijk dan wel vergelijkbaar vertrouwelijk bij andere overheidslagen, waarbij weerstand tegen statelijke actoren of vergelijkbare dreigers nodig is.

De keuze voor een BBN wordt gemaakt door de proceseigenaar en is gebaseerd op risicomanagement. De BIO gaat vergezeld van een methode van risicoafweging, de BBN-toets[25]. In Deel 2 wordt deze methode verder toegelicht[26].

24) De aanvullende eisen die gelden vanaf BBN3 zijn in deze huidige versie van de BIO nog niet nader uitgewerkt.
25) De BBN-toets is geen volwaardige vervanger van de Quickcan BIO of van een andere uitgebreide risicoanalysemethodiek. De BBN-toets zorgt er alleen voor dat eenvoudig het juiste BBN geselecteerd kan worden en dat bepaald kan worden in hoeverre extra eisen noodzakelijk zijn.
26) Gewerkt gaat worden aan een handreiking waarin ten opzichte van de drie BBN niveaus wisselingen in niveaus voor de aspecten integriteit en beschikbaarheid wisseling worden aangegeven. Wellicht gaan de controls en maatregelen nog nader gespecificeerd worden naar de drie verschillende aspecten.

2.2 Controls

Na de BBN-toets doorloopt het lijnmanagement alle toepasselijke controls[27] uit de BIO[28]. Op basis van een risicoafweging wordt bepaald hoe moet worden voldaan aan de gestelde beveiligingsdoelstellingen van de controls. Voor het voldoen aan deze doelstellingen kunnen implementatierichtlijnen uit de ISO 27002, overheidsmaatregelen en/of operationaliseringen in handreikingen worden gebruikt.

Er geldt een hardheidsbepaling: in het geval een control voor een specifiek geval niet van toepassing *kan* zijn, *is* de control niet toepassing. Dit geldt bijvoorbeeld voor een control die betrekking heeft op een externe koppeling, terwijl het betreffende informatiesysteem geen externe koppeling heeft. De organisatie hoeft zich daar niet over te verantwoorden.

2.3 Implementatierichtlijnen

Iedere control is in de ISO 27002 uitgewerkt in implementatierichtlijnen. Bij het uitvoeren van risicoafwegingen zijn de implementatierichtlijnen zeer nuttig. Ze helpen bij het kiezen van de benodigde beveiligingsmaatregelen. Deze richtlijnen moeten dus worden gezien als voorbeelden hoe de controls uitgewerkt *kunnen* worden in maatregelen; het volgen van deze richtlijnen is niet verplicht.

27) De Nederlandse versie van ISO27002 spreekt van beheersmaatregelen. Er zijn echter ook implementatiemaatregelen. Om het onderscheid daartussen makkelijker te maken, hanteert de BIO de Engelse term, namelijk 'controls'. Het gebruik van deze term sluit aan bij de informatiebeveiligingspraktijk.
28) Met uitzondering van twee controls (6.1.4 en 14.2.4) bevat de BIO alle controls uit de ISO 27002.

Deze implementatierichtlijnen zijn niet in de BIO opgenomen, hiervoor wordt verwezen naar de ISO 27002.

2.4 Overheidsmaatregelen

Een deel van de controls is uitgewerkt in verplichte maatregelen, omdat zij:

- voortvloeien uit *wet- en regelgeving*[29]. Het niet treffen van een dergelijke maatregel is dan in strijd met deze externe wet- en regelgeving;
- zo basaal zijn dat zij het *fundament* vormen van een betrouwbare c.q. professionele informatievoorziening;
- dienstbaar zijn aan de beveiliging in een procesketen of netwerk; niet-naleving door een enkele organisatie is per saldo niet *effectief* voor de gehele keten. Het vormt een risico voor alle andere partijen in de keten en leidt bij hen tot extra maatregelen en kosten. Voor de keten als geheel is dit niet *efficiënt*. Voor een *generieke dienst* geldt een afweging die analoog is aan het ketenvraagstuk.

De BIO noemt deze verplichte maatregelen 'overheidsmaatregelen'. De overheidsmaatregelen dekken niet de gehele beveiligingsdoelstellingen van de control af. Net als bij de controls, geldt hier een hardheidsbepaling: in het geval een maatregel voor een specifiek geval niet van toepassing *kan* zijn, vervalt de verplichting. Dit geldt bijvoorbeeld voor een overheidsmaatregel die betrekking heeft op een externe koppeling, terwijl het betreffende informatiesysteem geen externe koppeling heeft.

Bij een aantal overheidsmaatregelen zijn verwijzingen toegevoegd naar relevante wet- en regelgeving. Deze verwijzingen zijn of overheidsbreed geldend of specifiek toegesneden op een aandachtsgebied (bijvoorbeeld de 'Gedragsregeling voor digitale werkomgeving') en hebben een verplichtend karakter.

29) Het gaat dan enkel om de beveiligingseisen die voortvloeien uit wet- en regelgeving. Andere vereisten vallen buiten de scope van de BIO.

2.5 Addendum

De BIO is generiek geschreven en geldig voor alle doelgroepen. Sommige overheidslagen hebben specifieke wet- en regelgeving die alleen gelden binnen die overheidslaag.

Om tegemoet te komen aan de behoefte van deze overheidslagen en deze specifieke wet- en regelgeving niet verloren te laten gaan is er aan de BIO een addendum toegevoegd. In dit addendum is deze wet- en regelgeving gekoppeld aan de control of maatregel waartoe zij behoren. Het addendum is toegevoegd aan de BIO in deel 3.

2.6 Operationalisering in handreikingen

Om de praktische toepasbaarheid van de BIO te verhogen, wordt de BIO aangevuld met

handreikingen. Dit zijn aanbevelingen in het kader van de bedrijfsvoering die niet een verplichtend karakter hebben en niet essentieel zijn voor de werking van een stelsel. Een handreiking geeft dus advies hoe bepaalde normen, standaarden, technieken of maatregelen te implementeren of te hanteren zijn. Een handreiking kan meer specifiek zijn toegesneden op een overheidslaag (interdepartementaal, gemeentebreed, etc.), of op een bepaald aandachtsgebied.

In deze BIO zijn verwijzingen opgenomen naar goede handreikingen die nu reeds beschikbaar zijn; in de loop van de tijd kunnen hier handreikingen aan worden toegevoegd.

2.7 Rollen

In het algemeen geldt dat onderdelen van de BIO op verschillende plaatsen in de organisatie worden toegepast op grond van verschillende verantwoordelijkheden en gezagsverhoudingen. De BIO onderscheidt drie (hoofd)rollen: de Secretaris/algemeen directeur, de proceseigenaar en de dienstenleverancier. Deze rollen zijn hieronder beschreven vanuit het perspectief van informatiebeveiliging. Er zijn uiteraard meer rollen betrokken bij informatiebeveiliging, zoals toezichthouder en medewerker, maar het gaat hier om de verantwoordelijke voor de uitvoering van de control.

Secretaris/ algemeen directeur	Als eindverantwoordelijke voor het beveiligingsbeleid in de organisatie is de Secretaris/algemeen directeur verantwoordelijk voor de uitvoering van organisatiebrede vraagstukken ten aanzien van informatiebeveiliging.[30] In de praktijk kan deze rol worden uitgevoerd door bijvoorbeeld de CIO of een directeur Inkoop.[31]
Proceseigenaar	Onder de proceseigenaar wordt de lijnmanager verstaan die verantwoordelijk is voor de beveiliging van het betreffende proces / informatiesysteem.
Dienstenleverancier	Bedoeld wordt de dienstenleverancier (bijv. SSO) binnen de overheid of organisaties in de markt waaraan de Secretaris/algemeen directeur of proceseigenaar (een deel van) de beveiligingstaak inbesteedt respectievelijk uitbesteedt.

In de BIO staat aangegeven welke controls voor welke rol toepasselijk zijn. Omdat de overheid pluriform is georganiseerd, is deze toedeling indicatief. De BIO verplicht wel om de controls en overheidsmaatregelen die bij de rollen staan intern toe te delen en hierbij rekening te houden met voldoende functiescheiding. In het algemeen is de organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden terug te vinden in de organisatie informatiebeveiligingsbeleid.[32]

30) In sommige organisaties heet de eindverantwoordelijke "secretaris-generaal", "directeur" of "bestuursvoorzitter" en moet de term "Secretaris/algemeen directeur" als "secretaris-generaal", "directeur" of "bestuursvoorzitter" worden gelezen.
31) Bij het rijk kan dat bijvoorbeeld ook de beveiligingsambtenaar (BVA) zijn.
32) Artikel 3 sub b VIR.

3

Basisbeveiligingsniveaus

Zoals in paragraaf 2.1 beschreven, onderscheidt de BIO drie basisbeveiligingsniveaus (BBN's). Ieder BBN bestaat uit een aantal controls, een aantal verplichte overheidsmaatregelen en een verantwoordings- en toezichtregime. Elk niveau bouwt voort op het vorige niveau. Daarbij vult BBN2 de controls van BBN1 aan. BBN2 vult ook de overheidsmaatregelen van BBN1 aan of vervangt deze door maatregelen met meer gewicht. Hetzelfde geldt voor BBN3 in relatie tot BBN1 en BBN2.

3.1 BBN1

Informatiesystemen op BBN1 niveau zijn systemen waarvoor BBN2 als te zwaar wordt gezien. Het kan voorkomen dat er nog wel hogere beschikbaarheids- en integriteitseisen nodig zijn. BBN1 is waar alle overheidssystemen als minimum aan moeten voldoen.

Controls en overheidsmaatregelen komen voort uit:
- wet- en regelgeving;
- algemeen geldende beveiligingsprincipes (fundamentele controls en maatregelen).

3.2 BBN2

Voor informatiesystemen binnen de overheid vormt BBN2 het uitgangspunt. BBN2 is van toepassing indien[33]:
- er vertrouwelijke informatie wordt verwerkt;
- mogelijke incidenten leiden tot bestuurlijke commotie;
- er onzekerheid bestaat of ook alle informatie van derden open is;
- de veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem.

Het te beschermen belang van BBN2 is maximaal Departementaal Vertrouwelijk (DepV), (zoals gedefinieerd in het VIR-BI)/vergelijkbaar vertrouwelijk bij andere overheidslagen en privacygevoelige informatie met een verhoogd vertrouwelijkheidsniveau. Dergelijke informatie komt veelvuldig voor bij de overheid. Het gaat verder om commercieel vertrouwelijke informatie of informatie in het kader van beleidsvorming; het is dus niet beperkt tot DepV/vergelijkbaar vertrouwelijk bij andere overheidslagen gerubriceerde informatie.

BBN2 informatie wordt preventief beschermd tegen alle dreigingen met uitzondering van geavanceerde dreigingen, zoals Advanced Persistent Threats (APT's), afkomstig van statelijke actoren of beroepscriminelen. Daarvoor geldt een bescherming achteraf: zij dienen te kunnen worden gedetecteerd, waarop vervolgens passend gereageerd moet worden. Voor informatiesystemen waar Departementaal Vertrouwelijke informatie en vergelijkbaar vertrouwelijk bij andere overheidslagen wordt verwerkt en waar weerstand tegen de geavanceerde dreiging van statelijke actoren of gelijkwaardige beroepscriminelen is vereist, is het BBN2 dus niet voldoende.

De controls van het BBN2 omvatten de controls van BBN1. Dit geldt ook voor de maatregelen waarbij enkele maatregelen van BBN1 in de BBN2 variant verzwaard zijn. De keuze hiervoor komt voort uit:
- wet- en regelgeving, in het bijzonder beveiligingseisen a.g.v. WBP/AVG;
- aansluitvoorwaarden van generieke/gemeenschappelijke diensten;

33) Zie de BBN-toets in Deel 2 voor meer details.

- afhankelijkheden in ketens en netwerken;
- minimale eisen ten behoeve van een efficiënte beveiliging van BBN3.

3.3 BBN3

BBN3 richt zich op de bescherming van Departementaal Vertrouwelijk en vergelijkbaar vertrouwelijk bij andere overheidslagen gerubriceerde informatie waarbij weerstand geboden moet worden tegen de dreiging, zoals Advanced Persistant Threat's (APT's), die uitgaat van statelijke actoren en beroepscriminelen. BBN3 is van toepassing indien:

- verlies van informatie een grote impact heeft, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3;
- informatie met een rubricering (niet zijnde BBN2) wordt geleverd door derden;
- aansluiting op een infrastructuur BBN3 is vereist om informatie te kunnen verwerken op deze infrastructuur (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen);

Om redenen van efficiency sluit BBN3 aan op relevante NAVO-regelgeving waarin ook al rekening wordt gehouden met het bieden van weerstand tegen statelijke actoren[34]. Dit betekent dat BBN3 bestaat uit de controls en overheidsmaatregelen uit BBN2 aangevuld met relevante eisen uit het VIR-BI, relevante bepalingen uit regelingen andere overheidslagen en uit het NAVO-verdrag voor de beveiliging van informatie[35]. Niet alle delen/maatregelen zijn van toepassing voor de nationale context en voor NATO Restricted;[36]. In de uitwerking van BBN3 zal daarom specifiek aangegeven worden welke delen/maatregelen van het NAVO-verdrag specifiek van toepassing zijn.

34) Zowel voor EU als voor NAVO gerubriceerde informatie geldt dat de beveiligingsvoorschriften standaard rekening houden met het bieden van weerstand tegen statelijke actoren. Voor de BIO is uiteindelijk gekozen om aan te sluiten bij de NAVO regelgeving omdat de NAVO-eisen gedetailleerder zijn dan de EU en daarmee meer zekerheid bieden dat ook daadwerkelijk weerstand tegen statelijke actoren kan worden geboden. Voor de goede orde: alleen op NATO gerubriceerde informatie heeft het NAVO-verdrag rechtstreekse werking, BBN3 is Nederlandse informatie waarop het NAVO-verdrag niet rechtstreeks werkt; de toepasselijkheid van het NAVO-verdrag voor BBN3 is een keuze die de overheid zelf via deze BIO maakt.
35) CM(2002)49 met bijbehorende enclosures en directives.
36) Er zijn passages die enkel op de bescherming van informatie met een rubricering van NATO Confidential en hoger betrekking hebben.

4

Verantwoording over de BIO

De Secretaris/algemeen directeur van een organisatie is *eindverantwoordelijk* voor de integrale beveiliging en de inrichting en werking van de beveiligingsorganisatie[37]. In die hoedanigheid is hij eindverantwoordelijk voor de implementatie van alle beveiligingskaders in zijn organisatie, dus ook voor een juiste toepassing van de BIO.

De bestuurlijke verantwoording over de toepassing van de BIO is onderdeel van de verantwoording over de beveiliging van informatie(-systemen). Hier wordt ook verantwoording afgelegd aan de ketenpartners met wie afspraken over de beveiliging van informatie zijn gemaakt.

4.1 Verantwoordelijkheid afhankelijk van basisbeveiligingsniveau

De ISO 27001 en het VIR bepalen dat het lijnmanagement vaststelt dat de getroffen maatregelen aantoonbaar overeenstemmen met de betrouwbaarheidseisen en dat deze maatregelen worden nageleefd[38]. De proportionaliteit die eerder beschreven is, is ook van toepassing bij het toekennen van het niveau waar de verantwoordelijkheid voor risicomanagement wordt belegd:

- voor BBN1 is de proceseigenaar volledig verantwoordelijk voor het nemen van (verstandige) beslissingen. Slechts incidenteel en op verzoek informeert deze de CISO over de stand van zaken met betrekking tot zijn BBN1 informatiesystemen.
- voor BBN2 geldt dat de proceseigenaar het informatiesysteem voor ingebruikname (bij voorkeur in ontwerp/ontwikkelfase) ter consultatie voorlegt aan de CISO[39].
- voor BBN3 geldt dat vooraf toestemming verleend moet worden door de Secretaris/algemeen directeur voor het verwerken van bijzondere informatie (conform het VIR-BI).[40] Voor het verlenen van toestemming is mandatering mogelijk naar bijvoorbeeld de CIO of CISO en bij het rijk naar de BVA.

Organisaties kunnen voor BBN1 en BBN2 hiervan afwijken in het informatiebeveiligingsbeleid[41].

4.2 Explains op overheidsmaatregelen

Overheidsmaatregelen die niet van toepassing zijn, hoeven niet als *explain* te worden benoemd.

De organisatie dient te beschikken over een registratie van overheidsmaatregelen waaraan niet of nog niet geheel kan worden voldaan. Dit zijn explains volgens het '*comply or explain*' principe. Daarbij worden de daaruit voortvloeiende risico's tevens aangegeven.

Explains ten aanzien van overheidsmaatregelen kunnen bij het samenwerken in ketens zorgen voor een verschil in bescherming tussen partijen waardoor een risico ontstaat voor de verwerkte (en

37) Artikel 4 lid 1 BVR.
38) Artikel 4 sub b VIR.

39) Bij DepV informatie geldt, conform het VIR-BI, het BBN3-regime voor verantwoording.
40) Artikel 3 sub b VIR-BI.
41) Artikel 3 sub b VIR.

gedeelde) informatie. Partijen met explains, moeten dit afstemmen met hun (samenwerk- of keten) partners zodat ze samen passende maatregelen of tijdelijke maatregelen treffen die het risico mitigeren of verkleinen zolang de explains niet conform de BIO geïmplementeerd zijn.

Voor Rijksonderdelen geldt: explains die de veiligheid van andere delen van de Rijksdienst onderdelen raken, worden voorzien van een advies van de Security Accreditation Authority (SAA, ingevuld door de Subcommissie Informatiebeveiliging) en door het ministerie voorgelegd aan het CIO Beraad.

4.3 Ketensamenwerking

Binnen de overheid en met andere externe partijen wordt veel in ketens samengewerkt en daarom vormt, zoals in paragraaf 1.1 aangegeven, de gemeenschappelijke veiligheid van informatieketens ook een basis voor de concretisering van de overheidsmaatregelen.

Een keten is een samenwerkingsverband tussen organisaties die naast hun eigen doelstellingen, één of meer gemeenschappelijk gekozen (of door de politiek opgelegde) doelstellingen nastreven. Deze ketenpartners zijn zelfstandig, maar zijn ook afhankelijk van elkaar waar het gaat om het bereiken van de gezamenlijke (keten)doelstellingen.[42] Een informatieketen betreft de uitwisseling van informatie binnen zo'n samenwerkingsverband.

Ook in het kader van ketensamenwerking kan de verantwoordelijkheid voor informatiebeveiliging niet worden gedelegeerd.

In het geval dat een organisatie informatie aan ketenpartners toevertrouwt, blijft deze organisatie er verantwoordelijk voor dat ketenpartners de toevertrouwde informatie zorgvuldig beschermen. De organisatie moet daarom aansluitvoorwaarden eisen of stellen aan de leverende of afnemende partij. Tevens moet de organisatie leveringsgaranties bieden aan de afnemende partij. De organisatie moet hiervoor inzichtelijk hebben van welke informatiesystemen en infrastructuren zij afhankelijk is, welke afhankelijk zijn van haar en hoe de governance van beiden hierop is ingericht.

42) https://noraonline.nl/wiki/Ketensturing/De_wereld_van_ketens/Wat_is_een_keten%e3F.

4.4 Dienstenleveranciers

In de BIO wordt bij het van toepassing verklaren van controls en overheidsmaatregelen geen onderscheid gemaakt in interne of externe dienstenleveranciers. Ook bij de wijze waarop verantwoording wordt afgelegd over hun diensten worden interne en externe dienstenleveranciers gelijk behandeld. Dit betekent voor alle dienstenleveranciers het volgende.

- Periodiek leggen alle dienstenleveranciers verantwoording af via een Statement of Compliancy (of deel-ICV; met toepasselijke reikwijdte) aan de opdrachtgever bij de overheid.
- De dienstenleveranciers volgen de beveiligingseisen die de overheidsorganisaties of ketenpartners stellen aan de diensten van de dienstenleverancier. Uit efficiencyoverwegingen kan een dienstenleverancier een standaard beveiligingsniveau aanbieden, maar dit doet geen afbreuk aan de genoemde verantwoordelijkheid van de overheidsorganisaties.
- Voor diensten die aan één organisatie worden aangeboden, legt de dienstenleverancier verantwoording af aan het opdrachtgevende organisatie. De opdrachtgevende organisatie neemt de verantwoording op in haar ICV. De opdrachtgevende organisatie houdt ook toezicht op specifieke dienstverlening.
- Voor diensten die aan meerdere overheden of overheidsonderdelen worden aangeboden stelt de dienstenleverancier één verantwoording op ten behoeve van alle afnemers. Voor het Rijk wordt in het CIO-beraad jaarlijks vastgesteld wie toezicht houdt op de beveiliging van deze diensten.

Naast de verantwoording over hun diensten zijn de dienstenleveranciers ook zelf als organisatie gebonden aan informatiebeveiligingsregels. Hierbij is wel een onderscheid aanwezig tussen interne en externe dienstenleveranciers:

- Interne dienstenleveranciers zijn, als onderdeel van de overheid, zelf ook rechtstreeks gebonden aan de BIO. Ze zijn daarmee gehouden aan de reguliere verantwoordings- en toezichtprocedures van de betreffende overheidslagen. Bij het rijk geldt onder meer het toezicht vanuit de ADR, ARK en de BVA. De interne dienstenleverancier is ook gebonden aan het jaarlijks opleveren van een In Control Verklaring (ICV). Hierin verklaart de dienstenleverancier dat hij voor zijn eigen bedrijfsvoering aan de BIO voldoet (inclusief de overheidsmaatregelen).
- Externe dienstenleveranciers zijn geen onderdeel van de overheid en zijn daarmee zelf niet rechtstreeks gebonden aan de BIO of het opleveren van een ICV. Ze moeten wel voldoen aan de eisen van de opdrachtgever. Voorwaarden ten behoeve van informatiebeveiliging moeten daarom in het contract zijn vastgelegd. In de BIO zijn in hoofdstuk 15 over leveranciersrelaties controls en overheidsmaatregelen opgenomen die moeten zorgen voor een goede borging van informatiebeveiliging in contracten.

Het is mogelijk dat een (externe) dienstenleverancier beschikt over een kwaliteitskeurmerk zoals een ISO27001-certificaat of bijv. een ISAE3402-verklaring. De waarde van zo'n keurmerk of verklaring is afhankelijk van de reikwijdte en diepgang. Het zegt meestal iets over het proces dat bij de dienstenleverancier is ingericht. Hoewel dit dus wel meerwaarde heeft, overlap kent met de BIO-controls en gebruikt kan worden als onderdeel van de Statement of Compliancy, omvat en vervangt het niet volledig de verantwoording over de overheidsmaatregelen uit de BIO. Er zullen altijd aanvullende afspraken gemaakt moeten worden over de gap tussen keurmerk of verklaring en de BIO-controls. Hierover moet aanvullend worden verantwoord.

Deel 2

Kader BIO

Inleiding

Het Kader BIO bestaat uit een BBN-toets om het juiste Basis Beveiligingsniveau (BBN) te bepalen en de tabellen met de controls en maatregelen. De BBN toets wordt voor ieder informatiesysteem uitgevoerd. Het BBN bepaalt welke controls vervolgens moeten worden doorlopen. Per control moet worden bepaald welke maatregelen in aanvulling op de verplichte overheidsmaatregelen nodig zijn. Voor meer toelichting op de opzet van de BIO en de BBN's wordt verwezen naar Deel 1 van deze BIO.

In het document zijn de controls dan als volgt opgebouwd:

Controlnummer overeenkomstig met ISO 27002	BBN (1, 2 of 3)	Controltekst (ISO 27002)	**Verantwoordelijke(n)** Secretaris/algemeen directeur Proceseigenaar Dienstenleverancier
O-maatregel nummer	BBN (1, 2 of 3)	O-maatregel	
		Handreiking (optioneel)	

Om het verschil tussen de ISO 27002 controls en de overheidsmaatregelen te duiden, zijn ook verschillende kleurmarkeringen gebruikt:

- Blauw zijn de ISO controls
- Groen zijn overheidsmaatregelen (O-maatregel)

Waar passend wordt verwezen naar handreikingen om invulling te geven aan de maatregelen. Deze handreikingen zijn niet verplicht, hebben geen nummer en zijn als een link weergegeven.

In de kolom 'Verantwoordelijke(n)' staat aangegeven wie voor de uitvoering van de control verantwoordelijk is: Secretaris/algemeen directeur (eindverantwoordelijke voor de bedrijfsvoering van een organisatie), Proceseigenaar en/of Dienstenleverancier.

BBN-toets

Bij het doorlopen van deze toets is BBN2 het uitgangspunt voor alle informatiesystemen.

Stap 1: Is BBN2 voldoende?
Meestal is BBN2 van toepassing op een specifiek informatiesysteem. Het kan echter zijn dat BBN2 niet voldoende is. BBN2 is onvoldoende indien:

- de informatie beschermd dient te worden tegen statelijke actoren of vergelijkbare dreigers; of
- informatie wordt geleverd door derden en deze voor de beveiliging van betreffende informatie BBN3 eisen; of
- aansluiting op een infrastructuur het BBN3 vereist om informatie te kunnen verwerken op deze infrastructuur (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen)

In elk van deze gevallen is BBN3 of hoger (zie VIR-BI in geval van het Rijk) van toepassing.

Stap 2: Is BBN2 te zwaar?
Bij BBN2 informatiesystemen kan het ongewenst of onbedoeld openbaren van informatie leiden tot *BBN2-schade*:

- politieke schade aan een bestuurder: bestuurder moet verantwoording afleggen aan de (gekozen) controlerende organen, bijvoorbeeld n.a.v. verantwoordingsvragen; of
- diplomatieke schade te herstellen door ambtelijke opschaling; of
- financiële gevolgen: niet meer op te vangen binnen de begroting van de (uitvoerings)organisatie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of
- verlies van publiek respect; klachten van burgers of significant verlies van motivatie van medewerkers; of
- bindende aanwijzing van de AP in verband met schending van de privacy; of
- directe imagoschade, bijvoorbeeld door negatieve publiciteit.

Zijn dergelijke schades niet aan de orde, dan is BBN1 van toepassing.

Stap 3: Bepaal extra vereisten voor beschikbaarheid en/of integriteit
In het geval van BBN1: leidt uitval van systemen en/of het verminkt raken van informatie tot schade vergelijkbaar met *BBN2-schade*[43)]? In dat geval kan worden overwogen (een deel) van de BIO controls en maatregelen, die toezien op beschikbaarheid dan wel integriteit op het niveau van BBN2 te nemen. De verantwoording en toezicht vindt plaats volgens BBN2.

In het geval van BBN2 of BBN3: leidt uitval van systemen en/of het verminkt raken van informatie tot grotere schade dan de BBN2-schade[44)]? In dat geval wordt op basis van expliciete risicoafweging bepaald voor welke controls welke aanvullende en/of zwaardere maatregelen nodig zijn. De verantwoording en toezicht vindt plaats volgens BBN3.

43) Zie stap 2
44) Zie stap 2

Controls en overheidsmaatregelen

Voor de herkenbaarheid is gekozen om de nummering van de hoofdstukken en de controls in lijn te houden met de nummering uit de ISO27002.

5

Informatiebeveiligingsbeleid

5.1 Aansturing door de directie van de informatiebeveiliging

Doelstelling: Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.

5.1.1	1	**Beleidsregels voor informatiebeveiliging** Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Secretaris/ algemeen directeur
5.1.1.1	1	Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat tenminste de volgende punten: a. de strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid; b. de organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden; c. de toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers; d. de gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn; e. de frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd; f. de bevordering van het beveiligingsbewustzijn. **Handreikingen: BIO-001-Informatiebeveiligingsbeleid**	
5.1.2	1	**Beoordeling van het informatiebeveiligingsbeleid** Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	Secretaris/ algemeen directeur
5.1.2.1	1	Het informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of bij belangrijke wijzigingen als gevolg van reorganisatie of verandering in de verantwoordelijkheidsverdeling, beoordeeld en zo nodig bijgesteld.	

6

Organiseren van informatiebeveiliging

6.1 Interne organisatie

Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.

6.1.1	**1**	**Rollen en verantwoordelijkheden bij informatiebeveiliging** Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	Secretaris/ algemeen directeur
6.1.1.1	1	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.	
6.1.1.2	1	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.	
6.1.1.3	1	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.	
6.1.1.4	1	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	
		Handreiking: BIO-CISO-functieprofiel	
6.1.2	**1**	**Scheiding van taken** Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	Proceseigenaar Dienstenleverancier
6.1.2.1	1	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.	
6.1.3	**2**	**Contact met overheidsinstanties** Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden.	Secretaris/ algemeen directeur Proceseigenaar Dienstenleverancier
6.1.3.1	2	Er is door de organisatie uitgewerkt wie met welke (overheids) instanties en toezichthouders contact heeft ten aanzien van informatiebeveiligingsaangelegenheden (vergunningen/incidenten/ calamiteiten) en welke eisen voor deze aangelegenheden relevant zijn.	
6.1.3.2	2	Het contactoverzicht wordt jaarlijks geactualiseerd.	
6.1.4	**-**	**Vervallen**	-
6.1.5	**2**	**Informatiebeveiliging in projectbeheer** Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.	Proceseigenaar Dienstenleverancier

6.2 Mobiele apparatuur en telewerken

Doelstelling: Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.

6.2.1	1	**Beleid voor mobiele apparatuur** Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	Proceseigenaar Dienstenleverancier
		Handreiking: BIO Mobile Device Management[45]	
6.2.1.1	2	Mobiele apparatuur is zo ingericht dat geen bedrijfsinformatie onbewust wordt opgeslagen ('zero footprint'). Als zero footprint (nog) niet realiseerbaar is, biedt een mobiel apparaat (zoals een laptop, tablet en smartphone) de mogelijkheid om de toegang te beschermen door middel van een toegangsbeveiligingsmechanisme en, indien vertrouwelijke gegevens worden opgeslagen, versleuteling van die gegevens. In het geval van opslag van vertrouwelijke informatie moet op deze mobiele apparatuur 'wissen op afstand' mogelijk zijn.	
6.2.1.2	2	Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd: a. in bewustwordingsprogramma's komen gedragsaspecten van veilig mobiel werken aan de orde; b. het device maakt onderdeel uit van patchmanagement en hardening; c. het device wordt waar mogelijk beheerd en beveiligd via een MDM Mobile Device Management (MDM)-oplossing; d. gebruikers tekenen een gebruikersovereenkomst voor mobiel werken, waarmee zij verklaren zich bewust te zijn van de gevaren van mobiel werken en verklaren dit veilig te zullen doen. Deze verklaring heeft betrekking op alle mobiele apparatuur die de medewerker zakelijk gebruikt; periodiek wordt getoetst of de punten in lid b), c) en d) worden nageleefd.	
6.2.2	2	**Telewerken** Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen.	Secretaris/ algemeen directeur Dienstenleverancier
		Handreiking: BIO Telewerkbeleid	

45) Daar is ook MAM (Mobile Application Managent) onderdeel van.

7

Veilig personeel

Algemene handreiking: Personeelsbeleid

7.1 Voorafgaand aan het dienstverband

Doelstelling: Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor zij in aanmerking komen.

7.1.1	1	**Screening** Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn.	Secretaris/ algemeen directeur Proceseigenaar
7.1.1.1	1	Bij indiensttreding overleggen alle medewerkers (intern en extern) een specifiek voor de functie verstrekte Verklaring Omtrent het Gedrag (VOG).	
7.1.2	1	**Arbeidsvoorwaarden** De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.	Secretaris/ algemeen directeur Proceseigenaar
7.1.2.1	1	Alle medewerkers (intern en extern) zijn bij hun aanstelling of functiewisseling gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn eenvoudig toegankelijk.	

7.2 Tijdens het dienstverband

Doelstelling: Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.

7.2.1	1	**Directieverantwoordelijkheden** De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	Secretaris/ algemeen directeur
7.2.1.1	1	Er is aansluiting bij een klokkenluidersregeling, zodat iedereen in staat is om anoniem en veilig beveiligingsissues te kunnen melden.	

7.2.2	1	**Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging** Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	Secretaris/ algemeen directeur Proceseigenaar
7.2.2.1	1	Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen	
7.2.2.2	1	Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen- en diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.	
		Handreiking: iBewustzijn Overheid	
7.2.2.3	1	Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij haar medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen	
7.2.3	1	**Disciplinaire procedure** Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	Secretaris/ algemeen directeur

7.3 Beëindiging en wijziging van dienstverband

Doelstelling: Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.

7.3.1	1	**Beëindiging of wijziging van verantwoordelijkheden van het dienstverband** Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband behoren te worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer gebracht.	Secretaris/ algemeen directeur Proceseigenaar

8

Beheer van bedrijfsmiddelen

8.1 Verantwoordelijkheid voor bedrijfsmiddelen

Doelstelling: Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.

8.1.1	1	**Inventariseren van bedrijfsmiddelen** Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden.	Proceseigenaar Dienstenleverancier
		Handreiking: Samenhang beheerprocessen en informatiebeveiliging	
8.1.2	1	**Eigendom van bedrijfsmiddelen** Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben.	Proceseigenaar Dienstenleverancier
8.1.3	1	**Aanvaardbaar gebruik van bedrijfsmiddelen** Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten behoren regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	Secretaris/algemeen directeur Proceseigenaar
8.1.3.1	1	Alle medewerkers zijn aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen.	
8.1.3.2	1	De gedragsregels voor het gebruik van bedrijfsmiddelen zijn voor extern personeel in het contract vastgelegd overeenkomstig de huisregels of gedragsregels.	
8.1.4	1	**Teruggeven van bedrijfsmiddelen** Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst terug te geven.	Secretaris

8.2 Informatieclassificatie

Doelstelling: Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.

8.2.1	1	**Classificatie van informatie** Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	Proceseigenaar
		Handreiking: BIO-Dataclassificatie	
8.2.1.1	1	De informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd, zodat duidelijk is welke bescherming nodig is.	
8.2.2	1	**Informatie labelen** Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Proceseigenaar
8.2.3	1	**Behandelen van bedrijfsmiddelen** Procedures voor het behandelen van bedrijfsmiddelen behoren te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Proceseigenaar Dienstenleverancier

8.3 Behandelen van media

Doelstelling: Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.

8.3.1	1	**Beheer van verwijderbare media** Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	Proceseigenaar Dienstenleverancier
		Handreiking: Mobiele-gegevensdragers	
8.3.1.1	1	Er is een verwijderinstructie waarin is opgenomen dat van herbruikbare media die de organisatie verlaten de onnodige inhoud onherstelbaar verwijderd (ISO27002 - implementatierichtlijn 8.3.1.a).	
8.3.1.2	2	De wijze waarop vertrouwelijk of hoger geclassificeerde informatie is opgeslagen, voldoet aan de eisen van het NBV.	
8.3.2	2	**Verwijderen van media** Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	Dienstenleverancier
		Handreiking: Afvoer-ICT-middelen	
8.3.2.1	2	Media die vertrouwelijke informatie bevatten zijn opgeslagen op een plek die niet toegankelijk is voor onbevoegden. Verwijdering vindt plaats op een veilige manier, bijv. door verbranding of versnippering. Verwijdering van alleen gegevens is ook mogelijk door het wissen van de gegevens voordat de media worden gebruikt voor een andere toepassing in de organisatie (ISO27002 - implementatierichtlijn 8.3.2.a)	
8.3.2.2	2	Voor het wissen van alle data op het medium, wordt de data onherstelbaar verwijderd, bijvoorbeeld door minimaal twee keer te overschrijven met vaste data en één keer met random data. Er wordt gecontroleerd of alle data onherstelbaar verwijderd is.	
8.3.3	2	**Media fysiek overdragen** Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	Secretaris/ algemeen directeur
8.3.3.1	2	Er is voor de gehele organisatie beleid voor het fysiek transport van media vastgesteld.	
8.3.3.2	2	Het gebruik van koeriers of transporteurs voor vertrouwelijk of hoger geclassificeerde informatie voldoet aan vooraf opgestelde betrouwbaarheidseisen.	

9

Toegangsbeveiliging

Algemene handreiking: Beleid logisch toegangsbeveiliging

9.1 Bedrijfseisen voor toegangsbeveiliging

Doelstelling: Toegang tot informatie en informatie verwerkende faciliteiten beperken.

9.1.1	**1**	**Beleid voor toegangsbeveiliging** Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Secretaris
9.1.2	**1**	**Toegang tot netwerken en netwerkdiensten** Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	Dienstenleverancier
		Handreiking: MDM	
9.1.2.1	1	Alleen geauthenticeerde apparatuur kan toegang krijgen tot een vertrouwde zone.	
9.1.2.2	1	Gebruikers met eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone.	

9.2 Beheer van toegangsrechten van gebruikers

Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.

9.2.1	**1**	**Registratie en afmelden van gebruikers** Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Proceseigenaar Dienstenleverancier
9.2.1.1	1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.	
9.2.1.2	1	Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	

9.2.2	1	**Gebruikers toegang verlenen** Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	Proceseigenaar Dienstenleverancier
9.2.2.1	1	Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.	
9.2.2.2	1	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.	
9.2.2.3	2	Er is een actueel mandaatregister waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten dan wel functieprofielen.	
9.2.3	1	**Beheren van speciale toegangsrechten** Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	Proceseigenaar Dienstenleverancier
9.2.3.1	2	De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.	
9.2.4	1	**Beheer van geheime authenticatie-informatie van gebruikers** Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.	Dienstenleverancier
9.2.5	1	**Beoordeling van toegangsrechten van gebruikers** Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	Proceseigenaar Dienstenleverancier
9.2.5.1	1	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld.	
9.2.5.2	1	De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident.	
9.2.5.3	2	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.	
9.2.6	1	**Toegangsrechten intrekken of aanpassen** De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beeindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.	Proceseigenaar Dienstenleverancier

9.3 Verantwoordelijkheden van gebruikers

Doelstelling: Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie.

9.3.1	1	**Geheime authenticatie-informatie gebruiken** Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	Secretaris/ algemeen directeur Dienstenleverancier
9.3.1.1	2	Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis.	

9.4 Toegangsbeveiliging van systeem en toepassing

Doelstelling: Onbevoegde toegang tot systemen en toepassingen voorkomen.

9.4.1	1	**Beperking toegang tot informatie** Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	Proceseigenaar Dienstenleverancier
9.4.1.1	2	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.	
9.4.1.2	2	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	
9.4.2	1	**Beveiligde inlogprocedures** Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	Proceseigenaar Dienstenleverancier
9.4.2.1	1	Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.	
9.4.2.2	2	Voor het verlenen van toegang tot het netwerk door externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.	

9.4.3	**1**	**Systeem voor wachtwoordbeheer** Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.	Dienstenleverancier
9.4.3.1	1	Als er geen gebruik wordt gemaakt van two-factor authenticatie is de wachtwoordlengte minimaal 8 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen is vastgelegd.	
9.4.3.2	2	In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd (zie ook 9.4.2.1.).	
9.4.3.3	2	Het wachtwoordbeleid wordt geautomatiseerd afgedwongen.	
9.4.3.4	2	Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.	
9.4.3.5	2	Wachtwoorden die voldoen aan het wachtwoordbeleid hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van 6 maanden.	
9.4.4	**1**	**Speciale systeemhulpmiddelen gebruiken** Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd.	Dienstenleverancier
9.4.4.1	1	Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen.	
9.4.4.2	2	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek	
9.4.5	**1**	**Toegangsbeveiliging op programmabroncode** Toegang tot de programmabroncode behoort te worden beperkt.	Proceseigenaar Dienstenleverancier

10

Cryptografie

	Algemene handreiking: Encryptiebeleid

10.1 Cryptografische beheersmaatregelen

Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.

10.1.1	**2**	**Beleid inzake het gebruik van cryptografische beheersmaatregelen** Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	Secretaris
10.1.1.1	2	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) wanneer cryptografie ingezet wordt; (b) wie verantwoordelijk is voor de implementatie; (c) wie verantwoordelijk is voor het sleutelbeheer; (d) welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast; (e) de wijze waarop het beschermingsniveau vastgesteld wordt; (f) bij inter-organisatie communicatie wordt het beleid onderling vastgesteld.	
10.1.1.2	2	Cryptografische toepassingen voldoen aan passende standaarden.	
10.1.2	**1**	**Sleutelbeheer** Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd.	Dienstenleverancier
10.1.2.1	2	Ingeval van PKI-overheid certificaten: hanteer de PKI-Overheid-eisen t.a.v. het sleutelbeheer. In overige situaties: hanteer de standaard ISO-11770 voor het beheer van cryptografische sleutels.	
10.1.2.2	2	Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit risicoafweging blijkt dat deze noodzakelijk zijn.	

11

Fysieke beveiliging en beveiliging van de omgeving

Algemene handreiking: Toegangsbeleid

11.1 Beveiligde gebieden

Doelstelling: Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatie verwerkende faciliteiten van de organisatie voorkomen.

11.1.1	**1**	**Fysieke beveiligingszone** Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.	Secretaris/algemeen directeur
11.1.1.1	1	Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van standaarden.	
11.1.2	**1**	**Fysieke toegangsbeveiliging** Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Secretaris/algemeen directeur
11.1.2.1	2	In geval van concrete beveiligingsrisico's worden waarschuwingen, conform onderlinge afspraken, verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid.	
		Handreiking: Protocol uitwisseling van persoons gerelateerde beveiligingsinformatie	
11.1.3	**1**	**Kantoren, ruimten en faciliteiten beveiligen** Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.	Proceseigenaar Dienstenleverancier
11.1.3.1	1	Sleutelbeheer is ingericht op basis van een sleutelplan.	
11.1.4	**1**	**Beschermen tegen bedreigingen van buitenaf** Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	Proceseigenaar Dienstenleverancier
11.1.4.1	1	De organisatie heeft geïnventariseerd welke papieren archieven en apparatuur bedrijfskritisch zijn. Tegen bedreigingen van buitenaf zijn beveiligingsmaatregelen genomen op basis van een expliciete risicoafweging.	
11.1.4.2	1	Bij huisvesting van IT-apparatuur wordt rekening gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen.	

11.1.5	2	**Werken in beveiligde gebieden** Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.	Proceseigenaar Dienstenleverancier
11.1.6	1	**Laad- en loslocatie** Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.	Dienstenleverancier

11.2 Apparatuur

Doelstelling: Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.

11.2.1	1	**Plaatsing en bescherming van apparatuur** Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	Dienstenleverancier
11.2.2	1	**Nutsvoorzieningen** Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	Dienstenleverancier
11.2.3	1	**Beveiliging van bekabeling** Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.	Dienstenleverancier
11.2.4	1	**Onderhoud van apparatuur** Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	Dienstenleverancier
11.2.5	1	**Verwijdering van bedrijfsmiddelen** Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.	Dienstenleverancier
11.2.6	1	**Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein** Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	Dienstenleverancier
11.2.7	1	**Veilig verwijderen of hergebruiken van apparatuur** Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	Dienstenleverancier
		Zie overheidsmaatregelen van 8.3.2.	

11.2.8	1	**Onbeheerde gebruikersapparatuur** Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	Proceseigenaar Dienstenleverancier
11.2.9	1	**'Clear desk'- en 'clear screen'-beleid** Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatie verwerkende faciliteiten te worden ingesteld.	Secretaris/algemeen directeur Dienstenleverancier
11.2.9.1	2	Een onbeheerde werkplek in een ongecontroleerde omgeving is altijd vergrendeld.	
11.2.9.2	2	Informatie wordt automatisch ontoegankelijk gemaakt met bijvoorbeeld een screensaver na een inactiviteit van maximaal 15 minuten.	
11.2.9.3	2	Sessies op remote desktops worden op het remote platform vergrendeld na 15 minuten. Het overnemen van sessies op remote desktops op een ander client apparaat is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd.	
11.2.9.4	2	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van de token de toegangsbeveiligingslock automatisch geactiveerd.	
		Handreiking: Logische toegangsbeveiliging	

12

Beveiliging bedrijfsvoering

12.1 Bedieningsprocedures en verantwoordelijkheden

Doelstelling: Correcte en veilige bediening van informatie verwerkende faciliteiten waarborgen.

12.1.1	1	**Gedocumenteerde bedieningsprocedures** Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	Proceseigenaar Dienstenleverancier
12.1.2	1	**Wijzigingsbeheer** Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	Proceseigenaar Dienstenleverancier
12.1.2.1	1	In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: (a) het administreren van wijzigingen; (b) risicoafweging van mogelijke gevolgen van de wijzigingen; (c) goedkeuringsprocedure voor wijzigingen.	
		Handreiking: Samenhang beheersprocessen en informatiebeveiliging	
12.1.3	1	**Capaciteitsbeheer** Het gebruik van middelen behoort te worden gemonitord en afgestemd, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	Dienstenleverancier
12.1.3.1	1	In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijv. DDoS attacks, Distributed Denial of Service attacks) te signaleren en hierop te reageren.	
12.1.4	1	**Scheiding van ontwikkel-, test- en productieomgevingen** Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	Proceseigenaar Dienstenleverancier
12.1.4.1	2	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hierop worden afgeweken.	
12.1.4.2	2	Wijzigingen op de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hierop worden afgeweken.	

12.2 Bescherming tegen malware

Doelstelling: Waarborgen dat informatie en informatie verwerkende faciliteiten beschermd zijn tegen malware.

12.2.1	1	**Beheersmaatregelen tegen malware** Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	Secretaris/ algemeen directeur Dienstenleverancier
		Handreiking: Implementatie van detectie-oplossingen **Handreiking: Anti-malware beleid**	
12.2.1.1	1	Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.	
12.2.1.2	1	Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende linken.	
12.2.1.3	1	Software en bijbehorende herstelsoftware die malware opspoort zijn geïnstalleerd en worden regelmatig geüpdatet.	
12.2.1.4	1	Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan behoort te omvatten: (a) alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen; (b) bijlagen en downloads vóór gebruik.	
12.2.1.5	1	De malware scan wordt op verschillende omgevingen uitgevoerd, bijv. op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.	

12.3 Back-up

Doelstelling: Beschermen tegen het verlies van gegevens.

12.3.1	1	**Back-up van informatie** Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	Proceseigenaar Dienstenleverancier
		Handreiking: Back-up and recovery	
12.3.1.1	1	Er is een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld	
12.3.1.2	1	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.	
12.3.1.3	2	In het back-up beleid staan minimaal de volgende eisen: (a) dataverlies bedraagt maximaal 28 uur; (b) hersteltijd in geval van incidenten is maximaal 16 werkuren (2 dagen van 8 uur) in 85% van de gevallen.	
12.3.1.4	2	Het back-up proces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.	
12.3.1.5	2	De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de betrouwbaarheid te waarborgen als ze in noodgevallen uitgevoerd moet worden.	

12.4 Verslaglegging en monitoren

Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen.

12.4.1	1	**Gebeurtenissen registreren** Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Proceseigenaar Dienstenleverancier
		Handreiking: Loggingbeleid	
		Handreiking: NCSC-handreiking detectie-oplossingen	
12.4.1.1	1	Een logregel bevat minimaal de gebeurtenis; de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis.	
12.4.1.2	1	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	
12.4.1.3	2	De informatie verwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties), die worden ingezet op basis van een risico-inschatting, mede aan de hand van en de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.	
12.4.1.4	2	Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.	
12.4.1.5	2	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	
12.4.2	1	**Beschermen van informatie in logbestanden** Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	Dienstenleverancier
12.4.2.1	1	Er is een overzicht van logbestanden die worden gegenereerd.	
12.4.2.2	1	Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.	
12.4.2.3	2	Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.	
12.4.2.4	2	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16.	
12.4.3	1	**Logbestanden van beheerders en operators** ***Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.***	Dienstenleverancier
12.4.4	1	**Kloksynchronisatie** De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.	Dienstenleverancier

12.5 Beheersing van operationele software

Doelstelling: De integriteit van operationele systemen waarborgen.

12.5.1	1	**Software installeren op operationele systemen** Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.	Dienstenleverancier

12.6 Beheer van technische kwetsbaarheden

Doelstelling: Benutting van technische kwetsbaarheden voorkomen.

12.6.1	1	**Beheer van technische kwetsbaarheden** Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.	Dienstenleverancier
		Handreiking: Penetratietesten	
12.6.1.1	1	Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.	
12.6.2	1	**Beperkingen voor het installeren van software** Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	Dienstenleverancier
12.6.2.1	2	Gebruikers kunnen op hun werkomgeving niets zelf installeren, anders dan via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist).	

12.7 Overwegingen betreffende audits van informatiesystemen

Doelstelling: De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.

12.7.1	1	**Beheersmaatregelen betreffende audits van informatiesystemen** Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, behoren zorgvuldig te worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	Proceseigenaar Dienstenleverancier

13

Communicatiebeveiliging

13.1 Beheer van netwerkbeveiliging

Doelstelling: De bescherming van informatie in netwerken en de ondersteunende informatie verwerkende faciliteiten waarborgen.

13.1.1	1	**Beheersmaatregelen voor netwerken** Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Dienstenleverancier
13.1.2	1	**Beveiliging van netwerkdiensten** Beveiligingsmechanismen, dienstverleningsniveaus en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	Dienstenleverancier
13.1.2.1	2	Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt / geanalyseerd op kwaadaardige elementen middels detectie-voorzieningen (zoals beschreven in de richtlijn voor implementatie van detectie-oplossingen), zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties) of GDI, die worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen.	
		Handreiking: NCSC-handreiking detectie-oplossingen	
13.1.2.2	2	Bij ontdekte nieuwe dreigingen vanuit 13.1.2.1 worden deze, rekening houdend met de geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT, bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing).	
13.1.2.3	2	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied, wordt gebruik gemaakt van encryptie middelen waarvoor het NBV een positief inzetadvies heeft afgegeven.	
13.1.3	1	**Scheiding in netwerken** Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.	Dienstenleverancier
13.1.3.1	2	Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	

13.2 Informatietransport

Doelstelling: Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.

13.2.1	1	**Beleid en procedures voor informatietransport** Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	Secretaris/ algemeen directeur
13.2.2	1	**Overeenkomsten over informatietransport** Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	Proceseigenaar Dienstenleverancier
13.2.3	1	**Elektronische berichten** Informatie die is opgenomen in elektronische berichten behoord passend te zijn beschermd.	Dienstenleverancier
13.2.3.1	1	Voor de beveiliging van elektronische (e-mail)berichten gelden de vastgestelde open standaarden tegen phishing en afluisteren op de 'pas toe of leg uit'-lijst van het Forum. Voor beveiliging van websiteverkeer gelden de open standaarden tegen afluisteren op de 'pas toe of leg uit'-lijst van het Forum.	
13.2.3.2	2	Voor veilige berichtenuitwisseling met basisregistraties, wordt conform de 'pas toe of leg uit'-lijst van het Forum, gebruik gemaakt van de actuele versie van Digikoppeling	
13.2.3.3	2	Maak gebruik van PKI-Overheid certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn o.a. digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontlenen.	
13.2.3.4	2	Om zekerheid te bieden over de integriteit van het elektronische bericht wordt voor elektronische handtekeningen gebruik gemaakt van de AdES Baseline Profile standaard.	
13.2.4	1	**Vertrouwelijkheids- of geheimhoudingsovereenkomst** Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.	Secretaris/ algemeen directeur Proceseigenaar Dienstenleverancier

14

Acquisitie, ontwikkeling en onderhoud van informatiesystemen

14.1 Beveiligingseisen voor informatiesystemen

Doelstelling: Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken.

14.1.1	1	**Analyse en specificatie van informatiebeveiligingseisen** De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	Proceseigenaar
14.1.1.1	1	Bij nieuwe informatiesystemen en bij wijzigingen op bestaande informatiesystemen moet een expliciete risicoafweging worden uitgevoerd ten behoeve van het vaststellen van de beveiligingseisen, uitgaande van de BIO.	
		Handreiking: Risicoanalysemethode	
		Handreiking: Risicomanagement ISO-27005	
14.1.2	1	**Toepassingen op openbare netwerken beveiligen** Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	Dienstenleverancier
		Zie overheidsmaatregel 13.2.3.3.	
14.1.3	1	**Transacties van toepassingen beschermen** Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	Dienstenleverancier
		Zie overheidsmaatregel 13.2.3.3.	

14.2 Beveiliging in ontwikkelings- en ondersteunende processen

Doelstelling: Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.

14.2.1	1	**Beleid voor beveiligd ontwikkelen** Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast.	Secretaris/ algemeen directeur Proceseigenaar
14.2.1.1	1	De gangbare principes rondom Security by design zijn uitgangspunt voor de ontwikkeling van software en systemen	
		Handreiking: Grip op Secure Software Development (SSD).	
14.2.2	1	**Procedures voor wijzigingsbeheer met betrekking tot systemen** Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	Proceseigenaar Dienstenleverancier
		Handreiking: Proces wijzigingsbeheer	
14.2.2.1	1	Voor het wijzigingsbeheer gelden de algemeen geaccepteerde beheerframeworks, zoals ITIL, ASL of BiSL.	
14.2.3	2	**Technische beoordeling van toepassingen na wijzigingen besturingsplatform** Als besturingsplatforms zijn veranderd, behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.	Dienstenleverancier
14.2.4	-	**Vervallen**	-
14.2.5	1	**Principes voor engineering van beveiligde systemen** Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	Dienstenleverancier
14.2.5.1	1	Zie overheidsmaatregel 14.2.1.1	
14.2.6	1	**Beveiligde ontwikkelomgeving** Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	Dienstenleverancier
14.2.6.1	1	Uitgangspunt voor systeemontwikkeling trajecten is een expliciete risicoafweging. Deze heeft zowel de ontwikkelomgeving als ook het te ontwikkelen systeem in scope.	
14.2.7	1	**Uitbestede softwareontwikkeling** Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.	Proceseigenaar
14.2.7.1	1	Een voorwaarde voor uitbestedingstrajecten is een expliciete risicoafweging. De noodzakelijke beveiligingsmaatregelen die daaruit volgen worden aan de leverancier opgelegd.	
14.2.8	1	**Testen van systeembeveiliging** Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.	Dienstenleverancier
14.2.9	1	**Systeemacceptatietests** Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.	Proceseigenaar Dienstenleverancier
14.2.9.1	1	Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.	
14.2.9.2	1	Van de resultaten van de testen wordt verslag gemaakt.	

14.3 Testgegevens

Doelstelling: Bescherming waarborgen van gegevens die voor het testen zijn gebruikt.

14.3.1	2	**Bescherming van testgegevens** Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.	Proceseigenaar Dienstenleverancier

15

Leveranciersrelaties

15.1 Informatiebeveiliging in leveranciersrelaties

Doelstelling: De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.

15.1.1	**1**	**Informatiebeveiligingsbeleid voor leveranciersrelaties** Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd.	Secretaris/algemeen directeur Proceseigenaar
15.1.1.1	1	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, worden eisen t.a.v. informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) benoemd. Deze eisen zijn gebaseerd op een expliciete risicoafweging.	
15.1.1.2	2	Op basis van een expliciete risicoafweging worden de beheersmaatregelen met betrekken tot leveranciersoegang tot bedrijfsinformatie vastgesteld.	
15.1.1.3	2	Met alle leveranciers die als verwerker voor of namens de organisatie persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.	
		Handreiking: Whitepaper Cloud computing	
		Handreiking: Cloud computing	
		Handreiking: Verwerkersovereenkomsten (rijk), Model verwerkersovereenkomst gemeenten (gemeenten)	

15.1.2	**1**	**Opnemen van beveiligingsaspecten in leveranciersovereenkomsten** Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	Proceseigenaar Dienstenleverancier
15.1.2.1	1	De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in de (inkoop)contracten waar informatie een rol speelt.	
15.1.2.2	1	In de inkoopcontracten worden expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen.	
15.1.2.3	1	In situaties waarin contractvoorwaarden worden opgelegd door leveranciers, is voorafgaand aan het tekenen van het contract met een risicoafweging helder gemaakt wat de consequenties hiervan zijn voor de organisatie. Expliciet is gemaakt welke consequenties geaccepteerd worden en welke gemitigeerd moeten zijn bij het aangaan van de overeenkomst.	
15.1.2.4	1	Ter waarborging van vertrouwelijkheid of geheimhouding worden bij IT-inkopen standaard voorwaarden voor inkoop gehanteerd.	
15.1.2.5	2	Voordat een contract wordt afgesloten wordt in een risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is. Een vast onderdeel van het contract is een expliciete uitwerking van de exit-strategie.	
15.1.2.6	2	In inkoopcontracten wordt expliciet de mogelijkheid van een externe audit opgenomen waarmee de betrouwbaarheid van de geleverde dienst kan worden getoetst. Een audit is niet nodig als de contractant d.m.v. certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd.	
		Handreiking: Model voor een verwerkersovereenkomst	
15.1.3	**1**	**Toeleveringsketen van informatie- en communicatietechnologie** Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	Proceseigenaar Dienstenleverancier
15.1.3.1	2	Leveranciers moeten hun keten van toeleveranciers bekend maken en transparant zijn over de maatregelen die zij genomen hebben om de aan hun opgelegde eisen ook door te vertalen naar hun toeleveranciers.	
		Handreiking: Inkoopvoorwaarden en informatiebeveiligingseisen	
		Handreiking: Proces wijzigingsbeheer	

15.2 Beheer van dienstverlening van leveranciers

Doelstelling: Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.

15.2.1	**1**	**Monitoring en beoordeling van dienstverlening van leveranciers** Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.	Proceseigenaar
15.2.1.1	2	Jaarlijks wordt de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.	
		Handreiking: Proces wijzigingsbeheer	
		Handreiking: Contractmanagement	
15.2.2	**2**	**Beheer van veranderingen in dienstverlening van leveranciers** Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	Proceseigenaar

16

Beheer van informatie-beveiligingsincidenten

16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen

Doelstelling: Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatie-beveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.

16.1.1	**1**	**Verantwoordelijkheden en procedures** Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	Secretaris/algemeen directeur Proceseigenaar
		Handreiking: Samenhang beheerprocessen en informatiebeveiliging	
		Handreiking: Implementatie van detectie-oplossingen	
16.1.2	**1**	**Rapportage van informatiebeveiligingsgebeurtenissen** Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	Secretaris/algemeen directeur Proceseigenaar Dienstenleverancier
16.1.2.1	1	Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.	
16.1.2.2	1	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.	
16.1.2.3	1	Alle medewerkers en contractanten hebben aantoonbaar kennis genomen van de meldingsprocedure van incidenten.	
16.1.2.4	1	Incidenten worden zo snel als mogelijk, maar in ieder geval binnen 24 uur na bekendwording, gemeld bij het meldloket.	
16.1.2.5	1	De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.	
16.1.2.6	1	De opvolging van incidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.	
16.1.2.7	1	Informatie afkomstig uit de responsible disclosure procedure zijn onderdeel van de incidentrapportage.	
		Handreiking: Contractmanagement	

16.1.3	**1**	**Rapportage van zwakke plekken in de informatiebeveiliging** Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	Proceseigenaar Dienstenleverancier
		Zie overheidsmaatregel 16.1.2.4	
16.1.3.1	1	Een responsible disclosure procedure is gepubliceerd en ingericht.	
		Handreiking: Responsible Disclosure	
16.1.4	**1**	**Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen** Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	Proceseigenaar Dienstenleverancier
16.1.4.1	2	Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatie verwerkende systemen, behoren zo snel mogelijk (binnen 72 uur) al dan niet geautomatiseerd te worden gemeld aan het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT.	
16.1.5	**1**	**Respons op informatiebeveiligingsincidenten** Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Proceseigenaar Dienstenleverancier
		Handreiking: Incidentmanagement en response beleid	
16.1.6	**2**	**Lering uit informatiebeveiligingsincidenten** Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	Secretaris/ algemeen directeur Proceseigenaar Dienstenleverancier
16.1.6.1	2	Beveiligingsincidenten worden geanalyseerd met als doel te leren en het voorkomen van toekomstige beveiligingsincidenten.	
16.1.6.2	2	De analyses van de beveiligingsincidenten worden gedeeld met de relevante partners om herhaling en toekomstige incidenten te voorkomen.	
		Handreiking: Implementatie van detectie oplossingen	
16.1.7	**2**	**Verzamelen van bewijsmateriaal** De organisatie behoort procedures te definieren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	Secretaris/ algemeen directeur Proceseigenaar Dienstenleverancier
16.1.7.1	2	In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar.	

17

Informatiebeveiligings-aspecten van bedrijfs-continuïteitsbeheer

17.1 Informatiebeveiligingscontinuïteit

Doelstelling: Informatiebeveiligingscontinuïteit behoort te worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.

		Algemene handreiking: Bedrijfscontinuïteitsbeheer	
17.1.1	**1**	**Informatiebeveiligingscontinuïteit plannen** De organisatie behoort haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vast te stellen.	Secretaris/ algemeen directeur Proceseigenaar
		Handreiking: Samenhang beheerprocessen en informatiebeveiliging	
17.1.2	**1**	**Informatiebeveiligingscontinuïteit implementeren** De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	Proceseigenaar Dienstenleverancier
17.1.3	**1**	**Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren** De organisatie behoort de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	Proceseigenaar Dienstenleverancier
17.1.3.1	2	Continuïteitsplannen worden jaarlijks getest op geldigheid en bruikbaarheid.	
17.1.3.2	2	Door het uitvoeren van een expliciete risicoafweging worden de bedrijfskritische procesonderdelen met hun bijbehorende betrouwbaarheidseisen geïdentificeerd.	
17.1.3.3	2	De dienstverlening van de bedrijfskritische onderdelen wordt bij calamiteiten minimaal binnen een week hersteld.	

17.2 Redundante componenten

Doelstelling: Beschikbaarheid van informatie verwerkende faciliteiten bewerkstelligen.

17.2.1	1	**Beschikbaarheid van informatie verwerkende faciliteiten** Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Dienstenleverancier

18

Naleving

18.1 Naleving van wettelijke en contractuele eisen

Doelstelling: Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.

18.1.1	1	**Vaststellen van toepasselijke wetgeving en contractuele eisen** Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen behoren voor elk informatiesysteem en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.	Secretaris/ algemeen directeur Proceseigenaar Dienstenleverancier
18.1.2	1	**Intellectuele-eigendomsrechten** Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen behoren passende procedures te worden geïmplementeerd.	Secretaris/ algemeen directeur Proceseigenaar Dienstenleverancier
18.1.3	2	**Beschermen van registraties** Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	Proceseigenaar Dienstenleverancier
18.1.3.1	2	De proceseigenaar heeft per soort informatie inzichtelijk gemaakt wat de bewaartermijn is.	
18.1.4	1	**Privacy en bescherming van persoonsgegevens** Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Secretaris/ algemeen directeur Proceseigenaar Dienstenleverancier
18.1.4.1	1	In overeenstemming met de AVG heeft iedere organisatie een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren.	
18.1.4.2	2	Organisaties controleren regelmatig de naleving van de privacy regels en informatieverwerking en –procedures binnen haar verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	
		Zie overheidsmaatregel 14.2.6.1	
18.1.5	1	**Voorschriften voor het gebruik van cryptografische beheersmaatregelen** Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	Secretaris/ algemeen directeur
18.1.5.1	1	Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de 'pas toe of leg uit'-lijst van het Forum.	
		Zie overheidsmaatregel 10.1.1.1	

18.2 Informatiebeveiligingsbeoordelingen

Doelstelling: Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie.

18.2.1	1	**Onafhankelijke beoordeling van informatiebeveiliging** De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheerdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld.	Secretaris/ algemeen directeur Proceseigenaar Dienstenleverancier
18.2.1.1	2	Er is een information security information system (ISMS) waarmee aantoonbaar de gehele plan-do-check-act cyclus op gestructureerde wijze wordt afgedekt.	
		Aanwijzing: ISMS	
18.2.1.2	2	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.	
18.2.2	1	**Naleving van beveiligingsbeleid en -normen** De directie behoort regelmatig de naleving van de informatieverwerking en - procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Secretaris/ algemeen directeur Proceseigenaar Dienstenleverancier
18.2.2.1	1	In de P&C cyclus wordt gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring (ICV) over de informatiebeveiliging. Indien voldoende herkenbaar kan de ICV voor informatiebeveiliging onderdeel zijn van de reguliere, generieke verantwoording.	
18.2.3	1	**Beoordeling van technische naleving** Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	Proceseigenaar Dienstenleverancier
18.2.3.1	2	Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of pentesten.	
		Handreiking: Penetratietesten	

Bijlage 1: Wet- en regelgeving

Om de BIO praktisch uitvoerbaar te maken, zijn in veel overheidsmaatregelen verwijzingen opgenomen naar bestaande wet- en regelgeving. Deze verwijzingen hebben als voordeel dat degene die met de BIO aan de slag gaat er concreet op gewezen wordt dat er reeds bestaande wet- en regelgeving is waarin (beveiligings)eisen zijn vastgelegd. Bovendien zijn deze verwijzingen zo ook in het stramien van de ISO 27002-indeling gepositioneerd. Er is bewust gekozen voor het maken van verwijzingen en niet voor het herformuleren om misinterpretatie te voorkomen. Voor de genoemde wet- en regelgeving geldt dat de BIO alleen bepaalde beveiligingsaspecten heeft meegenomen. Het is niet de intentie dat de BIO de genoemde wet- en regelgeving volledig afdekt.

In de overheidsmaatregelen zijn verwijzingen opgenomen naar de volgende wet- en regelgeving:

- Ades baseline profile standard
- Algemeen Rijksambtenarenreglement (ARAR)
- Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT 2016)
- AVG (deze treedt in de plaats van de WBP en wordt 25 mei 2018 van kracht);
- Beveiligingsvoorschrift 2013 (BVR 2013), *Stcrt.* 2013, 15496
- CM(2002)49
- Gedragsregeling voor de digitale werkomgeving (1 juli 2016; SGO besluit)
- Het NKBR (Normenkader beveiliging Rijkskantoren) 2015
- Interne klokkenluidersregeling
- ITIL, ASL of BISL framework
- Kader Rijkstoegangsbeleid
- NCSC classificatie
- 'Pas toe of leg uit'-lijst van het Forum Standaardisatie.
- Programma van Eisen PKI Overheid
- Responsible disclosure procedure
- Voorschrift Informatiebeveiliging Rijksdienst (VIR2007), *Stcrt.* 2007, 122/11
- Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIR-BI 2013)
- Wet veiligheidsonderzoeken (WVO)
- Archiefwet
- Wet structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI);
- Wet basisregistratie personen (Wet BRP);
- Telecommunication Infrastructure Standard for Data Centers (TIA-942)

De BIO treedt niet in de plaats van een Data Protection Impact Assessment (DPIA). Een DPIA gaat namelijk over veel meer dan alleen de beveiliging van persoonsgegevens, zoals het vraagstuk van rechtmatigheid van verwerking.

Bijlage 2: Basisbeveiligingsniveaus

De basisbeveiligingsniveaus zijn uitgewerkt langs de lijnen beschikbaarheid, integriteit en vertrouwelijkheid. De BBN-toets helpt bij het kiezen van het best passende niveau. De beschikbaarheidsniveaus zijn gebaseerd op de geldende beschikbaarheidsniveaus die door de grote interne dienstenleveranciers worden gehanteerd. De vertrouwelijkheidsniveaus zijn in lijn gebracht met de schadescenario's die gelden voor de Te Beschermen Belangen. De onderverdeling is als volgt:

BBN1: beschikbaarheid = Laag; integriteit = Laag; vertrouwelijkheid = Laag
BBN2: beschikbaarheid = Midden; integriteit = Midden; vertrouwelijkheid = Midden
BBN3: beschikbaarheid = Midden; integriteit = Midden; vertrouwelijkheid = Hoog

BBN1	
Beschikbaarheid = Laag	Het informatiesysteem mag incidenteel uitvallen voor maximaal twee weken (ook in piekperiodes) en heeft nauwelijks of geen gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: • financiële gevolgen; op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; leidt nog niet uit het niet krijgen van een accountants verklaring; of • beperkt verlies van management control; of • irritatie en ongemak bij burgers geventileerd in de media; of • interne negatieve publiciteit (imagoschade). Deze gevolgen worden als volgt gekwantificeerd: • Kantoorautomatisering en organisatie specifieke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes; • maximaal dataverlies 28 uur; • maximale hersteltijd in geval van incidenten is binnen 40 werkuren (5 werkdagen van 8 uur) in 85% van de gevallen.
Integriteit = Laag	Er zijn geen bijzondere maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid van informatie te waarborgen.[46] Het verlies van integriteit kan leiden tot beperkte schade, bijvoorbeeld: • financiële gevolgen; op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; leidt nog niet uit het niet krijgen van een accountants verklaring; of • beperkt verlies van management control; of • irritatie en ongemak bij burgers geventileerd in de media; of • interne negatieve publiciteit (imagoschade).
Vertrouwelijkheid = Laag	Kennisname van informatie door ongeautoriseerden (buitenstaanders) is niet gewenst, maar leidt niet tot schade van enige omvang. Het gaat hier om ongerubriceerde informatie. Het openbaar worden van deze informatie kan leiden tot: • financiële gevolgen; op te vangen binnen de begroting van de organisatie of uitvoeringsorganisatie; of • irritatie en ongemak bij burgers geventileerd in de media; of • interne negatieve publiciteit (imagoschade).

46) VIR-Definitie

BBN2	
Beschikbaarheid = Midden	Het informatiesysteem mag beperkt korte tijd uitvallen voor maximaal één week (ook in piekperiodes) en heeft voelbare gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: • politieke schade aan een bestuurder: bestuurder moet zich verantwoorden n.a.v. verantwoordings vragen; of • schade te herstellen door ambtelijke opschaling; of • financiele gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of • belangrijk verlies van management control; of • verlies van publiek respect; klachten van burgers; of • organisatiebrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers. De beschikbaarheid wordt als volgt gekwantificeerd: • kantoorautomatisering en organisatie specifieke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes; • maximaal dataverlies 24 uur; • maximale hersteltijd in geval van incidenten is binnen 16 werkuren (2 dagen van 8 uur).
Integriteit = Midden	Er zijn passende maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid (VIR definitie) te waarborgen. Het verlies van integriteit kan leiden tot forse schade, bijvoorbeeld: • politieke schade aan een bestuurder: bestuurder moet zich verantwoorden n.a.v. verantwoordings vragen; of • schade te herstellen door ambtelijke opschaling; of • financiele gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of • belangrijk verlies van management control; of • verlies van publiek respect; klachten van burgers; of • organisatiebrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers.
Vertrouwelijkheid = Midden	Bescherming van gegevens èn andere te beschermen belangen in de processen van de overheid, waar o.a. vertrouwelijkheid aan de orde is, omdat het om gevoelige informatie gaat. Het openbaar worden van de gegevens, kan leiden tot: • politieke schade aan een bestuurder: bestuurder moet zich verantwoorden n.a.v. verantwoordings vragen; of • schade te herstellen door ambtelijke opschaling; of • financiele gevolgen: niet meer op te vangen binnen de begroting van de organisatie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of • verlies van publiek respect; klachten van burgers of significant verlies van motivatie van medewerkers; of • bindende aanwijzing van de AP in verband met schending van de privacy; of • directe imagoschade, bijvoorbeeld door negatieve publiciteit.

BBN3	
Beschikbaarheid = Midden	Het informatiesysteem mag beperkt korte tijd uitvallen voor maximaal één week (ook in piekperiodes) en heeft voelbare gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: • politieke schade aan een bestuurder: bestuurder moet zich verantwoorden n.a.v. verantwoordings vragen; of • schade te herstellen door ambtelijke opschaling; of • financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of • belangrijk verlies van management control; of • verlies van publiek respect; klachten van burgers; of • Organisatiebrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers. De beschikbaarheid wordt als volgt gekwantificeerd: • Kantoorautomatisering en organisatie specifieke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes; • maximaal dataverlies 24 uur; • maximale hersteltijd in geval van incidenten is binnen 16 werkuren (2 dagen van 8 uur).
Integriteit = Midden	Er zijn passende maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid (VIR definitie) te waarborgen. Het verlies van integriteit kan leiden tot forse schade, bijvoorbeeld: • politieke schade aan een bestuurder: bestuurder moet zich verantwoorden n.a.v. verantwoordings vragen; of • schade te herstellen door ambtelijke opschaling; of • financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of • belangrijk verlies van management control; of • verlies van publiek respect; klachten van burgers; of • Organisatiebrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers.
Vertrouwelijkheid = Hoog	Verlies van informatie heeft een grote impact, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3; • informatie wordt door derden geleverd met een rubricering (niet zijnde BBN2); of • aansluiting op een infrastructuur vereist (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen) BBN3 om informatie te kunnen verwerken op deze infrastructuur; of • weerstand tegen statelijke actoren is noodzakelijk.

Deel 3

Addendum BIO

Inleiding Addendum

In dit addendum worden alle eisen genoemd die specifiek en verplichtend zijn voor een bepaalde overheidslaag. Omdat de rijksoverheid een aantal specifieke documenten heeft zoals het VIR, VIR-BI en anderen, die niet gelden voor andere overheidslagen, zijn deze nadrukkelijk opgenomen in dit addendum. Voorts zijn teksten opgenomen die niet goed te verwerken waren in de eerste twee delen en dit komt dan voornamelijk door de rol van het NCSC voor de rijksoverheid en de aanwezigheid van een aantal sectorale CERT's bij de andere overheidslagen.

Het addendum is aanvullend op de teksten en normen uit deel 1 en 2.

5. Informatiebeveiligingsbeleid

5.1 Aansturing door de directie van de informatiebeveiliging

Maatregel	Organisatie	BBN	Richtlijn	Verantwoordelijke(n)
5.1.1.1	Rijk	1	Richtlijn: VIR, artikel 3	Secretaris/algemeen directeur
5.1.2.1	Rijk	1	Richtlijn: VIR, artikel 3, lid e.	Secretaris/algemeen directeur

6. Organiseren van informatiebeveiliging

6.1 Interne organisatie

6.1.1.2	Rijk	1	Richtlijn: VIR, VIR-BI, BVR	Secretaris/ algemeen directeur
6.1.1.2	Overheid	1	Wet: AVG	Secretaris/ algemeen directeur/ dienstenleverancier
6.1.3.3	Rijk (1)	1	De organisatie verstrekt contactgegevens aan het NCSC ten behoeve van de opvolging van incidenten, kwetsbaarheden en dreigingen.	Secretaris/ algemeen directeur/ Dienstenleverancier
6.1.3.3	Gemeente Waterschap	1	De organisatie verstrekt contactgegevens aan de sectorale-CERT ten behoeve van de opvolging van incidenten, kwetsbaarheden en dreigingen.	Secretaris/ algemeen directeur/ Dienstenleverancier

7. Veilig personeel

7.1 Voorafgaand aan het dienstverband

7.1.1	Rijk	1	Richtlijn: VIR-BI	Secretaris/ algemeen directeur Proceseigenaar

7.2 Tijdens het dienstverband

7.2.1	Rijk	1	Richtlijn: interne klokkenluidersregeling	Secretaris/ algemeen directeur

8. Beheer van bedrijfsmiddelen

8.1 Verantwoordelijkheid voor bedrijfsmiddelen

8.1	Rijk	1	Richtlijn: Gedragsregeling voor de digitale werkomgeving	Secretaris/ algemeen directeur Proceseigenaar

8.3 Behandelen van media

8.3.1	Rijk	2	VIR-BI: goedgekeurde producten NBV	Proceseigenaar Dienstenleverancier

11. Fysieke beveiliging en beveiliging van de omgeving

11.1 Beveiligde gebieden

11.1.1.1	Rijk	1	Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van: a: het Kader Rijkstoegangsbeleid (2010); b: het Normenkader Beveiliging Rijkskantoren (NkBR 2015); c: het Beveiligingsvoorschrift Rijk (BVR 2013).	Secretaris/ algemeen directeur
11.1.3.1	Rijk	1	Aanwijzing: NkBR 5.4	Proceseigenaar Dienstenleverancier

14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen

14.1 Beveiligingseisen voor informatiesystemen

14.1.1.1	Rijk	1	Handreiking: VIR	Proceseigenaar

15. Leveranciersrelaties

15.1 Informatiebeveiliging in leveranciersrelaties

15.1.2	Rijk	1	VIR-BI	Proceseigenaar Dienstenleverancier
15.1.2	Rijk	1	ARBIT	Proceseigenaar Dienstenleverancier
15.1.2	Gemeenten	1	GIBIT	Proceseigenaar Dienstenleverancier

16. Beheer van informatiebeveiligingsincidenten

16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen

16.1.4.1	2	Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatie verwerkende systemen, behoren zo snel mogelijk (binnen 72 uur) al dan niet geautomatiseerd te worden gemeld aan het NCSC door of namens het department security contact (DSC, operationele contactpersoon voor het NCSC) of de Chief Information Security Officer (CISO).