centrum informatiebeveiliging en privacybescherming

Criteria BIO-SA

Uitleg van de 16 BIO-criteria en de volwassenheidsniveaus

Februari 2021 [versie 1.0]

Het CIP betracht zorgvuldigheid bij het samenstellen van zijn publicaties. Het kan voorkomen dat er toch sprake is van omissies, onjuistheden en/of gedateerdheid. Het is altijd de verantwoordelijkheid van de lezer zelf dit te beoordelen en desgewenst te corrigeren indien hij zich baseert op of gebruik maakt van een CIP-publicatie. Het CIP ontvangt graag correctieverzoeken en suggesties.

© Centrum Informatiebeveiliging en Privacybescherming. Het CIP heeft voor deze publicatie licentie Creative Commons Naamsvermelding-GelijkDelen 4.0 Internationaal (CC BY-SA 4.0) verleend. Voor meer informatie zie: https://creativecommons.org/licenses/by-sa/4.0/deed.nl.

Criteria BIO-SA

Titel	Criteria BIO-SA
Datum	Februari 2021
Status	Versie 1.0
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming (CIP)
Regime	Individuele praktijk
Auteur	Marcel Koers (CIP)
Reviewers	Ruud de Bruijn (CIP) en Elleke Oosterwijk (CIP)

Considerans

CIP-producten steunen op kennis van professionals uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als de markt.

Opmerkingen en aanvullingen kun je melden op cip-overheid.nl/contact.

Managementsamenvatting

Het op orde krijgen van de informatiebeveiliging door te voldoen aan de Baseline Informatiebeveiliging Overheid (BIO) is doorgaans niet van de ene op de andere dag geregeld. De benodigde inspanning is een resultante van de omvang van de organisatie en de complexiteit van de ICT-voorziening. In grotere organisaties, met meerdere geschakelde verwerkingssystemen en processen, waarin informatiebeveiliging belangrijk is op meerdere niveaus en op meerdere plaatsen, moeten aanpassingen niet alleen op operationeel niveau worden gedragen, maar ook op organisatieniveau. Maar ook kleine organisaties met een relatief eenvoudige ICT doen er goed aan het veranderproces niet te onderschatten.

Volwassen omgaan met informatiebeveiliging begint met de BIO niet als louter afvinklijst te hanteren. Zonder internalisering in alle geledingen van de organisatie zal het voldoen aan de vereisten voortdurend een moeizaam en weinig efficiënt proces zijn. Bovendien een gemiste kans: een organisatie die trots kan melden dat zij voortdurend aandacht heeft voor informatiebeveiliging en resultaten boekt, zal dat in de kwaliteit van dienstverlening en haar marketingstrategie tot voordeel kunnen maken.

De BIO-SA (BIO Self-Assessment) kwantificeert de mate van samenwerking binnen de eigen organisatie en die met andere organisaties. De mate van samenwerking wordt uitgedrukt in het volwassenheidsniveau.

Het CIP biedt de BIO-SA aan als een hulpmiddel om de organisatie te laten groeien in het samenwerken.

BIO-SA is een krachtig doe-het-zelf instrument om te meten hoe volwassen de organisatie omgaat met informatiebeveiliging. Het is ook een stuurinstrument voor stapsgewijze planmatige verbetering en – in combinatie met de workshop – bovenal een krachtig middel voor het vergroten van bewustwording bij management en medewerkers.

De BIO-SA maakt gebruik van 16 criteria. Deze 16 criteria zijn een aggregatie van de BIO en dekken samen met de uitleg in dit document de volledige BIO af. Dit document bevat een beschrijving van de volwassenheidsniveaus, zoals die in de BIO-SA zijn gehanteerd.

Inhoud

Managementsamenvatting		3
1	Inleiding	5
1.1	Het meten van de volwassenheid van een organisatie	5
1.2	Het na te streven volwassenheidsniveau	6
1.3	Voor kleine, middelgrote en grote organisaties	6
1.4	Aggregatie van de BIO controls	6
1.5	Weging van de criteria op basis van het aantal BIO controls	8
1.6	Referenties	10
2	Het BIO-SA volwassenheidsmodel	11
2.1	Niveau 1 – Informeel	11
2.2	Niveau 2 – Beheerst proces	12
2.3	Niveau 3 – Vastgesteld proces	13
2.4	Niveau 4 – Voorspelbaar proces	14
2.5	Niveau 5 – Geoptimaliseerd	15
3	Beleid criteria	16
3.1	B.01 Informatiebeveiligingsbeleid	16
3.2	B.02 Informatiebeveiligingsorganisatie	17
3.3	B.03 Veilig personeel bij aangaan, tijdens en einde dienstverband	18
4	Uitvoering criteria	20
4.1	U.01 Veilige omgevingen, telewerken en (mobiele) apparatuur	20
4.2	U.02 Toegangsbeveiliging	23
4.3	U.03 Beheer van de operationele systemen	26
4.4	U.04 Beheer van informatiebeveiligingsincidenten en - verbeteringen	27
4.5	U.05 Technische kwetsbaarheden, inclusief malware	29
4.6	U.06 Netwerk en informatietransport	32
4.7	U.07 Ontwikkelprocessen, testgegevens en te ontwikkelen informatiesystemen	34
4.8	U.08 Naleving van wettelijke en contractuele eisen	36
4.9	U.09 Cryptografie	37
4.10	U.10 Bedrijfscontinuïteit, inclusief back-ups en redundantie	38
4.11	U.11 Bedrijfsmiddelen, inclusief media	39
4.12	U.12 Leveranciers	41
5	Control criteria	43
5.1	C.01 Beoordelen en auditen van de informatiebeveiliging	43

1 Inleiding

1.1 Het meten van de volwassenheid van een organisatie

De BIO-volwassenheid geeft aan hoe succesvol de organisatie is in het borgen van de BIO controls en overheidsmaatregelen voor informatiebeveiliging. Bij het bepalen van de volwassenheid moeten organisaties nagaan in welke mate zij de BIO hebben geborgd binnen hun organisatie. Hierbij spelen vragen als 'welke eisen stelt de BIO voor mijn organisatie', 'wat moet mijn organisatie regelen', 'waar staat mijn organisatie nu', 'waar moeten wij naar toe' en 'hoe komen wij daar'. De BIO-SA (BIO Self Assessment) is een krachtig doe-het-zelf instrument om te meten hoe volwassen de organisatie omgaat met informatiebeveiliging.

Het meten van de volwassenheid kan door organisaties worden ingezet om te bepalen hoe volwassen de organisatie is in het voldoen aan de BIO. Tevens kunnen de volwassenheidsniveaus gebruikt worden om te groeien in volwassenheid door het feitelijk verbeteren van de informatieveiligheid. De niveaus kunnen dan gebruikt worden om de organisatie stapsgewijs, in de vorm van verbetervoorstellen, mee te nemen naar het gewenste niveau, waarop aan de BIO wordt voldaan en op een volwassen niveau met informatiebeveiliging wordt omgegaan. Het vastgestelde volwassenheidsniveau en de verbetervoorstellen bieden daarbij overzicht en inzicht om het bewustzijn binnen de organisatie te vergroten.

In het onderliggende volwassenheidsmodel van de BIO-SA is per criterium beschreven waaraan voldaan moet zijn om een bepaald volwassenheidsniveau te bereiken. Wij hebben vijf volwassenheidsniveaus onderscheiden, de niveaus 1 t/m 5. Het volwassenheidsniveau 0, waarbij een organisatie niks doet, laten we hier buiten beschouwing. Volwassenheidsniveaus verschillen van elkaar in de mate waarin de BIO controls en overheidsmaatregelen zijn ingeregeld. Op niveau 1 is de aandacht voor informatiebeveiliging nog informeel en komen maatregelen ad hoc tot stand. Vanaf niveau 2 kan gesproken worden van beheerste processen. Op niveau 2 is dit op afdelingsniveau ingeregeld en op niveau 3 breed op organisatieniveau. Op niveau 4 zijn de genomen beveiligingsmaatregelen vergeleken met die van andere organisaties, zodat zichtbaar is dat de genomen maatregelen passend zijn voor de stand der techniek en wat gangbaar is bij andere organisaties. Op niveau 5 wordt performance van de organisatie gemeten door het verzamelen van gedetailleerde gegevens over de processen en hun kwaliteit, waardoor de werking van de organisatie wordt geoptimaliseerd.

In een oogopslag:

5	geoptimaliseerd
4	gelijkwaardig aan gebruik in de branche /voorspelbaar
3	vastgesteld op organisatieniveau
2	beheerst op afdelingsniveau
1	ad hoc / informeel
0	geen aandacht

1.2 Het na te streven volwassenheidsniveau

Elke organisatie is anders. Per organisatie is er ook verschil in de mate waarin volwassenheid wordt nagestreefd. Hoe belangrijker informatiebeveiliging is, hoe hoger het volwassenheidsniveau moet zijn. Het kan ook per organisatieonderdeel verschillen welk volwassenheidsniveau moet worden nagestreefd, omdat in sommige afdelingen met gevoeligere informatie wordt verwerkt dan in andere.

Niveau 3 wordt als minimum gezien om te kunnen stellen dat men zich aan de BIO houdt; op dit niveau is informatiebeveiliging bedrijfsbreed ingeregeld. Op niveau 4 leert men niet alleen van het eigen handelen ten aanzien van informatiebeveiliging (de mate waarin de benodigde maatregelen zijn genomen), maar leert men ook door het handelen actief te vergelijken met andere organisaties uit de branche. Op niveau 4 is daarmee inzicht in de mate waarin de genomen maatregelen passend zijn. Niveau 5 gaat nog een stapje verder: op dit niveau is er een sterk en expliciet (traceerbaar) verband tussen externe eisen, beveiligingsdoelstellingen, algemeen beleid, specifiek beleid en uitvoering en is elke (beleids)keuze gebaseerd op een uitgebreide, nauwkeurige analyse.

Om aan de BIO te voldoen moet minimaal aan volwassenheidsniveau 3 voldaan worden, alsmede een aantal eisen op niveau 4 en één op niveau 5. Om inzichtelijk te maken in welke mate aan het door de BIO vereiste volwassenheidsniveau wordt voldaan, wordt ook dit in de BIO-SA zichtbaar gemaakt en is daarmee als de mate van BIO-volwassenheid als KPI te gebruiken.

1.3 Voor kleine, middelgrote en grote organisaties

Omvang van een organisatie zegt niets over het aantal gegevensverwerkingen die beveiligd zouden moeten zijn. Omvang zegt in principe ook niets over de inspanning die nodig is om een hoger niveau van volwassenheid te bereiken. Maar voor alle organisaties die persoonsgegevens verwerken geldt dat zij informatiebeveiliging op orde moeten hebben. In de volwassenheidsniveaus van BIO-SA is bovendien verwerkt dat het voldoen aan de BIO niet alleen iets technisch is, maar ook gezien kan worden als kans om de samenwerking binnen bedrijfsafdelingen en zelfs tussen organisaties te laten groeien.

1.4 Aggregatie van de BIO controls

De BIO bevat 35 paragrafen (aandachtsgebieden) met totaal 110 controls. Deze controls zijn regelrecht afkomstig uit de ISO 27002.

Het bepalen van de volwassenheid van een organisatie op basis van de 35 paragrafen of van de 110 controls leidt tot een zeer gedetailleerde uitvraag. Door te kiezen voor het aggregeren van de aandachtsgebieden is een minder gedetailleerde uitvraag mogelijk. Door een uitleg te geven bij de criteria, met daarin alle BIO controls en overheidsmaatregelen, zijn de criteria toch een volledige afspiegeling van de BIO.

Het aggregeren van de 35 paragrafen met de 110 controls heeft geleid tot 16 criteria voor de BIO-SA. Hierbij is gekeken naar de logische samenhang tussen de controls, inclusief de overheidsmaatregelen.

De binnen de criteria beschreven controls en overheidsmaatregelen hebben daardoor bij het doen van de volwassenheidsmeting meer structuur en geven een beter overzicht.

Het doel van de aggregatie is enerzijds het hanteerbaar houden van het aantal vragen over volwassenheid in de BIO-SA en anderzijds het aantoonbaar en herleidbaar afdekken van alle BIO controls, inclusief alle overheidsmaatregelen.

Dit heeft geleid tot de volgende 16 criteria:

Criteria BIO-SA		Aandachtsgebieden BIO	
B.01	Informatiebeveiligingsbeleid	5.1	Aansturing door de directie van de informatiebeveiliging
B.02	Informatiebeveiligingsorganisatie	6.1	Interne organisatie
B.03	Veilig personeel bij aangaan, tijdens en einde dienstverband	7.1 7.2 7.3	Voorafgaand aan het dienstverband Tijdens het dienstverband Beëindiging en wijziging van dienstverband
U.01	Veilige omgevingen, telewerken en toegang tot (mobiele) apparatuur	11.1 11.2 6.2	Beveiligde gebieden Apparatuur Mobiele apparatuur en telewerken
U.02	Toegangsbeveiliging	9.1 9.2 9.3 9.4	Bedrijfseisen voor toegangsbeveiliging Beheer van toegangsrechten van gebruikers Verantwoordelijkheden van gebruikers Toegangsbeveiliging van systeem en toepassing
U.03	Beheer van de operationele systemen	12.1 12.5	Bedieningsprocedures en verantwoordelijkheden Beheersing van operationele software
U.04	Beheer van informatiebeveiligingsincidenten en - verbeteringen	16.1	Beheer van informatiebeveiligingsincidenten en - verbeteringen
U.05	Technische kwetsbaarheden, inclusief malware	12.2 12.4 12.6	Bescherming tegen malware Verslaglegging en monitoren Beheer van technische kwetsbaarheden
U.06	Netwerk en het informatietransport	13.1 13.2	Beheer van netwerkbeveiliging Informatietransport
U.07		14.1	Beveiligingseisen voor informatiesystemen

	Ontwikkelprocessen, testgegevens en te ontwikkelen informatiesystemen	14.2 14.3	Beveiliging in ontwikkelings- en ondersteunende processen Testgegevens
U.08	Wettelijke en contractuele eisen	18.1	Naleving van wettelijke en contractuele eisen
U.09	Cryptografie	10.1	Cryptografische beheermaatregelen
U10	Bedrijfscontinuïteit, inclusief back-ups en redundantie	17.1 17.2 12.3	Informatiebeveiligingscontinuïteit Redundante componenten Back-up
U.11	Bedrijfsmiddelen, inclusief media	8.1 8.2 8.3	Verantwoordelijkheid voor bedrijfsmiddelen Informatieclassificatie Behandelen van media
U.12	Leveranciers	15.1 15.2	Informatiebeveiliging in leveranciersrelaties Beheer van dienstverlening van leveranciers
C.01	Beoordelen en auditen van de informatiebeveiliging	12.7 18.2	Overwegingen betreffende audits van informatiesystemen Informatiebeveiligingsbeoordelingen

In de hoofdstuk 3 t/m 5 zijn de 16 criteria met de verklarende teksten beschreven. De criteria met de verklarende teksten zijn een aggregatie van de BIO controls en overheidsmaatregelen. In de tabellen staat in de linker kolom de in de criteria onderstreepte sleutelwoorden. In de rechterkolom staat de uitleg bij deze sleutelwoorden. Dit zijn tegelijkertijd de verklarende teksten van de criteria in de BIO-SA. De voetnoten in de tabellen verwijzen naar de vindplaatsen in de BIO.

In hoofdstuk 2 is als achtergrondinformatie het in de BIO-SA gehanteerde volwassenheidsmodel beschreven.

1.5 Weging van de criteria op basis van het aantal BIO controls

Bij de clustering van de BIO controls en de overheidsmaatregelen zijn, om te komen tot de criteria, bij elkaar horende BIO controls en overheidsmaatregelen geaggregeerd tot de 16 criteria. Daardoor bevat het ene criterium meer BIO controls dan een ander criterium. Een criterium met meer controls weegt daardoor zwaarder mee bij het bepalen van de volwassenheid dan een criterium met minder controls. Door deze combinatie van weging en clustering blijft het aantal vragen beperkt en geeft het resultaat

van de meting een juiste afspiegeling van de BIO volwassenheid van een organisatie. Het totaal aantal controls is 110.

De volgende tabel geeft per criterium het aantal controls dat is meegenomen. Hierdoor wordt duidelijk dat bijvoorbeeld U.02 (Toegangsbeveiliging) met 14 BIO controls 2 keer zo zwaar weegt bij het bepalen van de volwassenheid, als U.05 (Beschermen tegen en monitoren en vastleggen van technische kwetsbaarheden, inclusief malware) met 7 BIO controls.

Bij het bepalen van de volwassenheid van een organisatie wordt dus gekeken naar het aantal BIO controls per criterium. Door deze aanpak weegt iedere BIO control even zwaar mee in het bepalen van de volwassenheid. Er wordt dus niet gekeken naar het zwaarte van een control. Voor de ene organisatie kan het ene control belangrijker zijn dan een ander control. Het toekennen van organisatieafhankelijke gewichten aan controls heeft echter tot gevolg dat de uitslag van de assessment een onderlinge vergelijking tussen organisaties bemoeilijkt. Daarom is hiervoor niet gekozen en weegt iedere BIO control in de BIO-SA even zwaar mee bij het bepalen van de volwassenheid van de organisatie.

Criteria	aantal BIO controls
B.01 Informatiebeveiligingsbeleid	2
B.02 Informatiebeveiligingsorganisatie	4
B.03 Veilig personeel bij aangaan, tijdens en einde dienstverband	6
U.01 Veilige omgevingen, telewerken en toegang tot (mobiele) apparatuur	17
U.02 Toegangsbeveiliging	14
U.03 Beheer van de operationele systemen	5
U.04 Beheer van informatiebeveiligingsincidenten en - verbeteringen	6
U.05 Beschermen tegen en monitoren en vastleggen van technische kwetsbaarheden, inclusief malware	7
U.06 Beveiliging van het netwerk en het informatietransport	6
U.07 Beveiliging van ontwikkelprocessen, testgegevens en te ontwikkelen informatiesystemen	12
U.08 Naleving van wettelijke en contractuele eisen	5
U.09 Cryptografie	2
U10 Bedrijfscontinuïteit, inclusief back-ups en redundantie	5
U.11 Inventarisatie, gebruik en vernietiging van bedrijfsmiddelen, inclusief media	10
U.12 De inzet en het monitoren, beoordelen en auditen van leveranciers	5
C.01 Beoordelen en auditen van de informatiebeveiliging	4

1.6 Referenties

[1] https://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration#cite_note-Go08-1
[2] https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2020/04/BIO-versie-1.04-huisstijl-BIO-definitief.docx
[3] https://www.noraonline.nl/wiki/SIVA-methodiek

2 Het BIO-SA volwassenheidsmodel

Volwassenheidsmodellen vinden hun oorsprong in het 'Capability Maturity Model' (kort aangeduid als CMM). CMM is van oorsprong een model voor het bepalen van de volwassenheid bij het ontwikkelen van software. Inmiddels zijn er meerdere modellen ontwikkeld. BIO-SA is gebaseerd op CMMI (Capacility Maturity Model Integration), waarin meerdere modellen zijn geïntegreerd tot één model.

Voor het beschrijven van de volwassenheidsniveaus is naast CMMI ook gekeken naar 'Information Security Object Maturity Model' (ISOMM). ISOMM is een volwassenheidsmodel dat is opgesteld om te dienen als volwassenheidsmodel voor de invulling van de Nationaal Cyber Security Centrum (NCSC) richtlijnen en is gebaseerd op CobiT5, ISO/IEC-15504, CMMI for Services en SSE-CMM.

BIO-SA onderscheidt vijf niveaus (levels) van volwassenheid:



2.1 Niveau 1 – Informeel

Op niveau 1 worden de werkzaamheden informeel uitgevoerd. Analyse van CMMI en ISOMM wijst uit dat op niveau 1:

- □ Sprake is van een omgeving met stabiele uitgangspunten op individueel niveau:
  - Zaken worden benaderd vanuit een persoonlijke perspectief en daardoor afhankelijk van de kennis en kunde van individuele medewerkers;
  - Er is onvoldoende managementcommitment om te sturen met beleid, processen en procedures, waardoor:
    - Er geen formele richtlijnen zijn voor het uitvoeren van werkzaamheden;
    - Er een beperkte beschrijving van de taken, bevoegden en verantwoordelijkheden (TBV) aanwezig is;

- ♦ Beheerders naar eigen inzichten kunnen handelen. Dat kan een goede zaak zijn maar kent ook risico's voor de organisatie.
- Het inzicht in hoe de verwerking is samengesteld, is beperkt tot de individuele medewerkers. Dit inzicht heeft geen formele status vanuit de afdeling;
- Slechtst de deskundigen zijn op de hoogte van de samenhang tussen de aspecten die een rol spelen (heroïsche acties).

□ Sprake is van het hanteren van de uitgangspunten tot op individueel niveau:
- Er is onvoldoende managementcommitment om controle uit te voeren op het hanteren van beleid, processen en procedures, waardoor:
  - Er geen controle plaatsvindt op de werkzaamheden;
  - Er geen beheersing/evaluatie is van de uitgevoerde taken;
  - Er geen managementcyclus is voor de dimensies: beleid, uitvoering en controle.
- Verbeteringen kunnen verloren gaan door gebrek aan standaardisatie.

Dit betekent dat op niveau 1 de keuzes over hoe en welke beveiligingsmaatregelen worden genomen per systeemeigenaar op uitvoeringsniveau worden gemaakt vanuit persoonlijk perspectief en afhankelijk van de kennis en kunde van individuele medewerkers. Hierbij ontbreekt het aan formele processen om eisen te stellen aan hoe aan de BIO te voldoen en worden informeel keuzes gemaakt over hoe in een concreet geval wordt omgegaan met de informatieveiligheid. Op dit niveau kan wel vastlegging plaatvinden, maar er is geen sprake van vaststelling.

Er is geen managementcyclus, waardoor reactief wordt gereageerd op keuzes en incidenten die zich voordoen.

2.2 Niveau 2 – Beheerst proces

Op niveau 2 vinden de werkzaamheden in herhaalbare en binnen een afdeling beheerste processen plaats. Er wordt daardoor bewaakt dat men zich aan de discipline van de voorgeschreven processen houdt. Analyse van CMMI en ISOMM wijst uit dat op niveau 2:

□ Sprake is van een omgeving met stabiele uitgangspunten op afdelingsniveau:
- Zaken worden benaderd in overeenstemming met op afdelingsniveau uitgevaardigd beleid;
- Bij de formulering en toepassing van het beleid worden belanghebbenden betrokken;
- Er is op afdelingsniveau managementcommitment om te sturen met beleid, processen en procedures, waardoor op dit niveau:
  - Er formele richtlijnen zijn voor het uitvoeren van werkzaamheden;
  - Er voor het afdelingsniveau TVB beschrijvingen aanwezig zijn;
  - Beheerders in staat zijn de juiste "dingen" te doen voor het bereiken van de door henzelf geformuleerde doelen;
  - Informatie over hoe een verwerking is samengesteld, is beperkt tot afdelingsniveau. Deze informatie heeft binnen de afdeling een formele status.
- De afdeling is op de hoogte van de samenhang tussen de aspecten die een rol spelen.

□ Sprake is van beheersing van het hanteren van de uitgangspunten tot op afdelingsniveau:
- Er is op afdelingsniveau managementcommitment om controle uit te voeren op het hanteren van beleid, processen en procedures van de afdeling, waardoor op afdelingsniveau:
  - Controle plaatsvindt op de werkzaamheden;
  - Beheersing/evaluatie plaatsvindt van de van de uitgevoerde taken;

- Een managementcyclus wordt aangehouden voor de dimensies: beleid, uitvoering en controle.

▪ Bedrijfsbrede verbeteringen kunnen verloren gaan door gebrek aan standaardisatie.

Dit betekent dat op niveau 2 de keuzes over hoe en welke beveiligingsmaatregelen worden genomen op uitvoeringsniveau worden gemaakt op basis van operationeel beleid, richtlijnen en werkinstructies op afdelingsniveau en niet per systeemeigenaar.

Op dit niveau zijn het beleid, de richtlijnen en werkinstructies per afdeling vastgelegd en bekrachtigd, maar sluiten niet noodzakelijkerwijs aan bij de bedrijfsbrede wijze waarop beveiligingsmaatregelen moeten worden genomen. Daardoor is de werkwijze op lokaal afdelingsniveau wel traceerbaar, herhaalbaar en gestandaardiseerd, maar niet bedrijfsbreed. De organisatie leert slechts op lokaal afdelingsniveau. De verschillende afdelingen kunnen wel van elkaar leren.

Het voldoen aan de BIO controls en overheidsmaatregelen wordt wel steeds per systeemeigenaar op afdelingsniveau vastgesteld en bekrachtigd.

Er is wel structurele rapportage over informatiebeveiliging op projectniveau en afdelingsniveau, maar nog geen structurele rapportage van afdelingsniveau naar het hogere management.

Omdat de vastlegging van het beleid, richtlijnen en werkinstructies op afdelingsniveau geschiedt, wordt geen formele bekrachtiging vereist (er is dus alleen bekrachtiging op afdelingsniveau). Het kan zijn dat op organisatieniveau wel informatiebeveiligingsbeleid is, maar dat dit door de afdelingen niet altijd wordt gehanteerd. Op organisatieniveau is wel het voldoen aan de BIO vastgelegd, maar zijn de te nemen maatregelen niet officieel bekrachtigd en zijn controleprocessen om aan de BIO te voldoen niet bedrijfsbreed ingericht.

2.3 Niveau 3 – Vastgesteld proces

Op niveau 3 vinden de werkzaamheden plaats in herhaalbare en beheerste processen, die zijn gebaseerd op een bedrijfsbreed vastgestelde werkwijze. Er wordt daardoor op afdelings- en organisatieniveau bewaakt dat men zich aan de discipline van de voorgeschreven processen houdt. Analyse van CMMI en ISOMM levert op dat op niveau 3:

□ Sprake is van een omgeving met stabiele uitgangspunten op afdelings- en organisatieniveau:

- Bij de formulering en toepassing van het beleid worden belanghebbenden betrokken. Hierbij wordt rekening gehouden met externe ontwikkelingen;
- Zaken worden benaderd in overeenstemming met op organisatieniveau uitgevaardigd beleid;
- Specifieke standaarden, procesbeschrijvingen en procedures worden afgeleid vanuit de verzameling standaardprocessen van de organisatie en geschikt gemaakt voor (toegesneden op) specifieke situaties (project of organisatorische eenheid). Sub-processen zijn gerelateerd aan hoofdprocessen. Hierdoor worden zaken op een consistente wijze uitgevoerd;
- Op organisatieniveau is managementcommitment om te sturen met beleid, processen en procedures, waardoor op dit niveau:
  - Formele richtlijnen zijn voor het uitvoeren van werkzaamheden;
  - Bedrijfsbrede beschrijvingen zijn van taken, bevoegdheden en verantwoordelijkheden (TBV);
  - Beheerders in staat zijn de juiste "dingen" te doen voor het bereiken van de door henzelf geformuleerde doelen;

- Informatie over hoe verwerkingen zijn samengesteld is tot organisatieniveau beschikbaar. Deze informatie heeft binnen de afdeling en op organisatieniveau een formele status.

□ Sprake is van beheersing van het hanteren van de uitgangspunten voor het afdelings- en organisatieniveau:
  - Op organisatieniveau is managementcommitment om controle uit te voeren op het hanteren van beleid, processen en procedures van de afdeling, waardoor op organisatieniveau:
    - Controle plaatsvindt op de werkzaamheden;
    - Beheersing/evaluatie is van de uitvoering van de taken;
    - Een managementcyclus wordt aangehouden voor de dimensies: beleid, uitvoering en controle.
  - Standaardprocessen worden toegepast om consistentie in de organisatie tot stand te brengen. Hierdoor gaan bedrijfsbrede verbeteringen niet verloren en vindt het managen van processen proactief plaats.

Dit betekent dat op niveau 3 de keuzes over hoe en welke beveiligingsmaatregelen worden genomen op basis van operationeel beleid, richtlijnen en werkinstructies op organisatieniveau worden hergebruikt op afdelingsniveau. Het informatiebeveiligingsbeleid is op organisatieniveau vastgesteld en bekrachtigd. Er ligt een duidelijke relatie tussen het beleid, richtlijnen en/of werkinstructies op organisatieniveau en die binnen de afdelingen, doordat er periodiek evaluatie plaatsvindt van het beleid. De BIO vereisten voor de organisatie zijn ook vertaald naar de inrichting van de context, de systemen en de beheerprocessen. De organisatie leert bedrijfsbreed, omdat er een systematische samenhang bestaat tussen de uitvoerende onderdelen, beleidsonderdelen en controleonderdelen op zowel afdelingsniveau als bedrijfsniveau. Er is structurele rapportage over informatiebeveiliging naar het hogere management.

Er bestaat sturing op de naleving van het beleid, richtlijnen en (werk)instructies. In tegenstelling tot niveau 2 wordt de sturing afgestemd met het hogere management. Het hogere management is betrokken bij de handhaving van het beleid en de uitvoering. Hierbij wordt de rapportage aan het hogere management onderbouwd door informatie uit controlemiddelen. Dit leidt tot een lerend proces op zowel afdelings- als organisatieniveau.

2.4 Niveau 4 – Voorspelbaar proces

Op niveau 4 vinden de werkzaamheden plaats terwijl de performance van de processen wordt gemeten door het verzamelen van gedetailleerde gegevens over de processen en hun kwaliteit. Analyse van CMMI en ISOMM levert op dat op niveau 4, in aanvulling op niveau 3:

□ Een traceerbaar verband is tussen externe eisen, beveiligingsdoelstellingen, algemeen beleid, specifiek beleid en uitvoering;

□ Er beheersing is op zowel organisatie- als afdelingsniveau. De beheersing is op dit niveau ook gebaseerd op voorspellingen op basis van statistische en kwantitatieve technieken.
Daartoe:
  - Zijn kwantitatieve doelstellingen vastgesteld voor kwaliteit, procesprestaties en projecten;
  - Zijn de kwantitatieve doelstellingen gebaseerd op de behoeften van de klant, eindgebruikers, organisatie en procesuitvoerders;
  - Worden meetresultaten van procesprestaties verzameld en statistisch geanalyseerd;
  - Worden de kwalitatieve en kwantitatieve procesprestaties gebruikt als criteria bij het managen van processen en projecten.

Dit betekent dat op niveau 4 meetbaar wordt gestuurd op feitelijke informatieveiligheid, door te sturen op de kwaliteit van de beveiligingsmaatregelen en de snelheid waarmee deze worden gerealiseerd. De operationele werkelijkheid wordt voortdurend bewaakt en aangepast om de bedrijfsbrede beleidsdoelen te behalen. Het lerend vermogen in de uitvoerende en specifiek beleidsmatige laag is op niveau 4 geoptimaliseerd.

Het management van de organisatie heeft op ieder gewenst moment inzicht in de stand van zaken omtrent de informatiebeveiliging van de gehele informatievoorziening en kan die vergelijken met die van de branche. De organisatie communiceert naar buiten toe over haar informatieveiligheid.

2.5 Niveau 5 – Geoptimaliseerd

Op niveau 5 vinden de werkzaamheden plaats terwijl de performance van de organisatie wordt gemeten door het verzamelen van gedetailleerde gegevens over de processen en hun kwaliteit. De werking van de organisatie wordt geoptimaliseerd op basis van analyse van de metingen.

Analyse van CMMI en ISOMM levert op dat op niveau 5, in aanvulling op niveau 4:

- Sprake is van excellence beheersing, benchmarking, innovatie en procesoptimalisatie;
- De procesprestaties in een (geautomatiseerd) dashboard worden gepresenteerd via continue metingen.
- Het management zich bezig houdt met de totale prestaties van de organisatie, door gebruik te maken van verzamelde gegevens van meerdere projecten/processen:
  - Analyse van meetgegevens brengt tekortkomingen of gaten in de prestaties aan het licht;
  - Bevindingen zijn consequent aanleiding om procesverbeteringen in de organisatie in gang te zetten die meetbare verbetering van de prestaties opleveren.
- De organisatie kan dynamisch worden aangepast op basis van praktische ervaringen en prognoses en inzicht in de gerealiseerde bedrijfsdoelstellingen en procesprestaties.

Dit betekent dat op niveau 5 een sterk en expliciet (traceerbaar) verband is tussen externe eisen, beveiligingsdoelstellingen, algemeen beleid, specifiek beleid en uitvoering. Aan alle keuzes liggen uitgebreide, nauwkeurige analyses ten grondslag. Dit resulteert in de mogelijkheid om de genomen beveiligingsmaatregelen aan te passen op basis van eigen praktische ervaringen en prognoses van buiten de eigen organisatie. De operationele werkelijkheid en effectiviteit van beleid worden voortdurend bewaakt en kunnen snel worden aangepast bij plotselinge wijzigingen in de omgeving, zoals veranderende dreigingen, nieuwe overheidsmaatregelen en (best) practices. Bovendien is de organisatie in staat om daarbij prognoses af te geven over kosten en reactiesnelheid. Bij de bewaking en rapportages naar het hogere management worden externe factoren meegenomen in relatie tot het interne beleid en de uitvoering. De prestatie-indicatoren zijn eenvoudig vergelijkbaar met andere organisaties. Het lerend vermogen is, over alle lagen heen, geoptimaliseerd door verregaande geautomatiseerde terugkoppeling tussen alle lagen.

3 Beleid criteria

3.1 B.01 Informatiebeveiligingsbeleid

B.01	Informatiebeveiligingsbeleid
(BIO 5.1) BIO – Weging: 1	Het informatiebeveiligingsbeleid is opgesteld en vastgesteld, waarbij is aangetoond dat het passend, adequaat en doeltreffend is.
Uitleg	
Opgesteld en vastgesteld	De organisatie heeft informatiebeveiligingsbeleid opgesteld en vastgesteld, met daarin[1]: 1. De daarvoor geldende strategische uitgangspunten en randvoorwaarden, in lijn met het algemene beveiligingsbeleid en het informatievoorzieningsbeleid; 2. De organisatie van de informatiebeveiligingsfunctie, waaronder: a. Verantwoordelijkheden, taken en bevoegdheden; b. De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers. 3. De gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn; 4. De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd; 5. De bevordering van het beveiligingsbewustzijn.
Passend, adequaat en doeltreffend	Het beleid is passend, adequaat en doeltreffend[2]: De beoordeling en zo nodig de bijstelling hiervan gebeurt periodiek en in aansluiting op de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen[3].

[1] BIO 5.1.1.1

[2] BIO 5.1.2

[3] BIO 5.1.2.1

3.2 B.02 Informatiebeveiligingsorganisatie

B.02	Informatiebeveiligingsorganisatie
(BIO 6.1) BIO – Weging: 1	De informatiebeveiligingsverantwoordelijkheden (inclusief de contacten met (overheids)instanties en toezichthouders) en de functie van CISO, zijn gedefinieerd en toegewezen (ook binnen projecten). Er zijn passende contacten met (overheids)instanties en toezichthouders.
Uitleg	
Informatie-beveiligings-verantwoor-delijkheden:	De organisatie heeft de verantwoordelijkheden die bij informatiebeveiliging behoren gedefinieerd en toegewezen[4]. Hierbij: 1. Wordt voldaan aan de relevante voorschriften en wetten[5]; 2. Is minimaal een Chief Information Security Officer (CISO) aangesteld conform een vastgesteld CISO-functieprofiel[6], waarbij in het profiel de rol en verantwoordelijkheden van de CISO zijn vastgelegd; 3. Komt informatiebeveiliging in alle projecten aan de orde[7].
Passende contacten:	Er zijn passende contacten met (overheids)instanties en toezichthouders over informatiebeveiligingsaangelegenheden (vergunningen/incidenten/calamiteiten)[8]. Hierbij is bekend[9]: 1. Wie welke contacten heeft; 2. Welke eisen gesteld worden ten aanzien van de informatiebeveiligingsaangelegenheden.

[4] BIO 6.1.1

[5] BIO 6.1.1.2

[6] BIO 6.1.1.4

[7] BIO 6.1.5

[8] BIO 6.1.3

[9] De norm is dat er een jaarlijks geactualiseerd contactoverzicht is (BIR 6.1.3.2).

3.3 B.03 Veilig personeel bij aangaan, tijdens en einde dienstverband

B.03	Veilig personeel bij aangaan, tijdens en einde dienstverband
(BIO 7.1, 7.2 en 7.3) BIO – Weging: 1	Voorafgaand aan en tijdens een dienstverband is het medewerkers en contractanten duidelijk dat zij gehouden zijn bedrijfsinformatie te beschermen en te beveiligen. Hiertoe zijn hun verantwoordelijkheden vastgelegd en up-to-date en is een specifiek voor de functie verstrekte VOG overlegd. Bij beëindiging of wijziging van het dienstverband is duidelijk welke afspraken van kracht blijven.
Uitleg	
Voorafgaand	Voorafgaand aan een dienstverband zijn de verantwoordelijkheden voor informatiebeveiliging van (interne en externe) medewerkers (inclusief contractanten) en de organisatie contractueel vastgelegd[10]. Hiervoor[11]: 1. Zijn alle medewerkers bij hun aanstelling of functiewisseling hierop gewezen; 2. Zijn de voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging eenvoudig toegankelijk; 3. Is bij indiensttreding geverifieerd of de achtergrond van een (interne en externe) medewerker in overeenstemming is met relevante wet- en regelgeving en ethische overwegingen en of deze in verhouding staat tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's[12]; 4. Heeft de organisatie een vastgesteld screeningsbeleid[13]; 5. Is een specifiek voor de functie verstrekte Verklaring Omtrent het Gedrag (VOG) gevraagd[14].
Tijdens	Alle medewerkers (inclusief contractanten) hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Daartoe geldt (voor zover relevant) dat ze: 1. Door de directie erop zijn gewezen informatiebeveiliging toe te passen in overeenstemming met vastgestelde beleidsregels en procedures[15]; 2. De regels en verplichtingen met betrekking tot informatiebeveiliging en, daar waar relevant, de speciale eisen voor gerubriceerde omgevingen kennen[16]; 3. Een passende bewustzijnsopleiding en -training krijgen, inclusief een regelmatige bijscholing over beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie[17]; 4. Binnen drie maanden na indiensttreding een training I-bewustzijn succesvol volgen, als ze gebruikmaken van de informatiesystemen en -diensten[18]; 5. Door het management (bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken) worden gewezen op het belang en periodiek volgen van opleiding en training op het gebied van informatiebeveiliging[19];

[10] BIO 7.2.1
[11] BIO 7.2.1.1
[12] BIO 7.1.1
[13] BIO 7.1.1.1
[14] BIO 7.1.1.1
[15] BIO 7.2.1
[16] BIO 7.2.2.1
[17] BIO 7.2.2
[18] BIO 7.2.2.2
[19] BIO 7.2.2.3

	6. Formeel bekend zijn met disciplinaire maatregelen, waarmee actie wordt ondernomen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging[20]; 7. Via een klokkenluidersregeling anoniem en veilig beveiligingsissues kunnen melden[21].
Beëindiging of wijziging	Bij beëindiging of wijziging van verantwoordelijkheden van het dienstverband zijn de verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven[22]: 1. Gedefinieerd; 2. Gecommuniceerd aan de medewerker of contractant; 3. Van toepassing.

[20] BIO 7.2.3 [21] BIO 7.2.1.1 [22] BIO 7.3.1

4 Uitvoering criteria

4.1 U.01 Veilige omgevingen, telewerken en (mobiele) apparatuur

U.01	Veilige omgevingen, telewerken en (mobiele) apparatuur
(BIO 11.1, 11.2 en 6.2) BIO – Weging: 2	Fysieke beveiligingszones beschermen gevoelige en essentiële informatie passend op basis van een expliciete risicoafweging. Apparatuur, verbindingen en informatie worden beschermd tegen verlies, schade, diefstal, compromittering en onderbreking van de bedrijfsvoering, door: Bij telewerken is de informatie beveiligd. Bij de inzet van mobiele apparatuur zijn de gebruikers zich bewust van de gevaren, geldt voor vertrouwelijke (bedrijfs-) informatie een 'zero footprint' en wordt mobiele apparatuur middels MDM beheerd.
Uitleg	
Fysieke beveiligingszones	Fysieke beveiligingszones beschermen gebieden met gevoelige of essentiële informatie[23], waarbij: 1. De bescherming in het ontwerp en inrichting van kantoren, ruimten en faciliteiten is meegenomen en toegepast[24], inclusief de bescherming tegen natuurrampen, kwaadwillige aanvallen of ongelukken[25]; 2. In het ontwerp en bij de inrichting: a. Vormt een expliciete risicoafweging de basis [26]; b. Voldoet de inrichting aan standaarden[27]; c. Is de toegangsbeveiliging passend, zodat alleen bevoegd personeel toegang krijgt[28]; d. Is sleutelbeheer ingericht op basis van een sleutelplan[29]; e. Zijn voor het werken in beveiligde gebieden procedures ontwikkeld en toegepast[30]; f. Is iedere mogelijk toegang[31] beheerst en zo mogelijk afgeschermd van informatieverwerkende faciliteiten[32]; g. Heeft de organisatie geïnventariseerd welke papieren archieven en apparatuur bedrijfskritisch zijn[33]. 3. Bij concrete beveiligingsrisico's waarschuwingen worden verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid, conform onderlinge afspraken[34]; 4. Bij huisvesting van IT-apparatuur rekening wordt gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen[35].
Apparatuur, verbindingen en informatie	Apparatuur, verbindingen en informatie worden beschermd tegen verlies, schade, diefstal, compromittering en onderbreking van de bedrijfsvoering. Hiertoe:

[23] BIO 11.1.1

[24] BIO 11.1.3

[25] BIO 11.1.4

[26] BIO 11.1.4.1

[27] BIO 11.1.1.1

[28] BIO 11.1.2

[29] BIO 11.1.3.1

[30] BIO 11.1.5

[31] Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden.

[32] BIO 11.1.6

[33] BIO 11.1.4.1

[34] BIO 11.1.2.1

[35] BIO 11.1.4.2

	1. Wordt apparatuur geplaatst en beschermd tegen bedreigingen en gevaren van buitenaf, inclusief onbevoegde toegang[36]; 2. Worden voedings- en telecommunicatiekabels beschermd tegen interceptie, verstoring of schade[37]; 3. Wordt de apparatuur correct onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen[38]; 4. Wordt apparatuur, informatie en software niet van de locatie meegenomen zonder voorafgaande goedkeuring[39]; 5. Worden bedrijfsmiddelen die zich buiten het terrein bevinden passend beveiligd[40]; 6. Worden gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig overschreven[41]; 7. Beschermen gebruikers onbeheerde apparatuur; 8. Wordt 'clear desk'-beleid toegepast voor papieren documenten en verwijderbare opslagmedia[42]; 9. Wordt 'clear screen'-beleid[43] toegepast voor informatieverwerkende faciliteiten. Hiertoe: a. Is een onbeheerde werkplek in een ongecontroleerde omgeving altijd vergrendeld[44]; b. Wordt informatie automatisch ontoegankelijk gemaakt met bijvoorbeeld een screensaver na een inactiviteit van maximaal 15 minuten[45]; c. Worden sessies op remote werkplekken op het remote platform vergrendeld na 15 minuten[46]; d. Is het overnemen van sessies op remote werkplekken op een andere werkplek alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd. Na een expliciete risicoafweging mag hiervan worden afgeweken[47]; e. Wordt bij het verwijderen van een chipcardtoken[48] de toegangsbeveiligingslock automatisch geactiveerd[49].
Telewerken	Ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen zijn beleid en ondersteunende beveiligingsmaatregelen geïmplementeerd.[50].
Inzet van mobiele apparatuur	Bij de inzet van mobiele apparatuur (zoals een laptop, tablet en smartphone) is er[51]: 1. Geen bedrijfsinformatie onbewust opgeslagen ('zero footprint'). Als dat (nog) niet realiseerbaar is, is de toegang ertoe afgeschermd, zijn vertrouwelijke gegevens versleuteld opgeslagen en is 'wissen op afstand' mogelijk; 2. In bewustwordingsprogramma's aandacht besteed aan gedragsaspecten van veilig mobiel werken; 3. Een periodiek getoetste Mobile Device Management (MDM)-oplossing, inclusief patchmanagement en hardening;

[36] BIO 11.2.1
[37] BIO 11.2.3
[38] BIO 11.2.4
[39] BIO 11.2.5
[40] BIO 11.2.6
[41] BIO 11.2.7
[42] BIO 11.2.9
[43] BIO 11.2.9
[44] BIO 11.2.9.1
[45] BIO 11.2.9.2
[46] BIO 11.2.9.3
[47] BIO 11.2.9.4
[48] Een chipcardtoken kan worden gebruikt als extra authenticatiefactor voor de toegang tot systemen
[49] BIO 11.2.9.5
[50] BOI 6.2.2
[51] BIO 6.2.1.1 en 6.2.1.2

	4. Een door gebruikers getekende gebruikersovereenkomst, inclusief een verklaring dat zij zich bewust zijn van de gevaren van mobiel werken en dit veilig te zullen doen.

4.2 U.02 Toegangsbeveiliging

U.02	Toegangsbeveiliging
(BIO 9.1, 9.2, 9.3 en 9.4) BIO – Weging: 4	Toegang tot het netwerk en de netwerkdiensten is beperkt tot bevoegde gebruikers en afhankelijk van de authenticatie van de apparatuur. Hierbij: 1. Is de toegang vanuit een onvertrouwde zone alleen mogelijk met (ten minste) two-factor authenticatie; 2. Wordt van gebruikers verlangd dat zij passend omgaan met geheime authenticatie-informatie en worden zij daarin ondersteund; 3. Is de toegang tot informatie en systeemfuncties en specifiek broncode beperkt en verloopt via een inlogprocedure, waarbij het gebruik van sterke wachtwoorden geautomatiseerd wordt afgedwongen; 4. Wordt de toegang gelogd en nauwkeurig gecontroleerd als met de toegang beheermaatregelen kunnen worden omzeild. Het toekennen, intrekken en beoordelen van toegangsrechten is geformaliseerd, waarbij het toekennen van rechten gebaseerd is op een risicoafweging en functiescheiding. Groepsaccounts en speciale rechten worden, waar niet noodzakelijk, voorkomen.
Uitleg	
Toegang tot het netwerk	Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. Hiertoe: 1. Is toegangsbeveiligingsbeleid vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen[52]; 2. Kan alleen geauthentiseerde apparatuur toegang krijgen tot een vertrouwde zone[53]; 3. Krijgen gebruikers met eigen of ongeauthentiseerde apparatuur (Bring Your Own Device) alleen toegang tot een onvertrouwde zone[54]; 4. Vindt toegang vanuit een onvertrouwde zone naar een vertrouwde zone plaats met minimaal two-factor authenticatie[55].
Geheime authenticatie-informatie	Van gebruikers wordt verlangd dat zij passend omgaan met geheime authenticatie-informatie[56]. Medewerkers worden hierin geholpen door het beschikbaar stellen van een wachtwoordenkluis[57].
Inlogprocedure	Toegang tot systemen en toepassingen verloopt via een beveiligde inlogprocedure, indien het beleid voor toegangsbeveiliging dit vereist[58]. Hierbij geldt dat aan externe leveranciers toegang tot het netwerk wordt verleend na een risicoafweging. De risicoafweging bepaald de voorwaarden van de toegang. Uit een registratie blijkt hoe de rechten zijn toegekend[59]. Wachtwoordbeheer wordt geautomatiseerd afgedwongen[60] en is interactief en waarborgt sterke wachtwoorden[61]. Hierbij: 1. Is bij gebruik van alleen wachtwoorden als authenticatie-factor[62]:

[52] BIO 9.1.1
[53] BIO 9.1.2.1
[54] BIO 9.1.2.2
[55] BIO 9.4.2.1
[56] BIO 9.3.1
[57] BIO 9.3.1.1
[58] BIO 9.4.2
[59] BIO 9.4.2.2
[60] BIO 9.4.3.3
[61] BIO 9.4.3
[62] BIO 9.4.3.1, BIO 9.4.3.2 en BIO 9.4.3.5

	a. De wachtwoordlengte minimaal 8 posities; b. De samenstelling complex, tenzij de wachtwoordlengte 20 posities of meer is; c. Is het aantal inlogpogingen maximaal 10; d. Is de tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen vastgelegd; e. Wordt minimaal halfjaarlijks het wachtwoord vernieuwd; f. Hebben wachtwoorden een levensduur van een jaar. Als niet voldaan is aan voorgaande 5 eisen, dan geldt een maximale geldigheidsduur van 6 maanden. 2. Hebben initiële wachtwoorden en wachtwoorden die gereset zijn een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd[63].
Omzeild	Toegang tot systeemhulpmiddelen die in staat zijn om beheermaatregelen voor systemen en toepassingen te omzeilen worden[64]: 1. Beperkt: a. Alleen bevoegd personeel heeft toegang[65]; b. Toegang tot de programmabroncode wordt beperkt[66]. 2. Nauwkeurig gecontroleerd: Het gebruik wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek[67].
Toekennen, intrekken en beoordelen	Het toekennen en intrekken van toegangsrechten is geformaliseerd, waarbij geldt dat: 1. Voor alle typen gebruikers en voor alle systemen[68] het toewijzen gebeurt volgens een formele registratie- en afmeldingsprocedure[69]. Hierbij: a. Is de registratie sluitend[70]; b. Zijn er geen groepsaccounts, tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar[71]; c. Wordt de toegang uitsluitend verleend na autorisatie door een bevoegde functionaris[72]; d. Is de toegang gebaseerd op een risicoafweging[73] en functiescheiding[74], zodat conflicterende taken en verantwoordelijkheden zijn gescheiden om onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen te voorkomen[75]; e. Is er een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten[76]; f. Is het toewijzen en gebruik van speciale toegangsrechten beperkt[77], dit wordt minimaal ieder kwartaal beoordeeld[78]; g. Vindt het toewijzen van authenticatie-informatie plaats via een formeel beheersproces[79];

[63] BIO 9.4.3.4
[64] BIO 9.4.4
[65] BIO 9.4.4.1
[66] BIO 9.4.5
[67] BIO 9.4.4.2
[68] BIO 9.2.2
[69] BIO 9.2.1
[70] BIO 9.2.1.1
[71] BIO 9.2.1.2
[72] BIO 9.2.2.1
[73] BIO 9.2.2.2
[74] BIO 9.2.2.3
[75] BIO 6.1.2
[76] BIO 9.2.2.4
[77] BIO 9.2.3
[78] BIO 9.2.3.1
[79] BIO 9.2.4

	h. Worden de toegangsrechten bij beëindiging van een dienstverband, contract of overeenkomst de toegangsrechten van een medewerker of gebruiker verwijderd en bij een wijziging aangepast[80]. 2. Toegang tot informatie en systeemfuncties van toepassingen is beperkt in overeenstemming met het beleid voor toegangsbeveiliging[81]. Hierbij: a. Is informatie met specifiek belang fysiek en/of logisch geïsoleerd[82]; b. Geldt voor gebruikers het "need-to-know"-principe[83]. 3. Toegangsrechten van gebruikers worden regelmatig beoordeeld door de eigenaren van bedrijfsmiddelen[84]. Hierbij: a. Worden uitgegeven toegangsrechten minimaal eenmaal per half of heel jaar beoordeeld[85]; b. Wordt de opvolging van bevindingen gedocumenteerd en wordt de bevinding behandeld als beveiligingsincident[86].

[80] BIO 9.2.6

[81] BIO 9.4.1

[82] BIO 9.4.1.1

[83] BIO 9.4.1.2

[84] BIO 9.2.5

[85] BIO 9.2.5.1 (per jaar) of BIO 9.2.5.3 (per half jaar)

[86] BIO 9.2.5.2

4.3 U.03 Beheer van de operationele systemen

U.03	Beheer van de operationele systemen
(BIO 12.1 en 12.5) BIO – Weging: 2	Het wijzigen van de informatieverwerkende faciliteiten en systemen vindt gedocumenteerd plaats volgens procedures en na het testen in gescheiden ontwikkel-, test- en productieomgevingen, tenzij de proceseigenaar een afwijking formeel heeft goedgekeurd. Systeemprestaties worden gewaarborgd door het opstellen van toekomstige capaciteitseisen en door het gebruik te monitoren en de beschikbare capaciteit hierop af te stemmen.
Uitleg	
Wijzigen **Gescheiden**	Het beheer en het wijzigen van de informatieverwerkende faciliteiten en systemen vindt volgens procedures en gedocumenteerd[87] plaats[88]. Daarbij geldt dat: 1. Wijzigingen: a. Worden volgens een procedure goedgekeurd na een risicoafweging van mogelijke gevolgen[89]; b. Zijn geadministreerd[90]; c. Zijn gedeeld met gebruikers[91]; d. Wordt software op operationele systemen geïnstalleerd volgens vaste procedures[92] die de integriteit van de systemen gewaarborgd. 2. De scheiding van ontwikkel-, test- en productieomgevingen verlaagt het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving[93], waarbij niet in de productieomgeving wordt getest, maar de wijzigingen zijn getest, voordat zij in productie worden gebracht. Dit tenzij er voorafgaand goedkeuring heeft plaatsgevonden door de proceseigenaar, inclusief schriftelijke vastlegging[94].
Systeem-prestaties	Capaciteitsbeheer waarborgt de vereiste systeemprestaties[95]. Hierbij geldt dat: 1. Het gebruik van middelen wordt gemonitord en afgestemd[96]; 2. Verwachtingen worden opgesteld voor toekomstige capaciteitseisen[97].

[87] BIO 12.1.1
[88] BIO 12.1.2
[89] BIO 12.1.2.1
[90] BIO 12.1.2.1
[91] BIO 12.1.1
[92] BIO 12.5.1
[93] BIO 12.1.4
[94] BIO 12.1.4.1 en BIO 12.1.4.2
[95] BIO 12.1.3
[96] BIO 12.1.3
[97] BIO 12.1.3

4.4 U.04 Beheer van informatiebeveiligingsincidenten en -verbeteringen

U.04	Beheer van informatiebeveiligingsincidenten en - verbeteringen
(BIO 16.1) BIO – Weging: 1	Informatiebeveiligingsgebeurtenissen en waargenomen of vermeende zwakheden worden geregistreerd en gerapporteerd volgens vaste procedures. Zij worden als informatiebeveiligingsincident geclassificeerd om zo nodig passend te kunnen reageren, ervan te leren en herhaling te voorkomen.
Uitleg	
Vaste procedures	Om de informatiebeveiligingsincidenten om te zetten naar verbeteringen: 1. Zijn de directieverantwoordelijkheden en -procedures vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen[98]; 2. Is van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren[99] . Hiervoor is een Coordinated Vulnerability Disclosure (CVD) procedure ingericht en gepubliceerd[100]; 3. Worden informatiebeveiligingsgebeurtenissen zo snel mogelijk via de juiste leidinggevende niveaus gerapporteerd[101]. Hiervoor: a. Is er een meldloket voor beveiligingsincidenten[102]; b. Is er een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven[103]; c. Hebben alle medewerkers en contractanten aantoonbaar kennis genomen van de meldingsprocedure voor incidenten[104]; d. Worden incidenten zo snel mogelijk, maar in ieder geval binnen 24 uur na bekendwording, intern gemeld[105]; e. Is de proceseigenaar verantwoordelijk voor het oplossen van beveiligingsincidenten[106]; f. Wordt de opvolging van incidenten maandelijks gerapporteerd aan de verantwoordelijke[107]; g. Is informatie afkomstig uit de CVD procedure onderdeel van de incidentrapportage[108]. 4. Wordt van informatiebeveiligingsgebeurtenissen vastgesteld of zij geclassificeerd moeten worden als informatiebeveiligingsincident[109], waarna: a. Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatieverwerkende systemen, zo snel mogelijk (binnen 72 uur) al dan niet geautomatiseerd worden gemeld aan het Nationaal

[98] BIO 16.1.2
[99] BIO 16.1.3
[100] BIO 16.1.3.1
[101] BIO 16.1.2
[102] BIO 16.1.2.1
[103] BIO 16.1.2.2
[104] BIO 16.1.2.3
[105] BIO 16.1.2.4
[106] BIO 16.1.2.5
[107] BIO 16.1.2.6
[108] BIO 16.1.2.7
[109] BIO 16.1.4

	Cyber Security Centrum(NCSC) (alleen voor rijksoverheidsorganisaties) of het sectorale Computer Emergency Response Team (CERT)[110]; b. Op informatiebeveiligingsincidenten wordt gereageerd in overeenstemming met de gedocumenteerde procedures[111]; c. Kennis, die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen, wordt gebruikt om van te leren[112] en om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen[113]; d. De analyses van de beveiligingsincidenten worden gedeeld met de relevante partners om herhaling en toekomstige incidenten te voorkomen[114]. 5. Heeft de organisatie procedures gedefinieerd en toegepast voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen[115]. Hierbij is in geval van een (vermoed) informatiebeveiligingsincident de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar[116].

[110] BIO 16.1.4.1
[111] BIO 16.1.5
[112] BIO 16.1.6.1
[113] BIO 16.1.6
[114] BIO 16.1.6.2
[115] BIO 16.1.7
[116] BIO 16.1.7.1

4.5 U.05 Technische kwetsbaarheden, inclusief malware

U.05	Technische kwetsbaarheden, inclusief malware
(BIO 12.2, 12.4, 12.6) BIO – Weging: 3	Informatie over technische kwetsbaarheden van informatiesystemen wordt tijdig verkregen, geëvalueerd en omgezet naar maatregelen. Hierbij hebben gebruikers een passend bewustzijn en zijn ze niet vrij in hun keuze software te installeren. Tegen malware worden routinematig scans uitgevoerd. Aanvallen worden met een SIEM en/of SOC gemonitord en gedetecteerd en geregistreerd in beschermde logbestanden van gebeurtenissen van gebruikersactiviteiten, uitzonderingen, informatiebeveiligingsgebeurtenissen en activiteiten van systeembeheerders en -operators.
Uitleg	
Informatie	Informatie over technische kwetsbaarheden van informatiesystemen wordt tijdig verkregen, zodat het risico dat ermee samenhangt wordt aangepakt[117]. Hiertoe: 1. Wordt het blootstellen van de organisatie aan dergelijke kwetsbaarheden geëvalueerd; 2. Worden passende maatregelen genomen; 3. Worden, als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC classificatie kwetsbaarheidswaarschuwingen) [118]: a. Patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd; b. In de tussentijd op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.
Gebruikers	Voor het installeren van software door gebruikers zijn regels vastgesteld en geïmplementeerd[119], zodat gebruikers op hun werkomgeving niets (zelf) kunnen installeren, anders dan wat via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist)[120].
Malware	Tegen malware zijn maatregelen voor detectie, preventie en herstel geïmplementeerd, inclusief een passend bewustzijn van gebruikers[121]. Hierbij: 1. Is het downloaden van bestanden beheerst en beperkt op basis van risico en need-of-use[122]; 2. Zijn gebruikers voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende links[123]; 3. Is software, inclusief bijbehorende herstelsoftware, geïnstalleerd, die: a. Malware opspoort[124]; b. Actueel is en ondersteund wordt door periodieke updates[125]; c. Computers en media routinematig scant als voorzorgsmaatregel[126]. d. Bestanden, bijlagen en downloads vóór gebruik op malware scant, indien die zijn ontvangen via netwerken of via enige vorm van opslagmedium[127];

[117] BIO 12.6.1
[118] BIO 12.6.1.1
[119] BIO 12.6.2
[120] BIO 12.6.2.1
[121] BIO 12.2.1
[122] BIO 12.2.1.1
[123] BIO 12.2.1.2
[124] BIO 12.2.1.3
[125] BIO 12.2.1.3
[126] BIO 12.2.1.4
[127] BIO 12.2.1.4

	e. Verschillende omgevingen scant, bijv. mailservers, desktopcomputers en de toegang tot het netwerk van de organisatie[128].
Gemonitord en gedetecteerd	Bedreigingen en aanvallen op informatieverwerkende omgevingen worden gemonitord en gedetecteerd in Security Information & Event Management (SIEM) en/of Security Operations Center (SOC) middels detectievoorzieningen, aanvallen[129] . Hiertoe: 1. Worden de detectievoorzieningen ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen[130]; 2. Hebben de SIEM en/of SOC heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management[131]; 3. Worden gedetecteerde nieuwe aanvallen binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het Nationaal Cyber Security Centrum(NCSC) (alleen voor rijksoverheidsorganisaties) of via het sectorale Computer Emergency Response Team (CERT) (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen[132].
Logbestanden	In logbestanden van gebeurtenissen vindt registratie plaats van: 1. Gebruikersactiviteiten, 2. Uitzonderingen, 3. Informatiebeveiligingsgebeurtenissen, 4. Activiteiten van systeembeheerders en -operators[133]. waarna logbestanden worden bewaard en regelmatig beoordeeld[134]. Hiertoe: 1. Worden de logfaciliteiten en informatie in logbestanden beschermd tegen vervalsing en onbevoegde toegang[135]. Hiertoe: a. Is er een overzicht van logbestanden die worden gegenereerd[136]; b. Is de bewaarperiode van de logging bepaald op basis van een expliciete risicoafweging. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd[137]; c. Wordt minimaal halfjaarlijks getoetst op het ongewijzigd bestaan van logbestanden, middels een (onafhankelijke) interne audit procedure[138]; d. Wordt oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens zo snel mogelijk gemeld als beveiligingsincident[139]. 2. Bevat een logregel a. Minimaal [140]: a. De gebeurtenis; b. De informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; c. Het gebruikte apparaat; d. Het resultaat van de handeling; e. Een datum en tijdstip van de gebeurtenis.

[128] BIO 12.2.1.5

[129] Het Nationaal Detectie Netwerk biedt rijksoverheid breed detectievoorzieningen.

[130] BIO 12.4.1.3

[131] BIO 12.4.1.5

[132] BIO 12.4.1.4

[133] BIO 12.4.3

[134] BIO 12.4.1

[135] BIO 12.4.2

[136] BIO 12.4.2.1

[137] BIO 12.4.2.2

[138] BIO 12.4.2.3

[139] BIO 12.4.2.4

[140] BIO 12.4.1.1

	b. In geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden[141]; 3. Zijn de klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein gesynchroniseerd met één referentietijdbron[142].

[141] BIO 12.4.1.2

[142] BIO 12.4.4

4.6 U.06 Netwerk en informatietransport

U.06	Netwerk en informatietransport
(BIO 13.1 en 13.2) BIO – Weging: 2	Op de netwerken wordt de informatie in systemen en toepassingen beschermd met beschermingsmechanismen en -diensten, inclusief de bewaking van het dataverkeer en het volgen en delen van (nieuwe) dreigingen en de scheiding van het verkeer met een verschillend beveiligingsniveau. Het informatietransport via communicatiefaciliteiten is passend beschermd conform: 1. Beleidsregels; 2. Vertrouwelijkheids- of geheimhoudingsovereenkomsten; 3. Overeenkomsten over informatietransport; 4. De voor de overheid vastgestelde open standaarden.
Uitleg	
Netwerken	Netwerken worden beheerd en beheerst, zodat de informatie in systemen en toepassingen is beschermd[143]. Hiertoe: 1. Zijn beveiligingsmechanismen, dienstverleningsniveaus en eisen aan beheer voor alle netwerkdiensten geïdentificeerd en opgenomen in overeenkomsten betreffende interne en uitbestede netwerkdiensten[144]; 2. Wordt het dataverkeer dat de organisatie binnenkomt of uitgaat bewaakt/geanalyseerd op kwaadaardige elementen middels detectievoorzieningen. Dit kan door de inzet[145] van: a. Detectievoorzieningen, zoals beschreven in de richtlijn voor implementatie van detectie-oplossingen; b. Het Nationaal Detectie Netwerk (NDN) (alleen voor rijksoverheidsorganisaties); c. De Generieke Digitale Infrastructuur (GDI). Een detectievoorziening wordt ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen; 3. Worden ontdekte nieuwe dreigingen, rekening houdend met de geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het Nationaal Cyber Security Centrum (NCSC) (alleen voor rijksoverheidsorganisaties) of het sectorale Computer Emergency Response Team (CERT), bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing) [146]; 4. Wordt gebruik gemaakt van encryptiemiddelen, waarvoor het Nationaal Bureau voor Verbindingsbeveiliging (NBV) een positief inzetadvies heeft afgegeven, bij[147]: a. Draadloze verbindingen, zoals wifi; b. Bij bedrade verbindingen buiten het gecontroleerd gebied. 5. Zijn in koppelpunten met externe of onvertrouwde zones 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[148];

[143] BIO 13.1.1
[144] BIO 13.1.2
[145] BIO 13.1.2.1
[146] BIO 13.1.2.2
[147] BIO 13.1.2.3
[148] BIO 13.1.2.4

	6. Hebben alle groepen van informatiediensten, -gebruikers en -systemen een gedefinieerd beveiligingsniveau[149] en zijn alle groepen van elkaar gescheiden in het netwerk[150].
Informatietransport	Het informatietransport via alle soorten communicatiefaciliteiten is beschermd. Hiertoe: 1. Zijn formele beleidsregels, procedures en beheermaatregelen voor transport van kracht[151]; 2. Weerspiegelen de eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten de behoeften van de organisatie en zijn deze vastgesteld, regelmatig beoordeeld en gedocumenteerd[152]; 3. Ligt het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen vast in overeenkomsten over informatietransport[153]; 4. Is de informatie die is opgenomen in elektronische berichten passend beschermd[154]. Hierbij: a. Gelden tegen phishing en afluisteren van elektronische (e-mail)berichten de vastgestelde open standaarden op de 'pas toe of leg uit'(PToLU)-lijst van het Forum Standaardisatie[155]; b. Gelden voor beveiliging van websiteverkeer de open standaarden tegen afluisteren op de PToLU-lijst[156]; c. Wordt voor berichtenuitwisseling met basisregistraties gebruik gemaakt van de actuele versie van Digikoppeling, conform de PToLU-lijst[157]; d. Wordt bij web- en mailverkeer van gevoelige gegevens[158] gebruik gemaakt van PKIoverheid-certificaten[159]; e. Wordt voor de integriteit van elektronische berichten gebruik gemaakt van elektronische handtekeningen van de AdES Baseline Profile standaard[160].

[149] BIO 13.1.3.1

[150] BIO 13.1.3

[151] BIO 13.2.1

[152] BIO 13.2.4

[153] BIO 13.2.2

[154] BIO 13.1.3

[155] BIO 13.2.3.1 tegen phishing en afluisteren

[156] BIO 13.2.3.1

[157] BIO 13.2.3.2

[158] Gevoelige gegevens zijn onder andere digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontlenen.

[159] BIO 13.2.3.3

[160] BIO 13.2.3.4

4.7 U.07 Ontwikkelprocessen, testgegevens en te ontwikkelen informatiesystemen

U.07	Ontwikkelprocessen, testgegevens en te ontwikkelen informatiesystemen
(BIO 14.1, 14.2 en 14.3) BIO – Weging: 3	Een nadelige impact op de bedrijfsvoering en testgegevens wordt voorkomen, door: 1. Het maken van een risicoafweging op de te ontwikkelen systemen en de (uitbestede) ontwikkelomgevingen. Hiertoe worden informatiebeveiligingseisen in de gehele levenscyclus van informatiesystemen integraal meegenomen, ook bij systemen in diensten die extern worden afgenomen; 2. Het toepassen van Security by Design; 3. Het voorkomen van nadelige impact van updates van besturingssystemen op bedrijfskritische toepassingen; 4. Het volgen van wijzigingsbeheerprocedures.
Uitleg	
Gehele levenscyclus	Informatiebeveiliging maakt in de gehele levenscyclus integraal deel uit van informatiesystemen, inclusief de informatiesystemen die via openbare netwerken als dienst worden afgenomen. Hiertoe: 1. Worden de beveiligingseisen opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen[161], waarbij een expliciete risicoafweging is uitgevoerd ten behoeve van het vaststellen van de beveiligingseisen, uitgaande van de BIO[162]; 2. Wordt de informatie die deel uitmaakt van externe diensten en die via openbare netwerken wordt uitgewisseld beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging[163]; 3. Wordt de informatie in transacties beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen[164].
Security by Design	Voor een veilige ontwikkeling en implementatie van software en systemen: 1. Waarborgt vastgesteld beleid[165] dat gangbare principes rondom Security by design uitgangspunt zijn voor de ontwikkeling van software en systemen[166]. Hierbij[167] worden de principes voor de engineering van beveiligde systemen vastgesteld, gedocumenteerd, onderhouden en toegepast[168]; 2. Worden ontwikkelomgevingen passend beveiligd op basis van een expliciete risicoafweging[169]; 3. Zijn de ontwikkelomgevingen voor verrichtingen op het gebied van systeemontwikkeling en integratie passend beveiligd[170] en worden testgegevens zorgvuldig gekozen, beschermd en gecontroleerd[171]; 4. Staat uitbestede systeemontwikkeling onder supervisie van en monitoring door de organisatie[172]. Hierbij:

[161] BIO 14.1.1
[162] BIO 14.1.1.1
[163] BIO 14.1.2
[164] BIO 14.1.3
[165] BIO 14.2.1
[166] BIO 14.2.1.1
[167] BIO 14.2.5.1
[168] BIO 14.2.5
[169] BIO 14.2.6.1
[170] BIO 14.2.6
[171] BIO 14.3.1
[172] BIO 14.2.7

	a. Is voor uitbestedingstrajecten een expliciete risicoafweging een voorwaarde[173]; b. Worden de noodzakelijke beveiligingsmaatregelen die daaruit volgen aan de leverancier opgelegd[174].
Updates	Updates van besturingssystemen worden pas doorgevoerd, wanneer door het beoordelen en testen van bedrijfskritische toepassingen is gewaarborgd dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie[175].
Wijzigingsbeheerprocedures	Het wijzigen van software en systemen verloopt via vastgestelde procedures voor wijzigingsbeheer[176]. Hierbij: 1. Gelden de algemeen geaccepteerde een beheerframeworks[177]; 2. Zijn programma's voor het uitvoeren van acceptatietests en gerelateerde criteria vastgesteld voor nieuwe informatiesystemen, upgrades en nieuwe versies[178]; 3. Wordt de beveiligingsfunctionaliteit getest[179]; 4. Worden gestructureerde testmethodieken gebruikt voor acceptatietesten van systemen, met bij voorkeur geautomatiseerde testen[180]; 5. Wordt een verslag gemaakt van de testresultaten[181].

[173] BIO 14.2.7.1
[174] BIO 14.2.7.1
[175] BIO 14.2.3
[176] BIO 14.2.2
[177] BIO 14.2.2.1
[178] BIO 14.2.9
[179] BIO 14.2.8
[180] BIO 14.2.9.1
[181] BIO 14.2.9.2

4.8 U.08 Naleving van wettelijke en contractuele eisen

U.08	Naleving van wettelijke en contractuele eisen
(BIO 18.1) Weging: 1	Schendingen worden aantoonbaar voorkomen van wetten en contracten, inclusief: 1. De AVG; 2. Die voor intellectuele eigendom; 3. Die voor registraties; 4. Die voor het gebruik van cryptografie. De aanpak van de organisatie waarborgt dat aantoonbaar aan deze eisen wordt voldaan.
Uitleg	
Aantoonbaar voorkomen	Voor de organisatie en elk informatiesysteem worden expliciet vastgesteld, gedocumenteerd en actueel gehouden [182]: 1. De relevante wettelijke statutaire, regelgevende, contractuele eisen en 2. De aanpak van de organisatie om hieraan te voldoen.
Wetten en contracten	Schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen worden voorkomen: 1. Bescherming van persoonsgegevens: Privacy en bescherming van persoonsgegevens is gewaarborgd in overeenstemming met relevante wet- en regelgeving[183]. Hiertoe: a. Heeft (in overeenstemming met de AVG) iedere organisatie een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren[184]; b. Controleren organisaties regelmatig de naleving van de privacyregels en informatieverwerking en de daarbij horende procedures binnen hun verantwoordelijkheidsgebied aan de hand van de van toepassing zijnde beleidsregels, normen en andere beveiligingseisen[185]; 2. Intellectueel eigendom: Het implementeren van passende procedures ten behoeve van het naleven van wettelijke, regelgevende en contractuele eisen in verband met intellectuele eigendomsrechten en het gebruik van eigendomssoftwareproducten[186]; 3. Beschermen van registraties: Het beschermen tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave van registraties. Dit in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen[187]. Hiertoe heeft de proceseigenaar per soort informatie de bewaartermijn inzichtelijk gemaakt[188]; 4. Cryptografie: Cryptografie wordt toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving[189]. Hiertoe sluiten de cryptografische beheermaatregelen expliciet aan bij de standaarden op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie[190].

[182] BIO 18.1.1
[183] BIO 18.1.4
[184] BIO 18.1.4.1
[185] BIO 18.1.4.2
[186] BIO 18.1.2
[187] BIO 18.1.3
[188] BIO 18.1.3.1
[189] BIO 18.1.5
[190] BIO 18.1.5.1

4.9 U.09 Cryptografie

U.09	Cryptografie
(BIO 10.1) BIO - Weging 1	Cryptografie, inclusief het sleutelbeheer, wordt beleidsmatig toegepast, waarbij duidelijk is wanneer en door wie cryptografie wordt ingezet en beheerd. De toepassing voldoet aan passende standaarden. Bij communicatie tussen organisaties is het beleid onderling vastgesteld.
Uitleg	
Beleidsmatig	Cryptografie (voor het beschermen van informatie) wordt beleidsmatig toegepast[191], waarbij het beleid duidelijkheid geeft over[192]: 1. Wanneer cryptografie ingezet wordt; 2. Wie verantwoordelijk is voor de implementatie; 3. Wie verantwoordelijk is voor het sleutelbeheer; 4. Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum Standaardisatie worden toegepast; 5. Hoe het beschermingsniveau wordt vastgesteld.
De toepassing	De toepassing: 1. Voldoet aan passende standaarden[193], inclusief het sleutelbeheer[194]: a. Bij PKI-overheid-certificaten aan de PKI-Overheid-eisen; b. In overige situaties aan de standaard ISO-11770. 2. Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit risicoafweging blijkt dat deze noodzakelijk zijn[195].
Communicatie tussen organisaties	Bij communicatie tussen organisaties is tevens het beleid onderling vastgesteld.

[191] BIO 10.1.1 en BIO 10.1.2
[192] BIO 10.1.1.1
[193] BIO 10.1.1.2
[194] BIO 10.1.2.1
[195] BIO 10.1.2.2

4.10 U.10 Bedrijfscontinuïteit, inclusief back-ups en redundantie

U10	Bedrijfscontinuïteit, inclusief back-ups en redundantie
(BIO 17.1, 17.2 en 12.3) BIO - Weging 2	Om de continuïteit van het bedrijf te waarborgen zijn de eisen hieromtrent duidelijk en zijn de maatregelen, inclusief redundantie in componenten en back-ups, geïmplementeerd en regelmatig geverifieerd en getest. De eisen zijn het resultaat van het back-upbeleid en van een expliciete risicoafweging.
Uitleg	
Eisen en maatregelen	Om de continuïteit van het bedrijf te waarborgen zijn de eisen duidelijk en de maatregelen geïmplementeerd en regelmatig geverifieerd. Hiertoe: 1. Heeft de organisatie haar eisen vastgesteld voor de continuïteit in ongunstige situaties, bijv. een crisis of een ramp[196]; 2. Zijn, door middel van een expliciete risicoafweging, de bedrijfskritische procesonderdelen met hun bijbehorende betrouwbaarheidseisen geïdentificeerd[197]; 3. Zijn processen, procedures en beheermaatregelen vastgesteld, gedocumenteerd en geïmplementeerd om het vereiste niveau van continuïteit te waarborgen[198]. Hierbij worden informatieverwerkende faciliteiten met voldoende redundantie geïmplementeerd om aan beschikbaarheidseisen te voldoen[199]; 4. Worden de maatregelen regelmatig geverifieerd om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties[200]. Hierbij worden continuïteitsplannen jaarlijks getest op geldigheid en bruikbaarheid[201]; 5. Wordt aangetoond dat de dienstverlening van de bedrijfskritische onderdelen bij calamiteiten uiterlijk binnen een week is hersteld[202].
Back-ups	In overeenstemming met een overeengekomen back-upbeleid zijn, van informatie, software en systeemafbeeldingen, regelmatig back-upkopieën gemaakt en getest[203]. Hierbij: 1. Definieert het back-up beleid de eisen voor het bewaren en beschermen[204]; 2. Is het back-up beleid vastgesteld[205]; 3. Is in een expliciete risicoafweging bepaald[206]: a. Wat het maximaal toegestane dataverlies is; b. Wat de maximale hersteltijd is na een incident. 4. Staan in het back-up beleid minimaal de volgende eisen: a. Dataverlies betreft maximaal 28 uur[207]; b. Hersteltijd in geval van incidenten is maximaal 16 werkuren (2 dagen van 8 uur) in 85% van de gevallen[208]. 5. Voorziet het back-up proces in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere[209]; 6. Wordt de restoreprocedure minimaal jaarlijks en na een grote wijziging getest. Met de test wordt gewaarborgd dat in noodgevallen de restore betrouwbaar is[210].

[196] BIO 17.1.1
[197] BIO 17.1.3.2
[198] BIO 17.1.2
[199] BIO 17.2.1
[200] BIO 17.1.3
[201] BIO 17.1.3.1
[202] BIO 17.1.3.3
[203] BIO 12.3.1
[204] BIO 12.3.1.1
[205] BIO 12.3.1.1
[206] BIO 12.3.1.2
[207] BIO 12.3.1.3
[208] BIO 12.3.1.3
[209] BIO 12.3.1.4
[210] BIO 12.3.1.5

4.11 U.11 Bedrijfsmiddelen, inclusief media

U.11	Bedrijfsmiddelen, inclusief media
(BIO 8.1, 8.2 en 8.3) BIO - Weging 3	Informatie, bedrijfsmiddelen en informatieverwerkende faciliteiten staan in een up-to-date inventarisatie en worden aantoonbaar gebruikt volgens vastgelegde regels. De informatie is na een expliciete risicoafweging geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging. De vernietiging en het transport van (informatie op) media is passend voor de classificatie van de informatie.
	Uitleg
Inventarisatie	Er is een inventarisatie opgesteld[211] van informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten. Hierbij: 1. Zijn de middelen geïdentificeerd en wordt de inventarisatie onderhouden[212]; 2. Hebben de bedrijfsmiddelen een eigenaar[213].
Gebruik	Voor een aanvaardbaar gebruik van informatie en van bedrijfsmiddelen[214]: 1. Zijn regels geïdentificeerd, gedocumenteerd en geïmplementeerd[215]; 2. Zijn alle medewerkers aantoonbaar gewezen op de gedragsregels voor het gebruik[216]; 3. Zijn gedragsregels voor het gebruik van bedrijfsmiddelen door extern personeel in het contract vastgelegd overeenkomstig de huisregels of gedragsregels[217]. 4. Geven alle medewerkers en externe gebruikers alle bedrijfsmiddelen van de organisatie terug die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst[218].
Geclassificeerd	Alle informatie is geclassificeerd[219] met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging[220]. Hiertoe: 1. Is een passende reeks procedures ontwikkeld en geïmplementeerd[221] in overeenstemming met een door de organisatie vastgesteld informatieclassificatieschema[222]; 2. Is de informatie door middel van een expliciete risicoafweging geclassificeerd, zodat duidelijk is welke bescherming nodig is[223].
Vernietiging en het transport	De vernietiging en het transport[224] van informatie en van media is passend voor de classificatie van de informatie: 1. Voor verwijderbare media zijn procedures vastgesteld, zodat het beheer ervan in overeenstemming is met het classificatieschema dat door de organisatie is vastgesteld[225].

[211] BIO 8.1
[212] BIO 8.1.1
[213] BIO 8.1.2
[214] BIO 8.1
[215] BIO 8.1.3
[216] BIO 8.1.3.1
[217] BIO 8.1.3.2
[218] BIO 8.1.4
[219] BIO 8.2
[220] BIO 8.2.1
[221] BIO 8.2.2
[222] BIO 8.2.3
[223] BIO 8.2.1.1
[224] BIO 8.3
[225] BIO 8.3.1

	Hiervoor is er een verwijderinstructie, waarin is opgenomen dat van verwijderbare media die herbruikbaar zijn en die de organisatie verlaten de onnodige inhoud onherstelbaar wordt verwijderd (ISO27002 – implementatierichtlijn 8.3.1.a) [226]; 2. Het verwijderen van media gebeurt op een veilige en beveiligde manier overeenkomstig formele procedures[227]. Hierbij: a. Zijn media met vertrouwelijke informatie niet toegankelijk voor onbevoegden[228]; b. Vindt verwijdering plaats op een veilige manier, bijvoorbeeld 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 (ISO 27002 – implementatierichtlijn 8.3.2.a)[229]; c. 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. 3. Media met informatie zijn beschermd tegen onbevoegde toegang of corruptie tijdens transport[230]. Hierbij: a. Geldt voor de gehele organisatie beleid en een vastgestelde procedure voor het fysieke transport van media[231]; b. Voldoen koeriers of transporteurs voor transport van op BBN2 of hoger geclassificeerde informatie aan vooraf opgestelde betrouwbaarheidseisen[232].

[226] BIO 8.3.1.1
[227] BIO 8.3.2
[228] BIO 8.3.2.1
[229] BIO 8.3.2.3
[230] BIO 8.3.3
[231] BIO 8.3.3.1
[232] BIO 8.3.3.2

4.12 U.12 Leveranciers

U.12	Leveranciers
(BIO 15.1 en 15.2) BIO - Weging 2	Een leverancier krijgt toegang tot de bedrijfsmiddelen en bedrijfsinformatie als er een risicoafweging is gemaakt, er een verwerkersovereenkomst is en in de leveranciersovereenkomst de vastgestelde informatiebeveiligingseisen zijn vastgelegd, inclusief de prestatie-indicatoren en de uitwerking van een exitstrategie. De dienstverlening van leveranciers wordt regelmatig gemonitord, beoordeeld en ge-audit. Bij veranderingen in de dienstverlening vindt herbeoordeling van risico's plaats.
Uitleg	
Toegang	Een leverancier krijgt alleen toegang tot de bedrijfsmiddelen en bedrijfsinformatie als: 1. Op basis van een expliciete risicoafweging de beheermaatregelen voor de toegang zijn vastgesteld[233]; 2. Er een verwerkersovereenkomst is gesloten, waarin alle wettelijk (AVG-gerelateerde) vereiste afspraken zijn vastgesteld, indien de verstrekte toegang (mogelijk) de verwerking van persoonsgegevens tot gevolg heeft [234]; 3. Een leveranciersovereenkomsten is gesloten[235] met daarin de relevante informatiebeveiligingseisen[236]. Hiertoe: a. Zijn bij de offerteaanvragen de eisen voor informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) benoemd. Deze eisen zijn gebaseerd op een expliciete risicoafweging[237]; b. Zijn de beveiligingseisen uit de offerteaanvraag expliciet opgenomen in de (inkoop)contracten waar informatie een rol speelt[238]; c. Zijn expliciet de prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen[239]; d. Zijn de consequenties voor de organisatie van (eventuele) contractvoorwaarden die zijn opgelegd door leveranciers duidelijk. Hierbij [240]: • Zijn de consequenties voorafgaand aan het tekenen van het contract met een risicoafweging helder gemaakt; • Is expliciet gemaakt welke consequenties geaccepteerd worden en welke gemitigeerd moeten zijn bij het aangaan van de overeenkomst. e. Zijn de standaardvoorwaarden voor inkoop gehanteerd, dit ter waarborging van vertrouwelijkheid of geheimhouding[241]; f. Is, voordat een contract wordt afgesloten, in een risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is; g. Is een expliciete uitwerking van de exitstrategie als vast onderdeel opgenomen[242]; h. Is expliciet vastgelegd hoe de betrouwbaarheid van de geleverde dienst kan worden getoetst. Dit kan door middel van certificering of anders een externe audit[243];

[233] BIO 15.1.1.2

[234] BIO 15.1.1.3

[235] BIO 15.1.2; Een relevante leverancier is een leveranciers die toegang heeft of biedt tot (IT-infrastructuurelementen ten behoeve van) de informatie van de organisatie, of deze informatie verwerkt, opslaat of communiceert

[236] BIO 15.1.1

[237] BIO 15.1.1.1

[238] BIO 15.1.2.1

[239] BIO 15.1.2.2

[240] BIO 15.1.2.3

[241] BIO 15.1.2.4

[242] BIO 15.1.2.5

[243] BIO 15.1.2.6

	i. Zijn de eisen opgenomen die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten[244]. Hierbij[245]: • Hebben de leveranciers hun keten van toeleveranciers bekend gemaakt; • Zijn de leveranciers transparant over de maatregelen die zij genomen hebben om de aan hen opgelegde eisen ook door te vertalen naar hun toeleveranciers.
Gemonitord, beoordeeld en ge-audit	De organisatie monitort, beoordeelt en audit regelmatig de dienstverlening van leveranciers[246]. Hierbij: 1. Wordt jaarlijks de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is[247]; 2. Vindt beheersing en herbeoordeling van risico's plaats bij veranderingen in de dienstverlening van leveranciers[248], met inbegrip van: a. Handhaving en verbetering van bestaande beleidslijnen; b. Procedures en beheermaatregelen voor informatiebeveiliging. En wordt rekening gehouden met het bedrijfskritische karakter van bedrijfsinformatie, betrokken systemen en processen.

[244] BIO 15.1.3
[245] BIO 15.1.3.1
[246] BIO 15.2.1
[247] BIO 15.2.1.1
[248] BIO 15.2.2

5 Control criteria

5.1 C.01 Beoordelen en auditen van de informatiebeveiliging

C.01	Beoordelen en auditen van de informatiebeveiliging
(BIO 12.7 en 18.2) BIO - Weging 2	Periodiek en bij belangrijke veranderingen vindt beoordelingen en audits plaats van: 1. De aanpak van de implementatie en het beheer van informatiebeveiliging; 2. De informatieverwerking en bijbehorende procedures; 3. De informatiesystemen. Dit gebeurt gepland en afgestemd, zodat de bedrijfsprocessen zo min mogelijk worden verstoord.
Uitleg	
Beoordelingen en audits	Met geplande tussenpozen en zodra zich belangrijke veranderingen voordoen: 1. Wordt de aanpak van de organisatie door een onafhankelijke partij beoordeeld ten aanzien van de implementatie en het beheer van informatiebeveiliging. Hierbij[249]: a. Wordt minimaal gekeken naar beheerdoelstellingen, beheermaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging; b. Is er een Information Security Management System (ISMS) waarmee aantoonbaar de gehele Plan-Do-Check-Act cyclus op gestructureerde wijze wordt afgedekt[250]; c. Is er een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd[251]; 2. Beoordeelt de directie binnen haar verantwoordelijkheidsgebied de naleving van de informatieverwerking en bijbehorende procedures aan de hand van de van toepassing zijnde beleidsregels, normen en andere beveiligingseisen[252]. Hierbij wordt in de P&C-cyclus[253] gerapporteerd over informatiebeveiliging en resulteert dit jaarlijks in een In Control Verklaring (ICV) over de informatiebeveiliging. Indien voldoende herkenbaar kan de ICV voor informatiebeveiliging onderdeel zijn van de jaarlijkse verantwoording over de bedrijfsvoering[254]; 3. Worden informatiesystemen beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging[255]. Hiertoe worden informatiesystemen jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en de identificatie en aanpak van risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten[256] uit te voeren.
Gepland en afgestemd	De auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, zijn zorgvuldig gepland en afgestemd met de proceseigenaren om bedrijfsprocessen zo min mogelijk te verstoren[257].

[249] BIO 18.2.1
[250] BIO 18.2.1.1
[251] BIO 18.2.1.2
[252] BIO 18.2.2
[253] Planning & Control cyclus
[254] BIO 18.2.2.1
[255] BIO 18.2.3
[256] BIO 18.2.3.1
[257] BIO 12.7.1