Clouddiensten

BIO Thema-uitwerking

Oktober 2021 [versie 2.1 definitief]

BIO Thema-uitwerking Clouddiensten

Titel	BIO Thema-uitwerking Clouddiensten
Datum	Oktober 2021
Versie	2.1 definitief
Opdrachtgever	Directeur CIP
Regime	Becommentarieerde praktijk
Auteurs	Wiekram Tewarie (UWV) en Jaap van der Veen (CIP)
Reviewers	Versie 1.0: Professionals uit het CIP-netwerk en het CIP-kernteam Versie 2.0: CIP-kernteam Versie 2.1: CIP-kernteam

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.

Leeswijzer

Voorafgaand aan hoofdstuk 3 Beleidsdomein, 4 Uitvoeringsdomein en 5 Control-domein, de kern van dit document, heeft elke BIO Thema-uitwerking een inleiding met een standaard paragraafindeling.

Aanvullend geldt:

- Voor de aanduiding van personen wordt de mannelijke vorm aangehouden (hij/hem/zijn) ongeacht het geslacht.
- De controls en maatregelen vermeld in deze thema-uitwerking zijn in het beleids-, uitvoerings- en control-domein georganiseerd, waarmee ze bij de overeenkomstige functionarissen kunnen worden geadresseerd. Deze functionarissen zijn niet benoemd omdat dit organisatie-afhankelijk is.
- Bijlagen zijn opgenomen alleen voor specifieke informatie uit hoofdstuk 3 Beleidsdomein, 4 Uitvoeringsdomein en/of 5 Control-domein.
- Van best practices (open standaarden al dan niet toegankelijk met een licentie) zijn de meest actuele versies afgekort vermeld, tenzij de actuele versie niet toereikend is.
- Voor een overzicht van alle gebruikte best practices, afkortingen en begrippen en een generieke toelichting op de opzet van de thema-uitwerkingen, zie de Structuurwijzer BIO Thema-uitwerkingen.

Inhoudsopgave

1	Inleiding	8
1.1	Doelstelling	9
1.2	Opzet BIO Thema-uitwerking	9
1.3	Context relatie tussen CSC en CSP	10
1.4	Context en globale structuur clouddiensten	12
1.4.1	Beleidsdomein	13
1.4.2	Uitvoeringsdomein	13
1.4.3	Control-domein	13
1.5	Scope en begrenzing clouddiensten	13
1.6	Aanleiding om gebruik te maken van clouddiensten	14
1.7	Toepassing BIO Thema-uitwerking	15
2	Risico's in relatie tot clouddiensten	16
2.1	Dreigingen/kwetsbaarheden	16
2.2	CSC-georiënteerde aandachtspunten	17
2.3	Beveiligingsobjecten voor clouddiensten	18
3	Beleidsdomein	20
3.1	Doelstelling	20
3.2	Risico's	20
3.3	Objecten, controls en maatregelen	20
3.3.1	B.01 Wet- en regelgeving	21
3.3.2	B.02 Cloudbeveiligingsstrategie	22
3.3.3	B.03 Exit-strategie	23
3.3.4	B.04 Clouddienstenbeleid	24
3.3.5	B.05 Transparantie	25
3.3.6	B.06 Risicomanagement	26
3.3.7	B.07 IT-functionaliteit	27
3.3.8	B.08 Bedrijfscontinuïteitsmanagement	28
3.3.9	B.09 Privacy en bescherming persoonsgegevens	30
3.3.10	B.10 Beveiligingsorganisatie	31
3.3.11	B.11 Clouddienstenarchitectuur	33
4	Uitvoeringsdomein	34

4.1	Doelstelling	34
4.2	Risico's	34
4.3	Objecten, controls en maatregelen	34
4.3.1	U.01 Standaarden voor clouddiensten	35
4.3.2	U.02 Risico-assessment	36
4.3.3	U.03 Bedrijfscontinuïteitsservices	37
4.3.4	U.04 Herstelfunctie voor data en clouddiensten	37
4.3.5	U.05 Dataprotectie	38
4.3.6	U.06 Dataretentie en gegevensvernietiging	39
4.3.7	U.07 Datascheiding	40
4.3.8	U.08 Scheiding dienstverlening	40
4.3.9	U.09 Malwareprotectie	41
4.3.10	U.10 Toegang IT-diensten en data	42
4.3.11	U.11 Cryptoservices	43
4.3.12	U.12 Koppelvlakken	44
4.3.13	U.13 Service-orkestratie	45
4.3.14	U.14 Interoperabiliteit en portabiliteit	46
4.3.15	U.15 Logging en monitoring	47
4.3.16	U.16 Clouddienstenarchitectuur	48
4.3.17	U.17 Multi-tenantarchitectuur	48
5	Control-domein	50
5.1	Doelstelling	50
5.2	Risico's	50
5.3	Objecten, controls en maatregelen	50
5.3.1	C.01 Servicemanagementbeleid en evaluatierichtlijn	51
5.3.2	C.02 Risico-control	51
5.3.3	C.03 Compliance en assurance	53
5.3.4	C.04 Technische kwetsbaarhedenbeheer	54
5.3.5	C.05 Security-monitoringsrapportage	55
5.3.6	C.06 Beheersorganisatie clouddiensten	56
Bijlage 1:	Verantwoording	58
Bijlage 2:	Toelichting objecten in het beleidsdomein	60

Bijlage 3:	Toelichting objecten in het uitvoeringsdomein	63
Bijlage 4:	Toelichting objecten in het control-domein	66
Bijlage 5:	Beslisboom voor risicobeoordeling IV-diensten	69
Bijlage 6:	Samenvatting AIVD-standpunt en beleidsverkenning BZK	72

Voorwoord

Dit document bevat een referentiekader voor de BIO Thema-uitwerking Clouddiensten, door het CIP opgesteld om overheidsorganisaties een beeld te geven van de meest relevante onderwerpen bij het verwerven van veilige clouddiensten. Het document is bedoeld als handreiking, gerelateerd aan de toepassing van de Baseline Informatiebeveiliging Overheid (BIO) en verschaft een overzicht van de uitwerking van clouddienstenobjecten vanuit de optiek van de CSC (Cloud Service Consumer). Voor de beperking van de omvang van dit document worden de geïdentificeerde objecten gerelateerd aan algemene clouddiensten. Dit document doet geen uitspraken over de vraag of cloud ingezet mag worden. Die keuze is onderworpen aan het vigerend beleid. Bij een keuze voor cloud, kan dit document worden gehanteerd bij de inrichting.

De BIO is verplicht verklaard voor de overheidspartijen. Vanwege de snelle ontwikkelingen van clouddiensten hebben overheidspartijen een grote behoefte aan overzicht en inzicht in de meest cruciale componenten die bij de verwerving van clouddiensten aandacht behoeven. Temeer omdat specifieke op clouddiensten gerichte beveiligingsobjecten ontbreken in de BIO. Dat komt omdat de BIO gebaseerd is op een generieke baseline NEN-EN-ISO/IEC 27002:2017 (hierna genoemd ISO 27002). Aanvullend op deze ISO-norm zijn door NEN-EN-ISO/IEC een aantal implementatiekaders opgesteld en bestaan er kaders zoals het Cybersecurity Framework (CSW) van National Institute of Standards and Technology (NIST) en de Cloud Control Matrix (CCM) van Cloud Security Alliance (CSA), gericht op de beveiliging van clouddiensten. Ook de The Standard of Good Practice (SoGP) 2018, standaarden van de Bundesamt für Sicherheit in der Informationstechnik (BSI), International Telecommunication Union (ITU) en de ICT-Beveiligingsrichtlijnen voor Webapplicaties van het Nationaal Cyber Security Centrum (NCSC) bevatten relevante controls en maatregelen voor clouddiensten. Een probleem voor overheidspartijen is dat een handig overzicht ontbreekt voor een samenvatting van alle relevante zaken over clouddiensten, eenduidig gerelateerd aan de BIO. Een veel gehoorde uitspraak is: ‘We zien door de bomen het bos niet meer.’.

De schrijfgroep heeft diverse workshops georganiseerd waarin verschillende overheidspartijen hebben geparticipeerd. Deze partijen hebben hun beleidsdocumenten ter beschikking gesteld en hun visie, risico’s en problematiek gedeeld waarmee ze in de praktijk geconfronteerd worden. Met deze informatie en risico’s verbonden aan clouddiensten heeft de schijfgroep dit document opgesteld en ter review aan de overheidspartijen aangeboden. Versie 1.1 bevat een compleet beeld van onderwerpen die voor informatieveiligheid en privacy de aandacht vereisen bij de verwerving van clouddiensten. De privacyaspecten zijn in de handreiking Cloudcomputing en Privacy van de Informatiebeveiligingsdienst (IBD) uitgewerkt.

Voor de structurering van dit document is dezelfde systematiek gekozen als bij de overige BIO Thema-uitwerkingen. De beschrijving van de systematiek is in dit document kort weergegeven.

Dit document beperkt zich tot die zaken, die vanuit de CSC richting de Cloud Service Provider (CSP) van belang zijn, inclusief de koppelvlakken tussen de CSC en de CSP. Uiteraard speelt de CSC in de informatieketen een belangrijke rol en moet zij haar IT-huishouding op orde hebben. Pas dan kan sprake zijn van een goede samenwerking tussen de CSC en de CSP. Dit gegeven is een belangrijk uitgangspunt voor stakeholders binnen de overheidspartijen.

Er zijn veel inhoudelijke suggesties en reacties ontvangen. De intentie van dit document is de lezer verder te helpen bij vraagstukken over clouddiensten. Daar waar verbeterd kan worden, kan deze thema-uitwerking verrijkt worden met aangeleverde teksten.

1 Inleiding

De toepassing van cloud-computing[1]-diensten, kortweg clouddiensten, is een methode voor het leveren van de ICT. Cloud-computing is een term die staat voor de omgeving waarbinnen CSP's functionaliteit of diensten in de vorm van een technologische black-box aanbieden. Dit betekent dat clouddiensten gekozen worden met een vooraf vastgestelde 'dienstenmenukaart'. De CSC kan als aanvullende eis stellen dat het effectieve beveiligingsniveau voor de betrokken CSC geen invloed ondervindt van onderhoud- en releasewerkzaamheden voor andere CSC's.

In het algemeen zijn er 3 soorten IT-clouds te onderscheiden:

1. Private (met een dedicated infrastructuur)
   De IT-voorzieningen zijn ingericht voor één CSC en opgezet met de standaarden van de CSP.
2. Private/shared (met een geheel of gedeeltelijk gedeelde infrastructuur)
   De IT-voorzieningen zijn toegankelijk voor één CSC en zij delen, om kosten te besparen, de onderliggende infrastructuur met andere CSC's (bijvoorbeeld de opslag en het netwerk).
3. Publiek
   De IT-voorzieningen zijn toegankelijk via het Internet. De voorzieningen worden meestal gedeeld met andere CSC's.

De meest bekende clouddiensten zijn:

- Software as a Service (SaaS)
  Bij SaaS staat de applicatie volledig onder controle van de dienstverlener.
- Platform as a Service (PaaS)
  Bij PaaS worden de platformen en de infrastructuur beheerd door de CSP en niet de applicaties.
- Infrastructure as a Service (IaaS)
  Bij IaaS wordt alleen de infrastructuur beheerd door de CSP en niet de applicaties en de platformen.

De toepassing van clouddiensten past in de verschuiving van maatwerkoplossingen naar standaard oplossingen. Sommige overheidsorganisatie maken al gebruik van bepaalde typen clouddiensten. Andere organisaties overwegen nog om gebruik te maken van clouddiensten. Ook hebben sommigen hiervoor een eigen cloud-beleid ontwikkeld. Bij veel overheidsorganisatie heerst er echter onzekerheid over:

- het verwerven van clouddiensten, omdat heel veel activiteiten buiten hun zicht plaatsvinden;
- het opslaan van data bij een derde partij.

Een ander belangrijk aandachtspunt bij de overheidsorganisatie is dat bij een toename van het aantal diensten en dienstverleners (CSP's) de regie-inspanning voor de afnemer (CSC) verder kan toenemen. Vooral wanneer CSP's andere CSP's inschakelen voor de te leveren diensten.

---

[1] Cloud computing is een model voor het snel beschikbaar stellen van on-demand (op verzoek) netwerktoegang tot een gedeelde pool van configureerbare IT-middelen (zoals netwerken, servers, opslag, applicaties en diensten) met een minimum aan managementinspanning of interactie met de aanbieder (NIST: https://csrc.nist.gov/publications/detail/sp/800-145/final).

Ondanks het feit dat voor clouddiensten verschillende baselines bestaan, vragen organisaties zich af op welke onderwerpen[2] zij zich dienen te focussen.

Overheden die IT-diensten willen aanbesteden, dienen zich vanuit hun bijzondere verantwoordelijkheid de vraag te stellen, welke data van medewerkers, burgers en bedrijven, opgeslagen kan worden in de (publieke) cloud en welke data binnen de bescherming van de rekencentra van de overheid moet blijven. Leidend daarbij zijn de antwoorden[3] van minister Plasterk op vragen vanuit de Tweede Kamer, mei 2014. De standpunten van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de verkenning Cloudbeleid Rijksdienst en de IBD-handreikingen voor clouddiensten zijn tevens richtinggevend bij de risicoanalyse, zoals verderop in deze thema-uitwerking is uitgewerkt.

1.1 Doelstelling

Het doel van deze BIO Thema-uitwerking is overheidsorganisaties een systematisch beeld te geven van de voornaamste objecten van clouddiensten, waarmee zij ondersteund worden bij een goed afgewogen inzet van clouddiensten en het onderkennen van de aspecten die van belang zijn bij het aangaan van een clouddienst. De focus van deze thema-uitwerking ligt op beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van de data en de betrouwbaarheid van de bedrijfsprocessen.

De uitwerking van de BIO Thema-uitwerking Clouddiensten dient als handreiking bij inkoop van clouddiensten. De keuze van de objecten dient plaats te vinden met de context van de organisatie en risicoanalyse.

1.2 Opzet BIO Thema-uitwerking

De BIO Thema-uitwerking Clouddiensten wordt uitgewerkt langs twee lijnen: structuur en objecten. De structuur van de BIO Thema-uitwerking Clouddiensten bestaat uit een indeling van beleid, uitvoering en control. De beveiligingsobjecten vormen de inhoudelijke onderwerpen die, vanuit de optiek van de CSC, van belang zijn. Door eerst op de objecten te focussen, wordt inzicht verkregen in en de relatie tussen de noodzakelijke objecten. Na het verkregen inzicht worden per object controls en onderliggende criteria voor maatregelen gedefinieerd. De objecten en de bijbehorende criteria voor maatregelen worden gestructureerd via het beleids-, uitvoerings- of control-domein.

Er wordt een standaard opzet voor BIO Thema-uitwerkingen gevolgd. Vanwege het bijzondere karakter van deze thema-uitwerking zijn voor betere begripsvorming enkele onderwerpen toegevoegd. Deze thema-uitwerking volgt de volgende opzet:

- Context van de relatie tussen de CSC en de CSP (zie paragraaf 1.3)
- Context en globale structuur van deze thema-uitwerking (zie paragraaf 1.4)
- Scope en begrenzing van de thema-uitwerking (zie paragraaf 1.5)
- Aanleiding om gebruik te maken van clouddiensten (zie paragraaf 1.6)
- Dreigingen/kwetsbaarheden (zie paragraaf 2.1)
- CSC-georiënteerde aandachtspunten (zie paragraaf 2.2)

[2] De uitwerkingen van de relevante onderwerpen wordt in dit document verder aangeduid als objecten.

[3] Zie https://www.openkamer.org/kamervraag/2014Z09632/.

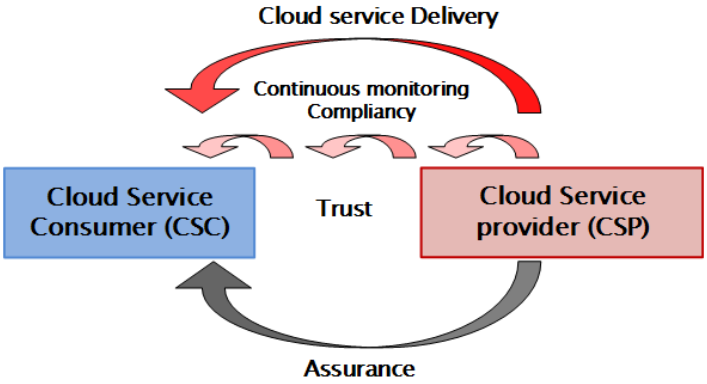
- Beveiligingsobjecten voor clouddiensten in het beleids-, uitvoerings- en control-domein (zie paragraaf 2.3) gerelateerd aan basiselementen (zie hoofdstuk 3, hoofdstuk 4 en hoofdstuk 5)

1.3 Context relatie tussen CSC en CSP

In de verhouding tussen de CSC en de CSP zijn drie issues waar organisaties steeds op focussen. Vanuit de CSC beredeneerd zijn dit:

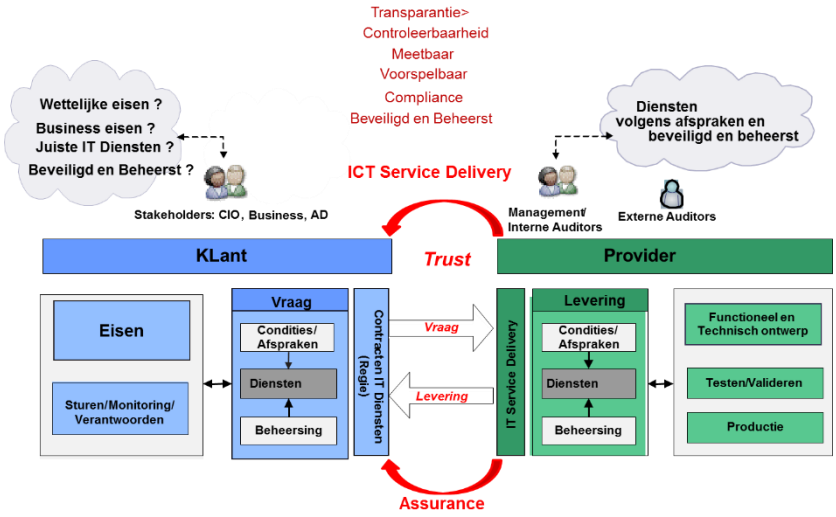
1. On-going
   Krijgt de CSC qua prestaties op dagelijkse basis de juiste diensten geleverd? Anders gezegd, voldoen de geleverde diensten aan prijs, kwaliteit, veiligheid- en continuïteitseisen? Dus hoe het gesteld is met de performance?
2. Continuous monitoring (near real time)
   Krijgt de CSC de zekerheid dat hij regulier, conform contracten, bedrijfseisen en beveiligingseisen, de juiste diensten ontvangt? Dus hoe het gesteld is met de beoogde conformiteit?
3. Compliancy (periodieke metingen en evaluaties)
   Krijgt de CSC de zekerheid dat hij in de afgelopen periode, conform wet- en regelgeving, contracten, bedrijfseisen en beveiligingseisen de juiste diensten heeft ontvangen? Dus hoe het gesteld is met de beoogde de compliance?

Bij de inkoop van clouddiensten levert de CSP niet alleen de gecontracteerde clouddiensten (ICT-servicelevering), maar ook de noodzakelijke continuous monitoring-, compliancy- en assurance-rapportages, zie afbeelding 1.



Afbeelding 1: Twee deliverables van een CSP

Afbeelding 1 is verder uitgewerkt is afbeelding 2.



Afbeelding 2: Twee CSP-deliverables en CSC-eisen/wensen

ICT-servicelevering

Dit betreft de daadwerkelijk door de CSC gevraagde publieke of private clouddiensten, die aan bepaalde functionele en beveiligingseisen moeten voldoen. De levering gaat vergezeld van prestatiemetingen over de geleverde diensten en de noodzakelijke verbetermaatregelen voor leveringen en beveiliging.

Assurance

Dit betreft een jaarlijkse rapportage gebaseerd op een onderzoek uitgevoerd door een derde partij. Met de assurance-rapportage geeft de CSP zekerheid aan de CSC dat de geleverde diensten aan de contractuele eisen hebben voldaan. De assurance-rapportage komt tot stand met een onderzoekstraject waarin een referentiekader als toetsingsmiddel wordt gehanteerd.

Trust

De inkoop van clouddiensten gaat gepaard met een gedragen en haalbaar ICT-servicecontract. Echter er zullen altijd aspecten zijn die bij de contractvorming over het hoofd worden gezien. Voor een duurzame relatie is daarom een vertrouwensrelatie tussen de CSC en de CSP vereist, anders lopen zij steeds het risico in een juridische strijd verwikkeld te raken.
Zowel aan de CSC-kant als aan de kant van de CSP spelen verschillende aspecten een rol. In de relatie tussen de CSC en CSP heeft iedere partij haar eigen rol. De relevante aspecten zijn hieronder beschreven.

CSC (vraagzijde)

Initieel stelt de CSC een Programma van Eisen en Wensen (PvEeW) vast voor de te verwerven clouddiensten en communiceert dit met de potentiële CSP's. Wanneer de CSC en de gekozen CSP overeenstemming bereiken, worden clouddiensten geleverd. Een belangrijke vraag voor overheidsdienstverlening is hierbij: 'Is de toepassing van Clouddienst, gelet op de, door de Tweede

Kamer geaccepteerde risico's toegestaan?'[4]. In bijlage 5 Beslisbomen voor risicobeoordeling IV-diensten zijn instrumenten, in de vorm van beslisbomen, opgenomen waarmee organisaties kunnen besluiten al dan niet gebruik te maken van clouddiensten.

CSP (leveringszijde)

De CSP maakt met het PvEeW een functioneel en technisch ontwerp. Vervolgens wordt de dienst gebouwd, getest en in productie genomen.

Deze geleverde diensten dienen altijd te voldoen aan de, in de vorm van wettelijke en business eisen, gestelde condities. Hiernaast komen de partijen overeen dat de geleverde diensten:

- meetbaar en voorspelbaar moeten zijn;
- compliant moeten zijn aan wet- en regelgeving, business- en beveiligingseisen van de CSC;
- beveiligd en beheerst moeten zijn.

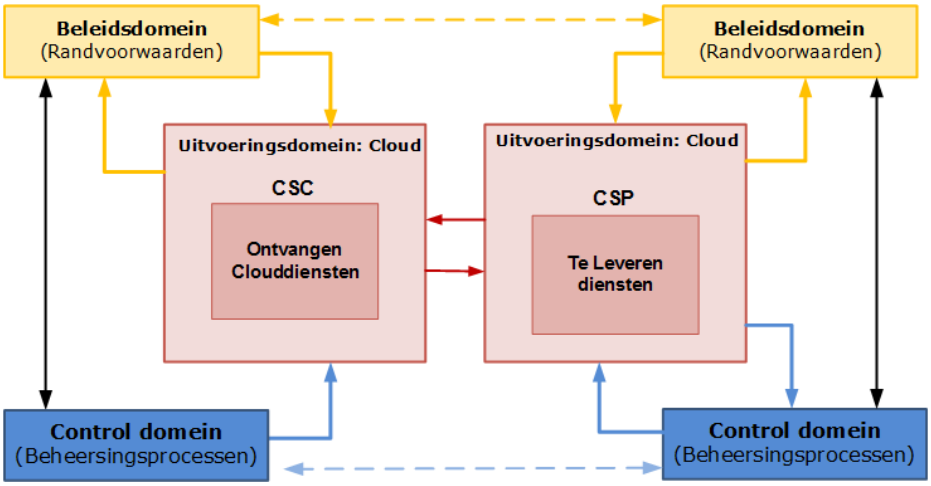
Geleverde diensten

Deze diensten dienen altijd te voldoen aan de, in de vorm van wettelijke en business eisen, gestelde condities. Hiernaast komen de partijen overeen dat de geleverde diensten:

- meetbaar en voorspelbaar moeten zijn;
- compliant moeten zijn aan wet- en regelgeving, business- en beveiligingseisen van de CSC;
- beveiligd en beheerst moeten zijn.

1.4 Context en globale structuur clouddiensten

Afbeelding 2 kan samengevat worden met het beleids-, uitvoerings- en control-domein. Dit wordt in afbeelding 3 geïllustreerd.



Afbeelding 3: Context CSC- en CSP-relatie bij clouddienstenverwerving

[4] Mail: J.L.M. Kuijpers (AIVD), betreft: Publieke clouddiensten en gerubriceerde gegevens van 9 september 2019.

Concept voor afstemming: Verkenning cloudbeleid voor de Nederlandse Rijksdienst, versie 0.96, d.d. 12 augustus 2019, https://www.earonline.nl/images/earpub/8/86/Quickscan_BIR2017_versie_1.pdf.

Beleidskader: Privacy en informatiebescherming 2019, versie 1.0 van d.d. 20 januari 2019.

Brief: Ferd Grapperhaus (Ministerie van Justitie en Veiligheid), Onderwerp: CLOUD act van oktober 2018.

1.4.1 Beleidsdomein

De CSC stelt een PvE(eW) op, dat als randvoorwaarde geldt. Voor zowel de CSC als de CSP is het PvE(eW) een toetsinstrument. Zij kunnen de volgende vragen stellen:

- CSC: heb ik de juiste dienst(en) geleverd gekregen?
- CSP: hoe kan ik aantonen dat ik de juiste diensten heb geleverd?

1.4.2 Uitvoeringsdomein

Binnen dit domein gaat het om de operationele levering van clouddiensten. Aan beide zijden moet transparantie zijn over de gevraagde en daadwerkelijke leveringen.

1.4.3 Control-domein

Binnen dit domein zijn de beheersingsprocessen ingericht. Voor de beoogde dienstverlening moeten de beheersingsprocessen aan de kant van de CSC en de CSP op elkaar zijn afgestemd.

1.5 Scope en begrenzing clouddiensten

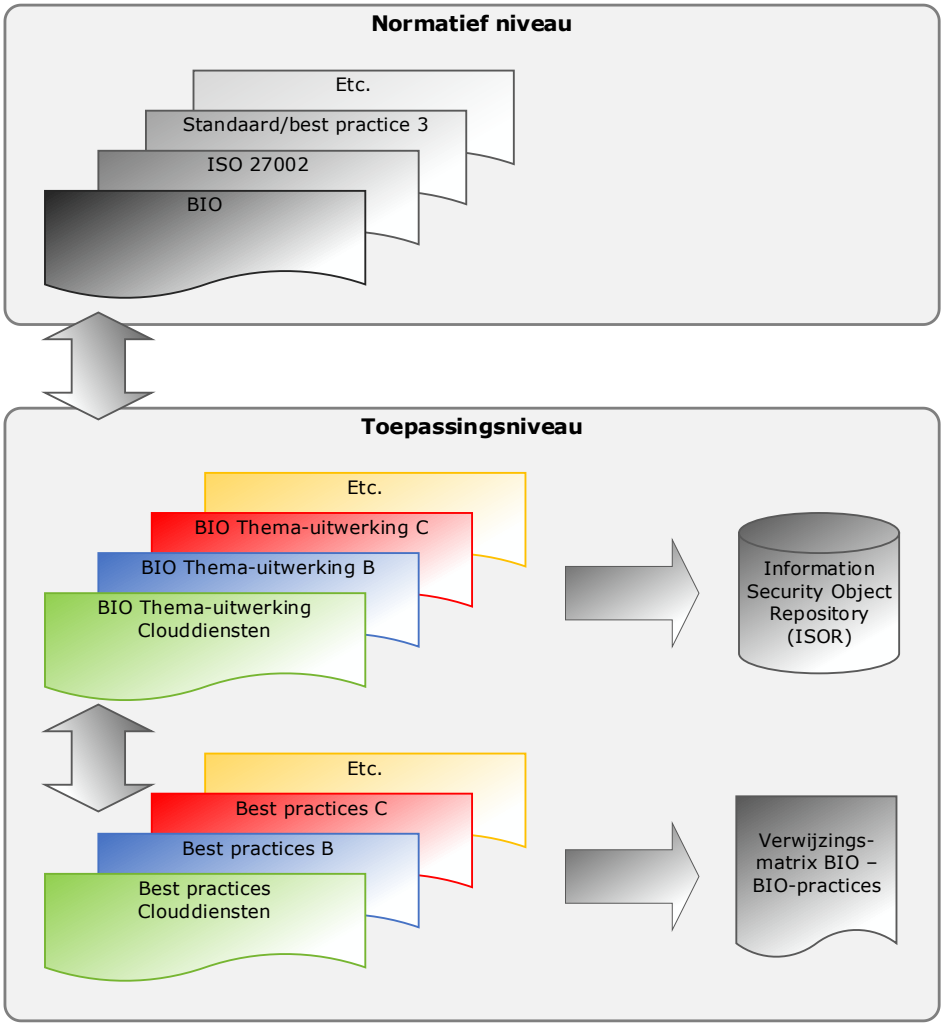
De scope van de BIO Thema-uitwerking Clouddiensten is de set van specifieke onderwerpen (objecten) waar organisaties aandacht aan moeten besteden bij het inkopen van clouddiensten. Deze thema-uitwerking richt zich hoofdzakelijk op het ‘wat’-aspect.

Het is ook van belang om te weten langs welke route organisaties naar de cloud kunnen. Hieraan liggen migratiestrategieën ten grondslag. De migratiestrategieën zullen niet worden beschreven. Het zogeheten ‘hoe’-aspect wordt in dit document niet uitgewerkt. In de praktijk zijn daarvoor verschillende baselines beschikbaar.

De algemene eisen uit de BIO en ISO 27001 en ISO 27002 blijven onverminderd van kracht. Het gaat in deze thema-uitwerking om specifieke additionele objecten die gerelateerd zijn aan clouddiensten. De maatregelen die gerelateerd zijn aan deze objecten moeten realistisch en implementeerbaar zijn voor een CSP.

Privacy-aspecten: Data Protection Impact Assessments (DPIA’s) worden niet expliciet in dit document opgenomen omdat DPIA’s vanuit de Algemene Verordening Gegevensbescherming (AVG) generiek bij elk project uitgevoerd dienen te worden.

De begrenzing van dit document is in onderstaande afbeelding 4 weergegeven.



Afbeelding 4: Relatie BIO Thema-uitwerking Clouddiensten met aanpalende documenten

1.6 Aanleiding om gebruik te maken van clouddiensten

Enkele belangrijke argumenten van overheden om gebruik te maken van clouddiensten zijn:

- de focus op kerntaken;
- een efficiënte bedrijfsvoering en het verlagen van de totale kosten;
- het binnen een kort tijdsbestek kunnen beschikken over nieuwe IT-functionaliteit en daarmee de dienstverlening aan burger en bedrijf sneller aan kunnen passen aan de (veranderende) behoefte;
- de zekerheid over gekwalificeerd personeel;
- het verlagen van IT-complexiteit in specifieke situaties;
- het verbeteren van beveiliging/beschikbaarheid;
- een herziene bedrijfsstrategie en vereiste specifieke beveiligingseisen voor processen en data.

Hiernaast kunnen organisaties met externe factoren overwegen om gebruik te maken van clouddiensten, zoals:

- Vigerende wet- en regelgeving voor:

  - een betrouwbare dienstverlening en het veilig omgaan met data van burgers en bedrijven;
  - het overheidsbeleid inzake data in de cloud en de invloed van internationale verdragen;
  - de noodzaak voor een weerbare overheid tegen cybercriminaliteit en statelijke actoren;
- Technologische ontwikkelingen
  Hierbij wil de CSC kunnen inspelen op innovaties, die kunnen leiden tot een efficiëntere bedrijfsvoering en verlaging van de totale kosten.

1.7 Toepassing BIO Thema-uitwerking

Dit document is een hulpmiddel bij het kiezen van een aantal te adresseren cloud-objecten bij het verwerven van clouddiensten. Bij de opzet van deze thema-uitwerking is het onderwerp cloud functioneel benaderd en niet uitgewerkt op de technische gelaagdheid van SaaS, PaaS en IaaS. Bij het verwerven van clouddiensten kan dit document als hulpmiddel dienen. Dit impliceert de volgende stappen:

- Bepaal als eerste de context van de case en het type dienst dat verworven moet worden.
- Identificeer vervolgens de operationele beveiligingsobjecten. Raadpleeg hierbij de objecten in het uitvoeringsdomein (zie hoofdstuk 4 Uitvoeringsdomein).
- Identificeer daarna de conditionele objecten. Raadpleeg hierbij de objecten in het beleidsdomein (zie hoofdstuk 3 Beleidsdomein).
- Identificeer tenslotte de beheersingsobjecten. Raadpleeg hierbij de objecten in het control-domein (zie hoofdstuk 5 Control-domein).
- Neem de beveiligingsobjecten op in het PvEeW voor de clouddienst, zodat deze objecten door de CSP kunnen worden gerelateerd aan de specificaties van bestaande ‘standaard diensten’ of worden vertaald in maatregelen voor de aangeboden specifieke dienstverlening.

2 Risico's in relatie tot clouddiensten

Relevante risico's verbonden aan clouddiensten kunnen ondergebracht worden in 2 risicogroepen:

1. Data
   Gegevens van de burger of CSC zijn verloren geraakt of misbruikt.
2. IT-dienstverlening
   De betrouwbare dienstverlening aan de burger en CSC is in gevaar.

Risico's worden bepaald door dreigingen en kwetsbaarheden en de kans dat daardoor schade ontstaat. Zowel dreigingen als kwetsbaarheden zijn hieronder concreet gemaakt. De factor 'kans' is niet berekenbaar voor clouddiensten, maar kan ingeschat worden door onderzoek vanuit de eigen context van de CSC en de zich ontwikkelende markt van CSP's.

2.1 Dreigingen/kwetsbaarheden[5]

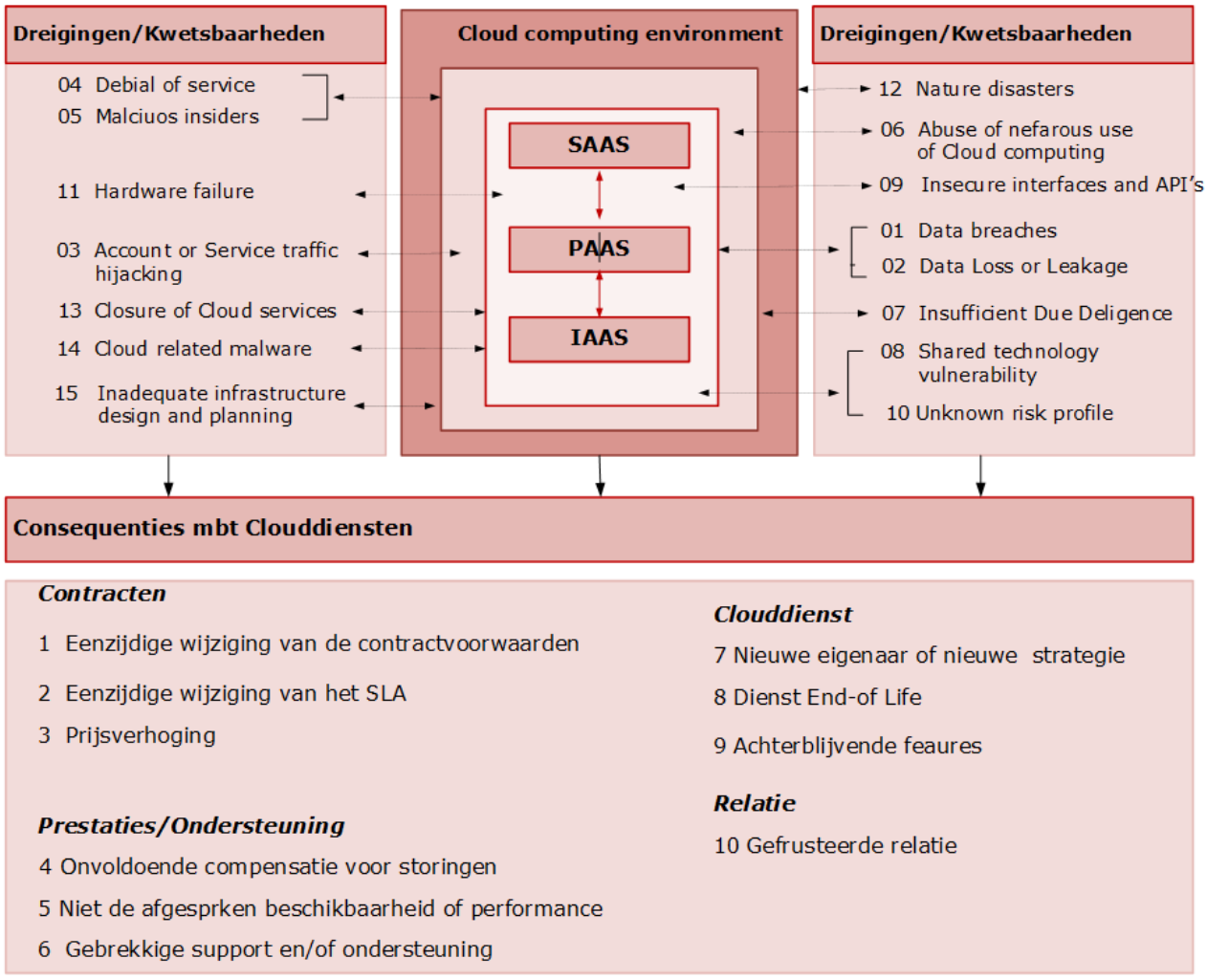
De vakliteratuur noemt verschillende dreigingen/kwetsbaarheden waarmee een CSC rekening dient te houden bij het verwerven van clouddiensten. Na de verwerving kan de CSC geconfronteerd worden met issues over contracten en prestaties van de clouddienst en over ondersteuning door en de relatie met de CSP. Bij het identificeren van objecten voor clouddiensten zijn beide hiervoor genoemde risicogroepen als invalshoek gebruikt. Tabel 1 Cloud Computing Vulnerabilities CSA and Greer and Jackson, 2017 en afbeelding 5 geven een overzicht van de belangrijkste kwetsbaarheden en voorkomende consequenties. Bijlage 2 Toelichting objecten in het beleidsdomein, bijlage 3 Toelichting objecten in het uitvoeringsdomein en bijlage 4 Toelichting objecten in het control-domein bevatten detailuitwerkingen van de dreigingen. Tabel 1 Cloud Computing Vulnerabilities CSA and Greer and Jackson, 2017 en afbeelding 5 zijn beperkt tot de set van CSA en Greer and Jackson.

Nr.	Cloud Computing Vulnerabilities CSA and Greer and Jackson, 2017		
1	Data	Data breaches	Dataverstoringen
2		Data loss or data leakage	Dataverlies of datalekken
3	Clouddiensten	Account or service traffic hijacking	Kapen van account of service verkeer
4		Denial of service	Denial of service
5		Malicious insiders	Kwaadwillende insiders
6		Abuse of nefarious use of cloud computing	Misbruik of misdadig gebruik van cloud computing
7		Insufficient due diligence	Onvoldoende due diligence
8		Shared technology vulnerabilities	Gedeelde technologie kwetsbaarheden
9		Insecure interfaces and application programming interfaces (API's)	Onveilige interfaces en API's
10		Unknown risk profile	Onbekend risicoprofiel
11		Hardware failure	Hardware falen

[5] Aandachtspunten voor consequenties is overgenomen van Weolcan: https://blog.weolcan.eu/wat-is-een-cloud-exit-strategie-precies-en-hoe-voer-je-het-uit.

Nr.	Cloud Computing Vulnerabilities CSA and Greer and Jackson, 2017		
12		Nature disasters	Natuurlijke rampen
13		Closure of cloud service	Afsluiten van de clouddienst
14		Cloud related malware	Cloud gerelateerde malware
15		Inadequate infrastructure design and planning	Inadequate infrastructuur ontwerp en planning

Tabel 1: Cloud Computing Vulnerabilities CSA and Greer and Jackson, 2017



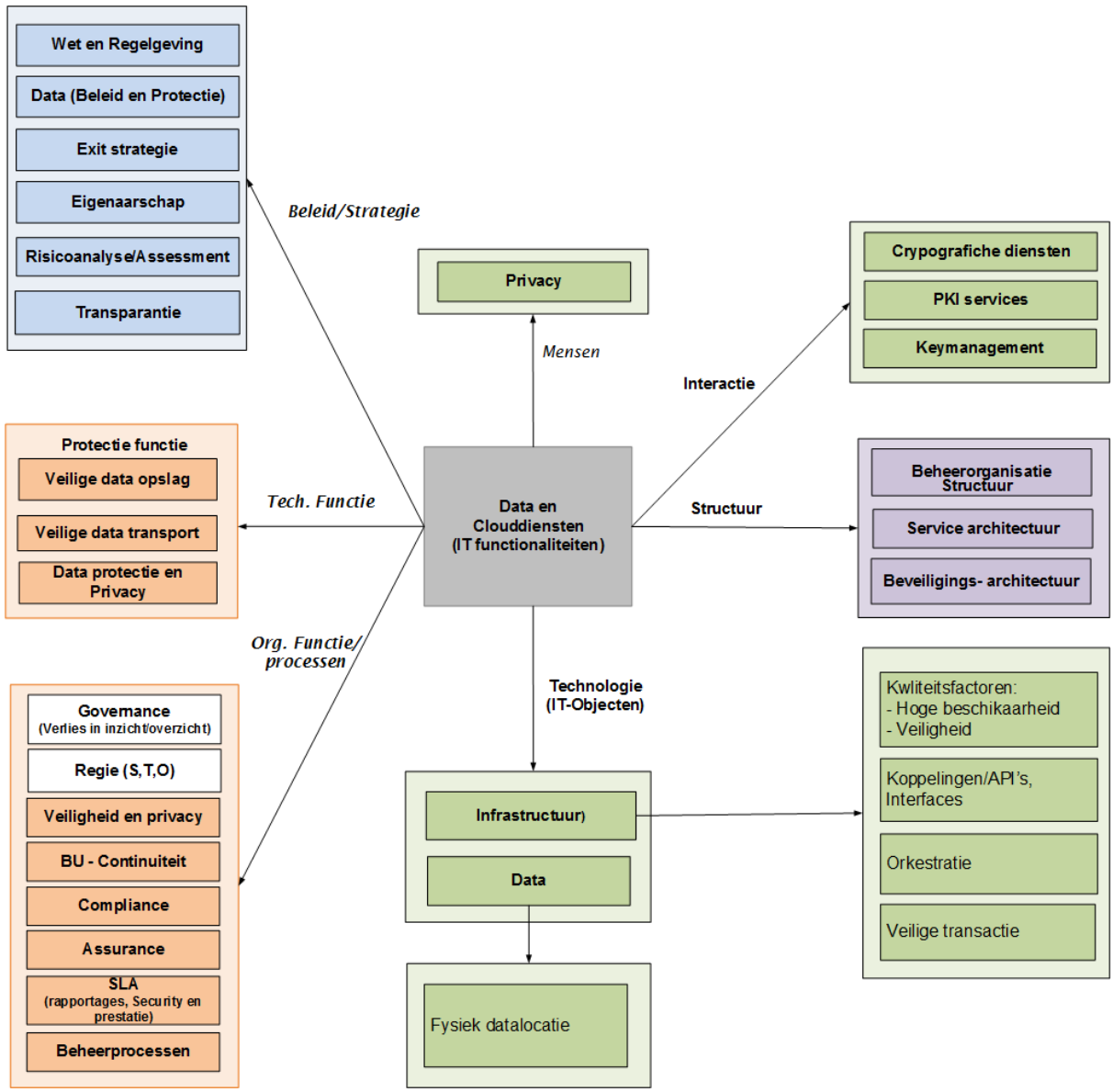
Afbeelding 5: Cloud-gerelateerde dreigingen en kwetsbaarheden

2.2 CSC-georiënteerde aandachtspunten

De schrijfgroep heeft voor clouddiensten diverse gesprekken gevoerd met CSC's en CSP's. Ook heeft de schrijfgroep verschillende beleidsdocumenten ontvangen van CSC's. Bij de besprekingen en het bestuderen van de documenten staan 2 vragen centraal:

1. Welke issues voor clouddiensten spelen een rol bij CSC's?
2. Waar maken CSC's zich de meeste zorgen over bij het verwerven van clouddiensten?

De geïdentificeerde issues zijn globaal onderverdeeld in een aantal generieke onderwerpen: beleid en strategie, processen/functies (technische en organisatorische), interacties, infrastructuur en structuur (architectuur en organisatiestructuur). Afbeelding 6 geeft een overzicht van de ingedeelde onderwerpen.



Afbeelding 6: CSC-georiënteerde aandachtspunten

2.3 Beveiligingsobjecten voor clouddiensten

Objecten worden geïdentificeerd met onderzoeksvragen en risicogebieden. De objecten hebben tot doel risico's te mitigeren. Ze zijn afgeleid van de algemene beveiligingseisen: beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid die vervolgens zijn ingedeeld in het beleids-, uitvoerings- en control-domein. De vragen die vanuit de optiek van deze domeinen hierbij spelen zijn:

- Welke randvoorwaardelijke elementen spelen een rol bij de inrichting van de clouddiensten en wat is de consequentie van het ontbreken van een of meer van deze elementen?
- Welke elementen spelen een rol bij de inrichting van de clouddiensten en wat is de consequentie van het ontbreken van een of meer van deze elementen?
- Welke elementen spelen een rol bij de beheersing van de clouddiensten en wat is de consequentie van het ontbreken van één of meer van deze elementen?

Uit de contextuele analyse blijkt dat verschillende onderwerpen niet in de BIO voorkomen. Voor de onderwerpen, waarvoor de BIO geen control heeft geformuleerd, zijn controls uit andere baselines geadopteerd.

3 Beleidsdomein

3.1 Doelstelling

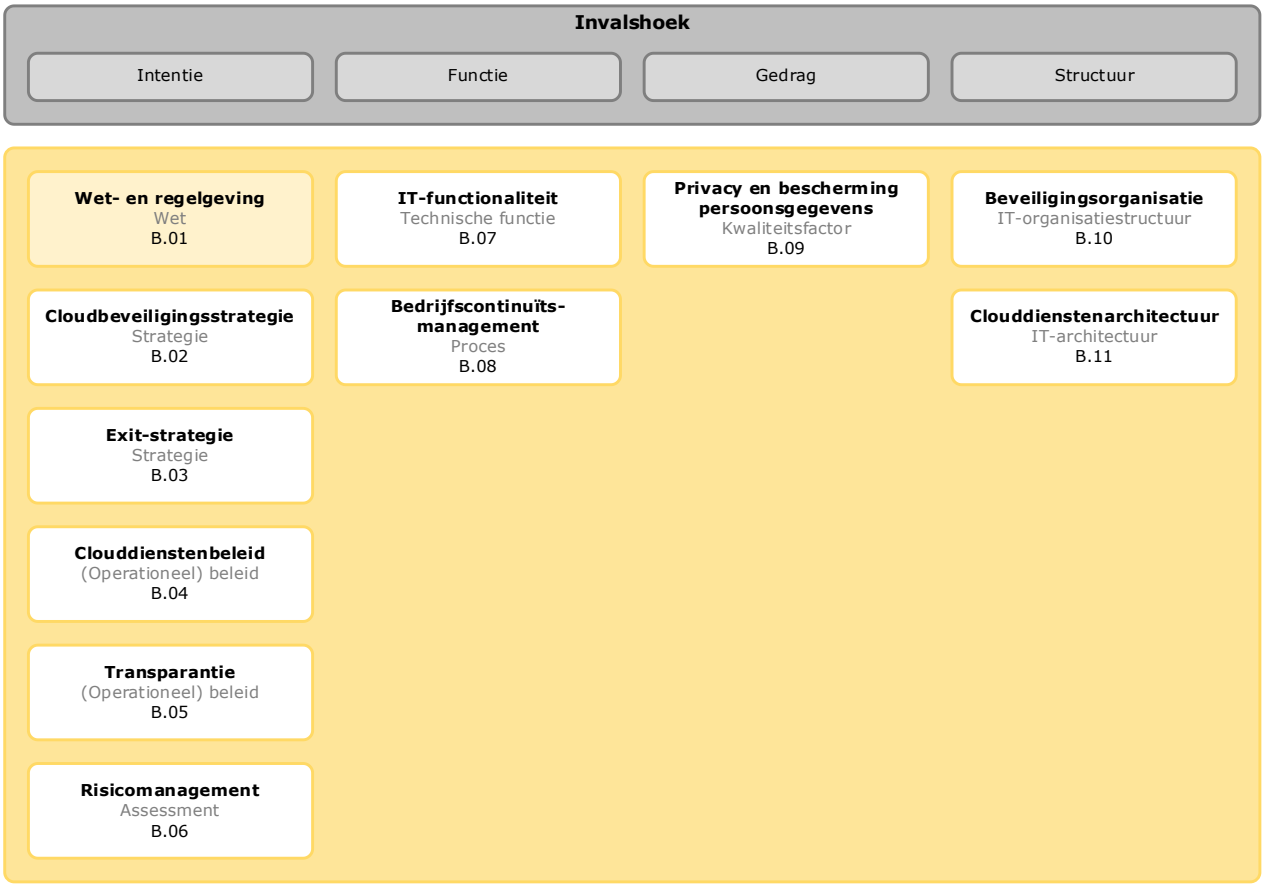
Het doel van het beleidsdomein is de conditionele elementen te identificeren die randvoorwaardelijk zijn om clouddiensten te kunnen inrichten, beveiligen en beheersen.

3.2 Risico's

Als de juiste beleidsaspecten voor de inrichting en het onderhoud van clouddiensten ontbreken, bestaat het risico dat onvoldoende sturing wordt gegeven aan een veilige inrichting en exploitatie van deze diensten. Daardoor komt de informatievoorziening van de organisatie als geheel in gevaar en bestaat er een reële kans dat datalekken optreden. In bijlage 2 Toelichting objecten in het beleidsdomein is per aandachtsgebied aangegeven welke risico's relevant zijn.

3.3 Objecten, controls en maatregelen

De onderwerpen die specifiek voor clouddiensten in het beleidsdomein een rol spelen, zijn in afbeelding 7 vermeld. Is een objectblok geel gekleurd, dan komt de bijbehorende control voor in de BIO. Betreft het een wit gemarkeerd objectblok, dan heeft de BIO geen control gedefinieerd, maar is dit object wel noodzakelijk voor deze BIO Thema-uitwerking.



Afbeelding 7: Overzicht objecten voor clouddiensten in het beleidsdomein

Per specifiek beveiligingsobject worden de control (hoofdnorm) en maatregelen (sub-normen) beschreven in de navolgende paragrafen.

3.3.1 B.01 Wet- en regelgeving

Objectdefinitie

Omvat de geldende nationale en internationale wetten en regelgeving die van toepassing is op clouddiensten.

Objecttoelichting

Nationale en internationale wet- en regelgeving die van toepassing is op clouddiensten, zoals vooral de AVG, heeft betrekking op de te nemen organisatorische en technische maatregelen, zoals bewustwording, mensen en fysieke middelen. De CSP zal deze vertalen naar specifieke eisen voor cloud-componenten.

Doelstelling	Het voorkomen van schendingen van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen en beveiligingseisen.		
Risico	Schade door wettelijke aansprakelijkheid.		
Control	Alle relevante **wettelijke, statutaire, regelgevende, contractuele eisen** en de **aanpak** van de CSP om aan deze eisen te voldoen behoren voor elke clouddienst en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.		BIO 2019: 18.1.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Wettelijke, statutaire, regelgevende eisen	1.	De CSP informeert de CSC welke wet- en regelgeving van toepassing is op clouddiensten.	ISO 27017 2015: 18.1.1
	2.	De CSP identificeert haar eigen relevante wettelijke eisen (zoals AVG-eisen en encryptietoepassing) om persoonsgegevens te kunnen beschermen.	ISO 27017 2015: 18.1.1
	3.	De voor de CSC van toepassing zijnde vereisten die voortvloeien uit wet- en regelgeving zijn geïdentificeerd, vooral waar het gaat om geografische gedistribueerde verwerkingen, opslag en communicatie waarvoor verschillende wetgeving bestaat, zoals maatregelen die voortvloeien uit de AVG.	ISO 27017 2015: 18.1.1
	4.	De CSP voorziet de CSC van zekerheid (op bewijs gebaseerde compliancy-rapportage) over (het voldoen aan) de van toepassing zijnde wettelijke eisen en contractuele vereisten.	ISO 27017 2015: 18.1.1
Contractuele eisen	5.	Voor clouddiensten zijn, om aan de wettelijke en contractuele eisen te kunnen voldoen, specifieke maatregelen getroffen en verantwoordelijkheden benoemd.	ISO 27002 2017: 18.1.1
Aanpak	6.	De CSP heeft, om aan de eisen van de CSC te kunnen voldoen, alle wet- en regelgeving die op haar van toepassing is op de clouddienstverlening vastgesteld.	ISO 27002 2017: 18.1.1

3.3.2 B.02 Cloudbeveiligingsstrategie

Objectdefinitie

Omvat het plan van handelen van de CSP waarmee zijn beveiligingsdoelstellingen voor de clouddienstenlevering kunnen worden gerealiseerd.

Objecttoelichting

Organisaties staan voor de vraag, welke clouddiensten ze moeten verwerven en waar en hoe ze deze veilig kunnen inzetten. Hiervoor moeten de IT-stakeholders van CSC's een beslissingsraamwerk ontwikkelen, waarmee systematisch de mogelijke scenario's kunnen worden onderzocht. Dit raamwerk richt zich met name op typen applicaties en technische karakteristieken. Een strategie omvat uitspraken over de doelstellingen bij de inzet van de clouddiensten die de organisatie wil nastreven en de wegen waarlangs of de wijze waarop dit moet plaatsvinden.

Om CSC's te kunnen bedienen, heeft de CSP vanuit haar eigen optiek een cloudbeveiligingsstrategie ontwikkeld. Deze strategie geeft de CSC's voldoende mogelijkheden om hun cloud-strategie te relateren aan de strategie van een specifieke CSP. Dit biedt de CSC de mogelijkheid om haar keuzes bij te stellen dan wel aanvullende eisen aan de CSP te stellen.

Doelstelling	Het vooraf vaststellen wat de CSC wil nastreven met de beveiliging van clouddiensten en hoe dat bereikt gaat worden.		
Risico	Het niet beschikken over een overeengekomen leidraad/globale manier van aanpak bij het beveiligen van clouddiensten.		
Control	De CSP behoort een **cloudbeveiligingsstrategie** te hebben ontwikkeld die **samenhangt** met de strategische doelstelling van de CSP en die aantoonbaar de informatieveiligheid ondersteunt.		SoGP 2018: SG2.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Cloud-beveiligings-strategie	1.	De cloudbeveiligingsstrategie van de CSP geeft aan op welke wijze zij de bedrijfsdoelstellingen van CSC('s) ondersteunt door onder andere te beschrijven: • een evenwichtige set van beveiligingsmaatregelen, waarin aandacht wordt besteed aan risicomanagement; • hoe (functioneel) cloud-beveiliging de weerbaarheid tegen hoge impactincidenten bewerkstelligt.	SoGP 2018: SG2.1.2
	2.	De cloudbeveiligingsstrategie van de CSP: • geeft onder andere aan hoe zij CSC's tegen bedreigingen beschermt; • besteedt aandacht aan de huidige beveiligingscontext van de CSP, inclusief vaardigheden, capaciteiten en informatiebeveiligingsfunctie.	SoGP 2018: SG2.1.3 SoGP 2018: SG2.1.6

Samenhangt	3.	De samenhang van beveiligingsmaatregelen van de CSP ondersteunt het behalen van de bedrijfsdoelen van de CSC. Hierin wordt aangegeven: • in welke mate de cloudbeveiligingsstrategie van de CSP in lijn is met de organisatiebrede doelstellingen van de CSC; • hoe de cloud-beveiligingsgovernance van de CSC wordt ondersteund door het management van de CSP; • dat de clouddiensten gedocumenteerd zijn en regelmatig worden gereviewd.	SoGP 2018: SG2.1.1

3.3.3 B.03 Exit-strategie

Objectdefinitie

Omvat het plan van handelen voor de beëindiging van de dienstverlening bij een bestaande CSP, alsmede het kunnen overzetten van data en IT-diensten naar een nieuwe CSP.

Objecttoelichting

Omdat geen enkel contract voor eeuwig is, moet een CSC op een zeker moment afscheid kunnen nemen van de CSP. Als bij het afsluiten van de clouddienst geen bindende afspraken zijn gemaakt over het afscheid nemen, kan het heel lastig of kostbaar worden om data te migreren naar een andere CSP.

De organisatie moet rekening houden met een 'vendor lock-in'. Het is daarom van belang, nog voor het aangaan van een overeenkomst met een CSP, een exit-strategie te ontwikkelen. De exit-strategie dient de voorwaarden voor mutaties van data te bevatten. Het is ook mogelijk de praktische uitwerking van de exit-strategie op te nemen in een Service Level Agreement (SLA).

Om verschillende redenen kan een CSC de dienstverlening van de CSP willen beëindigen. Enerzijds planmatig, zoals bij het einde van de contracttermijn, anderszins vanwege moverende redenen, zoals niet voldoen aan de afspraken, overname van de CSP door een andere organisatie. Het niet planmatig beëindigen is gerelateerd aan de exit-strategie, dat onderdeel is van bedrijfscontinuïteitsmanagement (BCM). Het planmatig beëindigen van de dienstverlening raakt de transitie en is onderdeel van Service Level Management (SLM).

Doelstelling	Het vooraf vaststellen wat de organisatie wil nastreven bij beëindiging van clouddiensten en hoe dat bereikt gaat worden.	
Risico	Het niet beschikken over een overeengekomen leidraad/globale manier van aanpak bij beëindiging van leverancierscontracten.	
Control	In de clouddienstenovereenkomst tussen de CSP en CSC behoort een exit-strategie te zijn opgenomen waarbij zowel een aantal **bepalingen**[6] over exit zijn opgenomen, als een aantal **condities6** die aanleiding kunnen geven tot een exit.	CIP-netwerk

[6] Weolcan: https://blog.weolcan.eu/wat-is-een-cloud-exit-strategie-precies-en-hoe-voer-je-het-uit.

Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
Bepalingen	1.	De CSC legt in de overeenkomst een aantal bepalingen over de exit-regeling vast, zoals: • De exit-bepaling geldt zowel bij het einde van de overeenkomst als om valide redenen aangedragen door de CSC (zie conformiteitsindicator Condities). • De overeenkomst (en eventuele verwerkersovereenkomst) duurt voort totdat de exit-regeling helemaal is uitgevoerd. • De opzegtermijn geeft voldoende tijd om te kunnen migreren. • Data en configuratiegegevens (indien relevant) mogen pas na succesvolle migratie verwijderd worden. • Door een onafhankelijke partij wordt gecontroleerd en vastgesteld dat alle data is gemigreerd. • De exit-regeling wordt aangepast/anders ingevuld als de software die gebruikt wordt voor de clouddienst is gewijzigd.	BSI C5 2020: PI-02

Condities	2.	De CSC kan buiten het verstrijken van de contractperiode besluiten over te gaan tot exit als sprake is van aspecten die gerelateerd zijn aan:
		• Contracten:
		  • niet beschikbaarheid zijn van afgesproken performance;
		  • eenzijdige wijziging door de CSP van de SLA;
		  • prijsverhoging.
		• Geleverde prestatie/ondersteuning:
		  • onvoldoende compensatie voor storingen;
		  • niet leveren van de afgesproken beschikbaarheid of performance;
		  • gebrekkige support.
		• Clouddienst(en):
		  • nieuwe eigenaar of nieuwe strategie;
		  • end-of-life van clouddienst(en);
		  • achterwege blijvende features.
			CIP-netwerk

3.3.4 B.04 Clouddienstenbeleid

Objectdefinitie

Omvat het resultaat van een besluitvorming over welke beveiligingsdoelen voor clouddiensten bereikt moeten worden.

Objecttoelichting

Het onderwerp clouddiensten moet een specifiek onderdeel zijn van het informatiebeveiligingsbeleid van de CSC. Een CSC kan ook kiezen voor een specifiek clouddienstenbeleid, waarbij in de informatiebeveiligingsparagraaf het algemene informatiebeveiligingsbeleid specifiek voor clouddiensten wordt uitgewerkt of ingevuld. Het beleid zal uitgangspunten moeten bevatten over de wijze waarop, binnen welk tijdsbestek en met welke middelen clouddiensten de doelstellingen moeten bereiken. In dit

beleid zal ook aandacht moeten worden besteed aan archiveringsbeleid, cryptografiebeleid, certificering en verklaringen.

Om de CSC te kunnen bedienen, zal de CSP vanuit haar eigen optiek een cloud-beveiligingsbeleid hebben ontwikkeld. Dit beleid geeft de CSC mogelijkheden om haar cloud-beleid te relateren aan de strategie van de CSP en biedt de CSC de mogelijkheid om de keuzes bij te stellen dan wel aanvullende eisen aan de CSP te stellen.

Doelstelling	Het beheersen van clouddiensten; dat clouddiensten bijdraagt aan het leveren van producten waarmee de organisatie haar doelstellingen kan realiseren.		
Risico	Onvoldoende mogelijkheid om sturing te geven aan inspanningen voor clouddiensten, waardoor deze niet of onvoldoende bijdragen aan de doelstellingen van de organisatie.		
Control	De CSP behoort haar informatiebeveiligingsbeleid uit te breiden met een **cloud-beveiligingsbeleid** om de voorzieningen en het gebruik van cloud-services te adresseren.		ISO 27017 2015: 5.1.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**

Cloud-beveiligings-beleid	1.	Het cloud-beveiligingsbeleid bevat:
		• Organische georiënteerde maatregelen:
		  • informatiebeveiligingsvereisten die van toepassing zijn bij het ontwerp en de implementatie van cloud-services;
		  • communicatie met de CSC in relatie tot en tijdens wijzigingen;
		  • communicatie van beveiligingsinbreuken en het delen van informatie;
		  • richtlijnen voor de ondersteuning van (forensische) onderzoeken;
		  • compliancy-maatregelen op wet- en regelgeving.
		• Technisch georiënteerde maatregelen:
		  • multi-tenancy en isolatie van de CSC;
		  • toegangsprocedures, bijvoorbeeld sterke authenticatie voor toegang tot cloud-services;
		  • toegang tot en protectie van de data van de CSC;
		  • levenscyclusmanagement van CSC-accounts;
		  • risico's gerelateerd aan niet geautoriseerde insiders;
		  • virtualisatie beveiliging;
		  • beveiligingsarchitectuur en -maatregelen voor het beschermen van data, applicaties en infrastructuur.
			ISO 27017 2015: 5.1.1

3.3.5 B.05 Transparantie

Objectdefinitie

Omvat de inzichtelijkheid van de relaties en samenhang van organisatie, technologie en contracten daarover tussen CSC en CSP.

Objecttoelichting

Een eenduidige communicatie, waarmee de CSP de verantwoordelijke functionarissen binnen de CSC en CSP inzicht geven over de status van de implementatie en het functioneren van de clouddiensten. Transparantie is in de relatie tussen de CSC en CSP een belangrijk item, dat wordt ondersteund door de clouddienstenarchitectuur. Hierin beschrijft de CSP de relaties tussen de componenten van de clouddiensten (hoe deze aan elkaar gekoppeld zijn). Het verschaft inzicht en overzicht over ICT-componenten en hun onderlinge samenhang. Uit de clouddienstenarchitectuur blijkt hoe de componenten de bedrijfsprocessen van de CSC ondersteunen.

Doelstelling	De verantwoordelijke functionarissen binnen de CSC en CSP inzicht geven over de status van de implementatie en het functioneren van clouddiensten.		
Risico	De CSP kan levert een dienstverlening die niet of onvolledig is afgestemd op de behoefte van de CSC.		
Control	De CSP voorziet de CSC in een **systeembeschrijving** waarin de clouddiensten inzichtelijk en transparant worden gespecificeerd en waarin de **jurisdictie**, **onderzoeksmogelijkheden** en **certificaten** worden geadresseerd.		BSI C5 2020: BC-01 BSI C5 2020: BC-05 BSI C5 2020: BC-06
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Systeem-beschrijving	1.	De systeembeschrijving bevat de volgende aspecten: • typen en scope van clouddiensten weergegeven met SLA's; • principes, procedures en maatregelen om ontwikkeling en operationalisering weer te geven; • beschrijving van de infrastructuurcomponenten die deel uitmaken van het ontwikkelen en operationaliseren van clouddiensten; • hoe met beveiligingsincidenten wordt omgegaan; • rollen en verantwoordelijkheden van de CSP en CSC, inclusief de verplichting om samen te werken; • (welke) onderdelen van de clouddiensten en/of functies toegekend of uitbesteed zijn aan sub-contractanten.	BSI C5 2020: 3.4.4.1
Jurisdictie	2.	De SLA of systeembeschrijving voorziet in een specificatie van jurisdictie over dataopslag, verwerking en back-up-locatie, ook als deze (of delen hiervan) uitbesteed is aan subcontractors.	BSI C5 2020: BC-01
Onderzoeks-mogelijkheden	3.	De SLA of systeembeschrijving voorziet in een specificatie voor publicatievereisten en onderzoeksmogelijkheden.	CIP-netwerk
Certificaten	4.	De SLA of systeembeschrijving voorziet in een specificatie over het beschikbaar zijn van valide certificaten.	BSI C5 2020: BC-06

3.3.6 B.06 Risicomanagement

Objectdefinitie

Betreft een besturingsproces voor een methodische aanpak van beveiligingsrisico's.

Objecttoelichting

Clouddiensten zijn voortdurend onderhevig aan dreigingen, zwakheden en risico's. Het is van belang om een risicomanagementproces in te richten en de verantwoordelijkheden hiervoor te benoemen, waarbij een risicomanagementaanpak(methode) en de te hanteren scope worden vastgesteld. Hierbij gaat het om het identificeren en kwantificeren van risico's voor clouddiensten en het vaststellen van beheersmaatregelen. Met beheersmaatregelen worden de activiteiten bedoeld waarmee de kans van optreden en/of de gevolgen van een incident worden beperkt.

Het risicomanagementproces maakt onderdeel uit van een Information Security Management Systeem (ISMS), zoals beschreven is in de ISO 27001 Managementsystemen voor informatiebeveiliging - Eisen en is uitgewerkt in de ISO 27005 Information security risk management.

Doelstelling	Om personen die verantwoordelijk zijn voor clouddiensten in staat te stellen effectief en tijdig belangrijke informatierisico's te identificeren, evalueren en de behandeling te bepalen nodig om deze risico's binnen aanvaardbare grenzen te houden.		
Risico	De getroffen beveiligingsmaatregelen liggen buiten de aanvaardbare grenzen. De clouddiensten worden onder- of overbeveiligd.		
Control	De CSP behoort de organisatie en **verantwoordelijkheden** voor het **risicomanagementproces** voor de beveiliging van clouddiensten te hebben opgezet en onderhouden.		ISO 27005 2018: 7.4
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Verantwoor-delijkheden	1.	De verantwoordelijkheden van de CSP zijn onder andere het: • ontwikkelen van het risicomanagementproces voor informatiebeveiliging dat toegespitst is op de omgeving van de CSP; • identificeren van analyses van de stakeholders; • definiëren van de rollen en verantwoordelijkheden van in- en externe partijen; • vaststellen van de vereiste relaties tussen de eigen organisatie en stakeholders en de relatie met de hoog niveau risicomanagementfunctie en met relevante projecten of activiteiten.	ISO 27005 2018: 7.4
	2.	De organisatie van het risicomanagementproces is goedgekeurd door managers van de CSP.	ISO 27005 2018: 7.4
Risicomanage-mentproces	3.	Het risicomanagementproces is systematisch beschreven met aandacht voor beleid, procedures en richtlijnen voor activiteiten over communiceren, adviseren, vaststellen van de context van onderzoeken, behandelen, monitoren, reviewen, vastleggen en rapporteren van risico's.	ISO 31000 2019: 6.1

3.3.7 B.07 IT-functionaliteit

Objectdefinitie

Omvat toepassingsfuncties die door clouddiensten worden geleverd.

Objecttoelichting

IT-diensten leveren functionaliteiten met technologie gerelateerd aan het internet. Voorbeelden van zulke diensten zijn: generieke diensten, zoals: applicatiediensten (SaaS), storagediensten, Cloud Virtual Private Server, infrastructuur, Global Positioning System (GPS) informatiedienst, maar ook specifieke diensten, zoals: GPS Douanediensten. Deze clouddiensten kunnen ook aan dreigingen worden blootgesteld. Vandaar dat deze IT-diensten aan de vereiste beveiligingsaspecten moeten voldoen.

Doelstelling	Zorgen dat IT-functionaliteiten aan de vereiste beveiligingsaspecten voldoen.		
Risico	IT-functionaliteiten zijn een zwakke schakel in de beveiliging.		
Control	**IT-functionaliteiten** behoren te worden verleend vanuit een **robuuste en beveiligde systeemketen** van de CSP naar de CSC.		SoGP 2018: BC1.3
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
IT-functionali-teiten	1.	Voor de beveiliging van IT-functionaliteiten (verwerking, opslag, transport en opvraag van informatie) zijn beschikbaarheids-, integriteits- en vertrouwelijkheidsmaatregelen getroffen.	CIP-netwerk
	2.	Technische beveiligingsmaatregelen in de vorm van sterke toegangsbeveiliging, encryptie en data-analysemethoden zijn getroffen tegen bescherming van de infrastructuur.	ITU-T FG Cloud TR Part 5 2012: 8.5
	3.	De IT-infrastructuur wordt, om veilige clouddiensten te kunnen verlenen, continue bewaakt en beheerst ter bescherming tegen bedreigingen.	ITU-T FG Cloud TR Part 5 2012: 8.8
Robuuste en beveiligde systeemketen	4.	De infrastructuur wordt ingericht met betrouwbare hardware- en softwarecomponenten.	SoGP 2018: BC1.3.1
	5.	Er zijn gedocumenteerde standaarden en procedures om geavanceerde cyberaanvallen het hoofd te bieden.	SoGP 2018: TM1.5.1

3.3.8 B.08 Bedrijfscontinuïteitsmanagement

Objectdefinitie

Betreft een besturingsproces voor activiteiten die organisaties beschermen tegen ontwrichtende gebeurtenissen.

Objecttoelichting

BCM beschrijft de eisen voor een managementsysteem om organisaties te beschermen tegen ontwrichtende gebeurtenissen, om de kans op deze gebeurtenissen te verkleinen en om te zorgen dat een organisatie daar volledig van kan herstellen. Hierbij zal de organisatie zich onder andere richten op ontwikkeling, implementatie en onderhoud van beleid, strategieën en programma's om de effecten van mogelijk ontwrichtende gebeurtenissen de organisatie te kunnen beheersen. In de cloud-omgeving vertrouwt de CSC, de CSP als derde partij. De CSP zal de CSC zekerheid moeten geven over documentatie over assets en resources, incidentmanagement, bedrijfscontinuïteit, herstelplannen, beleid, beheerprocessen en back-up-management.

Doelstelling	Het hervatten van kritieke bedrijfsprocessen binnen kritieke tijdschema's.		
Risico	Het niet effectief reageren op het manifest worden van omvangrijke storingen en (on)bekende risico's (ramp/noodsituaties). De bedreiging wordt niet zo snel als mogelijk gestopt en de gevolgschade wordt niet zo veel als mogelijk beperkt.		
Control	De CSP behoort haar BCM-proces adequaat te hebben georganiseerd, waarbij de volgende aspecten zijn geadresseerd: **verantwoordelijkheid voor BCM**, **beleid en procedures**, **bedrijfscontinuïteitsplanning**, **verificatie en updaten** en **computercentra**.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Verantwoordelijkheid voor BCM	1.	De CSP heeft een proceseigenaar voor het BCM-proces benoemd en hem verantwoordelijk gegeven voor het vormgeven van BCM en compliancy met het uitgestippeld beleid.	BSI C5 2020: BCM-01
	2.	De verantwoordelijke voor BCM stelt zeker dat adequate resources beschikbaar zijn voor het uitvoeren van een effectief BCM-proces.	BSI C5 2020: BCM-01
	3.	Het management van de CSP committeert zich aan de vastgestelde BCM-vereisten.	BSI C5 2020: BCM-01
	4.	Het BCM-beleid en beleid voor business impact analyses zijn vastgesteld en gecommuniceerd.	BSI C5 2020: BCM-02
Beleid en procedures	5.	Het beleid en de procedures voor het vaststellen van de impact van storingen van cloud-services zijn gedocumenteerd en gecommuniceerd, waarbij aandacht wordt besteed aan: • beschikbaarheid van data en functionaliteit in relatie tot vendor lock-in en transitie naar andere CSP's of exit-strategie (voor de mogelijke op risicoanalyse gebaseerde scenario's); • identificatie van kritische producten en services; • identificaties van afhankelijkheden, processen, en business partners en derde partijen; • consequenties van verstoringen; • schattingen van vereiste resources voor herstel.	BSI C5 2020: BCM-02
Bedrijfscontinuïteitsplanning	6.	De CSP beschikt over een gedocumenteerd raamwerk voor het plannen van bedrijfscontinuïteit waarin onder andere aandacht wordt besteed aan: • definiëren van de scope waarbij rekening wordt gehouden met de afhankelijkheden; • toegankelijkheid van deze plannen voor verantwoordelijke functionarissen; • toewijzen van een verantwoordelijke voor de review, update en goedkeuring; • definiëren van communicatiekanalen; • herstelprocedures; • methode voor het implementeren van het BCM-plan; • continu verbeteringsproces van het BCM-plan; • relaties met beveiligingsincidenten.	BSI C5 2020: BCM-03

Verificatie en updaten	7.	Business impact analyses en continuïteitsplannen worden geverifieerd, geactualiseerd en regelmatig getest.	BSI C5 2020: BCM-04
	8.	Bij het testen wordt aandacht besteed aan de beïnvloeding van CSC's (tenants) en derde partijen.	BSI C5 2020: BCM-04
Computer-centra	9.	De voorzieningen van de computercentra zijn veilig gesteld en worden gemonitord (bewaakt), onderhouden en regelmatig getest.	CIP-netwerk

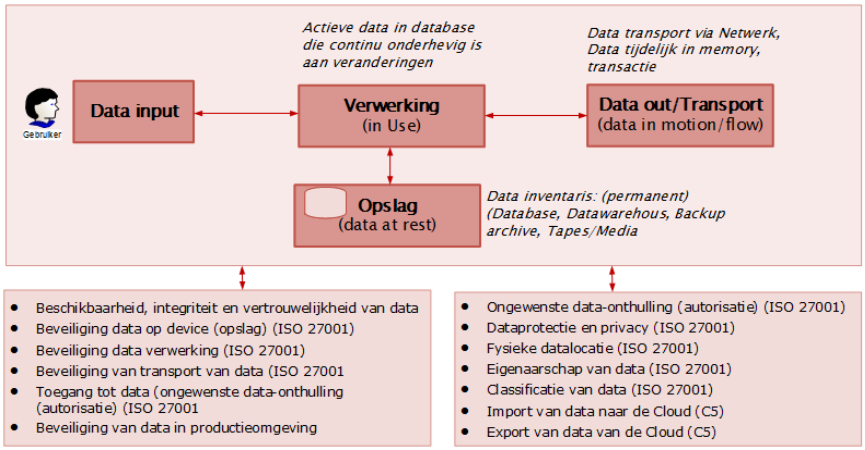
3.3.9 B.09 Privacy en bescherming persoonsgegevens

Objectdefinitie

Privacy betreft de persoonlijke vrijheid, het recht om alleen gelaten te worden. Bescherming persoonsgegevens betreft het proces van de bescherming van deze gegevens.

Objecttoelichting

De data waar dreigingen en privacybeschermende regels aan gerelateerd zijn. Zowel data- als privacybescherming moeten voldoen aan door de wettelijke en door de CSC gestelde eisen aan de beveiliging. Data en privacy omvat de inventarisatie en classificatie van gegevens volgens een specifiek labelingsbeleid. Databescherming vindt plaats in drie toestanden van data: in rust, in verwerking en op transport. Data in apparaten kan worden beheerst door te richten op drie momenten: verwijdering, vervoer en verplaatsing. Data kan gerelateerd worden aan bedrijfsgegevens en persoonsgegevens. Ter bescherming van persoonsgegevens worden de noodzakelijke maatregelen getroffen. Beveiliging van data kan vanuit verschillende aspecten worden benaderd. In afbeelding 8 worden de voornaamste aspecten benoemd.



Afbeelding 8: Data in verschillende bedrijfstoestanden

Doelstelling	Het verkrijgen van een gedegen set aan beveiligingsmaatregelen.
Risico	De bedrijfs- en persoonlijke data wordt onderbeveiligd.

Control	De CSP behoort, ter bescherming van bedrijfs- en persoonlijke data, beveiligingsmaatregelen te hebben getroffen vanuit verschillende dimensies: **beveiligingsaspecten en stadia**, **toegang en privacy**, **classificatie/labelen**, **eigenaarschap** en **locatie**.		ITU-T FG Cloud TR Part 5 2012: 8.5
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Beveiligings-aspecten en stadia	1.	Voor de opslag, de verwerking en het transport van data zijn beschikbaarheids-, integriteits- en vertrouwelijkheidsmaatregelen getroffen.	NIST CFW 2018: PR.DS-1 NIST CFW 2018: PR.DS-2
Toegang en privacy	2.	Ter bescherming van data en privacy zijn beveiligingsmaatregelen getroffen, in de vorm van data-analyse, DPIA, sterke toegangsbeveiliging en encryptie.	CIP-netwerk
Classificatie/ labelen	3.	Aan data en middelen waarin/waarop zich data bevindt, wordt door de verwerkingsverantwoordelijke een classificatie toegekend gebaseerd op het datatype, de waarde, de gevoeligheid en het kritische gehalte voor de organisatie.	CSA CCM 2019: DSI-01
	4.	Data gerelateerd aan e-commerce en verstuurd via publieke netwerken is adequaat geclassificeerd en beschermd tegen fraude, ongeautoriseerde toegang en aantasten/corrumperen van data.	CSA CCM 2019: DSI-03
	5.	De CSP past een uniforme classificatie toe voor informatie en middelen die relevant is voor de ontwikkeling en het aanbieden van clouddiensten.	BSI C5 2020: AM-06
Eigenaarschap	6.	Het eigenaarschap van middelen die deel uitmaken van clouddiensten is vastgesteld.	CIP-netwerk
	7.	In de overeenkomst tussen de CSP en de CSC is bij het beëindigen van de clouddienst het eigenaarschap vastgelegd rond het gebruik, het retourneren en het verwijderen van data (data objects) en de fysieke middelen die data bevatten.	ISO 19086-1 2016: 10.7.1.2
Locatie	8.	De CSP specificeert en documenteert op welke locatie (in welk land) de data worden opgeslagen.	ISO 27018 2020: A.12.1

3.3.10 B.10 Beveiligingsorganisatie

Objectdefinitie

Betreft een doelgerichte bundeling van kennis en vaardigheden tussen personen met taken, verantwoordelijkheden en bevoegdheden voor de relationele samenhang van beveiliging.

Objecttoelichting

De beveiligingsfunctie omvat de geformaliseerde taken en verantwoordelijkheden voor clouddiensten. Binnen de beveiligingsfunctie is geregeld dat contact wordt onderhouden met verantwoordelijken binnen de CSC-organisatie wanneer sprake is van beveiligingsincidenten.

De beveiligingsorganisatie van de CSP zorgt/ziet toe op het naleven van het informatiebeveiligingsbeleid, clouddienstenbeleid en overig hieraan gerelateerd beleid. Hoewel een

'Beveiligingsfunctie' als zelfstandig object beschouwd kan worden, is voor de eenvoud gekozen om deze in deze BIO Thema-uitwerking te integreren met de organisatie.

Waar nodig grijpt de beveiligingsorganisatie in. De taken, verantwoordelijkheden, bevoegdheden en middelen die de beveiligingsorganisatie hiervoor heeft zijn vooraf expliciet, in relatie tot de CSC, benoemd en vastgesteld. Ook moet vooraf vaststaan hoe de rapportagelijnen tussen de beveiligingsverantwoordelijken zijn georganiseerd.

Doelstelling	Om een gedefinieerde, goedgekeurde, begrepen en werkende structuur op te zetten voor de opzet, bestaan en werking beheer van informatiebeveiliging binnen de CSP.		
Risico	Het niet effectief tot uiting komen van het clouddienstenbeleid.		
Control	De CSP behoort een **beveiligingsfunctie** te hebben benoemd en een beveiligingsorganisatie te hebben ingericht, waarin de **organisatorische positie**, de **taken, verantwoordelijkheden en bevoegdheden** van de betrokken **functionarissen** en de **rapportagelijnen** zijn vastgesteld.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Beveiligings-functie	1.	De beveiligingsfunctie, die geleid wordt door een Chief Security Officer (CSO), ondersteunt de CSP voor het bewerkstelligen en promoten van het cloud-beveiligingsbeleid door het: • ontwikkelen en onderhouden van een beveiligingsstrategie en het -beleid; • ontwikkelen van beveiligingsstandaarden, procedures en richtlijnen; • definiëren van een set beveiligingsdiensten; • coördineren van beveiliging door de gehele organisatie; • monitoren van de effectiviteit van clouddienstreglementen; • bieden van overzicht van en het doen van onderzoeken naar beveiligingsdiensten.	SoGP 2018: SM2.1.2
	2.	De beveiligingsfunctie voorziet in proactieve ondersteuning van: • activiteiten van cloud-risicoassessment; • classificeren van informatie en systemen; • gebruik van encryptie; • beveiligen van gerelateerde projecten; • ontwikkelen van bedrijfscontinuïteitsprogramma en beveiligingsaudits.	SoGP 2018: SM2.1.4
Organisato-rische positie	3.	De CSP heeft de informatiebeveiligingsorganisatie een formele positie binnen de gehele organisatie gegeven.	CIP-netwerk
Taken, verant-woordelijk-heden en bevoegdheden	4.	De CSP heeft de verantwoordelijkheden bij informatiebeveiliging voor het definiëren, coördineren en evalueren beschreven en toegewezen aan specifieke functionarissen.	BIO 2019: 6.1.1
	5.	De taken, verantwoordelijkheden en bevoegdheden zijn vastgelegd in een autorisatiematrix.	CIP-netwerk

Functiona-rissen	6.	De belangrijkste functionarissen (stakeholders) voor informatiebeveiliging zijn benoemd en de onderlinge relaties zijn met een organisatieschema inzichtelijk gemaakt.	CIP-netwerk
Rapportage-lijnen	7.	De verantwoordings- en rapportagelijnen tussen de betrokken functionarissen zijn vastgesteld.	~trust services
	8.	Het type, de frequentie en de eisen voor de inhoudelijke rapportages zijn vastgesteld.	~trust services

3.3.11 B.11 Clouddienstenarchitectuur

Objectdefinitie

Betreft een modelmatige beschrijving van een technische en organisatorische samenhang, waarin de CSP de relaties tussen de onderdelen van de clouddiensten en de ondersteuning van de CSC vastlegt.

Objecttoelichting

In de clouddienstenarchitectuur legt de CSP vast hoe de IT-functionaliteiten aan elkaar gerelateerd zijn en hoe zij onderling samenhangen. Uit de clouddienstenarchitectuur wordt duidelijk hoe IT-functionaliteiten de bedrijfsprocessen van de CSC ondersteunen.

Doelstelling	Het bieden van een clouddienstenlandschap en daarmee richting geven aan de clouddienst en een betrouwbare werking van de clouddienst garanderen.		
Risico	Geen of onvoldoende sturing hebben op de clouddiensten. De werking van de clouddiensten is onbetrouwbaar.		
Control	De CSP heeft een actuele architectuur vastgelegd die voorziet in een **raamwerk** voor de onderlinge **samenhang en afhankelijkheden** van de IT-functionaliteiten.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Raamwerk	1.	Het raamwerk bevat de volgende aspecten: • beveiligingsbeleid van de CSP met principes en wet- en regelgeving; • functioneel; typen en scope van de clouddiensten; • zoneringsmodel voor scheiding tussen CSC's; • trust framework (afspraken en maatregelen ter bevordering van de vertrouwensrelatie); • SLA's en valide certificaten; • risicomanagement.	CIP-netwerk
Samenhang en afhanke-lijkheden	2.	De onderlinge samenhang tussen IT-functionaliteiten die bij het aanbieden, gebruiken en onderhouden van clouddiensten zijn betrokken, benoemd en beschreven.	NCSC 2015: B.06.05

4 Uitvoeringsdomein

4.1 Doelstelling

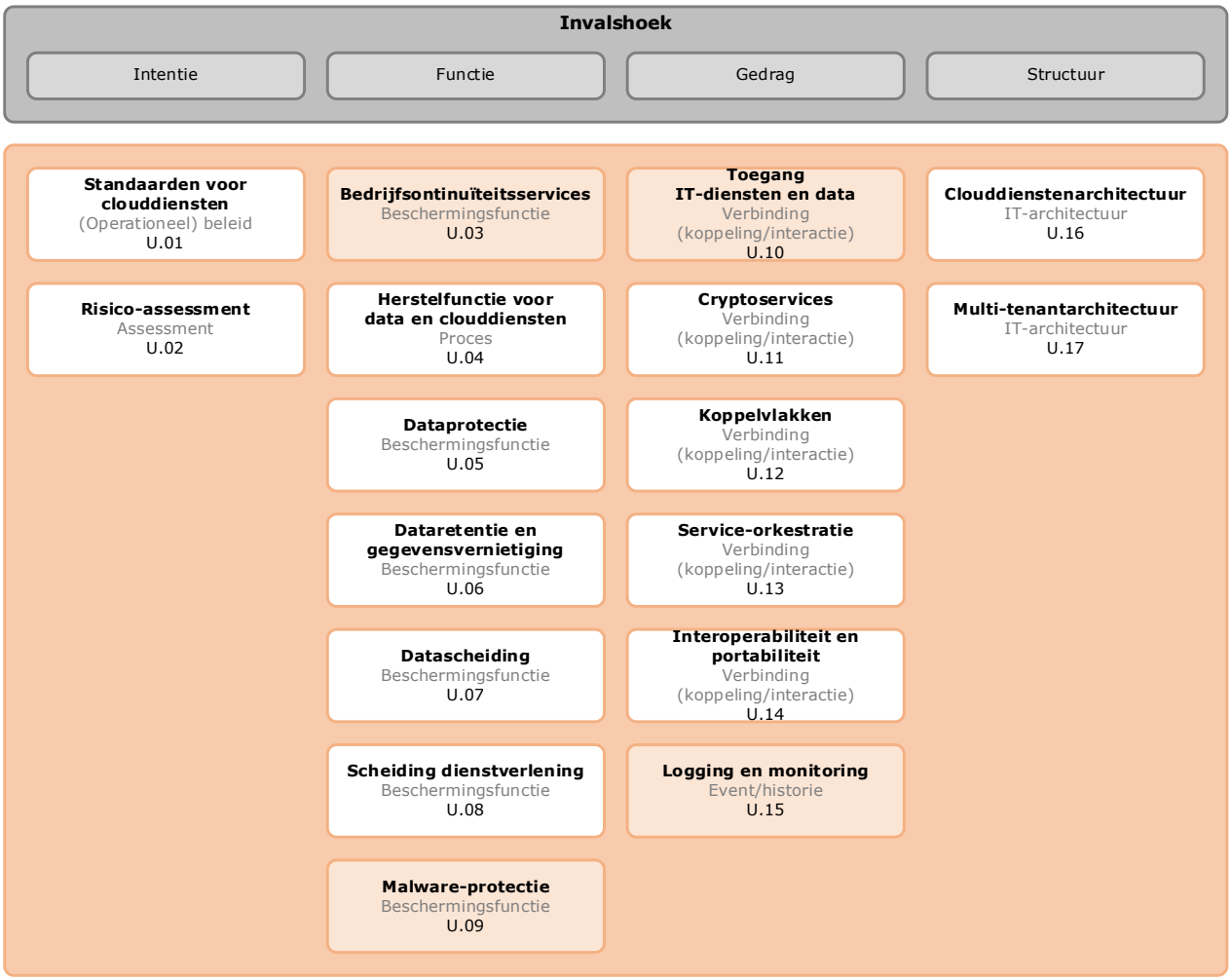
Het doel van het uitvoeringsdomein van clouddiensten is te waarborgen dat, overeenkomstig specifieke beleidsuitgangspunten, een betrouwbare en veilige dienstverlening geleverd wordt en dat de werking voldoet aan de eisen die door de CSC zijn gesteld.

4.2 Risico's

Als bij het aangaan of gedurende het toepassen van clouddiensten, adequate beveiligingsfuncties, het in de contracten benoemen van deze functies en de regie op naleving van de afspraken ontbreken, dan ontstaan continuïteitsrisico's en mogelijk datalekken of misbruik van gevoelige data. In bijlage 3 Toelichting objecten in het uitvoeringdomein is per aandachtsgebied aangegeven welke risico's relevant zijn.

4.3 Objecten, controls en maatregelen

Afbeelding 9 geeft de objecten weer die specifiek voor het uitvoeringsdomein een rol spelen. Is een objectblok oranje gekleurd, dan komt de bijbehorende control voor in de BIO. Betreft het een wit gemarkeerd objectblok, dan heeft de BIO geen control gedefinieerd, maar is dit object wel noodzakelijk voor deze BIO Thema-uitwerking.



Afbeelding 9: Overzicht objecten voor clouddiensten in het uitvoeringsdomein

4.3.1 U.01 Standaarden voor clouddiensten

Objectdefinitie

Omvat een set aan documenten met erkende afspraken, specificaties of criteria die de conditionering, inrichting en beheersing van clouddiensten ondersteunen.

Objecttoelichting

Het toepassen van (open) industrie-standaarden door CSP's, met name op het koppelvlak met de CSC, maakt het mogelijk dat data en IT-functionaliteiten, geboden via clouddiensten eenvoudiger, betrouwbaarder en veiliger geleverd kunnen worden aan de CSC. Dankzij deze standaarden kunnen IT-functionaliteiten en data, na een overeengekomen beëindiging van het contract tussen de CSC en de CSP, eenvoudig(er) worden overgedragen aan een nieuwe CSP.

Doelstelling	Het bewerkstelligen van de benodigde coördinatie van activiteiten voor de inrichting, dienstverlening en beheersing van clouddiensten.

Risico	Generieke risico's zijn niet of onvoldoende gemitigeerd.		
Control	De CSP past aantoonbaar relevante **nationale standaarden** en **internationale standaarden** toe voor de opzet en exploitatie van de diensten en de interactie met de CSC.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Nationale standaarden	1.	De CSP maakt haar dienstverlening transparant, zodat de CSC aantoonbaar aan de voor haar verplichte BIO en 'pas toe of leg uit'-standaarden kan voldoen.	CIP-netwerk
Internationale standaarden	2.	De CSP treft beveiligingsmaatregelen gebaseerd op internationale standaarden, zoals: • BSI-Standard 200-4 Business Continuity Management • ITU-T FG Cloud TR 1.0 2012 Part 5 Cloud security • NEN-ISO/IEC 17788 Overview and vocabulary • NEN-ISO/IEC 17789 Reference architecture • NEN-ISO/IEC 19941 Interoperability and portability • NEN-ISO/IEC 19944 Cloud services and devices • NEN-ISO/IEC 27017 Code of practice for cloud services • NEN-ISO/IEC 27018 Personally identifiable information (PII) in public clouds • NIST SP 800-145 Definition of Cloud Computing	ISO 27017 2015: 2.1

4.3.2 U.02 Risico-assessment

Objectdefinitie

Betreft een onderzoek naar de mogelijkheid dat een bepaald risico zich voordoet en naar de schadelijke effecten als het risico optreedt.

Objecttoelichting

Risico-assessment is een onderdeel van risicomanagement en omvat het onderkennen van dreigingen en kwetsbaarheden. Het risicomanagementproces maakt onderdeel uit van het managementsysteem voor informatiebeveiliging, zoals beschreven in de ISO 27001 'Managementsystemen voor informatiebeveiliging' en risicomanagement is uitgewerkt in de ISO 27005 'Information security risk management'.

Doelstelling	Een beeld krijgen van mogelijke risico's die van invloed kunnen zijn op clouddiensten en vaststellen op welke wijze de risico's beheerst kunnen worden of teruggebracht tot een aanvaardbaar niveau.	
Risico	Geen of onvoldoende zicht hebben op de risico's die van invloed zijn op clouddiensten.	
Control	De CSP behoort een risico-assessment uit te voeren, bestaande uit een **risico-analyse** en **risico-evaluatie** met de criteria en de doelstelling voor clouddiensten van de CSP.	ISO 27005 2018: 8.1
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Risico-analyse	1.	De risico's op de middelen die binnen de scope van clouddiensten ressorteren, worden geïdentificeerd, op waarde geschat (gekwantificeerd of gekwalificeerd) en beschreven met risico-evaluatiecriteria en -doelstellingen van de CSP.	ISO 27005 2018: 8.1
Risico-evaluatie	2.	De geïdentificeerde risico's worden geëvalueerd met risico-acceptatiecriteria.	ISO 27005 2018: 8.4

4.3.3 U.03 Bedrijfscontinuïteitsservices

Objectdefinitie

Omvat maatregelen, die tijdens normaal bedrijf en bij voorkomende calamiteiten, binnen de overeengekomen maximale uitvalduur, zorgen voor het herstel van de data en de dienstverlening, waarbij dataverlies wordt voorkomen.

Objecttoelichting

Omdat de CSC voor haar bedrijfsvoering sterk afhankelijk is van de CSP en van externe factoren zijn bedrijfscontinuïteitsservices van essentieel belang. Bedrijfscontinuïteitsservices omvatten het pakket van maatregelen, dat zowel voor normaal bedrijf (met Quality of Service (QoS)) als voor situaties van calamiteiten, zoals natuurrampen, binnen de overeengekomen maximale uitvalsduur Recovery Time Objective (RTO), zorgt voor het herstel van data en de kritische dienstverlening, waarbij dataverlies beperkt blijft tot het overeengekomen maximale dataverlies. Bekende continuïteitsmaatregelen zijn redundantie, disaster recovery en het periodiek aantonen dat herstelfuncties werken.

Doelstelling	Zorgen tijdens normaal bedrijf en bij voorkomende calamiteiten voor het herstel van de data en de dienstverlening binnen de overeengekomen maximale uitvalsduur, waarbij dataverlies wordt voorkomen.		
Risico	Data in de cloud is langer dan de overeengekomen maximale uitvalsduur niet beschikbaar.		
Control	Informatie verwerkende faciliteiten behoren met voldoende **redundantie** te worden geïmplementeerd om aan **continuïteitseisen** te voldoen.		BIO 2019: 17.2.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Redundantie	1.	De overeengekomen continuïteit wordt gewaarborgd door voldoende logisch of fysiek meervoudig uitgevoerde systeemfuncties.	ISO 27002 2017: 17.2.1
Continuïteits-eisen	2.	De met de CSC-organisatie overeengekomen continuïteitseisen voor cloud-services wordt gewaarborgd door specifieke in de systeemarchitectuur beschreven maatregelen.	ISO 27002 2017: 17.2.1

4.3.4 U.04 Herstelfunctie voor data en clouddiensten

Objectdefinitie

Betreft het herstellen van CSC-data en de dienstverlening na onderbrekingen of vernietiging van data en IT-middelen.

Objecttoelichting

Eén van de belangrijkste eisen voor de betrouwbaarheid van clouddienstverlening is de herstelbaarheid van de data en/of de dienstverlening na onderbreking of vernietiging van de data en bedrijfsmiddelen door storingen of calamiteiten: disaster recovery.

Doelstelling	Het zeker stellen dat clouddiensten en de data kan worden hersteld, binnen de overeengekomen periode, na onderbreking van de dienstverlening en/of vernietiging van de data.		
Risico	Overschrijden van het maximale dataverlies en/of uitvalsduur.		
Control	De **herstelfunctie** van de data en clouddiensten, gericht op ondersteuning van bedrijfsprocessen, behoort te worden gefaciliteerd met infrastructuur en IT-diensten, die robuust zijn en periodiek worden **getest**.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Herstelfunctie	1.	De data en clouddiensten worden in het geval van calamiteiten binnen de overeengekomen periode en maximale dataverlies hersteld en aan de CSC beschikbaar gesteld.	SoGP 2018: BC1.3.9
	2.	Het continue proces van herstelbaar beveiligen van data wordt gemonitord.	CIP-netwerk
Getest	3.	Het toereikend functioneren van herstelfuncties wordt periodiek getest door gekwalificeerd personeel en de resultaten daarvan worden gedeeld met de CSC.	BSI C5 2020: BCM-04

4.3.5 U.05 Dataprotectie

Objectdefinitie

Betreft het beschermen van de vertrouwelijkheid en integriteit van CSC-data.

Objecttoelichting

Data 'op transport' zijn bedrijfsgegevens die via de clouddienst, met de CSP worden uitgewisseld. Data 'in verwerking' betreft gegevens die worden bewerkt. Data 'in rust' betreft gegevens die voor korte of langere tijd zijn opgeslagen (bij de CSP). Aan deze drie situaties stelt de overheid strenge eisen.

Voor het toepassen van publieke clouddiensten geldt voor de Rijkdiensten dat een Secretaris Generaal vooraf toestemming verleent voor het in de publieke cloud verwerken van Basis BeveiligingsNiveau (BBN) 2-gerubriceerde informatie. Deze eis geldt ook voor persoonsgegevens.

Doelstelling	Het zorgen dat BBN2 of hoger classificeerde data beveiligd is met cryptografische maatregelen en voldoet aan de Nederlandse wetgeving.
Risico	Data met de classificatie BBN2 of hoger is onvoldoende beveiligd.

Control	Data ('op transport', 'in verwerking' en 'in rust') met de classificatie BBN2 of hoger behoort te worden beschermd met **cryptografische maatregelen** en te voldoen aan Nederlandse wetgeving.		ISO 27040 2016: 6.3.2.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Crypto-grafische maatregelen	1.	Gegevenstransport wordt naar de laatste stand der techniek beveiligd met cryptografie (conform Forum Standaardisatie), waarbij het sleutelbeheer zo mogelijk door de CSC zelf wordt uitgevoerd.	CIP-netwerk
	2.	Opgeslagen gegevens in de clouddienst worden naar de laatste stand der techniek beveiligd met encryptie en met een tenminste voor het doel toereikende sleutellengte, waarbij het sleutelbeheer zo mogelijk niet als clouddienst wordt afgenomen en door de CSC zelf wordt uitgevoerd.	CIP-netwerk

4.3.6 U.06 Dataretentie en gegevensvernietiging

Objectdefinitie

Omvat het bewaren en gecontroleerd wissen of vernietigen van CSC-data.

Objecttoelichting

Dataretentie betreft het duurzaam en technologieonafhankelijk opslaan en archiveren van data, waarbij de integriteit en leesbaarheid van de data gedurende de gehele bewaartijd niet wordt aangetast. (Persoons)gegevens moeten zodra ze niet meer benodigd zijn of aan het eind van de bewaartermijn worden gewist of vernietigd. Na de bewaarperiode moet de data teruggaan naar de CSC, naar een andere door de CSC te bepalen CSP of te worden gewist/vernietigd.

Doelstelling	Het beschikbaar blijven van gegevens indien nodig voor bijvoorbeeld verantwoording en indien gegevens niet meer archiefwaardig zijn, ze tijdig wissen/vernietigen.		
Risico	De beschikbaarheid en integriteit van de data wordt aangetast gedurende archivering en langer archiveren dan noodzakelijk.		
Control	Gearchiveerde data behoort gedurende de overeengekomen **bewaartermijn**, **technologie-onafhankelijk**, **raadpleegbaar**, **onveranderbaar** en integer te worden opgeslagen en op aanwijzing van de CSC/data-eigenaar te kunnen worden **vernietigd**.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Bewaartermijn	1.	De gegarandeerde en met de CSP overeengekomen opslagduur is contractueel vastgelegd en voldoet aan de Archiefwet.	ISO 27040 2016: 6.7.1
Technologie-onafhankelijk raadpleegbaar	2.	Gegevens zijn onafhankelijk van de door de CSP toegepaste technologie raadpleegbaar tijdens de gehele bewaartermijn.	ISO 27040 2016: 6.7.1
Onverander-baar	3.	Gegevens worden zo mogelijk gearchiveerd met Write Once Read Many (WORM)-technologie, waarmee de integriteit van de data wordt gegarandeerd.	ISO 27040 2016: 6.7.1

Vernietigd	4.	Voorafgaand aan het voor onderhoudsdoeleinden wijzigen van opslagmedia, wordt de data van de CSC, inclusief de back-up van gegevens en metadata veilig gewist of vernietigd.	ISO 27040 2016: 6.7.1
	5.	Bij het beëindigen van de contractrelatie wordt de data van de CSC, inclusief de back-up van gegevens en de metadata veilig gewist, om te voorkomen dat de CSC-gegevens naderhand door de CSP kunnen worden hersteld, bijvoorbeeld met forensische hulpmiddelen.	ISO 27040 2016: 6.7.1

4.3.7 U.07 Datascheiding

Objectdefinitie

Betreft het duurzaam isoleren van CSC-data van andere CSC's.

Objecttoelichting

Het isoleren van data (in bewerking of in rust) van de CSC, van alle data van de CSP en van de data van andere CSC's. Duurzame scheiding van CSC-data en van de data van andere bedrijven (secure multi-tenancy), zowel tijdens transport, in bewerking als opslag, is randvoorwaardelijk voor het afnemen van veilige clouddiensten.

Doelstelling	Zorgen dat de data van of in beheer van de CSC alleen toegankelijk is voor deze CSC.		
Risico	Andere CSC's en de CSP krijgen toegang tot de data of in beheer van de CSP en vice versa.		
Control	CSC-gegevens behoren tijdens transport, bewerking en opslag duurzaam **geïsoleerd** te zijn van **beheerfuncties** en data van en andere dienstverlening aan andere CSC's, die de CSP in beheer heeft.		ISO 27040 2016: 7.7.4
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Geïsoleerd	1.	Permanente isolatie van gegevens wordt gerealiseerd binnen een multi-tenantarchitectuur. Patches en aanpassingen van applicaties en infrastructuur worden op een gecontroleerde wijze gerealiseerd voor alle clouddiensten die de CSC afneemt.	CIP-netwerk
	2.	Isolatie van CSC-gegevens wordt gegarandeerd door deze onder alle bedrijfsomstandigheden minimaal logisch te scheiden van de data van andere CSC's.	CIP-netwerk
Beheerfuncties	3.	De bevoegdheden voor het inzien of wijzigen van CSC-data en/of van encryptiesleutels door beheerfuncties en beheerders worden gecontroleerd verleend en het gebruik van deze rechten wordt gelogd.	CIP-netwerk

4.3.8 U.08 Scheiding dienstverlening

Objectdefinitie

Betreft het door de CSP duurzaam isoleren van de te verrichten diensten tussen de verschillende CSC's en tussen CSC's en de CSP.

Objecttoelichting

Het isoleren van diensten/services van/voor de CSC, van alle diensten/services die niet voor die specifieke dienstverlening benodigd zijn, zoals die van/voor andere CSC's. De dienstverlening, die specifiek aan een bepaalde CSC wordt geleverd, is gescheiden van diensten die de CSP levert aan andere CSC's en is gescheiden van de interne informatievoorziening van de CSP. Ongewenste beïnvloeding of communicatie waardoor datalekken kunnen ontstaan, moet worden voorkomen.

Doelstelling	Het voorkomen van ongewenste beïnvloeding of communicatie van data tussen de CSC en CSP en andere CSC's.		
Risico	Beïnvloeding of communicatie van data.		
Control	De cloud-infrastructuur is zodanig ingericht dat de dienstverlening aan gebruikers van informatiediensten zijn **gescheiden**.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Gescheiden	1.	De CSP realiseert de volgende scheiding van clouddienstverlening: • onderlinge scheiding van de CSC's in een multi-tenant-omgeving; • scheiding tussen de afgenomen cloud-service en de interne informatievoorziening van de CSP; • de CSP maakt het mogelijk om de beoogde scheiding van clouddiensten te verifiëren.	CIP-netwerk

4.3.9 U.09 Malwareprotectie

Objectdefinitie

Omvat het continu beschermen van CSC-data tegen schadelijke software.

Objecttoelichting

Data in de informatieketen van de CSC en CSP wordt continu beschermd tegen malware, zoals virussen. Bij uitbesteding zal de CSP bescherming tegen malware toepassen, ook op de virtuele machines.

Doelstelling	Het zorgen dat informatie in de keten van de CSC en CSP continue beschermd wordt tegen malware.		
Risico	Malware wordt niet of te laat opgespoord en aangetroffen malware wordt niet of voldoende hersteld.		
Control	Ter bescherming tegen malware behoren **beheersmaatregelen** te worden geïmplementeerd voor **detectie, preventie en herstel** in combinatie met een passend bewustzijn van de gebruikers.		BIO 2019: 12.2.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Beheers-maatregelen	1.	De CSP specificeert, als onderdeel van de overeenkomst, welke maatregelen (voor onder andere malwareprotectie) op welke positie in de informatieketen van de CSC en CSP moeten worden genomen.	ISO 27017 2015: 15.1.2

	2.	De CSP heeft de voor ontwikkeling en exploitatie van clouddiensten gebruikte IT-systemen en netwerkperimeters waarvoor zij verantwoordelijk is, uitgerust met tools ter bescherming en verwijdering van malware.	CIP-netwerk
Detectie, preventie en herstel	3.	De malwareprotectie wordt op verschillende omgevingen uitgevoerd, zoals op mailservers, (desktop)computers en bij de toegang tot het netwerk van de organisatie. De scan op malware omvat onder andere: • alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, nog voor het gebruik; • alle bijlagen en downloads nog voor het gebruik; • virtuele machines; • netwerkverkeer.	BIO 2019: 12.2.1.5 ISO 27002 2017: 12.2.1g.1 en 2

4.3.10 U.10 Toegang IT-diensten en data

Objectdefinitie

Omvat processen en middelen voor het toekennen en bewaken van toegangsrechten tot CSC-data en bedrijfsprocessen.

Objecttoelichting

Toegang tot data en bedrijfsprocessen van alle mogelijke gebruikers zowel de CSC als de CSP wordt uitsluitend met identificatie, authenticatie en autorisatie verstrekt. NB De toegangsverlening heeft een directe relatie met het 'Bring Your Own Device' (BYOD)-beleid van een organisatie.

Doelstelling	Onbevoegde toegang tot bedrijfsprocessen/data in clouddiensten voorkomen.		
Risico	Misbruik en verlies van (gevoelige) gegevens.		
Control	**Gebruikers** behoren alleen toegang te krijgen tot IT-diensten en data waarvoor zij specifiek **bevoegd** zijn.		BIO 2019: 9.1.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Gebruikers	1.	De CSP biedt de CSC uitsluitend toegang tot services, IT-diensten en data waarvoor zij specifiek bevoegd is, waarbij: • Technische maatregelen voorkomen dat gebruikers en beheerders toegang hebben tot services, IT-diensten en data buiten datgene wat formeel is toegestaan. • Gebruikers met nood-toegangsrechten (tijdens calamiteiten, wanneer acties niet door bevoegde beheerders kunnen worden uitgevoerd) zijn gedocumenteerd door het management, geaccordeerd en wordt uitgevoerd met functiescheiding. Noodtoegang is geactiveerd zolang als nodig is voor de corresponderende taak/taken.	CIP-netwerk

	2.	Onder verantwoordelijkheid van de CSP wordt aan beheerders toegang verleend: • tot data met het least privilege-principe; • tot data met het need-to-know-principe; • met multi-factorauthenticatie; • tot data en applicatieve functies via technische maatregelen.	CIP-netwerk
	3.	Alleen gebruikers met geauthentiseerde apparatuur kunnen toegang krijgen tot IT-diensten en data.	BIO 2019: 9.1.2.1
Bevoegd	4.	Onder de verantwoordelijkheid van de CSP worden bevoegdheden (systeemautorisaties) voor gebruikers toegekend via formele procedures.	BSI C5 2020: IDM-03
	5.	Toegang tot IT-diensten en data is beperkt door technische maatregelen en is geïmplementeerd, bijvoorbeeld met het rollen- en rechtenconcept.	CIP-netwerk

4.3.11 U.11 Cryptoservices[7]

Objectdefinitie

Omvat technische functies voor het versleutelen en ontsleutelen van data, het maken van elektronische handtekeningen en het kunnen toepassen van versterkte authenticatie.

Objecttoelichting

De technische functies voor versleuteling en ontsleuteling van data, elektronische handtekening en versterkte authenticatie, al dan niet via Public-Key-Infrastructure (PKI)-technologie. Sleutelbeheer is een onderdeel van cryptoservices. Desgewenst kan de CSC in haar Programma van Eisen (PvE), de crypto-eisen van het Nationaal Bureau Verbindingsbeveiliging (NBV) specificeren.

Doelstelling	Het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van gevoelige data tijdens transport via netwerken en opslag.	
Risico	Gegevens zijn tijdens transport via netwerken en opslag te benaderen voor onbevoegden.	
Control	Gevoelige data van de CSC behoort conform het overeengekomen **beleid** inzake **cryptografische maatregelen** tijdens transport via netwerken en bij opslag bij CSP te zijn **versleuteld**.	CIP-netwerk
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

[7] Er volgt een object 'Cryptobeleid' waarin beleidsmaatregelen over cryptoservices is opgenomen AP WTJV.

Beleid	1.	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: • wanneer cryptografie ingezet wordt; • wie verantwoordelijk is voor de implementatie van cryptologie; • wie verantwoordelijk is voor het sleutelbeheer; • welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum Standaardisatie worden toegepast; • de wijze waarop het beschermingsniveau vastgesteld wordt; • bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.	BIO 2019: 10.1.1.1
Crypto-grafische maatregelen	2.	In geval van PKIoverheid-certificaten: hanteer de PKIoverheid-eisen ten aanzien van het sleutelbeheer. In overige situaties: hanteer de standaard ISO 11770 voor het beheer van cryptografische sleutels.	BIO 2019: 10.1.2.1
Versleuteld	3.	Gevoelige data (op transport en in rust) is altijd versleuteld, waarbij private sleutels in beheer zijn bij de CSC. Het gebruik van een private sleutel door de CSP is gebaseerd op een gecontroleerde procedure en moet gezamenlijk worden overeengekomen met de CSC-organisatie.	BSI C5 2020: CRY-03

4.3.12 U.12 Koppelvlakken

Objectdefinitie

Betreft connecties op grensvlakken in de keten tussen CSC en CSP.

Objecttoelichting

Een koppelvlak is de organisatorische of technische connectie op het grensvlak in de keten van de CSC en de CSP. Deze BIO Thema-uitwerking beperkt zich tot de technische connectie. Het beperken van het aantal koppelvlakken vereist de nodige aandacht en toezicht om risico's van dataverlies te beperken. Beheersing van het aantal koppelvlakken is dus noodzakelijk om risico's van dataverlies te beperken. Stelsels van koppelvlakken valt onder de ISO 270xx-categorie Netwerkdiensten.

Doelstelling	Het bewaken en beheersen van koppelvlakken in de keten van de CSP en de CSC.		
Risico	Data van of in beheer van de CSP komt via de koppelvlakken in handen van de CSP.		
Control	De onderlinge **netwerkconnecties** (koppelvlakken) in de keten van de CSC naar de CSP behoren te worden **bewaakt** en **beheerst** om de risico's van datalekken te beperken.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Netwerkcon-necties	1.	In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijvoorbeeld Distributed Denial of Service attacks (DDos)-aanvallen) te signaleren en hierop te reageren.	BIO 2019: 13.1.2.4

	2.	Fysieke en gevirtualiseerde netwerkcomponenten zijn zodanig ontworpen en geconfigureerd dat netwerkconnecties tussen vertrouwde en onvertrouwde netwerken worden beperkt en gemonitord (bewaakt).	CIP-netwerk
	3.	Beheeractiviteiten van de CSP zijn strikt gescheiden van de data van de CSC.	CIP-netwerk
	4.	Dataverkeer voor CSC's zijn in gezamenlijk gebruikte netwerkomgevingen gescheiden volgens een gedocumenteerd concept voor de op netwerkniveau (logische) segmentatie van CSC's, om zo de integriteit en vertrouwelijkheid van de verzonden gegevens te garanderen.	BSI C5 2020: COS-06
Bewaakt	5.	Het dataverkeer dat de CSP binnenkomt of uitgaat, wordt in relatie tot de aard van de te beschermen gegevens/informatiesystemen bewaakt en geanalyseerd op kwaadaardige elementen middels detectievoorzieningen.	BIO 2019: 13.1.2.1
	6.	De CSP heeft Intrusion Detection Prevention (IDP) en Intrusion Detection System (IDS) geïntegreerd in een allesomvattend Security Information and Event Management (SIEM), zodat beveiligingsgebeurtenissen en onbekende apparatuur vanuit de benodigde technische maatregelen worden opgemerkt en correctieve maatregelen kunnen worden genomen.	BSI C5 2020: COS-01
Beheerst	7.	Bij ontdekte nieuwe dreigingen worden deze, rekening houdend met geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale Computer Emergency Response Team (CERT), bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing).	BIO 2019: 13.1.2.2

4.3.13 U.13 Service-orkestratie

Objectdefinitie

Betreft het arrangeren, beoordelen en bijsturen door de CSC van de set van diensten die door een CSP worden geleverd.

Objecttoelichting

De CSP orkestreert de clouddiensten. Dat wil zeggen, dat zij de clouddiensten arrangeert (beoordeelt en bijstuurt) en dat de informatie met standaard berichten uitgewisseld kan worden tussen de clouddiensten van de CSP en de CSC's, zodat de kwaliteit van de te leveren clouddienst aan de CSC overeenkomt met de overeengekomen QoS, informatieveiligheid en kosten.

Doelstelling	De kwaliteit van de te leveren clouddienst aan de CSC komt overeen met de overeengekomen QoS, informatieveiligheid en kosten.
Risico	Niet of onvoldoende coördinatie, aggregatie en samenstelling van de servicecomponenten van de cloud-service.

Control	Service-orkestratie biedt **coördinatie**, aggregatie en samenstelling van de **servicecomponenten** van de cloud-service die aan de CSC wordt geleverd.		ISO 17789 2014: 9.2.3.4
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Coördinatie	1.	Cloud-orkestratietechnologie functioneert met heterogene systemen en mogelijk wereldwijde cloud-implementatie (op verschillende geografische locaties en met verschillende CSP's).	CIP-netwerk
Service-componenten	2.	De functionele samenhang van de servicecomponenten is beschreven.	CIP-netwerk
	3.	Voor orkestratie van cloud-services is de volgende informatie benodigd: • de CSC-identiteit; • de bedrijfsrelatie van de CSC binnen het cloud-netwerk; • het IP-adres van de CSC.	ITU-T: FG Cloud TR 1.0 Part 5 Cloud security 2012: II.2.3

4.3.14 U.14 Interoperabiliteit en portabiliteit

Objectdefinitie

Betreft het zonder bijzondere hulpmiddelen of aanpassingen met andere organisaties en systemen kunnen laten functioneren van diensten en uitwisselen van gegevens.

Objecttoelichting

Om het risico van vendor lock-in en afhankelijkheden van externe IT-voorzieningen te voorkomen, moet de CSP in dialoog met de CSC erop toezien, dat clouddiensten zodanig zijn ingericht, dat deze interoperabel zijn en dat de dataset van de CSC overdraagbaar is, zonder dat daarvoor bijzonder kostbare of complexe hulpmiddelen of bewerkelijke aanpassingen per clouddienst nodig zijn.

Doelstelling	Het zorgen dat cloud-services bruikbaar zijn op verschillende IT-platforms en data makkelijk kan worden doorgegeven aan een andere CSP zonder dat de integriteit en vertrouwelijkheid wordt aangetast.		
Risico	Cloudservices zijn niet toe te passen op andere IT-platforms en data kan niet naar een andere CSP worden overgedragen.		
Control	Cloud-services zijn bruikbaar (**interoperabiliteit**) op verschillende IT-platforms en kunnen met standaarden verschillende IT-platforms met elkaar verbinden en data overdragen (**portabiliteit**) naar andere CSP's.		BSI C5 2020: COS-02 ISO 19941 2017: 7.1.7
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Interoperabili-teit	1.	Om de interoperabiliteit van cloud-services te garanderen, zijn gegevens beschikbaar conform erkende industrie-standaarden en gedocumenteerde invoer- en uitvoerinterfaces.	BSI C5 2020: PI-01
Portabiliteit	2.	Om de portabiliteit van de data te garanderen, maakt de CSP gebruik van beveiligde netwerkprotocollen voor de import en export van data waarmee de integriteit en vertrouwelijkheid wordt gegarandeerd.	BSI C5 2020: PI-01

4.3.15 U.15 Logging en monitoring

Objectdefinitie

Omvat het vastleggen van informatiebeveiligingsgerelateerde gebeurtenissen en het bewaken en onderkennen van afwijkingen op beleidsregels.

Objecttoelichting

De beoogde werking van IT-functies in de informatieketen behoort via logging en monitoring te worden bewaakt. Monitoring is gericht op het onderkennen van eventuele afwijkingen op beleidsregels en logging is gericht op het vastleggen van gebeurtenissen, als bewijslast en ter verbetering en/of herstel.

Doelstelling	Het tijdig detecteren en vastleggen van ongeoorloofde en/of onjuiste activiteiten van medewerkers en storingen van IT-functies in de informatieketen.		
Risico	Afwijkingen van normaal gedrag zijn niet zichtbaar en niet te onderzoeken en herstelacties kunnen niet tijdig worden genomen.		
Control	Logbestanden waarin **gebeurtenissen** die gebruikersactiviteiten, uitzonderingen en informatiebeveiliging gebeurtenissen worden **geregistreerd**, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.		BIO 2019: 12.4.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Gebeurtenis-sen geregistreerd	1.	Het overtreden van de beleidsregels wordt door de CSP en de CSC vastgelegd.	CIP-netwerk
	2.	De SIEM en/of Security Operation Centre (SOC) hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	BIO 2019: 12.4.1.5
	3.	De CSP hanteert een lijst van alle activa die kritisch zijn in termen van logging en monitoring en beoordeelt deze lijst regelmatig op correctheid.	CIP-netwerk
	4.	Aan logboeken en bewaking worden strenge eisen gesteld. Voor de kritieke componenten zijn geavanceerde beveiligingen voor logboeken en bewaking gedefinieerd.	CIP-netwerk
	5.	De toegang tot en het beheer van de loggings- en monitoringsfunctionaliteit is beperkt tot geselecteerde en geautoriseerde medewerkers van de CSP.	CIP-netwerk
	6.	Wijzigingen in logging en monitoring worden gecontroleerd door onafhankelijke en geautoriseerde medewerkers. (Logregels mogen nooit worden gewijzigd; deze zijn immers bedoeld om als bewijslast te kunnen gebruiken.)	CIP-netwerk

4.3.16 U.16 Clouddienstenarchitectuur

Objectdefinitie

Betreft een modelmatige beschrijving van een technische en organisatorische samenhang, waarin de CSP de relaties tussen de onderdelen van de clouddiensten en de ondersteuning van de CSC vastlegt.

Objecttoelichting

In de clouddienstenarchitectuur legt de CSP de functionele relaties vast tussen IT-componenten in de gehele keten van de CSC en de CSP. Deze architectuur beschrijft hoe de IT-componenten moeten worden ingericht zodat ze de bedrijfsprocessen van de CSC ondersteunen.

Doelstelling	Het bieden van een cloud-landschap ter ondersteuning van de CSC-bedrijfsprocessen dat in samenhang is beveiligd en inzicht geeft in de inrichting daarvan.		
Risico	Geen of onvoldoende sturing hebben op clouddiensten.		
Control	De clouddienstenarchitectuur specificeert de **samenhang** en beveiliging van de services en de interconnectie tussen de CSC en de CSP en biedt transparantie en overzicht van randvoorwaardelijke omgevingsparameters, voor zowel de opzet, de levering en de portabiliteit van CSC-data.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Samenhang	1.	De architectuur specificeert ten minste het volgende: • IT-services in relatie met functionaliteit voor bedrijfsprocessen; • het vertrouwensniveau van de beveiliging van de clouddiensten; • de beschrijving van de infrastructuur, netwerk- en systeemcomponenten die worden gebruikt voor de ontwikkeling en de werking van de cloud-service(s); • rollen en verantwoordelijkheden van de CSP en de CSC, inclusief de plichten om samen te werken en de bijbehorende controles bij de CSC; • IT-functies die door de CSP zijn toegewezen of uitbesteed aan onderaannemers.	CIP-netwerk

4.3.17 U.17 Multi-tenantarchitectuur

Objectdefinitie

Betreft een specificatie waarin een CSP de onderlinge relaties van CSC's en de duurzame scheiding tussen de CSC's van clouddiensten beschrijft.

Objecttoelichting

Het stelsel van op gemeenschappelijke infrastructuur aangeboden clouddiensten, waarbij CSC's door een strikte (logisch en/of fysieke) scheiding van data en dienstverlening, elkaars gegevens nooit kunnen lezen of kunnen beïnvloeden. CSC's mogen geen hinder ondervinden van piekbelastingen vanuit andere organisaties (andere CSC's en/of CSP).

Doelstelling	Het bieden van een multi-tenantlandschap dat in samenhang is beveiligd en inzicht geeft in de inrichting daarvan.		
Risico	Geen of onvoldoende sturing hebben.		
Control	Bij multi-tenancy wordt de CSC-data binnen clouddiensten, die door meerdere CSC's worden afgenomen, in rust **versleuteld** en **gescheiden** verwerkt op **gehardende** (virtuele) machines.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Versleuteld	1.	CSC-data op transport en in rust is versleuteld.	ITU-T FG Cloud TR Part 5 2012: S12
Gescheiden	2.	Virtuele machine platforms voor CSC's met speciale/verhoogde beveiligingsvereisten zijn gescheiden ingericht.	ITU-T FG Cloud TR Part 5 2012: S12
Gehardende	3.	Virtuele machine platforms zijn gehardend.	ITU-T FG Cloud TR Part 5 2012: S12

5 Control-domein

5.1 Doelstelling

Het doel van het control-domein is om vast te stellen in hoeverre:

- controls voldoende zijn ingericht en functioneren om de beoogde beschikbaarheid, integriteit en vertrouwelijkheid van de clouddiensten te garanderen;
- infrastructurele diensten, functioneel en technisch, op het afgesproken niveau worden gehouden.

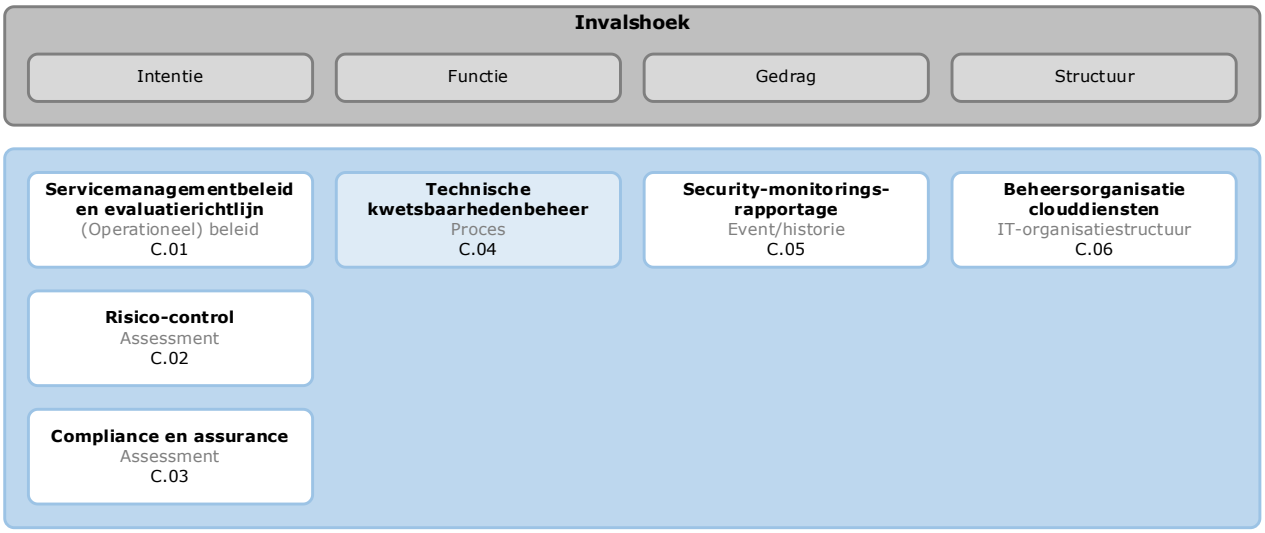
Dit houdt onder meer in dat binnen de CSP een adequate beheerorganisatie heeft ingericht, waarin de beheerprocessen zijn vormgegeven.

5.2 Risico's

Bij het ontbreken van de noodzakelijke maatregelen binnen de CSP is het niet zeker of de ontwikkeling en het onderhoud van de IT-componenten aan de beoogde organisatorische en beveiligingsvoorwaarden voldoet en dat de governance van de clouddiensten toereikend is ingericht. Ook kan niet worden vastgesteld of de gewenste maatregelen worden nageleefd. In bijlage 4 Toelichting objecten in het control-domein is per aandachtsgebied aangegeven welke risico's relevant zijn.

5.3 Objecten, controls en maatregelen

Afbeelding 10 geeft de onderwerpen weer die specifiek voor het control-domein een rol spelen. Is een objectblok blauw gekleurd, dan komt de bijbehorende control voor in de BIO. Betreft het een wit gemarkeerd objectblok, dan heeft de BIO geen control gedefinieerd, maar is dit object wel noodzakelijk voor deze BIO Thema-uitwerking.



Afbeelding 10: Overzicht objecten voor clouddiensten in het control-domein

De objecten, voor clouddiensten, die specifiek binnen het control-domein een rol spelen, zijn in onderstaande paragrafen uitgewerkt.

5.3.1 C.01 Servicemanagementbeleid en evaluatierichtlijn

Objectdefinitie

Betreft het resultaat van besluitvorming voor het inrichten van beheerprocessen en het systematisch ontwikkelde aanbevelingen voor het evalueren en uitvoeren van controle-activiteiten voor clouddiensten.

Objecttoelichting

Het servicemanagemetbeleid geeft richting aan de wijze waarop de beheerorganisatie voor clouddiensten moet zijn ingericht en de wijze waarop deze moet functioneren. Voor de ondersteuning van de specifieke beheerprocessen bestaan richtlijnen en procedures. De beheerorganisatiestructuur geeft de samenhang van de ingerichte processen weer.

Clouddiensten bestaan uit verschillende componenten en verschillende koppelvlakken. Het is van groot belang dat clouddiensten, vanwege risicomanagement, periodiek geëvalueerd worden. De evaluatie-activiteiten dienen ondersteund te worden met evaluatierichtlijnen, procedures en instructies, ter voorkoming van het risico dat de resultaten van de controle-activiteiten niet voldoen aan de gestelde eisen.

Doelstelling	Richting geven aan de wijze waarop de beheerorganisatie voor clouddiensten moet zijn ingericht en de wijze waarop deze moet functioneren.		
Risico	De resultaten van controle-activiteiten uitgevoerd op clouddiensten voldoet niet aan de gestelde eisen.		
Control	De CSP heeft voor clouddiensten een servicemanagementbeleid geformuleerd met daarin **richtlijnen** voor de beheersingsprocessen, **controle-activiteiten en rapportages**.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Richtlijnen	1.	De CSP beschikt voor clouddiensten over richtlijnen voor de inrichting van de service-managementorganisatie.	CIP-netwerk
	2.	De CSP heeft relevante beheerprocessen beschreven en effectief ingericht conform een vastgestelde cyclus, waaronder: registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.	CIP-netwerk
Controle-activiteiten en rapportages	3.	De CSP beschikt voor clouddiensten over richtlijnen voor het: • uitvoeren van controle-activiteiten, waaronder penetratie- en kwetsbaarheidstesten; • evalueren van en rapporteren over de performance, conformance en leveringsprestaties.	CIP-netwerk

5.3.2 C.02 Risico-control

Objectdefinitie

Betreft het beoordelen van continu onderzoek naar dreigingen en kwetsbaarheden en het beoordelen van de beheersing van onderkende risico's.

Objecttoelichting

Risico-control is het monitoren en reviewen van activiteiten van de risico-assessment in relatie met risicomanagement. Het monitoren en reviewen van risico's is noodzakelijk omdat risicofactoren: waarde van assets, impact, dreigingen, zwakheden en kans op voorkomen steeds veranderen. Risico-control kan ondersteund worden door extern verkregen informatie over dreigingen en zwakheden.

Doelstelling	Tijdig nagaan of er veranderingen aanwezig zijn die van invloed zijn op de uitkomst van de risico-assessment.		
Risico	Het niet of te laat anticiperen op risicofactoren die van invloed zijn op de uitkomst van de risico-assessment.		
Control	Risicomanagement en het risico-assessmentproces behoren continu te worden **gemonitord en gereviewd** en zo nodig te worden verbeterd.		ISO 27005 2018: 12.1 ISO 27005 2018: 12.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Gemonitord en gereviewd	1.	De CSP verifieert regelmatig de criteria die gebruikt worden om de risico's te meten en om vast te stellen of ze steeds consistent zijn met de organisatiedoelstellingen, de strategie, het beleid en/of de context van de organisatie steeds in beschouwing worden genomen.	ISO 27005 2018: 12.2
	2.	Vastgestelde risico's dienen in relatie met de factoren: waarde van de assets, dreigingen, zwakheden, kans op voorkomen en impact te worden gemonitord en geëvalueerd, om een compleet risicobeeld te behouden en tijdig veranderingen vast te (kunnen) stellen.	ISO 27005 2018: 12.1
	3.	De CSP zal voor het monitoren van risico's zich continu richten op: • nieuwe assets die deel behoren uit te maken van het toepassingsgebied van een risico-assessment; • veranderingen in de waarde van assets; • de mogelijkheid dat nieuwe of toegenomen zwakheden kunnen leiden tot dreigingen; • de mogelijkheid dat eerder vastgestelde zwakheden aan nieuwe dreigingen blootstaan; • toegenomen impact of consequenties van de beoordeelde risico's en zwakheden resulterend in een onacceptabel risiconiveau; • informatiebeveiligingsincidenten.	ISO 27005 2018: 12.1
	4.	De CSP voert regelmatig de monitoringsactiviteiten uit en mitigeert de vastgestelde risico's.	ISO 27005 2018: 12.1
	5.	Bij het monitoren en reviewen worden onder andere de volgende elementen geadresseerd: • wet- en regelgeving en organisatorische/technische context; • risico-assessmentaanpak; • waarde assets en categorieën; • risico-evaluatiecriteria; • risico-acceptatiecriteria.	ISO 27005 2018: 12.2

5.3.3 C.03 Compliance en assurance

Objectdefinitie

Betreft de besturing op het voldoen aan de geldende wet- en regelgeving, beleid, richtlijnen en procedures en de onafhankelijke toetsing op de naleving hiervan.

Objecttoelichting

Met compliance wordt aangeduid dat de CSP werkt conform de geldende wet- en regelgeving en het uitgestippeld cloud-beveiligingsbeleid. Aan de CSC wordt zekerheid geboden over het beoogde beveiligingsniveau van de aangeboden clouddienst. Hiervoor zal de CSP een compliance-functie moeten hebben ingericht die het management van de CSP bijstaat bij het in control houden van de CSP-organisatie om te werken volgens de geldende wet- en regelgeving en het overeengekomen beveiligingsbeleid.

Assurance is zekerheid geven over de naleving van wet- en regelgeving door een onafhankelijke toetsing. Daarmee wordt aan de CSC zekerheid geboden van het beoogde beveiligingsniveau van de aangeboden clouddienst. Dit vindt plaats met een assurance-rapportage.

Doelstelling	Het voorkomen van het overtreden van wet- en regelgeving, het beveiligingsbeleid, de richtlijnen en de procedures en zekerheid bieden over het beoogde beveiligingsniveau van de clouddienst.		
Risico	Het ongecontroleerd afwijken van hetgeen gesteld is in wet- en regelgeving, het beveiligingsbeleid, de richtlijnen en de procedures en geen zekerheid hebben over het ingevoerde beveiligingsniveau.		
Control	De CSP behoort regelmatig de naleving van de cloud-beveiligingsovereenkomsten op **compliancy** te beoordelen, jaarlijks een **assurance**-verklaring aan de CSC uit te brengen en te zorgen voor onderlinge **aansluiting** van de resultaten uit deze twee exercities.		ISO 27002 2017: 18.2.1 ISO 27002 2017: 18.2.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Compliancy	1.	Voor de governance van de clouddienstverlening aan de CSC heeft de CSP een compliance-proces ingericht, waarmee continue compliance op wet- en regelgeving en het overeengekomen cloud-beveiligingsbeleid vorm wordt gegeven.	CIP-netwerk
	2.	De CSP registreert de regulier uitgebrachte prestatie-, beveiligings- en compliance-rapportages in een administratie.	CIP-netwerk
	3.	Het compliance-proces is bij voorkeur aangesloten op een informatiebeveiligingsmanagementsysteem.	CIP-netwerk
Assurance	4.	De CSP laat jaarlijks door een derde partij een onderzoek (audit) uitvoeren op de inrichting en beheersing van de gecontracteerde clouddiensten.	CIP-netwerk
	5.	Bij de assessment wordt door de derde partij zowel de cloud-omgeving als de administratie betrokken.	CIP-netwerk

Aansluiting	6.	De CSP zorgt ervoor dat de uitkomsten uit de jaarlijkse assurance-rapportage (Third Party Mededeling (TPM)), de uitkomsten van de periodieke servicerapportages en de uitkomsten uit de continue compliance op het cloud-beveiligingsbeleid op elkaar aansluiten.	CIP-netwerk

5.3.4 C.04 Technische kwetsbaarhedenbeheer

Objectdefinitie

Betreft een instandhoudingsproces voor het onderzoek naar en het oplossen van technische kwetsbaarheden.

Objecttoelichting

Het verzamelen en beheren van security-kwetsbaarheden en issues in clouddiensten. Voor wat betreft de services van de CSC, het transparant communiceren van kwetsbaarheden van de genomen (of nog te nemen) maatregelen voor IT en organisatie. De CSC wenst op een transparante wijze op de hoogte gesteld te worden van de kwetsbaarheden en issues gerelateerd aan de beveiliging van de clouddiensten.

Door technische assessments uit te voeren op de ICT-componenten worden aanwezige kwetsbaarheden zichtbaar en kunnen deze worden weergegeven in een rapportage. Met deze rapportage kan de CSP de afweging maken welke kwetsbaarheden relevant zijn en verholpen moeten worden en welke risico's ten aanzien van deze kwetsbaarheden geaccepteerd kunnen worden.

De frequentie voor het uitvoeren van technische assessments moet zijn vastgesteld met het voor de clouddienst actuele risicoprofiel en actie moet worden ondernomen als geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of als tekortkomingen worden geconstateerd.

Doelstelling	Het voorkomen van het benutten van technische kwetsbaarheden door onbevoegden.		
Risico	Een technische kwetsbaarheid wordt niet of niet tijdig ontdekt.		
Control	Informatie over **technische kwetsbaarheden** van gebruikte informatiesystemen behoort tijdig te worden verkregen; de blootstelling aan dergelijke kwetsbaarheden dienen te worden **geëvalueerd** en passende maatregelen dienen te worden genomen om het risico dat ermee samenhangt aan te pakken.		BIO 2019: 12.6.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Technische kwetsbaar-heden	1.	De CSP stelt de CSC informatie beschikbaar over het beheer van de technische kwetsbaarheden die de clouddiensten kunnen beïnvloeden.	ISO 27017 2015: 12.6.1
	2.	De CSP heeft de rollen en verantwoordelijkheden in relatie tot het beheersen van technische kwetsbaarheden, waaronder coördineren, monitoren, beoordelen van risico's en mitigeren van kwetsbaarheden, gedefinieerd en vastgesteld.	ISO 27002 2017: 12.6.1a

	3.	Als de kans op misbruik en de verwachte schade beiden 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.	BIO 2019: 12.6.1
	4.	Het tijdspad waarbinnen gereageerd moet worden op aankondigingen van potentieel relevante kwetsbaarheden is gedefinieerd.	ISO 27002 2017: 12.6.1c
	5.	Periodiek worden penetratietests op ICT-componenten uitgevoerd om zwakheden te identificeren.	SoGP 2018: TM1.1.7
	6.	Technische zwakheden kunnen worden verholpen door het tijdig uitvoeren van patchmanagement, wat inhoud: • het identificeren, registreren en verwerven van patches; • de besluitvorming rond het inzetten van patches; • het testen van patches; • het uitvoeren van patches; • het registreren van doorgevoerde patches.	SoGP 2018: TM1.1.9
Geëvalueerd	7.	Evaluaties van technische kwetsbaarheden worden geregistreerd en gerapporteerd.	CIP-netwerk
	8.	De evaluatierapportages bevatten verbeteringsvoorstellen en worden gecommuniceerd met verantwoordelijken/eigenaren van ICT-componenten waarin kwetsbaarheden en zwakheden gevonden zijn.	NCSC 2015: C.03.04

5.3.5 C.05 Security-monitoringsrapportage

Objectdefinitie

Omvat het continu bewaken van security-gebeurtenissen en de rapportage over de geconstateerde afwijking van het overeengekomen beveiligingsniveau.

Objecttoelichting

Onder security-monitoring wordt voor clouddiensten verstaan, het reviewen, analyseren, signaleren en tijdig rapporteren van zwakheden, onveilige interfaces en ongeautoriseerde toegangspogingen, om misbruik te voorkomen en om met de ernst van de signalering acties te ondernemen.

De bewakingsfunctie is voorbehouden aan de daartoe verantwoordelijke functionaris(sen) en vindt mede plaats met geregistreerde gegevens (logging).

De loggegevens behoren regelmatig te worden geanalyseerd en de resultaten van deze analyses moeten worden gerapporteerd (alerting). Ook moet de CSP regelmatig rapporteren over of en de mate waarin afwijkingen zijn geconstateerd op het overeengekomen beveiligingsniveau.

Doelstelling	Gebeurtenissen (performance van de informatiebeveiliging van de cloud-omgeving) vastleggen, bewijs verzamelen en betrokkenen daarvan op de hoogte te stellen.

Risico	Misbruik van de performance van informatiebeveiliging van de cloud-omgeving.		
Control	De performance van de informatiebeveiliging van de cloud-omgeving behoort regelmatig te worden **gemonitord en** hierover behoort tijdig te worden **gerapporteerd** aan verschillende stakeholders.		ISO 27002 2017:12.4 SoGP 2018: SI2.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Gemonitord en gerapporteerd	1.	Richtlijnen en afspraken voor het monitoren en rapporteren over informatiebeveiliging van de cloud-omgeving zijn vastgesteld en worden toegepast.	SoGP 2018: S12.1.1
	2.	Het monitoren en rapporteren over de informatiebeveiliging zijn gerelateerd aan: • geformuleerde strategische- en bedrijfsdoelen; • risico's die het bereiken van de strategische doelen kunnen beïnvloeden; • beveiligingsincidenten, zoals cybersecurity-aanvallen.	SoGP 2018: SI2.1.2
	3.	Het monitoren van informatiebeveiliging en rapportages vindt plaats met: • het verzamelen van informatie uit interne en externe bronnen; • het inzicht door verzamelde informatie uit de combinatie van Key Performance Indicators (KPI's) en Key Risk Indicators (KRI's).	SoGP 2018: SI2.1.5
	4.	Informatiebeveiligingsrapportages worden in samenhang met rapportages uit andere beheerdisciplines (compliance en assurance-management en vulnerability-management) geanalyseerd.	SoGP 2018: S12.6
	5.	Aantoonbaar wordt opvolging gegeven aan verbetervoorstellen uit analyserapportages.	CIP-netwerk
	6.	De beveiligingsplannen worden periodiek geactualiseerd en toegewezen aan de hiervoor verantwoordelijke functionarissen.	NCSC 2015: 07.11

5.3.6 C.06 Beheersorganisatie clouddiensten

Objectdefinitie

Betreft een doelgerichte bundeling van kennis en vaardigheden tussen personen met taken, verantwoordelijkheden en bevoegdheden voor het functionele en technische beheer van clouddiensten.

Objecttoelichting

Voor het adequaat beheersen en beheren van clouddiensten moet de CSP een beheersingsorganisatie hebben ingericht, waarin de structuur en verantwoordelijkheden voor beheersprocessen met toereikende bevoegdheden zijn uitgedrukt en op het juiste niveau zijn gepositioneerd.

In de relatie tussen de beheersingsprocessen van de CSP en de CSC zijn ook de taken en verantwoordelijkheden tussen het functioneel en technisch beheer overeengekomen.

Doelstelling	Het adequaat beheersen en beheren van clouddiensten.

Risico	De cloudiensten verlopen niet zoals noodzakelijk is.		
Control	De CSP heeft een beheersorganisatie ingericht waarin de **processtructuur** en de **taken, verantwoordelijkheden en bevoegdheden** van de betrokken **functionarissen** zijn vastgesteld.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Proces-structuur	1.	De samenhang van processen wordt in een processtructuur vastgelegd.	NCSC 2015: B.06.07
Taken, verant-woordelijk-heden en bevoegdheden	2.	De CSP heeft de taken en verantwoordelijkheden voor de uitvoering van de beheer(s)werkzaamheden beschreven en de bijbehorende bevoegdheden vastgelegd in een autorisatiematrix.	CIP-netwerk
Functionaris-sen	3.	De belangrijkste functionarissen (stakeholders) voor de beheersingsorganisatie zijn benoemd en de onderlinge relaties zijn met een organisatieschema inzichtelijk gemaakt.	CIP-netwerk

Bijlage 1: Verantwoording

Deze bijlage geeft een korte verantwoording over de aanpak, de keuzes die gemaakt zijn en de inhoudelijke objecten die gebruikt zijn in deze BIO Thema-uitwerking. Om te komen tot een document dat breed draagvlak heeft en toegevoegde waarde biedt aan overheidsorganisaties zijn de objecten getraceerd langs:

1. CSC-eisen
2. Bedreigingen/kwetsbaarheden
3. Baselines

Overheidsorganisaties die inmiddels over specifieke normenkaders voor clouddiensten beschikken, zijn gevraagd om hun kaders, via deze thema-uitwerking voor een groter publiek open te stellen voor hergebruik.

CSC-eisen

Om de specifiek CSC-georiënteerde aandachtspunten te traceren, zijn vragen gesteld aan overheidsorganisaties om te komen tot een set van eisen en wensen. Met de eisen en wensen zijn objecten geïdentificeerd. Hierbij zijn aan doelorganisaties en cloud-groepssessies enkele vragen gesteld, zoals:

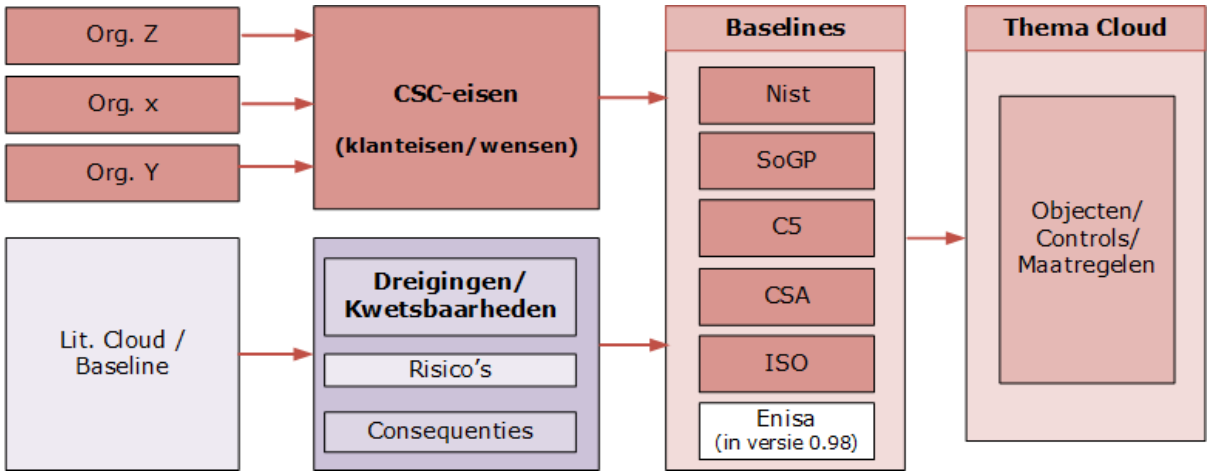
- Hoe kan deze thema-uitwerking de organisatie helpen bij het verwerven van clouddiensten?
- Wat moet minimaal uitgewerkt worden in de BIO Thema-uitwerking clouddiensten?
- Welke eisen worden door overheidsorganisaties gesteld bij het verwerven van clouddiensten?
- Zijn vanuit deze thema-uitwerking verbindingen noodzakelijk met functionele eisen voor clouddiensten en normatiek?

Bedreigingen/kwetsbaarheden

Om specifieke objecten te identificeren, is ook gericht op de algemene dreigingen en kwetsbaarheden die voortvloeien uit het toepassen van clouddiensten.

Baselines

Hiernaast zijn bestaande baselines geraadpleegd, voor zover ze specifiek zijn voor clouddiensten. De specifieke objecten, ook vanuit de eisen en wensen van de CSC-zijde en de dreigingen, zijn uit de baselines geselecteerd en toegespitst op voor de cloud-omgeving. Verder is een koppeling gelegd met de BIO en met de ISO 27017, die specifiek gericht is op clouddiensten. Afbeelding 11 geeft een overzicht van de beschreven stappen.



Afbeelding 11: Traject totstandkoming BIO Thema-uitwerking Clouddiensten

Bijlage 2: Toelichting objecten in het beleidsdomein

Hieronder volgt per invalshoek een toelichting op het beleidsdomein:

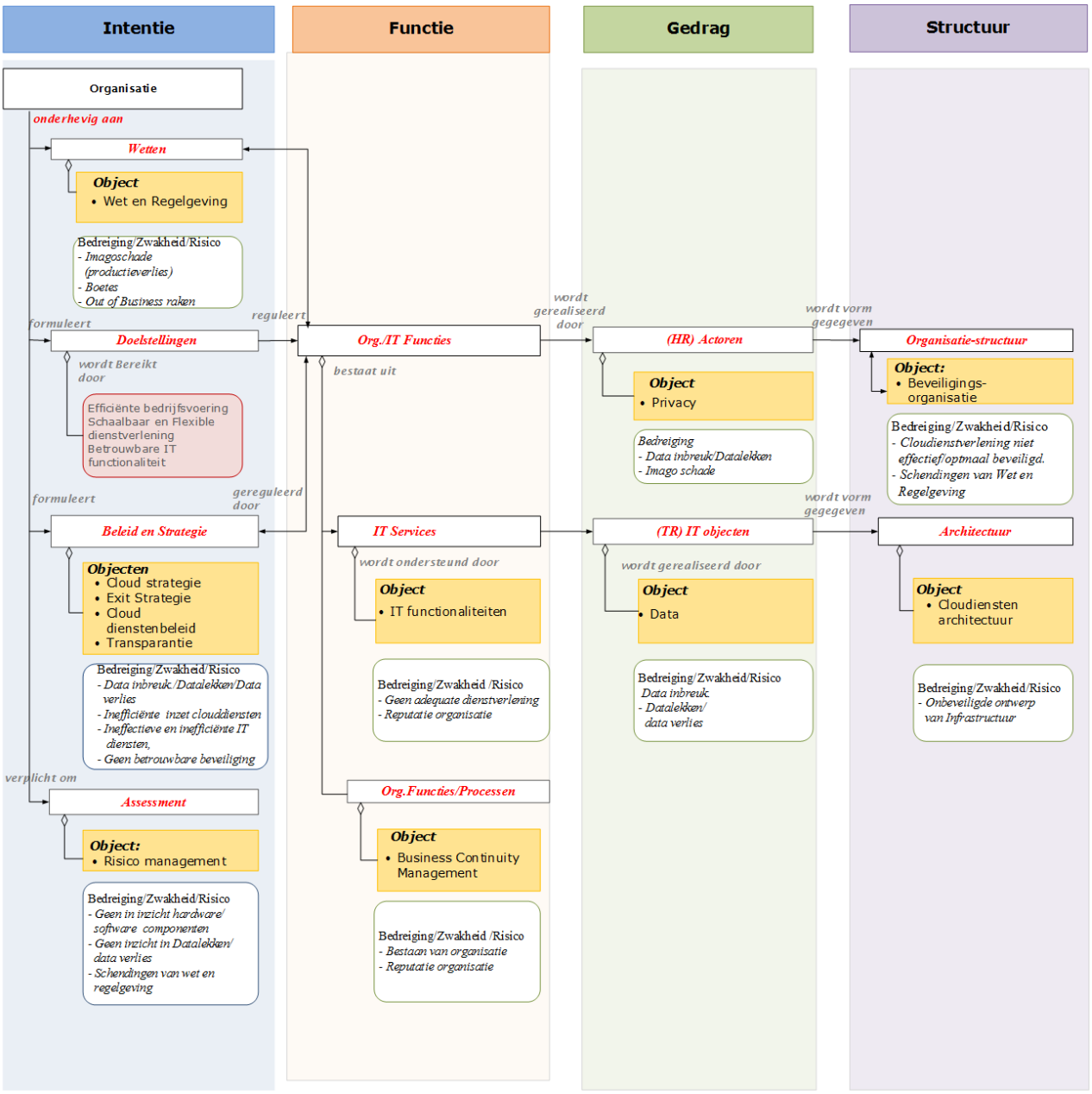
- Intentie
  Een organisatie heeft bij het verwerven van clouddiensten doelstellingen geformuleerd, zoals: een efficiënte bedrijfsvoering en een schaalbare en flexibele dienstverlening. Hiervoor ontwikkelt zij beleid en strategie. Omdat dit met onzekere informatie wordt ontwikkeld, laten stakeholders risicoanalyse(s) uitvoeren. Voor het uitvoeren van risicoanalyses is een te hanteren risicoaanpak (methode) vastgesteld (risicomanagement).

- Functie
  Om aan de doelstellingen te kunnen voldoen, kan de organisatie besluiten functionele eisen vast te stellen. Zij moeten de IT-functionaliteiten en gerelateerde processen en beveiligingsfuncties beschrijven.

- Gedrag
  De IT-functionaliteiten worden gerealiseerd door actoren (human resources) en IT-objecten (technische resources). Human resources refereert aan mensen waaraan eisen worden gesteld, zoals educatie, competentie/vaardigheid. IT-resources zijn 'Data' en IT-objecten (applicaties, servers en infrastructuur).

- Structuur
  De inzet van de actoren dienen goed georganiseerd te worden door een organisatiestructuur en de benodigde IT-objecten een architectuur.

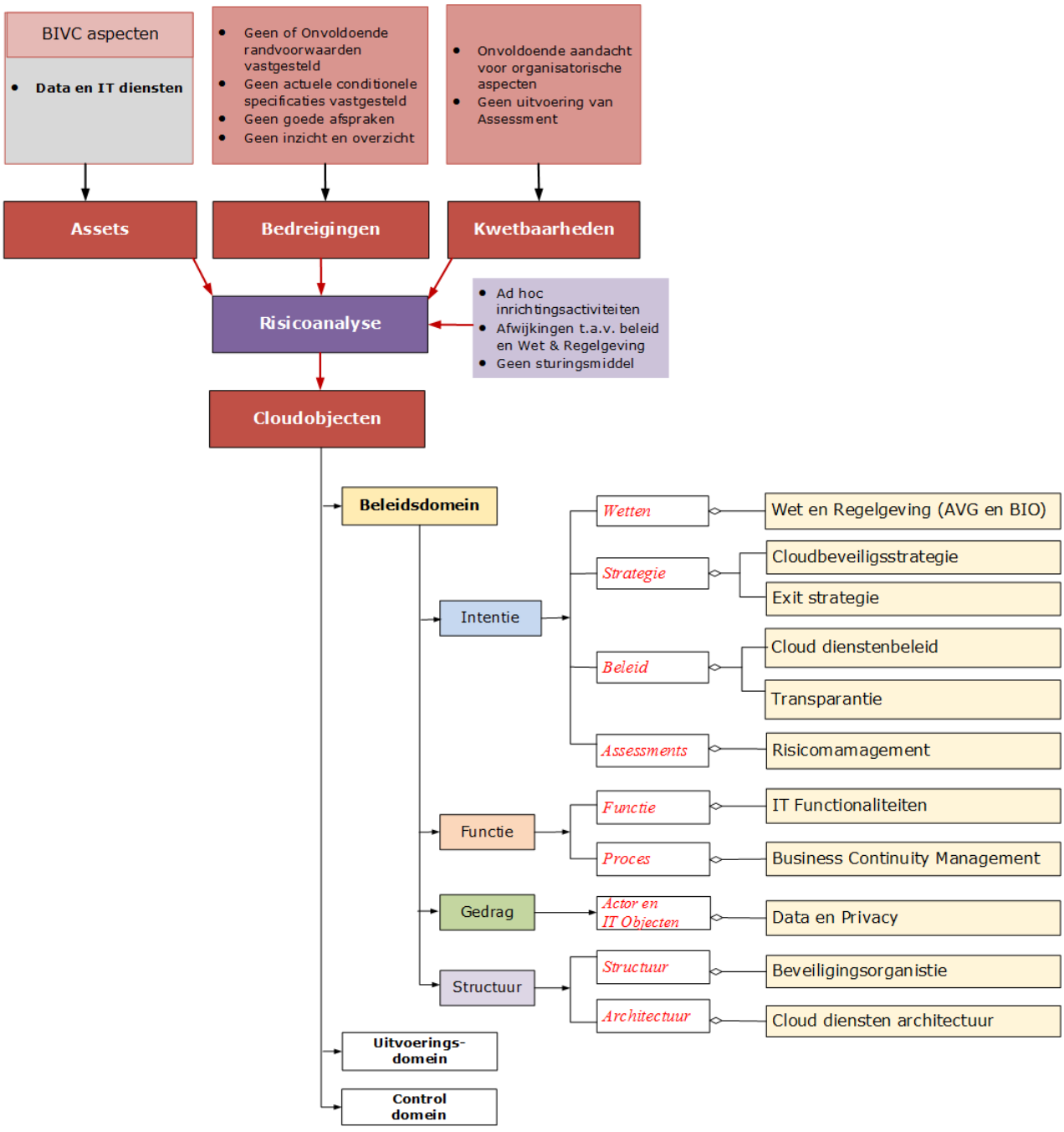
Afbeelding 12 toont dreigingen/kwetsbaarheden van de genoemde beleidsobjecten.



Afbeelding 12: Dreigingen/kwetsbaarheden van beleidsobjecten

Dreigingen/kwetsbaarheden cloud-beleidsobjecten

Afbeelding 13 geeft voor het beleidsdomein en dankzijde vermelde dreigingen/kwetsbaarheden en risico's de geïdentificeerde beveiligingsobjecten voor clouddiensten weer. Deze dreigingen/kwetsbaarheden en risico's zijn niet uitputtend en illustreert de wijze waarop de schrijfgroep tot relevante beleidsobjecten is gekomen: eerst een longlist en vervolgens een shortlist. De objecten uit de shortlist zijn vervolgens gestructureerd met de SIVA-methodiek. SIVA staat voor Structuur, Inhoud, Vorm en Analysevolgorde. Ze zijn ingedeeld in de 3 domeinen: beleid, uitvoering en control en 4 invalshoeken: intentie, functie, gedrag en structuur.



Afbeelding 13: Beleidsobjecten gestructureerd met de SIVA-methodiek

Bijlage 3: Toelichting objecten in het uitvoeringsdomein

Hieronder volgt per invalshoek een toelichting op het uitvoeringsdomein:

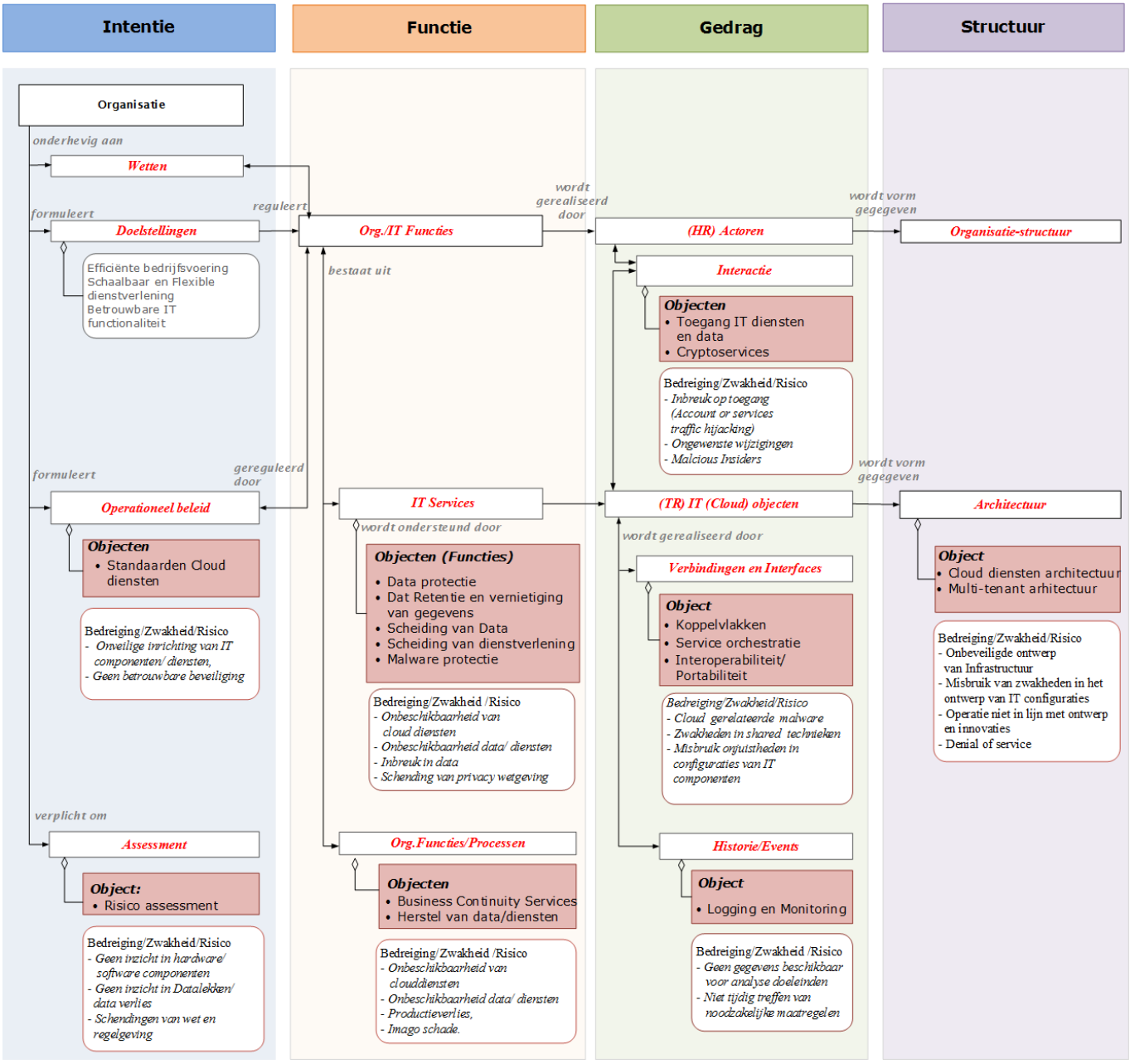
- Intentie
  In het uitvoeringsdomein zal de organisatie onder andere haar beleid vertalen naar richtlijnen voor het uitvoeren van een risicoanalyse en de implementatie vertalen naar procedures.

- Functie
  In dit domein worden voor clouddiensten organisatorische en technisch georiënteerde maatregelen getroffen.

- Gedrag
  De clouddiensten kennen een aantal specifieke elementen, zoals toegang en technisch georiënteerde componenten.

- Structuur
  De clouddiensten moeten een goed overzicht bieden via een architectuur.

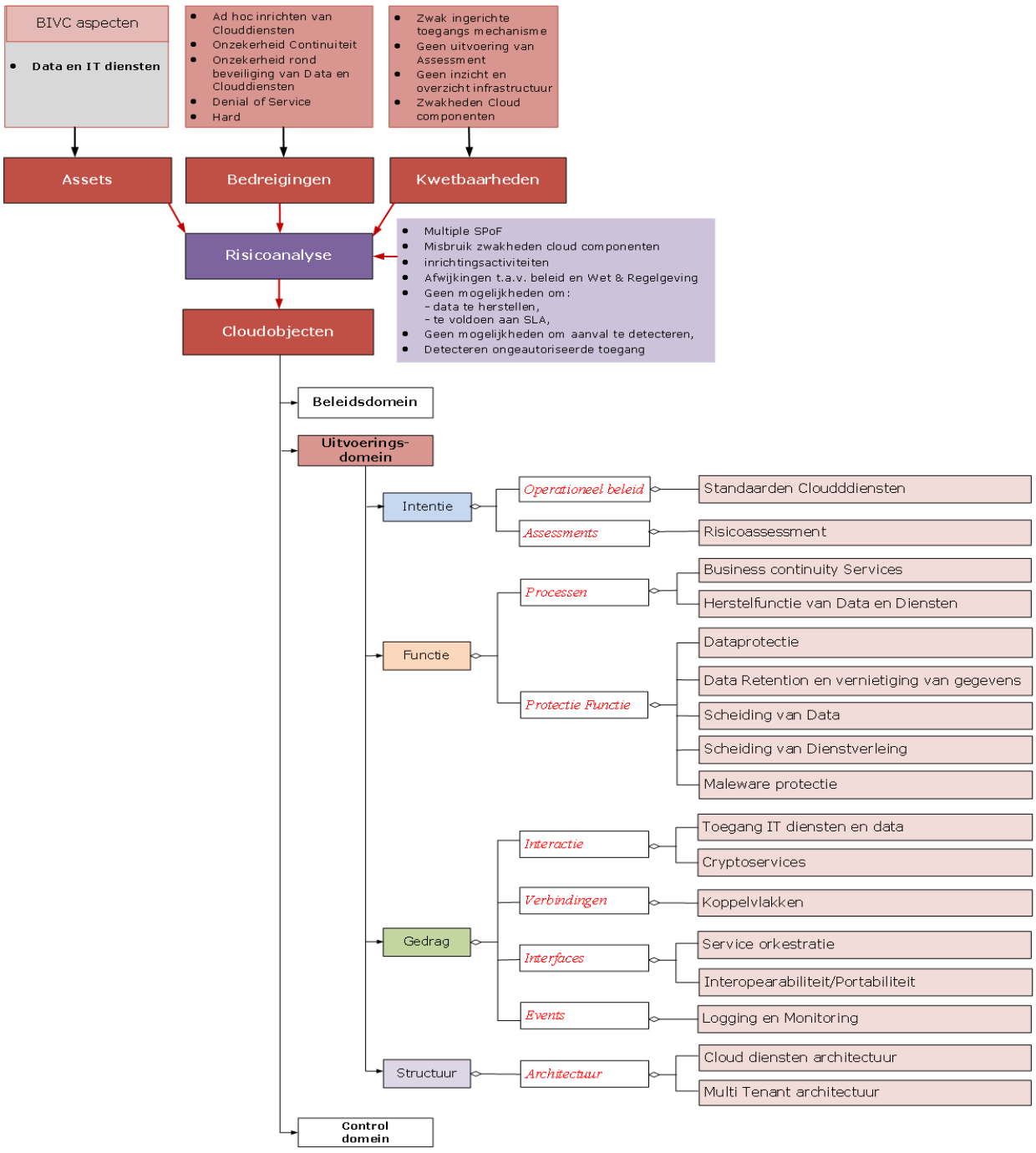
Afbeelding 14 toont de dreigingen/kwetsbaarheden van de genoemde uitvoeringsobjecten.



Afbeelding 14: Dreigingen/kwetsbaarheden van uitvoeringsobjecten

Dreigingen/kwetsbaarheden cloud-uitvoeringsobjecten

Het uitvoeringsdomein is op dezelfde wijze geanalyseerd als vermeld bij Bijlage 2 Toelichting objecten in het beleidsdomein. Ook hier zijn de vermelde dreigingen/kwetsbaarheden en risico's niet uitputtend benoemd. Afbeelding 15 geeft voor het uitvoeringdomein en dankzijde vermelde dreigingen/kwetsbaarheden en risico's de geïdentificeerde beveiligingsobjecten voor clouddiensten weer.



Afbeelding 15: Uitvoeringsobjecten gestructureerd met de SIVA-methodiek

Bijlage 4: Toelichting objecten in het control-domein

Hieronder volgt per invalshoek een toelichting op het control-domein:

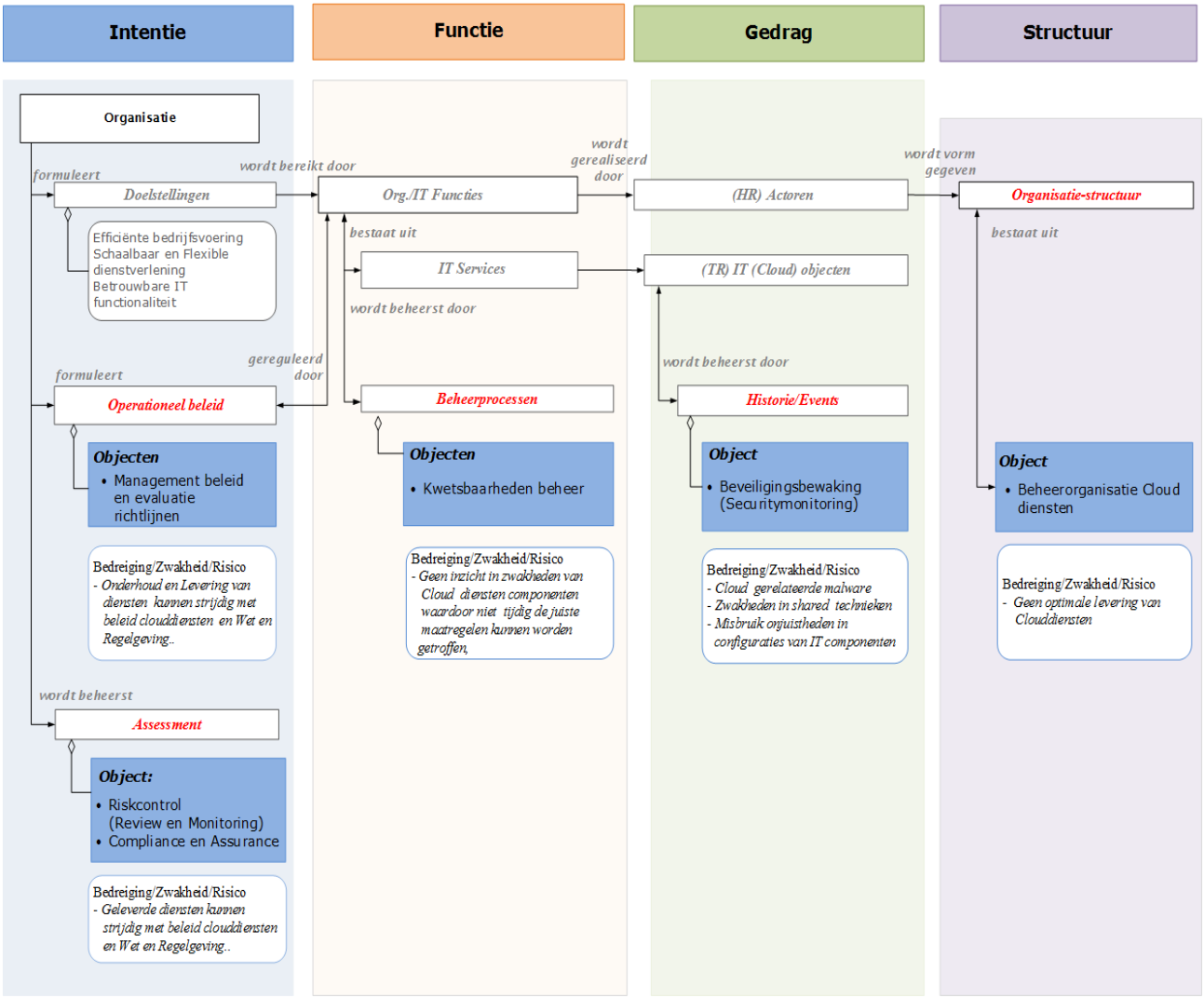
- Intentie
  De organisatie heeft haar beleid voor clouddiensten vertaald naar een servicemanagementbeleid en evaluatierichtlijnen voor het inrichten, evalueren en bewaken van het functioneren en van de bescherming van de clouddiensten en activiteiten uitvoeren voor het monitoren en reviewen van de risico's.

- Functie
  De organisatie heeft beheersingsprocessen ingericht en verricht voor beveiligingscontroles en kwetsbaarheden van de clouddiensten.

- Gedrag
  De organisatie verricht in haar processen activiteiten voor het monitoren van clouddiensten en technische kwetsbaarheden.

- Structuur
  De organisatie heeft voor de clouddiensten een beheersingsorganisatie ingericht.

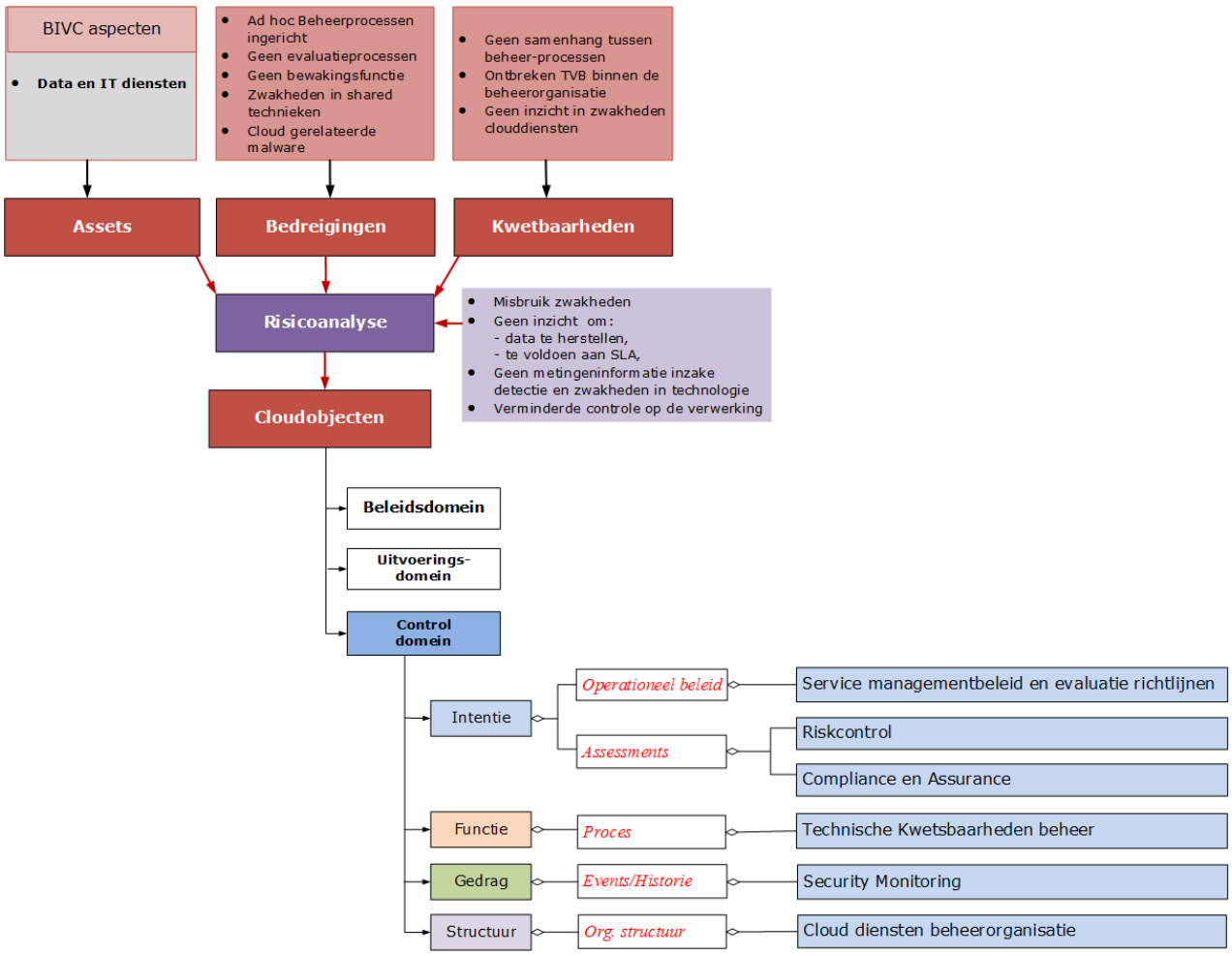
Afbeelding 16 toont de dreigingen/kwetsbaarheden van de genoemde control-objecten.



Afbeelding 16: Dreigingen/kwetsbaarheden van control-objecten

Dreigingen/kwetsbaarheden cloud-control-objecten

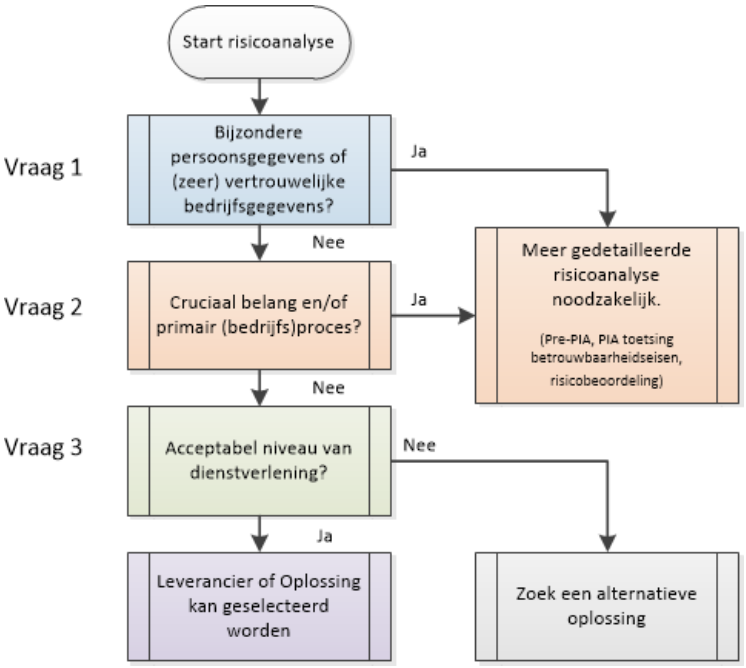
Het control-domein is op dezelfde wijze geanalyseerd als vermeld bij het Bijlage 2 Toelichting objecten in beleidsdomein. Ook hier zijn de vermelde dreigingen/kwetsbaarheden en risico's niet uitputtend benoemd. De relevante objecten binnen het control-domein worden weergegeven in afbeelding 17.



Afbeelding 17: Control-objecten gestructureerd met de SIVA-methodiek

Bijlage 5: Beslisboom voor risicobeoordeling IV-diensten

De beslisboom in afbeelding 18 ondersteunt de stakeholders voor cloud-services bij het nemen van verantwoorde beslissingen voor het onderbrengen van gegevens en/of bedrijfsprocessen in de publieke cloud, private cloud, als uitbestede IT of in het eigen rekencentrum 'on premise'. De beslisboom is uitgewerkt in relatie tot de risicoafweging.



Afbeelding 18: Beslisboom voor risicobeoordeling

Belangrijk daarbij is om de context van de overheid in de overweging mee te nemen. Overheden worden geacht om verantwoord om te gaan met gevoelige gegevens van burgers en bedrijven, maar ook met gegevens van eigen medewerkers. Zie voor de vraag die in stap 1 gesteld wordt over gegevens bijlage 6 Samenvatting AIVD-standpunt en beleidsverkenning van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK).

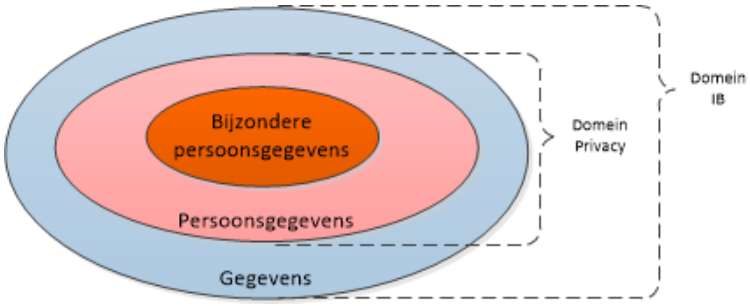
De beslisboom wordt gebruikt als zelfassessment en toetst achtereenvolgens op:

1. Afhankelijkheid en kwetsbaarheid
   Gaat het om een primair bedrijfsproces met gevoelige gegevens van burgers en/of bedrijven, waarbij (bijzondere) persoonsgegevens vanwege de AVG extra zwaar wegen, zeker als het de persoonlijke veiligheid/privacy van eigen medewerkers betreft?

2. Te beschermen belangen
   Gaat het om zogenaamde cruciale belangen die van primair belang zijn voor het voortbestaan van de organisatie, waarbij het vertrouwen van de burger en het bedrijf in de betrouwbare overheid op het spel komt te staan indien die bescherming onvoldoende geborgd is?

3. Betrouwbaarheid van producten en diensten
   De betrouwbaarheid van de levering van producten en diensten is essentieel voor de organisatie. De CSP vervuld daarin als belangrijkste actor een cruciale rol. Daarom is een passende dienstverlening nodig, waarbij het karakter van de te verwerken gegevens/processen daarvoor geschikt moet zijn.

Afhankelijk van de situationele context, zal het ook gaan om bedrijfsgegevens die vallen in één van de geschetste domeinen uit afbeelding 19 en die de daarbij behorende passende maatregelen vergen.



Afbeelding 19: Schematische weergave soorten gegevens

Afhankelijkheid en kwetsbaarheid

Vraag 1: Gaat het om persoonsgegevens[8] en/of (zeer) vertrouwelijke bedrijfsgegevens[9]?
Ja, er is een meer gedetailleerde risicoanalyse[10] noodzakelijk (pre-DPIA, DPIA en/of risicobeoordeling).
Nee, ga naar vraag 2.

Te beschermen belangen

Vraag 2: Gaat het om één van de volgende typen processen (is het karakter van de processen)?

---

8 Onder persoonsgegevens verstaat de AVG alle informatie over een geïdentificeerd of identificeerbaar natuurlijk persoon (de betrokkene) die direct of indirect kan worden geïdentificeerd. Bijvoorbeeld via naam, identificatienummer (BSN), locatiegegevens of via elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Direct identificeerbaar: gegevens die naar hun aard rechtstreeks betrekking hebben op een persoon, zoals iemands naam.

Indirect identificeerbaar: gegevens die naar hun aard mede bepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld.

Voorbeelden van indirect zijn het type huis of auto van een betrokkene, omdat dit iets zegt over het inkomen en vermogen van de betrokkene. Ook gegevens die in combinatie met andere gegevens tot identificeerbaarheid kunnen leiden, worden aangemerkt als persoonsgegeven.

9 Vertrouwelijke bedrijfsgegevens, bijvoorbeeld (nog vertrouwelijke) financiële, technische of juridische informatie, budgetten, beleidsvoornemens, aanbestedingen en beursgevoelige informatie. Kortom alle informatie die (nog) niet voor derden is bestemd.

10 De gedetailleerde risicoanalyse zal in het geval van (a) privacygevoelige gegevens bestaan uit een zogenaamde pre-DPIA (risico-inschatting met 9 vragen), afhankelijk van de uitkomst gevolgd door een formele DPIA; (b) in het geval van vertrouwelijke informatie zal de classificatie plaatsvinden door de betrouwbaarheidseisen te toetsen (is het gewenste niveau van beschikbaarheid, integriteit en vertrouwelijkheid).

Vraag 2a: Gaat het om de verwerking van gegevens en/of geldstromen in een of meerdere processen van onze organisatie die niet in de handen mogen vallen van de criminaliteit, omdat dat het vertrouwen dat de burger en het bedrijf stellen in de overheid als betrouwbare ernstig zou kunnen schaden?

Vraag 2b: Gaat het om een primair proces of processen van onze organisatie, waarbij geldt dat wanneer deze processen op enig moment worden belemmerd of gestopt, in dit voorbeeld de schade voor onze organisatie groot zal zijn (zowel in financiële zin als ook in termen van imago schade)?

Ja, er is een meer gedetailleerde risicoanalyse noodzakelijk (betrouwbaarheidseisen toetsen en zo nodig meer en/of zwaardere beveiligingsmaatregelen overeenkomen, inclusief risicobeoordeling).

Nee, ga naar vraag 3.

Betrouwbaarheid van producten en diensten

Vraag 3: Biedt de CSP een acceptabel niveau van dienstverlening?

Vraag 3a: Is de CSP van de toepassing/applicatie ISO 27001 gecertificeerd?

Vraag 3b: Indien sprake is van de opslag van data bij een extern datacenter is dat datacenter ISO 27001 gecertificeerd of anderszins gecertificeerd (ISAE3402 ‘Assurance Reports on Controls at a Service Organization’ of Service Organization Control (SOC) 2)?

Vraag 3c: Waar worden eventuele (bron)gegevens van de provincie opgeslagen die gebruikt worden bij het werken met de toepassing/applicatie vanwege ongewenste opslag buiten Europa?

Vraag 3d: Is de CSP bereid tot een externe (onafhankelijke) audit op compliance met wet- en regelgeving?

Als één van de 4 sub-vragen uit vraag 3 negatief wordt beantwoord, geldt dat een alternatieve oplossing gezocht dient te worden voor publieke clouddiensten, zoals een private cloud-omgeving, nu of in de toekomst geleverd vanuit de overheid, zoals Rijkscloud, of IT-outsourcing of on premise in een eigen rekencentrum.

Bijlage 6: Samenvatting AIVD-standpunt en beleidsverkenning BZK

In 2019 is de Algemene Inlichtingen en Veiligheidsdienst (AIVD) om een standpunt gevraagd over het gebruik van publieke clouddiensten voor gerubriceerde gegevens of vitale overheidsprocessen, waarvoor weerstand tegen statelijke actoren noodzakelijk is. Tevens heeft het ministerie van Binnenlandse Zaken en Koninkrijkrelaties (BZK) een beleidsverkenning gedaan. De AIVD maakt overigens in haar standpunt geen onderscheid tussen Rijksdiensten en de andere overheden.

Hieronder volgen enkele citaten die de kern van het AIVD-standpunt weergeven, waarop ook de beleidsverkenning van BZK is gebaseerd.

NBV-standpunt Publieke Clouddiensten (citaten uit de AIVD-brief d.d. 09/09/2019)

Publieke clouddiensten bieden in de huidige situatie geen controleerbaar afdoende weerstand tegen statelijke actoren omdat nu nog onvoldoende zekerheid kan worden verkregen:

- dat de overheidsgegevens en -processen technisch en procedureel voldoende zijn afgeschermd tegen de clouddienstverlener, zijn onderaannemers en zijn medewerkers;
- dat de clouddienstverlener spionage- en sabotage-aanvallen van statelijke actoren betrouwbaar preventief kan afweren;
- dat de clouddienstverlener spionage- en sabotage-aanvallen van statelijke actoren betrouwbaar kan detecteren én hierop adequaat zal reageren;
- dat voldoende controle en toezicht mogelijk is op publieke clouddienstverleners.

Daarbij gebruiken publieke clouddiensten vaak het internet, zodat de toegang en beschikbaarheid extra zorg vragen. Kortom, op dit moment is onvoldoende zekerheid dat publieke clouddienstverleners kunnen voldoen aan het VIR-BI en de BIO. Dit NBV-standpunt is gebaseerd op de huidige stand van cloud-technologie, statelijke cyberdreiging, nationale en internationale regelgeving en contractmogelijkheden. De ontwikkelingen op dit gebied gaan snel en het zal nodig zijn om dit standpunt periodiek, bijvoorbeeld jaarlijks, te heroverwegen.

Conclusie

In de huidige situatie is gebruik van publieke clouddiensten daarom niet geschikt voor gerubriceerde nationale informatie (Dep.V tot en met Stg.ZG), gerubriceerde EU- en NAVO-informatie en voor vitale overheidsprocessen waarvoor betrouwbare weerstand tegen statelijke actoren nodig is. Het gebruik van publieke clouddiensten is daarom ook ongeschikt voor Dep.V gerubriceerde informatie waarvoor betrouwbare detectie van statelijke actoren nodig is.

Als via risicoanalyse is vastgesteld dat geen weerstand tegen en geen detectie van statelijke actoren nodig is, dan kunnen publieke clouddiensten gebruikt worden. (Einde citaten uit de AIVD-brief.)

Verkenning Cloudbeleid voor Nederlandse Rijksdiensten (citaten uit brief aan CIO-Rijk, 16/09/2019)

= Concept voor brede discussie=

Dit document bevat een verkenning voor Cloudbeleid van de Nederlandse Rijksdienst. Doel van deze verkenning is om richting te geven aan het gebruik en verdere ontwikkeling van clouddiensten door departementen, en om ambities te formuleren, waarbij rekening wordt gehouden inzichten van de AIVD voor het omgaan met dreigingen door Advanced Persistent Threats (APT's) zoals statelijke actoren. Uitgangspunt is dat clouddiensten moeten voldoen aan de voorwaarden van het algemeen beleid. Deze voorwaarden zijn in grote lijnen beschreven in de strategische i-agenda voor de Rijksdienst 2019 -2021.

Overwegingen en beleidsvoornemen

Het cloud-beleid dient duidelijkheid te scheppen hoe veilig gebruik gemaakt kan worden van private, hybride en publieke clouddiensten door overheidspartijen. Omdat de Baseline Informatiebeveiliging Rijksdienst (BIR) inmiddels, formeel, in de BIO is overgegaan wordt in het vervolg van dit document gesproken over BIO-BBN niveaus terwijl de focus van dit document (thans) de Rijkdienst betreft.

In deze bijlage zijn vanwege risicomanagement de mogelijke beleidslijnen uitgewerkt rond het toepassen van BBN 1, 2 en 3 voor diverse cloud-implementatie-scenario's. De BIO bepaalt op basis van eisen voor vertrouwelijkheid. Het onderscheid in drie BBN's voorkomt dat voor eenvoudige systemen zonder vertrouwelijke informatie of zonder eigen voor hoge beschikbaarheid te veel administratieve last wordt opgeroepen. Terwijl de BIO zich met name richt op confidentialiteit van gegevens, wordt in Nederland, gedreven door internationale ontwikkelingen, ook meer aandacht gevraagd voor de beschikbaarheid van 'vitale systemen en processen'. In beide toepassingen is risicomanagement met een proportionele set aan maatregelen een logische aanpak.

Risicomanagement betreft 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.

Uitgangspunten

Voor alle toepassingen geldt, dat zal moeten zijn voldaan aan geldende kaders.

De versie van 1 oktober 2019 geeft aan dat aanpassingen worden meegenomen, zodra nieuwe inzichten daar aanleiding toe geven. Het streven is om deze jaarlijks te herzien, of zoveel eerder als ontwikkelingen daar aanleiding toe geven.

Met de voorgaande overwegingen en de input van veiligheidsexperts zijn de volgende beleidsvoornemens tot stand gekomen: Voor alle niveaus (zoals in de matrix geschetst) geldt de voorwaarde: er is een samenhangende risicoanalyse uitgevoerd, waarin rekening is gehouden met eisen voor vitale en kritieke processen en gevoelige data, en deze is opgevolgd. De restrisico's zijn of gemitigeerd of zijn geaccepteerd door de eigenaar.

Classificatie volgens QIS:	Non-Cloud in ODC	Private Cloud in ODC	Private Cloud bij leverancier	Public of Hybride Cloud
BIO-BBN1	Toegestaan, mits (1)	Toegestaan, mits (1)	Toegestaan, mits (1)	Toegestaan, mits (1)
BIO-BBN2 en ongerubriceerd	Toegestaan, mits (1)	Toegestaan, mits (1,2)	Toegestaan, mits (1,2)	Toegestaan, mits (1,2)
BIO-BBN2 en DepV-gerubriceerd	Toegestaan, mits (1)	Toegestaan, mits (1,2,3)	Toegestaan, mits (1,2,3)	Niet toegestaan, tenzij (1,2,3,4)
BIO-BBN3, incl. EU/NATO gerubriceerd	Toegestaan, mits (1)	Thans niet mogelijk	Niet toegestaan	Niet toegestaan

Afbeelding 20: Voorgenomen Cloudbeleid 1 oktober 2019 in matrix-overzicht

Conclusie: One Cloud doesn't fit All.

Betekenis van de nummers 1, 2, 3 en 4 in de matrix:

1. Er is voldaan aan:
    - Er moet een samenhangende risicoanalyse voor vitale en kritieke processen en gevoelige data zijn uitgevoerd en de resultaten daarvan zijn opgevolgd.
    - De uitkomsten zijn vastgelegd en (auditeerbaar) gecommuniceerd.
    - De restrisico's zijn door de systeem- of proces-eigenaar geaccepteerd:
        - voor departementale processen: met input van de CISO;
        - voor interdepartementale processen: met input van de CISO-Rijk.
2. Er dienen passende voorzieningen beschikbaar te zijn om activiteiten van APT's zoals statelijke actoren te kunnen signaleren en daarop in te grijpen. Dit betreft een set aan detectie voorzieningen en maatregelen, waarvan expert diensten (AIVD, MIVD of NCSC) hebben aangegeven dat deze zinvol zijn te opzicht van het risico dat het departement met de voorziening of proces loopt.
3. De verwerking van de (Dep.V) gerubriceerde BIO-BBN2 gegevens is vóóraf door de SG goedgekeurd.
4. Voor de goedkeuring van de SG dient het expert advies van de AIVD over Clouddiensten (zie hierboven) expliciet te worden meegewogen. Daarin staat vermeld (citaat) 'het gebruik van publieke clouddiensten is daarom ook ongeschikt voor Dep.V gerubriceerde informatie waarvoor betrouwbare detectie van statelijke actoren nodig is' (einde citaten).