Clouddiensten

BIO Thema-uitwerking

inclusief een 10-stappenplan voor
het verwerven en inzetten van clouddiensten

Mei 2026 [versie 3.0 definitief]

BIO Thema-uitwerking Clouddiensten

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



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

Titel	BIO Thema-uitwerking Clouddiensten
Datum	Mei 2026
Versie en status	3.0 definitief
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming (CIP)
Regime	Becommentarieerde praktijk
Auteurs	CIP-kernteamleden
Reviewers	Versie 1.0: Professionals uit het CIP-netwerk en het CIP-kernteam Versie 2.0: CIP-kernteam Versie 2.1: CIP-kernteam Versie 2.2: CIP-kernteam Versie 2.4: CIP-kernteam Versie 3.0: 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.

Wijzigingsbeheer

In de onderstaande tabel worden alle relevante wijzigingen in dit document bijgehouden, om eenvoudig inzicht te krijgen in de uitgevoerde aanpassingen.

Versie	Datum	Wijziging	Door
1.0	Januari 2021		CIP
1.1	Mei 2021		CIP
2.0	Juni 2021		CIP
2.1	Oktober 2021		CIP
2.2	Maart 2023	Tekstverbetering	CIP
2.4	Juli 2025	Actualisatie en aanscherping aansturing	CIP
3.0	Mei 2026	BIO2 v1.3 verwerkt	CIP

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.
- 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 10

1.1 Doelstelling 11

1.2 Opzet BIO Thema-uitwerking 11

1.3 Voorwaarden vanuit CIO Rijk 12

1.4 De relatie tussen CSC en CSP 12

1.5 Het inzetten van de objecten bij de keuze van de toepassing van clouddiensten 13

1.5.1 Beleidsdomein 13

1.5.2 Uitvoeringsdomein 13

1.5.3 Control-domein 13

1.6 Scope en begrenzing van de thema-uitwerking 13

1.7 Toepassing BIO Thema-uitwerking Clouddiensten in een 10-stappenplan 13

1.8 Referenties 14

2 Risico's in relatie tot clouddiensten 15

2.1 Dreigingen/kwetsbaarheden 15

2.2 CSC-georiënteerde aandachtspunten 17

3 Beleidsdomein 19

3.1 Doelstelling 19

3.2 Risico's 19

3.3 Objecten, controls en maatregelen 19

3.3.1 B.01 Beleidsregels voor informatiebeveiliging bij de inzet van clouddiensten 19

Objecttoelichting 19

3.3.2 B.02 Rollen en verantwoordelijkheden bij informatiebeveiliging in de keten CSC-CSP 21

Objecttoelichting 21

3.3.3 B.03 Identificeren van de relevante wet- en regelgeving 23

Objecttoelichting 23

3.3.4 B.04 Waarborgen van de wet- en regelgeving bij de selectie van een CSP 25

Objecttoelichting 25

3.3.5 B.05 Risicoafweging bij de selectie van een clouddienst van een CSP 27

Objecttoelichting 27

3.3.6 B.06 Risicoafweging voorafgaand aan de verwerking van persoonsgegevens 30
Objecttoelichting 30
3.3.7 B.07 Afspraken over risicomanagement tijdens de inzet van de clouddienst 32
Objecttoelichting 32
4 Uitvoeringsdomein 35
4.1 Doelstelling 35
4.2 Risico's 35
4.2.1 U.01 Leveranciersovereenkomsten 35
Objecttoelichting 35
4.2.2 U.02 Retourneren, verplaatsen en verwijderen van bedrijfsmiddelen 37
Objecttoelichting 38
4.2.3 U.03 Veilige software 41
Objecttoelichting 41
4.2.4 U.04 Wijzigingsbeheer 42
Objecttoelichting 42
4.2.5 U.05 Intellectuele eigendomsrechten 43
Objecttoelichting 44
4.2.6 U.06 Kloksynchronisatie 44
Objecttoelichting 45
4.2.7 U.07 Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen 45
Objecttoelichting 46
4.2.8 U.08 Identiteits- en toegangsmanagement 47
Objecttoelichting 48
4.2.9 U.09 Beperking toegang tot informatie en speciale toegangsrechten 50
Objecttoelichting 50
4.2.10 U.10 Gebruik van cryptografie 52
Objecttoelichting 52
4.2.11 U.11 Logging en monitoring 55
Objecttoelichting 55
4.2.12 U.12 Toegangsbeveiliging in een multi-tenant-omgeving 57
Objecttoelichting 57

4.2.13 U.13 Netwerksegmentatie en koppelvlakken 59
Objecttoelichting 59
4.2.14 U.14 Beschermen van registraties 61
Objecttoelichting 61
4.2.15 U.15 Inzicht in de beschikbare speciale systeemhulpmiddelen 62
Objecttoelichting 63
4.2.16 U.16 Gedocumenteerde bedieningsprocedures 64
Objecttoelichting 64
4.2.17 U.17 Bewustwording, opleiding en training 65
Objecttoelichting 65
4.2.18 U.18 Beheer van technische kwetsbaarheden 66
Objecttoelichting 67
4.2.19 U.19 Melden van informatiebeveiligingsgebeurtenissen 68
Objecttoelichting 68
4.2.20 U.20 Opvolging informatiebeveiligingsincidenten 70
Objecttoelichting 70
4.2.21 U.21 Waarborgen van de bedrijfscontinuïteit 72
Objecttoelichting 72
4.2.22 U.22 Capaciteitsbeheer 74
Objecttoelichting 74
4.2.23 U.23 Back-up van informatie 75
Objecttoelichting 75
5 Control-domein 78
5.1 Doelstelling 78
5.2 Risico’s 78
5.3 Objecten, controls en maatregelen 78
5.3.1 C.01 Registratie cloudgebruik en bijhouden risicoanalyses 78
5.3.2 C.02 Onpartijdige beoordeling CSP 80
5.3.3 C.03 Beheerorganisatie CSC-CSP inzet clouddiensten 83
5.3.4 C.04 Controle op de afhandeling van beveiligingsgebeurtenissen 84
5.3.5 C.05 Controle op de afspraken uit leveranciersovereenkomst en SLA 86

Objecttoelichting 86

Voorwoord

Voor je ligt 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 (BIO2) en verschaft een overzicht van de uitwerking van clouddienstenobjecten vanuit de optiek van de CSC (Cloud Service Consumer).

De BIO2 is verplicht verklaard voor alle 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. Dat komt omdat de BIO2 gebaseerd is op een generieke baseline NEN-EN-ISO/IEC 27002:2022 (hierna genoemd ISO 27002:2022). Aanvullend op deze ISO-norm zijn door NEN-EN-ISO/IEC een aantal implementatiekaders opgesteld en bestaan er kaders, zoals Cloud Controls Matrix and CAIQ v4 (CCM) (verder aangeduid als CCM:2020) van Cloud Security Alliance (CSA) [1] en de Cloud computing criteria catalogue (C5) van Bundesamt für Sicherheit in der Informationstechnik (BSI) (verder aangeduid als BSI C5:2021) [2] die relevante controls en maatregelen voor clouddiensten bevatten.

De privacyaspecten, die aanvullend op de aspecten van informatiebeveiliging van toepassing zijn, zijn bijeengebracht in een apart privacy-supplement. Daar waar de AVG-wetgeving van invloed is op de vereisten voor de inzet van de clouddienst, is de AVG meegenomen. Ook de Informatiebeveiligingsdienst (IBD) heeft een handreiking Cloudcomputing en Privacy.

Voor de structurering van dit document is dezelfde systematiek gekozen als bij de overige BIO Thema-uitwerkingen. De intentie van dit document is de lezer verder te helpen bij vraagstukken over clouddiensten. Als onderdeel van dit document biedt het CIP een 10-stappenplan voor het verwerven en inzetten van clouddiensten.

Daar waar verbeterd kan worden, kan deze thema-uitwerking verrijkt worden met aangeleverde teksten.

1 Inleiding

Cloudcomputing[1]-diensten, ookwel clouddiensten, is het via internet beschikbaar stellen van applicaties, platformen en infrastructuren. Cloud Service Provider (CSP) biedt de clouddiensten in de vorm van een black box aan. Dit betekent dat clouddiensten gekozen worden met een veelal vooraf vastgestelde 'dienstenmenukaart'. De Cloud Service Customer (CSC) kan, doordat het standaard diensten betreft, beperkt eisen stellen aan de inrichting van de clouddienst.

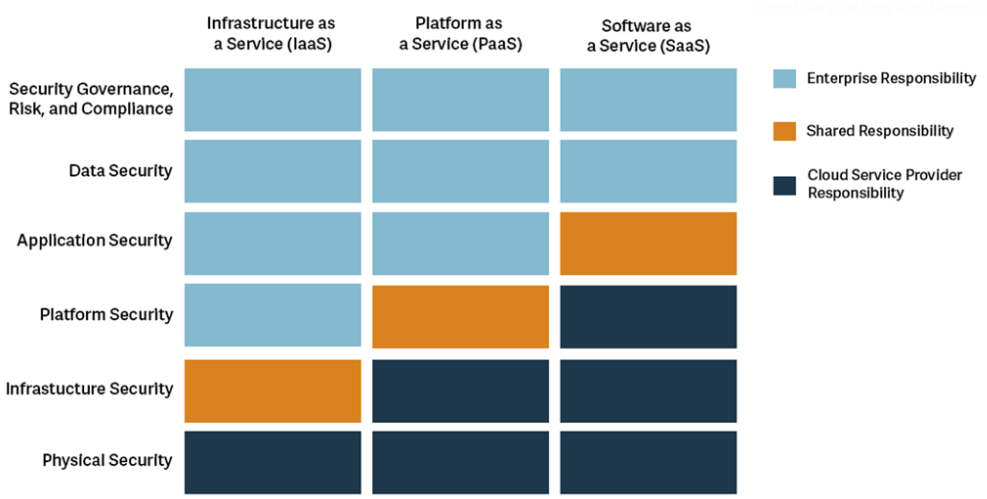
In het algemeen zijn er drie soorten clouddiensten te onderscheiden:

1. **Private (met een dedicated infrastructuur):**
   De clouddienst is ingericht voor één CSC (één 'tenant').
2. **Private/shared (met een geheel of gedeeltelijk gedeelde infrastructuur):**
   Een clouddienst is toegankelijk voor één CSC, maar meerdere CSC's delen (om kosten te besparen) de onderliggende infrastructuur met andere CSC's (bijvoorbeeld de opslag en het netwerk).
3. **Public (met een gedeelde infrastructuur):**
   De clouddiensten zijn toegankelijk via het internet. De clouddiensten worden, met de juiste scheiding tussen de verschillende CSC's, meestal gedeeld met andere CSC's (in een multi-tenant-omgeving).

De meest bekende typen clouddiensten zijn:

- **Software as a Service (SaaS):**
  Bij SaaS heeft de afnemer geen controle over het onderliggende platform, de infrastructuur, zoals het netwerk, en de fysieke beveiliging van de rekencentrums. De software is een gedeelde verantwoordelijkheid.
- **Platform as a Service (PaaS):**
  Bij PaaS wordt de infrastructuur beheerd door de CSP. Het platform is een gedeelde verantwoordelijkheid. Op het platform worden gestandaardiseerde diensten aangeboden, zoals toegangsbeheersing en integratiemogelijkheden.
- **Infrastructure as a Service (IaaS):**
  Bij IaaS wordt alleen de infrastructuur en de fysieke omgeving door de CSP aangeboden. De infrastructuur is een gedeelde verantwoordelijkheid.

[1] Cloudcomputing 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).



Bron: The Official (ISC)² Guide to the CCSP CBK, 2nd Edition

Afbeelding 1: Verantwoordelijkheden per type clouddienst

1.1 Doelstelling

Het doel van deze BIO Thema-uitwerking is het aanbieden aan overheidsorganisaties van een handreiking die toegepast kan worden bij de inzet van clouddiensten en die systematisch de daarbij van belang zijnde aspecten belicht. De focus van deze thema-uitwerking ligt op informatiebeveiliging en privacybescherming.

Dit document kan gebruikt worden in het inkoopproces bij de selectie van een cloudddienstenleverancier en de keuze welke verwerkingen binnen de clouddienst van die cloudddienstenleverancier mogelijk zijn. De keuze van beheersmaatregelen dient plaats te vinden op basis van een risicoafweging.

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.

Door eerst op de objecten te focussen, wordt inzicht verkregen in de relatie tussen en 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 ingedeeld in respectievelijk het beleids-, uitvoerings- en control-domein.

Door de juiste afspraken kunt u als opdrachtgevende partij komen tot een veilig inzetbare clouddienst en de risico’s in alle fasen van de levenscyclus van de clouddienst beheersen. De beveiligingsobjecten vormen de inhoudelijke onderwerpen, waarover afspraken gemaakt moeten worden.

De standaard opzet voor BIO Thema-uitwerkingen wordt ook in dit document gevolgd. Vanwege het bijzondere karakter van deze thema-uitwerking zijn, voor betere begripsvorming, enkele onderwerpen toegevoegd:

- Voorwaarden vanuit CIO Rijk (zie paragraaf 1.3).
- De relatie tussen de CSC en de CSP (zie paragraaf 1.4).
- Het inzetten van de objecten bij de keuze van de clouddiensten (zie paragraaf 1.5).
- Scope en begrenzing van de thema-uitwerking (zie paragraaf 1.6).
- Toepassing BIO Thema-uitwerking Clouddiensten in een 10-stappenplan (zie paragraaf 1.7).
- Dreigingen/kwetsbaarheden (zie paragraaf 2.1).
- CSC-georiënteerde aandachtspunten (zie paragraaf 2.2).
- Beveiligingsobjecten voor clouddiensten in het beleids-, uitvoerings- en control-domein gerelateerd aan basiselementen (zie hoofdstuk 3, hoofdstuk 4 en hoofdstuk 5).

1.3 Voorwaarden vanuit CIO Rijk

Overheden die clouddiensten willen aanbesteden, dienen zich vanuit hun eindverantwoordelijkheid de vraag te stellen welke gegevens van medewerkers, burgers en bedrijven opgeslagen kunnen worden in de (publieke) cloud en welke gegevens binnen de bescherming van de rekencentra van de overheid moet blijven. Om hier antwoord op te kunnen geven is het Rijksbreed cloudbeleid (verder aangeduid als RBC:2022) [3] en het Implementatiekader risicoafweging cloudgebruik (verder aangeduid als IK:2023) [4] door CIO Rijk opgesteld. Voor overheidspartijen is het Rijksbreed cloudbeleid RBC:2022 en het bijbehorende Implementatiekader risicoafweging cloudgebruik IK:2023 een verplichting. Dit cloudbeleid staat overheidsdiensten, met enkele uitzonderingen, onder voorwaarden toe publieke clouddiensten te gebruiken. Deze uitzonderingen en voorwaarden zijn in deze thema-uitwerking meegenomen. Tevens is bij de totstandkoming van deze thema-uitwerking gekeken naar de bestaande normenkaders. Omdat de inzet van clouddiensten ook moet voldoen aan wet- en regelgeving is gekeken naar de bestaande wetten, zoals de Cbw (NIS2). Bedenk daarbij ook dat de clouddienstenleverancier is gebonden aan de wet- en regelgeving die geldt in het land waar de gegevens worden verwerkt. De impact hiervan is als aandachtsgebied meegenomen. De voorwaarden die in het RBC:2022 en het bijbehorende IK:2023 zijn beschreven zijn in dit thema-document meegenomen.

1.4 De relatie tussen CSC en CSP

Vanuit de CSC beredeneerd zijn er drie mechanismen die sturing geven aan de verhouding tussen de CSC en de CSP:

1. **Het Service Level Agreement (SLA):**
   Krijgt de CSC qua prestaties op dagelijkse basis de juiste diensten geleverd, zoals die in de SLA zijn vastgelegd. Anders gezegd, de geleverde diensten voldoen wel of niet aan de prijs, kwaliteit, veiligheids- en continuïteitseisen?
2. **De leveranciersovereenkomst:**
   Krijgt de CSC zekerheid dat afspraken die nodig zijn voor de CSC om zijn eindverantwoordelijkheid voor de informatieveiligheid en de privacybescherming in te vullen, terwijl de CSP de juiste informatie krijgt om de dienst conform de vereisten in te vullen?
3. **Het aantonen van compliancy:**

   Krijgt de CSC de zekerheid dat de **bedrijfsvoering** van de CSP in de afgelopen periode is verlopen conform wet- en regelgeving, normenkaders en contracten, met daarin de bedrijfseisen en beveiligingseisen?

1.5 Het inzetten van de objecten bij de keuze van de toepassing van clouddiensten

De objecten zijn verdeeld naar beleids-, uitvoerings- en control-domein.

Een deel van de objecten is alleen van belang voor de CSC. Het overgrote deel is echter van belang voor zowel de CSC als de CSP. De CSC neemt op basis van een risicoafweging de beslissing welke objecten en welk deel van de maatregelen mee te nemen in de keuze voor een clouddienst. Voor zowel de CSC als de CSP is het vervolgens van belang om overeenstemming te bereiken over hoe de maatregelen vormgegeven moeten gaan worden. Zij kunnen zich de volgende vragen stellen:

- CSC: Krijg ik de juiste dienst(en) geleverd van de CSP?
- CSP: Lever ik straks de dienst die aansluit bij de eisen en verwachtingen van de CSC?

1.5.1 *Beleidsdomein*

In het beleidsdomein stelt de CSC enerzijds de randvoorwaarden op voor een veilige inzet en anderzijds voert het een risicoafweging of die veilige inzet mogelijk is. Van beide zijden moet er transparantie zijn over het gevoerde beleid.

1.5.2 *Uitvoeringsdomein*

Binnen dit domein gaat het om de operationele levering van clouddiensten. Aan beide zijden moet transparantie zijn over de gevraagde en daadwerkelijke leveringen. Voor de beoogde dienstverlening moeten de afspraken hierover aan de kant van de CSC en de CSP op elkaar zijn afgestemd.

1.5.3 *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.

1.6 Scope en begrenzing van de thema-uitwerking

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.

Migratiestrategieën voor het overgaan naar clouddienstverlening vallen buiten de scope van dit document. In de praktijk zijn daarvoor verschillende handreikingen beschikbaar.

De algemene eisen uit de BIO2, ISO 27001:2022 en ISO 27002:2022 blijven onverminderd van kracht. Het gaat in deze thema-uitwerking om specifieke additionele objecten die gerelateerd zijn aan clouddiensten, met gerelateerde maatregelen die realistisch en implementeerbaar zijn voor een CSP.

1.7 Toepassing BIO Thema-uitwerking Clouddiensten in een 10-stappenplan

Het gebruik van publieke clouddiensten kan interessante voordelen opleveren, maar er zijn ook risico’s aan verbonden. Voor overheidspartijen is informatieveiligheid en de bescherming van de privacygevoelige gegevens van groot belang. Dit thema-document richt zich op een verantwoorde inzet van public clouddiensten en beschrijft daartoe de vereisten om die risico’s te beheersen. De vereisten

stelt de overheidspartijen in staat de vereiste afspraken met clouddienstenleveranciers te maken en goed risicomanagement in te richten.

Bij de opzet van deze thema-uitwerking is het onderwerp cloud benaderd onafhankelijk van het type clouddienst (SaaS, PaaS en IaaS). Het verwerven en inzetten van clouddiensten aan de hand van dit document vergt implementatie aan de hand van een 10-stappenplan.

Het 10-stappenplan voor het verwerven en inzetten van clouddiensten:

1. Bepaal als eerste de case en het type dienst dat verworven moet worden.
2. Bepaal de beleidsregels en de rollen en verantwoordelijkheden voor informatiebeveiliging bij de inzet van clouddiensten (zie B.01 en B.02).
3. Bepaal, wanneer bekend is wie de potentiële dienstverlener is, welke wet- en regelgeving voor u als CSC en voor de CSP geldt (zie B.03).
4. Maak een risicoafweging bij het bepalen van de CSP en de keuze een verwerking over te zetten naar die CSP (zie B.04 en B.05).
5. Ga na of de juiste afspraken met de CSP zijn te maken over risicomanagement tijdens de inzet van de clouddienst (zie B.07).
6. Identificeer vervolgens de operationele beveiligingsobjecten. Raadpleeg hierbij de objecten in het uitvoeringsdomein (zie hoofdstuk 4 Uitvoeringsdomein).
7. Identificeer daarna de conditionele objecten. Raadpleeg hierbij de objecten in het beleidsdomein (zie hoofdstuk 3 Beleidsdomein).
8. Identificeer tenslotte de beheersingsobjecten. Raadpleeg hierbij de objecten in het control-domein (zie hoofdstuk 5 Control-domein).
9. Neem de beveiligingsobjecten op in het programma van Eisen 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.
10. Leg, nadat de leverancier is gekozen, de afspraken (die een uitwerking zijn van de maatregelen in de objecten) vast in de leveranciersovereenkomst.

1.8 Referenties

[1] CSA. CCM v4.0 Implementation Guidelines van Cloud Security Alliance (CSA). https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/

[2] BSI (2020). Cloud computing C5 criteria catalogue. https://www.BSI.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

[3] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2022). Rijksbreed cloudbeleid 2022. https://www.rijksoverheid.nl/documenten/kamerstukken/2023/01/24/aanbiedingsbrief-documenten-over-rijksbreed-cloudbeleid-2022

[4] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2023). Implementatiekader risicoafweging cloudgebruik. https://www.rijksoverheid.nl/documenten/rapporten/2023/01/05/implementatiekader-risicoafweging-cloudgebruik

2 Risico's in relatie tot clouddiensten

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

1. Gegevens
   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[2]

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 geeft de belangrijkste kwetsbaarheden en voorkomende consequenties aan.

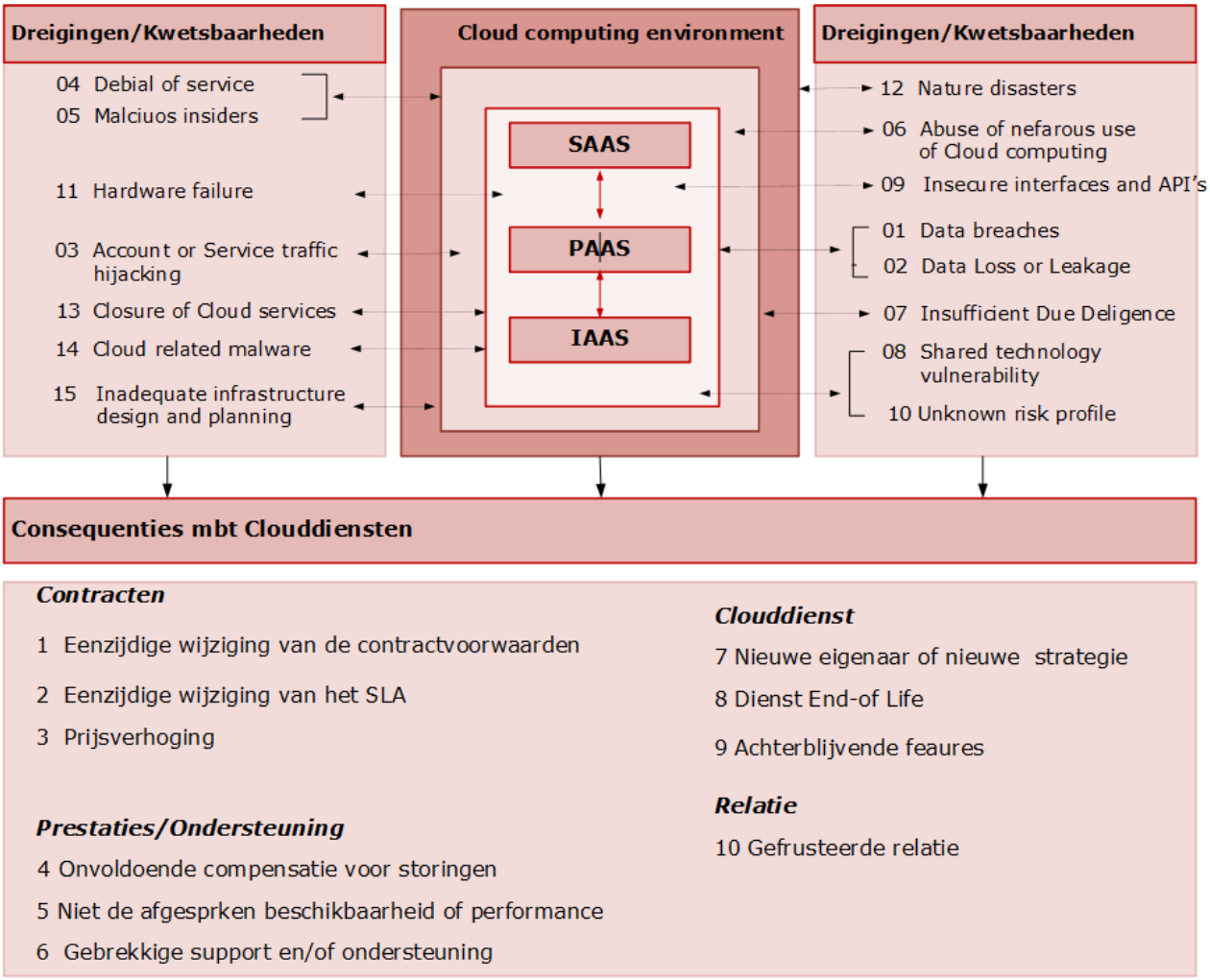
Afbeelding 2 beschrijft de consequenties van die belangrijkste dreigingen voor het contract, de prestaties/ondersteuning, de clouddienst en de relatie tussen CSC en CSP.

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 (DoS)
5		Malicious insiders	Kwaadwillende insiders

[2] 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		
6		Abuse of nefarious use of cloud computing	Misbruik of misdadig gebruik van cloudcomputing
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
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

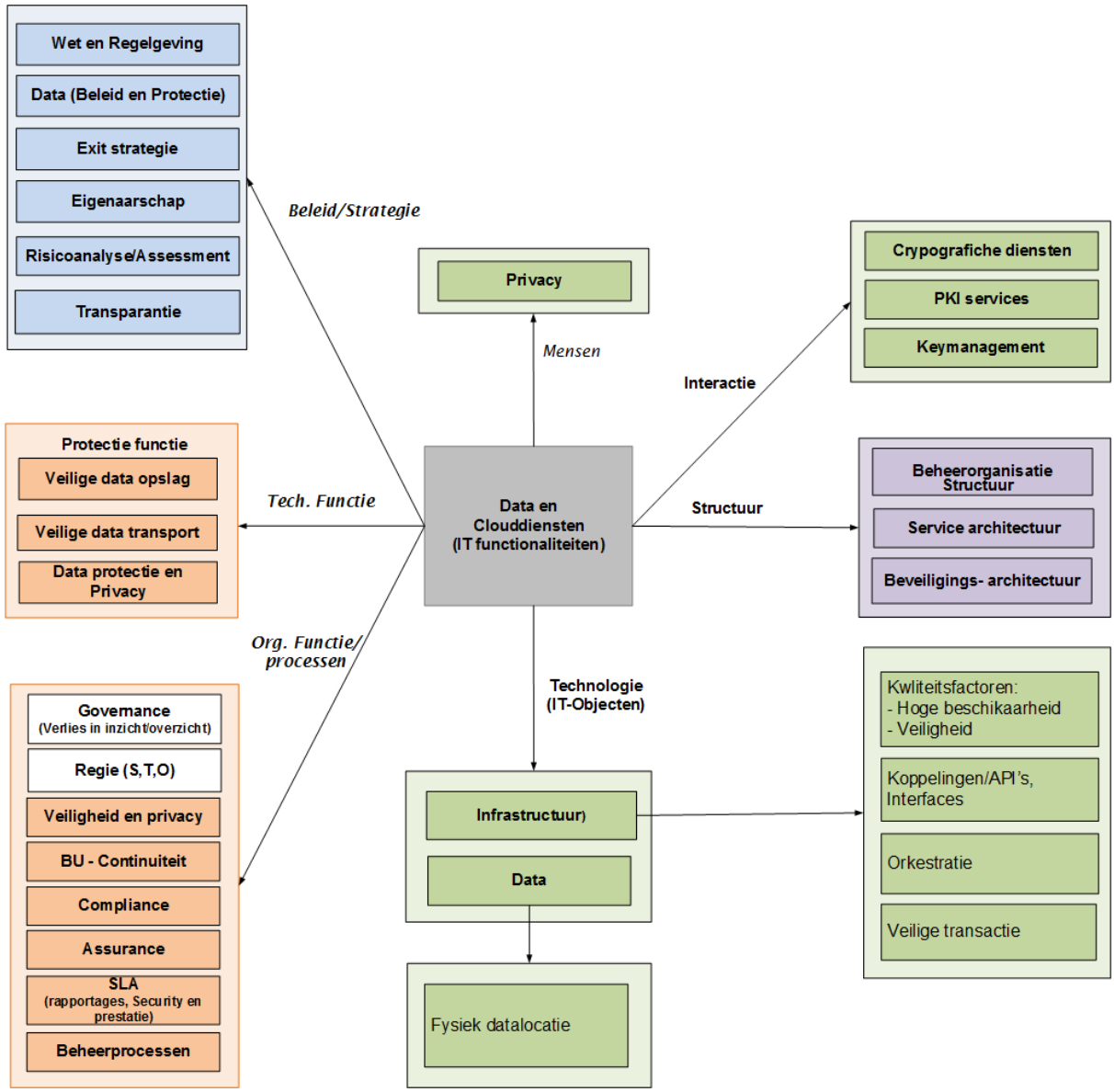
Tabel 1: Cloud Computing Vulnerabilities CSA and Greer and Jackson, 2017



Afbeelding 2: Cloud-gerelateerde dreigingen en kwetsbaarheden

2.2 CSC-georiënteerde aandachtspunten

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 3 geeft een overzicht van de ingedeelde onderwerpen.



Afbeelding 3: CSC-georiënteerde aandachtspunten

3 Beleidsdomein

3.1 Doelstelling

De doelstelling van het beleidsdomein is het identificeren en beschrijven van de conditionele elementen die voorwaardelijk zijn voor het inrichten, beveiligen en beheersen van clouddiensten. De hierbij van belang zijnde beveiligingsobjecten zijn uitgewerkt in controls en gerelateerde maatregelen.

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.

3.3 Objecten, controls en maatregelen

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

3.3.1 *B.01 Beleidsregels voor informatiebeveiliging bij de inzet van clouddiensten*

Objectdefinitie

De beleidsregels voor informatiebeveiliging bij de inzet van clouddiensten legt de intenties en richting vast met betrekking tot de veilige inzet van clouddiensten, zodat de beschikbaarheid, integriteit en vertrouwelijkheid van informatie en de verwerking ervan veilig gebeurt. De ontwikkeling van het beleid komt cyclisch tot stand, zodat het beleid kan worden bijgestuurd en gecorrigeerd.

Objecttoelichting

De beleidsregels betreffen het beleid van de eigen organisatie, in deze van de CSC, en heeft betrekking op de informatie- en bedrijfsprocessen bij de keuze voor de inzet van clouddiensten.

Het vraagt dan extra aandacht om het beleid van de CSC en van de CSP op elkaar aan te laten sluiten.

Doelstelling	De voortdurende geschiktheid, toereikendheid, doeltreffendheid van de sturing en ondersteuning door het management overeenkomstig de bedrijfseisen en de eisen van wet- en regelgeving, statutaire en contractuele eisen te bewerkstelligen.
Risico	Als onderwerp-specifieke beleidsregels voor informatiebeveiliging bij clouddiensten ontbreken of onvoldoende zijn uitgewerkt, bestaat het risico dat clouddiensten worden gekozen en gebruikt zonder aantoonbare aansluiting op bedrijfs-, wettelijke en contractuele eisen, waardoor tekortkomingen in beveiliging en compliance ontstaan.

Control	Informatiebeveiligingsbeleid en **onderwerp specifieke beleidsregels** voor de inzet van clouddiensten behoren te worden **gedefinieerd**, **goedgekeurd** door het management, gepubliceerd, gecommuniceerd aan en erkend door relevant personeel en relevante belanghebbenden en met geplande tussenpozen en als zich significante wijzigingen voordoen, te worden beoordeeld.		ISO 27002:2022 5.1
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
onderwerp-specifieke beleidsregels	1.	Er zijn in lijn met het Rijksbreed cloudbeleid specifieke beleidsregels die de veiligheid bij het gaan inzetten van clouddiensten waarborgt.	RCB-voorwaarde 1
	2.	Het informatiebeveiligingsbeleid van de CSC bevat onderwerp specifieke beleidsregels voor cloudcomputing.	ISO 27017:2015 5.1.1
	3.	Het informatiebeveiligingsbeleid van de CSC voor cloudcomputing is consistent met de aanvaardbare niveaus van informatiebeveiligingsrisico's van de organisatie voor zijn informatie- en andere bedrijfsmiddelen.	ISO 27017:2015 5.1.1
gedefinieerd	4.	Bij het definiëren van het informatiebeveiligingsbeleid voor cloudcomputing moet de CSC rekening houden met: • informatie die is opgeslagen in de cloudcomputing-omgeving kan onderworpen zijn aan toegang en beheer door de CSP; • bedrijfsmiddelen kunnen worden onderhouden in de cloudcomputing-omgeving, bijvoorbeeld applicatieprogramma's; • processen kunnen draaien op een gevirtualiseerde clouddienst met meerdere tenants; • de gebruikers van de clouddienst en de context waarin zij de clouddienst gebruiken; • de clouddienstbeheerders van de CSC die bevoorrechte toegang hebben; • de geografische locaties van de organisatie van de CSP en de landen waar de CSP de CSC-gegevens kan opslaan (zelfs tijdelijk).	ISO 27017:2015 5.1.1

	5.	Bij het definiëren van het informatiebeveiligingsbeleid voor clouddiensten moet de CSP rekening houden met: • de basisvereisten voor informatiebeveiliging die van toepassing zijn op het ontwerp en de implementatie van de clouddienst; • risico's van geautoriseerde insiders; • multi-tenancy en CSC-isolatie (inclusief virtualisatie); • toegang tot CSC-middelen door personeel van de CSP; • toegangscontroleprocedures, bijvoorbeeld sterke authenticatie voor administratieve toegang tot clouddiensten; • communicatie met CSC's tijdens wijzigingsbeheer; • virtualisatiebeveiliging; • toegang tot en bescherming van CSC-gegevens; • levenscyclusbeheer van CSC-accounts; • communicatie over inbreuken en richtlijnen voor het delen van informatie ter ondersteuning van onderzoeken en forensisch onderzoek; • de verplaatsing of overdracht van bedrijfsmiddelen, inclusief informatie.	ISO 27017:2015 5.1.1 BSI C5:2021 DCS-02
	6.	Door de CSC zijn de basisvereisten voor het beveiligen van de verschillende applicaties vastgesteld en gedocumenteerd.	CCM:2020 AIS-02
goedgekeurd	7.	Het informatiebeveiligingsbeleid voor cloudcomputing moet zijn goedgekeurd door het voor cloudcomputing verantwoordelijke management.	ISO 27002:2022 5.1
	8.	Het management van de CSP heeft een informatiebeveiligingsbeleid goedgekeurd en gecommuniceerd naar interne en externe medewerkers en de CSC’s.	BSI C5:2021 OIS-02

3.3.2 *B.02 Rollen en verantwoordelijkheden bij informatiebeveiliging in de keten CSC-CSP*

Objectdefinitie

Het definiëren en toewijzen van rollen en verantwoordelijkheden in de keten CSC-CSP gebeurt overeenkomstig de behoefte van de CSC en de CSP. Daarbij moeten de coördinatie van en het toezicht op de informatiebeveiligingsaspecten van leveranciersrelaties worden geïdentificeerd en gedocumenteerd. De betrokken personen dienen competent te zijn voor de gegeven opdracht.

Objecttoelichting

Ook wanneer binnen en tussen de partijen de verantwoordelijkheden zijn vastgelegd, is de CSC aansprakelijk voor de beslissing om van de dienst gebruik te maken. Die beslissing moet worden

genomen in overeenstemming met de rollen en verantwoordelijkheden die binnen de organisatie van de CSC zijn vastgesteld.

De CSP is verantwoordelijk voor de informatiebeveiliging zoals vastgelegd in de clouddienstovereenkomst. De implementatie en inrichting van informatiebeveiliging moet plaatsvinden in overeenstemming met de rollen en verantwoordelijkheden die binnen de organisatie van de CSP zijn vastgesteld.

Doelstelling	Een gedefinieerde, goedgekeurde en duidelijk te begrijpen structuur voor de implementatie, uitvoering en het beheer van informatiebeveiliging tussen de CSC en de CSP inrichten.		
Risico	Als rollen, verantwoordelijkheden en bevoegdheden tussen CSC en CSP niet expliciet zijn vastgesteld en geborgd, bestaat het risico dat beveiligingstaken en besluitvorming niet eenduidig worden uitgevoerd (met name bij incidenten, wijzigingen en escalaties), waardoor beheersmaatregelen uitblijven en de kans op beveiligings- en contractuele geschillen toeneemt.		
Control	Rollen en verantwoordelijkheden bij informatiebeveiliging behoren te worden **gedefinieerd en toegewezen** overeenkomstig de **behoeften** en **privacy-vereisten** van de betrokken organisaties.		ISO 27002:2022 5.2
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
gedefinieerd en toegewezen	1.	De processen van de CSC voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten behoren overeenkomstig de informatiebeveiligingseisen van de organisatie te worden opgesteld.	ISO 27002:2022 5.23
	2.	De CSC moet met de CSP overeenstemming bereiken over een passende toewijzing van rollen en verantwoordelijkheden op het gebied van informatiebeveiliging, en bevestigen dat hij de toegewezen rollen en verantwoordelijkheden kan vervullen. De rollen en verantwoordelijkheden op het gebied van informatiebeveiliging van beide partijen moeten in de leveranciersovereenkomst worden vastgelegd.	ISO 27017:2015 6.1.1
	3.	De CSP moet een passende toewijzing van rollen en verantwoordelijkheden op het gebied van informatiebeveiliging overeenkomen en documenteren met zijn CSC's, CSP's en leveranciers.	ISO 27017:2015 6.1.1

behoeften	4.	De CSC moet zijn relatie met de ondersteunings- en zorgfunctie van de CSP identificeren en beheren.	ISO 27017:2015 6.1.1
privacy-vereisten	5.	Bij de toewijzing van rollen en verantwoordelijkheden moet rekening worden gehouden met de CSC-gegevens en de CSC-aanvragen, waarbij de CSP de verwerker is.	ISO 27017:2015 6.1.1

3.3.3 *B.03 Identificeren van de relevante wet- en regelgeving*

Objectdefinitie

Het identificeren van de relevante wet- en regelgeving betreft het identificeren ervan door zowel de CSC als de CSP en dan wel voor alle rechtsgebieden waar CSC-gegevens kunnen worden opgeslagen, verwerkt of verzonden, inclusief waar vandaan de clouddienst wordt beheerd, omdat dit laatste ook een vorm van verwerking is, zoals gedefinieerd in de AVG.

Objecttoelichting

De beheersmaatregel gaat over het identificeren en zodoende kunnen naleven van alle voor de inzet en uitvoering van de clouddienst relevante wettelijke, statutaire, regelgevende en contractuele informatiebeveiligingseisen. Informatie over geografische locaties waar de CSC-gegevens kunnen worden opgeslagen, verwerkt of verzonden, is voor de CSC van belang om te kunnen bepalen wat de toezichthoudende autoriteiten en de rechtsgebieden zijn.

Doelstelling	Identificatie van de van toepassing zijnde juridische, regelgevende, zelfopgelegde of contractuele vereisten voor informatiebeveiliging voor zowel CSC als CSP.	
Risico	Als toepasselijke wet- en regelgeving en contractuele eisen voor de clouddienst (incl. landen waar opslag/verwerking plaatsvindt) niet volledig en actueel worden geïdentificeerd, bestaat het risico dat de organisatie onbewust niet-compliant is of eisen niet kan afdwingen bij de CSP, met mogelijke sancties, herstelkosten en onderbreking van dienstverlening tot gevolg.	
Control	De CSC en CSP behoren contact met de **relevante instanties** te leggen en te onderhouden, zij behoren daarbij de **wettelijke, statutaire, regelgevende en contractuele eisen** die relevant zijn voor informatiebeveiliging en de aanpak van de organisatie om aan deze eisen **te voldoen**, te identificeren, te documenteren en actueel te houden.	ISO 27002:2022 5.5, 5.6 en 5.31
Conformiteitsindicator, nummer en maatregel		Afgeleid/afkomstig van

relevante instanties	1.	De CSP moet de CSC informeren over de geografische locaties van de organisatie van de CSP en de landen waar de CSP de CSC-gegevens kan opslaan. Bij het bepalen van de geografische locaties wordt ook gekeken naar alle plaatsen waar (vandaan) verwerking, inclusief (technische) beheeractiviteiten, plaatsvinden.	ISO 27017:2015 6.1.3 CIP-netwerk AVG art. 4
	2.	De CSC moet de autoriteiten identificeren die relevant zijn voor de gecombineerde werking van de CSC en de CSP.	ISO 27017:2015 6.1.3
wettelijke, statutaire, regelgeven-de en contractuele eisen	3.	De CSC houdt, naast de wet- en regelgeving die voor de CSC geldt (zie ook B.04), rekening met de voor de CSP geldende wet- en regelgeving.	ISO 27017:2015 18.1.1
	4.	De CSP moet de CSC informeren over de jurisdicties die van toepassing zijn op de clouddienst.	ISO 27017:2015 18.1.1
	5.	De CSP moet zijn eigen relevante wettelijke vereisten identificeren (bijvoorbeeld met betrekking tot encryptie). Deze informatie moet ook aan de CSC worden verstrekt wanneer daarom wordt gevraagd.	ISO 27017:2015 18.1.1
te voldoen	6.	De CSC moet bewijs vragen van de naleving door de CSP van de relevante regelgeving en normen die vereist zijn voor de activiteiten van de CSC. Dergelijk bewijs kunnen de certificeringen zijn die door externe auditors zijn geproduceerd.	ISO 27017:2015 18.1.1
	7.	De CSP moet de CSC voorzien van bewijs van zijn huidige naleving van de toepasselijke wetgeving en contractuele vereisten.	ISO 27017:2015 18.1.1
	8.	De CSC dient te verifiëren dat de set cryptografische controles die van toepassing zijn op het gebruik van een clouddienst voldoet aan relevante afspraken, wet- en regelgeving.	ISO 27017:2015 18.1.5

	9.	De CSP moet beschrijvingen verstrekken van de door de CSP geïmplementeerde cryptografische controles aan de CSC voor het beoordelen van de naleving van toepasselijke overeenkomsten, wet- en regelgeving.	ISO 27017:2015 18.1.5

3.3.4 *B.04 Waarborgen van de wet- en regelgeving bij de selectie van een CSP*

Objectdefinitie

Het waarborgen van de wet- en regelgeving betreft het waarborgen van de relevante wet- en regelgeving, voorafgaand aan de inzet/verwerving/aanbesteding van een clouddienst en dus voorafgaand aan de contractering of, als er voor de inzet geen contract nodig zou zijn, het gebruik.

Objecttoelichting

Het betreft hier weer alle wetsgebieden, dus die van CSC en CSP. Omdat het waarborgen verschilt per geografische locatie, waar de CSC-gegevens kunnen worden opgeslagen, verwerkt of verzonden, wordt onderscheid gemaakt tussen de verwerking binnen en buiten de grenzen van de Europese Economische Ruimte (EER).

Doelstelling	Clouddiensten worden alleen ingezet wanneer aan de wet- en regelgeving kan worden voldaan.	
Risico	Als bij selectie van de CSP/clouddienst niet aantoonbaar is geborgd dat aan wet- en regelgeving en verplichtingen kan worden voldaan, bestaat het risico dat de clouddienst later moet worden aangepast of beëindigd, met verstoring van dienstverlening, extra kosten en compliance-incidenten tot gevolg.	
Control	De **wet- en regelgeving** van toepassing op de verwerking van vertrouwelijke gegevens en de verwerking **buiten de grenzen** van de EER is duidelijk.	Rijksbreed cloudbeleid RCB:2022
Conformiteitsindicator, nummer en maatregel		Afgeleid/afkomstig van

wet- en regelgeving	1.	De CSC voldoet aan de wet en regelgeving: a. de eisen uit het Voorschrift Informatiebeveiliging Rijksdienst (VIR)[3]; b. het voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIRBI)[4]; c. de BIO[5], de regels omtrent archiveren[6]; d. de AVG[7]; e. de Wet Open Overheid (WOO)[8]; f. de Wet Politiegegevens (WPG)[9].	RCB-voorwaarde 5
buiten de grenzen	2.	Landen met een actief cyberprogramma dat gericht is tegen Nederlandse belangen worden uitgesloten van het kunnen aanbieden van een clouddienst. Mocht er een risico zijn op dreiging van statelijke actoren, wordt voortijdig dreigings- en beveiligingsadvies ingewonnen van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en/of Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Voor de overige landen sluiten aan bij het Europese beleid op dit terrein dat waarborgen biedt tegen misbruik van de informatie die in een cloud is opgeslagen.	RCB-voorwaarde 7, de C2000 criteria en volgens hoofdstuk V van de AVG art. 5

[3] https://wetten.overheid.nl/BWBR0022141/2007-07-01

[4] Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013) - BWBR0033507 (overheid.nl)

[5] Baseline Informatiebeveiliging Overheid

[6] Regels voor archieven overheid | Archieven | Rijksoverheid.nl

[7] Algemene verordening gegevensbescherming EUR-Lex - 32016R0679

[8] wetten.nl - Regeling - Wet open overheid - BWBR0045754

[9] Wet politiegegevens - BWBR 0022463

	3.	De opslag en verwerking van persoonsgegevens voldoet aan de vereisten inzake doorgiften van persoonsgegevens (hoofdstuk V van de AVG), en daarbij wordt voldaan aan één van de onderstaande eisen: a. opslag en verwerking binnen de EER of, b. in landen waarvoor een adequaatheidsbesluit bestaat, of, c. op basis van een passend doorgiftemechanisme dat voldoet aan de vereisten (van art. 46, hoofdstuk V) van de AVG, zoals een modelcontract (standaard contractbepalingen of 'standard contractual clauses'). Indien niet aantoonbaar aan één van die eisen (a, b of c) is voldaan, dan wordt voor die verwerking en alle daarbij behorende subverwerkingen de uitgevoerde (pre-scan of formele) Data Protectie Impact Assessment (DPIA) zo spoedig mogelijk na vaststelling aan CIO Rijk toegezonden. De opslag en verwerking van bijzondere persoonsgegevens voldoet aan eisen a. of b. Als aan c. wordt voldaan geldt aanvullend de eis 'pas-toe-of-leg-uit' (comply or explain), met minimaal een uitgevoerde (pre-scan of formele) DPIA, die zo spoedig mogelijk na vaststelling aan CIO Rijk wordt toegezonden.	RCB-voorwaarde 9 RCB-voorwaarde 10
	4.	De CSC kan de locaties (locatie/land) van de gegevensverwerking en -opslag, inclusief gegevensback-ups, specificeren volgens de contractueel beschikbare opties. De CSP ondersteunt de keuze tot specificatie door middel van een cloudarchitectuur. De vastlegging van de architectuur is gebaseerd op de behoeften van materiedeskundigen van de CSC, zodat de CSC de geschiktheid van de clouddienst kan beoordelen met betrekking tot de wettelijke en regelgevende vereisten.	BSI C5:2021 PSS-12

3.3.5 *B.05 Risicoafweging bij de selectie van een clouddienst van een CSP*

Objectdefinitie

De risicoafweging bij de selectie van een clouddienst van een CSP betreft de risicoafweging voorafgaand aan de contractering van de clouddienst of, als er voor de inzet geen contract nodig zou zijn, het inzetten van een clouddienst, zodat de risico's tijdig kunnen worden voorkomen.

Objecttoelichting

Vanuit het Rijksbreed cloudbeleid worden eisen gesteld aan de inzet van publieke clouddiensten.

Doelstelling	Bij het tegen elkaar afzetten van de voor- en nadelen worden de beveiligings- en privacy-eisen meegenomen.		
Risico	Als beveiligings- en privacyrisico's niet volledig en aantoonbaar worden meegewogen bij de selectie van CSP en clouddienst, bestaat het risico dat de organisatie een dienst afneemt met niet-acceptabele of niet-mitigeerbare risico's, waardoor achteraf dure correcties, aanvullende maatregelen of vervanging noodzakelijk worden.		
Control	Op basis van **vooraf** vastgestelde informatiebeveiligings- en privacy-eisen wordt een **risicoanalyse** en **DPIA** uitgevoerd alvorens een clouddienst van een CSP te selecteren.		ISO 27002:2022 5.8
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
vooraf	1.	Er behoren informatiebeveiligingseisen te worden vastgesteld voor alle bedrijfsprocessen die gebruik gaan maken van de clouddienst(en).	ISO 27002:2022 5.8
risicoanalyse	2.	Bij het selecteren van een CSC wordt rekening gehouden met: 1. onderbouwing van de noodzaak (subsidiariteit) van het cloudgebruik; 2. privacyvoorwaarden en het vooraf onderhandelen daarover; 3. kaders voor publieke waarden zoals voor open source, mensenrechten en duurzaamheid.	IK-voorwaarde 5
	3.	Tijdens de risicoanalyse is het Strategisch Leveranciersmanagement voor de Rijksoverheid (SLM) geraadpleegd[10].	IK-voorwaarde 4
DPIA	4.	Er is een DPIA (gegevensbeschermingseffectbeoordeling), inclusief een relevante risicoafweging op basis van de CIO Rijk implementatierichtlijn, waarbij de besluitvorming toetsbaar en auditeerbaar is.	RCB-voorwaarde 2 CCM:2020 DSP-09

[10] Zie https://slmrijk.pleio.nl/.

	5.	De CSC beschrijft in de toegespitste risicoanalyse ten minste de volgende onderdelen: 1. De context van het cloudgebruik en de karakteristieken van het betreffende cloudgebruik zoals: ○ de beoogde baten; ○ de selectie van de hoofdleverancier en zijn toeleverancier; ○ het type dienstverlening (publieke, private, hybride, community cloud en IaaS, SaaS, PaaS); ○ de gevoeligheid van de type gegevens; ○ de geografische regio van verwerking en opslag van gegevens. 2. De relevante risico's waarbij aandacht is voor: a. de C2000 criteria van het Rijksbreed cloudbeleid. Als er sprake is van risico's voortkomende uit deze criteria wordt conform cloudbeleid tijdig dreigings- en beveiligingsadvies ingewonnen van AIVD en/of MIVD. Indien nationale veiligheidsrisico's niet voldoende kunnen worden beheerst, worden waar mogelijk dergelijke partijen uitgesloten[11]; b. de public cloud risicoscenario's van het Nationaal Bureau voor Verbindingsbeveiliging (NBV); c. de vergelijking met de on-premise verwerking; d. risico's voor veiligheid van personen voor wie er extra risico's zijn indien persoonsgegevens gelekt worden[12]; e. continuïteitsrisico's onder meer voor de uitvoering van taken. 3. De analyse van de getroffen technische en organisatorische maatregelen waaruit blijkt dat CSC en de CSP voldoen aan de gestelde informatiebeveiligingseisen. Hierbij is aandacht voor: a. het door de cloudleverancier toelaten van verantwoordingsonderzoeken of rapportages daarover; b. een beschrijving van de exitstrategie; c. de wijze waarop de leverancier zijn leveranciers beoordeeld, onder meer voor ketenrisico's; d. de beoordeling van de opzet, bestaan en, bij de eerste actualisatie, de werking van de maatregelen; e. de afweging dat de risico's voldoende gemitigeerd worden met eventuele rest-risico's en de borging daarvan. 4. Hoe is geregeld dat de CSP controle en verantwoordingsonderzoeken toelaat of daarover rapporteert. Er bestaat een 'right-to audit' voor de opdrachtgevende organisatie of is er hierover contractueel voldoende zekerheid via (SLM).	RCB-voorwaarde 6 IK-voorwaarde 4 en 6 en IK-bijlage 1 en 2

[11] Conform dreigingsbeeld Statelijke Actoren 2, AIVD, MIVD en NCTV, november 2022: Rusland, China, Iran en Noord-Korea.

[12] Bewindslieden, BN'ers, medewerkers van inlichtingendiensten, getuigen en advocaten in megaprocessen e.d.

	6.	De risicoanalyse is formeel vastgesteld conform een mandateringsregeling.	IK-voorwaarde 4 lid 4
	7.	Risico's moeten bekend en voldoende gemitigeerd zijn en blijven.	RCB-voorwaarde 2

3.3.6 *B.06 Risicoafweging voorafgaand aan de verwerking van persoonsgegevens*

Objectdefinitie

De risicoafweging voorafgaand aan verwerking van persoonsgegevens betreft het waarborgen van de compliance met de AVG voorafgaand aan én per gegevensverwerking in een publieke clouddienst.

Objecttoelichting

Het delen van informatie over de risicoafweging tussen overheden onderling vergroot het lerend vermogen binnen de overheid. Het verstrekken van informatie naar burgers over de besluitvorming biedt de wettelijk vereiste transparantie.

Doelstelling	Het maken van een risicoafweging voorafgaand aan de verwerking van persoonsgegevens en het bieden van openheid hierover.	
Risico	Als voorafgaand aan verwerking van persoonsgegevens in clouddiensten geen (aantoonbare) risicoafweging wordt uitgevoerd en vastgelegd, bestaat het risico dat persoonsgegevens onrechtmatig of onvoldoende beschermd worden verwerkt, met mogelijke schade voor betrokkenen, meldplichten en sancties (AVG) tot gevolg.	
Control	De verwerking van persoonsgegevens vindt pas plaats na het uitvoeren van een **(pre-scan of formele) DPIA**, terwijl de opslag en verwerking van een **basisregistratie** pas plaatsvindt na advies van CIO Rijk, de besluitvorming is **openbaar**.	RBC:2022
Conformiteitsindicator, nummer en maatregel		Afgeleid/afkomstig van

(pre-scan of formele) DPIA	1.	Indien er persoonsgegevens verwerkt gaan worden, dient voorafgaand aan feitelijke verwerking een pre-scan DPIA uitgevoerd te worden en voor hoog-risico verwerkingen een formele DPIA. De DPIA is formeel vastgesteld zijn, conform een mandateringsregeling.	IK-voorwaarde 8 – (Pre-scan) DPIA[13] en AVG art. 35
	2.	In een pre-scan DPIA[14] moeten ten minste de volgende onderdelen herkenbaar zijn[15]: a. Een beschrijving van de verwerking inclusief een beschrijving van het type persoonsgegevens (content, telemetrie, diagnostisch, website en helpdesk), de omvang van de gegevensset de omvang van de verwerking, de betrokkenen en het te ondersteunen proces. b. Omschrijving van de gebruikersgroepen waaronder de afnemers van de dienst en de afnemers van de informatie. c. Voor de formele DPIA dient het rijksbrede model toegepast te worden. d. Indien geen DPIA wordt uitgevoerd, een beschrijving hoe voldaan wordt aan de gestelde privacy-eisen, de beoordeling dat de maatregelen daarvoor feitelijk functioneren en de (lage) rest-risico's. Bij overdracht naar landen buiten de EER zonder een adequaatheidsbesluit[16], is een DPIA nodig conform aanbevelingen van de European Dataprotection Board (EDPB)[17] en bij bijzondere persoonsgegevens extra terughoudendheid conform cloudbeleid en dezelfde aanbevelingen van de EDPB.	IK-voorwaarde 8
openbaar	3.	Indien geen formele DPIA nodig is, moet op een andere wijze aantoonbaar worden voldaan aan de AVG, waaronder een onderbouwing van de rechtmatigheid, proportionaliteit, noodzaak (subsidiariteit) e.d.	IK-voorwaarde 8

[13] Data Protection Impact Assessment; ook wel gegevensbeschermingseffectbeoordeling (GEB) genoemd.

[14] Data Protection Impact Assessment; ook wel gegevensbeschermingseffectbeoordeling genoemd.

[15] Artikel 35, lid 1,3 4 en 5 AVG. Aanvullende lijst AP conform artikel 35, lid 4, opgehaald van: https://autoriteitpersoonsgegevens.nl/nl/nieuws/definitieve-dpia-lijst-beschikbaar#:~:text=Een%20DPIA%20is%20verplicht%20als,ook%20wel%20een%20gegevensbeschermingseffectbeoordeling%20genoemd.

[16] Voorwaarde 9.c uit het Rijksbreed Cloudbeleid 2022.

[17] Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, vastgesteld op 18 juni 2021, opgehaald van: https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf.

Basisregi-stratie	4.	Bij de opslag en verwerking van een basisregistratie in de public cloud geeft CIO Rijk hieraan voorafgaand een advies, waarbij het advies wordt gegeven op basis van minimaal: • de uitleg waarom cloudgebruik noodzakelijk is; • de risicoanalyse; • bij verwerking van persoonsgegevens, de (pres-scan of formele) DPIA en eventueel een DTIA en eventuele rest-risico's voor privacy.	RCB-voorwaarde 11 IK-voorwaarde 12
	5.	De besluitvorming door de eigenaar is openbaar toegankelijk, waaronder de besluitvorming over de DPIA's en indien van toepassing, adviezen van de Privacy Adviseur Rijk (PAR) (Wet Open Overheid (WOO)[18]). Dit gebeurt uiterlijk drie maanden na de ingebruikname.	RCB-voorwaarde 8 IK-voorwaarde 10

3.3.7 *B.07 Afspraken over risicomanagement tijdens de inzet van de clouddienst*

Objectdefinitie

Het risico betreft de kans en de dreiging van elke onverwachte of onverhoopte gebeurtenis die schade kan toebrengen aan de bedrijfsmiddelen, waaronder informatie, van de CSC en de kans en de dreiging van het schaden van de privacy van eenieder, zoals beschreven in de AVG. Het is van belang dit in een cyclisch proces te identificeren, te analyseren en te verrijken, zodat een risicobeeld van de dreiging kan worden opgebouwd en de risico's kunnen worden beperkt.

Objecttoelichting

Bij het rapporteren over de risico's moet ervoor worden gezorgd dat het openbaar maken van implementatiedetails over beveiligingscontroles wordt beperkt tot die betrokkenen van de CSC die over een geheimhoudingsovereenkomst beschikken.

Doelstelling	De verwerking voldoet blijvend aan de informatiebeveiligings- en privacyvereisten.
Risico	Als tijdens gebruik van de clouddienst geen expliciete afspraken en mechanismen bestaan voor doorlopend risicomanagement (bij wijzigingen in dienst, configuratie, keten of dreigingen), bestaat het risico dat nieuwe of gewijzigde risico's niet tijdig worden onderkend en beheerst, waardoor beveiliging en compliance gaandeweg afnemen.

[18] wetten.nl - Regeling - Wet open overheid - BWBR0045754

Control	Informatie met betrekking tot informatiebeveiligingsdreigingen behoort te worden **verzameld en geanalyseerd** op basis van informatie over dreigingen in geselecteerde interne en externe bronnen, dit start al **voorafgaand aan het inzetten** van de clouddienst en geldt voor de gehele (toeleverings)keten van ICT-producten en -diensten.		ISO 27002:2022 5.7 en 5.8
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
verzameld en geanaly-seerd	1.	De CSP en de CSC verzamelen en analyseren informatie die beschikbaar is in geselecteerde interne en externe bronnen over bestaande of opkomende dreigingen teneinde weloverwogen maatregelen mogelijk te maken om te voorkomen dat de dreigingen schade aan de betrokken organisatie toebrengen.	ISO 27002:2022 5.7 en 5.8
	2.	De CSP en de CSC informeren iedereen van de organisaties en elkaar, waarbij de bedreiging impact kan hebben op de hele organisatie, nauwkeurig en gedetailleerd, zodat de partijen snel en doeltreffend kunnen handelen op basis van de informatie.	ISO 27002:2022 5.7 en 5.8
	3.	De toepaste risicomanagementaanpak: • is in lijn met het informatiebeveiligingsbeleid; • is gedocumenteerd volgens een uniforme structuur; • is gebaseerd op erkende standaarden en methoden; • beslaat de gehele levenscyclus van de clouddienst vanaf de start bij de verwerving van de clouddienst tot en met de beëindiging van de clouddienst; • bevat afspraken tussen de CSC en de CSP, zodat de samenwerking op elkaar aansluit.	BSI C5:2021 DEV-01 en SP-01
voorafgaand aan het inzetten	4.	De CSC moet zijn informatiebeveiligingseisen voor de clouddienst bepalen en vervolgens beoordelen of de door een CSP aangeboden diensten aan deze eisen kunnen voldoen.	ISO 27017:2015 14.1.1
	5.	Voor deze analyse moet de CSC informatie over de informatiebeveiligingscapaciteiten opvragen bij de CSP.	ISO 27017:2015 14.1.1
	6.	De CSP moet informatie verstrekken aan de CSC's over de informatiebeveiligingsmogelijkheden die zij gebruiken. Deze informatie moet informatief zijn, zonder informatie vrij te geven die nuttig kan zijn voor iemand met kwade bedoelingen.	ISO 27017:2015 14.1.1

	7.	De CSP biedt CSC's richtlijnen en aanbevelingen voor het veilig gebruik van de aangeboden clouddienst. De daarin opgenomen informatie is bedoeld om de CSC te helpen bij het veilig configureren, installeren en gebruiken van de clouddienst, voor zover van toepassing op de clouddienst en onder de verantwoordelijkheid van de cloudgebruiker. Het type en de reikwijdte van de verstrekte informatie is gebaseerd op de behoeften van materiedeskundigen van de CSC die informatiebeveiligingseisen stellen, deze implementeren of de implementatie verifiëren.	BSI C5:2021 PSS-01

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

Bij de verwerving en het gebruik van de clouddiensten is er geen sturing op het gebruik van de clouddienst, waardoor geen veilige inzet van de clouddienst is gewaarborgd.

4.2.1 *U.01 Leveranciersovereenkomsten*

Objectdefinitie

In een leveranciersovereenkomst worden informatiebeveiligingseisen, processen en procedures vastgelegd die overeengekomen worden met een leverancier. Wat wordt overeengekomen hangt samen met de informatiebeveiligingsrisico's die verband houden met het gebruik van de producten en diensten van deze leverancier.

Objecttoelichting

Gegevens en bestanden op de systemen van de CSP die tijdens het gebruik van de clouddienst worden aangemaakt of gewijzigd, kunnen van cruciaal belang zijn voor de veilige werking, het herstel en de continuïteit van de dienst. Afspraken hierover, inclusief het eigendom van alle bedrijfsmiddelen en de informatie en de partijen die verantwoordelijk zijn voor de activiteiten die verband houden met deze bedrijfsmiddelen, zoals back-up- en hersteloperaties, moeten worden gedefinieerd en gedocumenteerd. Anders bestaat het risico dat de CSP ervan uitgaat dat de CSC bepaalde vitale taken uitvoert (of andersom) en kan er gegevensverlies optreden.

Doelstelling	Overeenkomen van afspraken over en het niveau van dienstverlening waaronder informatiebeveiliging in de leveranciersrelaties CSC-CSP.
Risico	Als afspraken over dienstverlening en informatiebeveiliging tussen CSC en CSP niet expliciet, eenduidig en volledig zijn vastgelegd, bestaat het risico dat verantwoordelijkheden en verwachtingen verschillend worden geïnterpreteerd, waardoor essentiële beveiligings- en beheertaken niet of niet tijdig worden uitgevoerd en dit kan leiden tot verlies van gegevens, verstoring van de dienstverlening en verminderde continuïteit.

Control		Relevante informatiebeveiligingseisen behoren te worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie te worden **overeengekomen**, hierbij wordt ook gekeken naar de **toeleveringsprocessen** van de CSP.	ISO 27002:2022 5.20
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
Overeenge-komen	1.	De CSC moet de rollen en verantwoordelijkheden op het gebied van de dienstverlening waaronder informatiebeveiliging met betrekking tot de clouddienst bevestigen, zoals beschreven in de serviceovereenkomst. Deze kunnen de volgende processen omvatten: • malware bescherming; • back-up; • cryptografische controles; • kwetsbaarheidsbeheer; • probleembehandeling; • technische nalevingscontrole; • beveiligingstests; • auditing; • verzamelen, onderhouden en beschermen van bewijsmateriaal, inclusief logboeken en audittrails; • bescherming van informatie bij beëindiging van de dienstverleningsovereenkomst; • authenticatie en toegangscontrole; • identiteits- en toegangsbeheer.	ISO 27017:2015 15.1.2
	2.	De serviceovereenkomst tussen de CSC en de CSP bevat in ieder geval de volgende bepalingen en/of voorwaarden: • de omvang, kenmerken en locatie van zakelijke relaties en aangeboden diensten; • de informatiebeveiligingseisen; • het verandermanagementproces; • de mogelijkheid tot registratie en monitoring; • de incidentbeheer- en communicatieprocedures; • het recht op audit en beoordeling door derden; • beëindiging van de dienst; • vereisten voor interoperabiliteit en portabiliteit; • de vereisten voor het waarborgen van de privacy van degene waarvan de gegevens worden verwerkt.	CCM:2020 STA-09
	3.	De CSP moet als onderdeel van een overeenkomst de relevante informatiebeveiligingsmaatregelen specificeren die de CSP zal implementeren om misverstanden tussen de CSP en de CSC te voorkomen.	ISO 27017:2015 15.1.2

	4.	De relevante informatiebeveiligingsmaatregelen die de CSP zal implementeren, kunnen variëren afhankelijk van het type clouddienst dat de CSC gebruikt.	ISO 27017:2015 15.1.2
Toeleve-ringsproces-sen	5.	Als een CSP clouddiensten van collega-CSP's gebruikt, moet de CSP ervoor zorgen dat de informatiebeveiligingsniveaus voor zijn eigen CSC's worden gehandhaafd of overschreden.	ISO 27017:2015 15.1.3
	6.	Wanneer de CSP clouddiensten levert op basis van een toeleveringsketen, moet de CSP informatiebeveiligingsdoelstellingen aan leveranciers verstrekken en elk van de leveranciers verzoeken risicobeheeractiviteiten uit te voeren om de doelstellingen te bereiken en geeft de CSC gedetailleerde informatie over het toepassen van de informatiebeveiligingsdoelstellingen en het periodiek uitvoeren van beveiligingsbeoordelingen in de hele toeleveringsketen.	ISO 27017:2015 15.1.3 CCM:2020 STA-03 CCM:2020 STA-14
	7.	De CSP geeft de CSC duidelijkheid over hoe derde partijen wier diensten bijdragen aan het aanbieden van de clouddienst, met daarin: • hoe de risico's die voortvloeien uit de inkoop van diensten van derden zijn beperkt; • duidelijkheid dat hier sprake is van een subverwerker in het kader van de AVG; • duidelijkheid over het gebruik van erkende industriestandaards; • duidelijkheid over toepasselijke wettelijke en regelgevende vereisten; • eisen aan het omgaan met kwetsbaarheden, beveiligingsincidenten en storingen. Met daarbij de: • specificaties voor de contractuele overeenstemming van deze eisen; • specificaties voor het monitoren van deze eisen; en • specificaties om deze eisen ook toe te passen op door de derde partijen gebruikte dienstverleners, voor zover de door deze dienstverleners geleverde diensten ook bijdragen aan het aanbieden van de clouddienst.	BSI C5:2021 SSO-01 AVG- art. 4

4.2.2 *U.02 Retourneren, verplaatsen en verwijderen van bedrijfsmiddelen*

Objectdefinitie

Het retourneren, verplaatsen en verwijderen van bedrijfsmiddelen betreft het verstrekken van bedrijfsmiddelen aan de CSP, omdat deze middelen nodig zijn bij het uitvoeren van de clouddienst. Het teruggeven daarvan is van belang vanwege het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie in het kader van de bedrijfsvoering van de CSC. De bedrijfsmiddelen van de CSC bevatten de (bedrijfs-)middelen, inclusief de informatie die afkomstig is van de CSC of door het gebruik door de CSC van de clouddienst zijn verkregen. De bedrijfsmiddelen kunnen de door de CSC gelicentieerde software bevatten.

Objecttoelichting

Om verschillende redenen kan een CSC de dienstverlening van de CSP willen wijzigen of beëindigen. Enerzijds planmatig, zoals bij het einde van de contracttermijn, anderszins vanwege redenen als het niet voldoen aan de afspraken, of een voor de CSC ongewenste overname van de CSP door een andere organisatie.

Voor het op beheerste wijze afscheid kunnen nemen van een CSP is het nodig om bij het aangaan van het contract een exitstrategie te hebben. Als bij het afsluiten van de clouddienst geen bindende afspraken zijn gemaakt over het afscheid nemen, kan het heel lastig of kostbaar worden om de dienstverlening onder te brengen bij een andere partij.

Een goede exitstrategie mitigeert ook het risico van ‘vendor lock-in’.

Aanvullende informatie over veilige verwijdering kunt u vinden in ISO/IEC 27040.

Doelstelling	De bedrijfsmiddelen van de organisatie beschermen als onderdeel van de procedure voor het wijzigen of beëindigen van de dienst, het contract of de overeenkomst.	
Risico	Als bij het wijzigen of beëindigen van de clouddienst geen bindende en uitvoerbare afspraken bestaan over het retourneren, verplaatsen en verwijderen van bedrijfsmiddelen en gegevens, bestaat het risico dat de CSC de controle over haar middelen en informatie verliest, waardoor de bedrijfsvoering wordt verstoord en de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens niet langer zijn gewaarborgd.	
Control	De CSP behoort, conform de **exitstrategie** van de CSC, alle bedrijfsmiddelen van de organisatie die zij in hun bezit hebben bij beëindiging of wijziging van de dienst, contract of overeenkomst te **retourneren**, te kunnen **verplaatsen** of op verzoek te **verwijderen** en biedt hiervoor passende **voorzieningen**.	ISO 27002:2022 5.11 en 7.14
Conformiteitsindicator, nummer en maatregel		Afgeleid/afkomstig van

exitstrategie	1.	Een exitstrategie borgt de continuïteit van bedrijfsprocessen en het opruimen van data bij beëindiging van de dienstverlening. De borging gaat zowel via maatregelen voor de eigen organisatie, waaronder budget, als via contractuele afspraken met de leverancier. Onderdelen in de exitstrategie zijn: • voorwaarden aan de CSP (en toeleveranciers) met aandacht voor dataportabiliteit, serviceportabiliteit en datavernietiging inclusief de processen en voorzieningen die daarvoor nodig zijn; • een alternatieve CSP of interne landingsplaats; • een strategie, voorwaarden en budget, voor direct vertrek in verband met een crisis of plotselinge (geopolitieke) ontwikkelingen; • een strategie en budget bij de reguliere afloop van de overeenkomst.	IK-voorwaarde 7
	2.	Er is een exitstrategie opgenomen in de overeenkomst met de CSP. Hierin staat hoe, bij beëindiging van de overeenkomst, data worden overgedragen en hoe wordt geregeld dat de verzameling data bij de leverancier vernietigd wordt.	RCB-voorwaarde 4
	3.	In de overeenkomst met de CSP wordt met betrekking tot de exitstrategie de volgende aspecten vastgelegd, voor zover deze van toepassing zijn op de clouddienst: • soort, omvang en formaat van de gegevens die de CSP aan de CSC verstrekt; • definitie van het tijdsbestek waarbinnen de CSP de gegevens aan de CSC ter beschikking stelt; • definitie van het tijdstip vanaf welk de CSP de gegevens ontoegankelijk maakt voor de CSC en deze verwijdert; • de verantwoordelijkheden en verplichtingen van de CSC's om mee te werken aan het verstrekken van de gegevens. De definities zijn gebaseerd op de behoeften van materiedeskundigen van de CSC, zodat de CSC de geschiktheid van de clouddienst kan beoordelen met betrekking tot de afhankelijkheid van de CSP en de wettelijke en regelgevende vereisten.	BSI C5:2021 PI-02
retourneren	4.	De CSP behoort alle bedrijfsmiddelen van de CSC die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst te retourneren.	ISO 27002:2022 5.11
verplaatsen	5.	De CSP hanteert voor het verhuis- of overdrachtsverzoek van bedrijfsmiddelen van de CSC, een schriftelijke of cryptografisch verifieerbare autorisatie.	ISO 27002:2022 5.14 BSI C5:2021 DCS-02

	6.	De CSP moet informatie verstrekken over de regelingen voor de tijdige teruggave en verwijdering van eventuele bedrijfsmiddelen van CSC bij beëindiging van de overeenkomst. De beschrijving moet alle bedrijfsmiddelen vermelden en het schema voor de beëindiging van de overeenkomst documenteren.	ISO 27017:2015 CLD.8.1.5
	7.	De regelingen voor het retourneren en verwijderen van bedrijfsmiddelen moeten in de overeenkomst worden gedocumenteerd en moeten tijdig worden uitgevoerd. In de regelingen moet worden gespecificeerd welke bedrijfsmiddelen moeten worden teruggegeven en verwijderd.	ISO 27017:2015 CLD.8.1.5
	8.	De CSC moet bevestiging vragen dat de CSP beschikt over het beleid en de procedures voor het veilig verwijderen of hergebruiken van hulpbronnen.	ISO 27017:2015 11.2.7
verwijderen	9.	De CSP moet ervoor zorgen dat er tijdig regelingen worden getroffen voor de veilige verwijdering of hergebruik van hulpbronnen (bijvoorbeeld apparatuur, gegevensopslag, bestanden, geheugen).	ISO 27017:2015 11.2.7
	10.	De CSP moet waarborgen dat gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat de opslagruimte wordt verwijderd of hergebruikt. De verwijdering omvat gegevens van en over de CSC, inclusief metadata en gegevens die zijn opgeslagen in de back-ups van gegevens. Hiertoe worden door de industrie geaccepteerde methoden toegepast. De verwijdering voorkomt herstel met forensische middelen.	ISO 27002:2022 7.14 BSI C5:2021 PI-03 CCM:2020 DSP-02
Voorzienin-gen	11.	De overeenkomst tussen CSC en CSP bevat bepalingen die de toegang van de CSC tot gegevens specificeert bij beëindiging van het contract, met daarin: • het gegevensformaat; • hoelang de gegevens worden bewaard; • de omvang van de gegevens die worden bewaard en ter beschikking worden gesteld aan de CSC; • het beleid voor het verwijderen van gegevens.	CCM:2020 IPY-04

	12.	Om interoperabiliteit en portabiliteit mogelijk te maken, biedt de CSP applicatie-interface(s) aan, zodat CSC hun gegevens geautomatiseerd kan verplaatsen of verwijderen en biedt hiervoor cryptografisch veilige en gestandaardiseerde netwerkprotocollen.	CCM:2020 IPY-02 CCM:2020 IPY-03

4.2.3 *U.03 Veilige software*

Objectdefinitie

Veilige software is geen vanzelfsprekendheid, het meenemen van de informatieveiligheid tijdens de ontwikkeling en het up-to-date houden van de te nemen maatregelen vormen de basis voor veilige software.

Objecttoelichting

Informatie over de samenwerking tussen opdrachtgever en opdrachtnemer om veilig software veilig te krijgen kunt u vinden in ‘Grip op SSD’ van het CIP.

Doelstelling	Informatiebeveiligingsmaatregelen worden ontworpen en geïmplementeerd tijdens de gehele levenscyclus van software.		
Risico	Als informatiebeveiligingsmaatregelen niet structureel worden meegenomen tijdens alle fasen van de software-levenscyclus, bestaat het risico dat kwetsbaarheden in de software ontstaan of blijven bestaan, waardoor beveiligingsincidenten kunnen optreden met impact op de vertrouwelijkheid, integriteit en beschikbaarheid van informatie en dienstverlening.		
Control	Voor het veilig ontwikkelen van software en het voorkomen van besmetting met malware zijn regels **vastgesteld** en **toegepast**.		ISO 27002:2022 8.25
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
vastgesteld	1.	Door de CSC en de CSP worden de basisvereisten voor het beveiligen van applicaties toegepast en up-to-date gehouden.	CCM:2020 AIS-02

	2.	De CSC vraagt bij de CSP informatie op over de door de CSP gebruikte informatiebeveiligingsmaatregelen binnen de ontwikkelingscyclus, ook wanneer (een deel van) de ontwikkeling bij een toeleverancier plaatsvindt. Deze informatie moet informatief zijn, zonder informatie vrij te geven die nuttig kan zijn voor iemand met kwade bedoelingen.	ISO 27017:2015 14.2.1
toegepast	3.	De CSP waarborgt dat nieuwe informatiesystemen/software, upgrades en nieuwe versies veilig zijn door deze te testen op de vereisten voor het beveiligen van applicaties en ze tijdig te implementeren. De CSP doet dit door daar waar mogelijk te voldoen aan de principes van continuous delivery.	CCM:2020 AIS-05
	4.	De CSP voorziet de componenten/software binnen de clouddienst van malwarebescherming. Als er beveiligingsprogramma's zijn opgezet met handtekening en gedrag gebaseerde detectie en verwijdering van malware, worden deze beveiligingsprogramma's minimaal dagelijks bijgewerkt.	BSI C5:2021 OPS-05

4.2.4 *U.04 Wijzigingsbeheer*

Objectdefinitie

Wijzigingsbeheer is het proces dat zich richt op het effectief doorvoeren van wijzigingen.

Objecttoelichting

De effectiviteit kan worden vergroot door het maken van afspraken tussen de CSP en de CSC en de gehanteerde procedures, zodat wijzigingen geen of slechts beperkt nadelige gevolgen heeft voor de bedrijfsvoering van de CSC.

De informatie die voorafgaand aan een wijziging gedeeld wordt tussen de CSP en CSC, kan worden vastgelegd in bijvoorbeeld de leveranciersovereenkomst of de SLA.

Doelstelling	De dienstverlening waaronder het informatiebeveiligingsniveau behouden tijdens het uitvoeren van wijzigingen.

Risico	Als wijzigingen aan de clouddienst niet gecontroleerd, afgestemd en voorspelbaar worden doorgevoerd, bestaat het risico dat het informatiebeveiligingsniveau en de continuïteit van de dienstverlening onbedoeld worden aangetast, waardoor (gedeeltelijke) onbeschikbaarheid ontstaat en de bedrijfsvoering van de CSC wordt verstoord.		
Control	Wijzigingen in de clouddienst behoren onderworpen te zijn aan **procedures** voor wijzigingsbeheer, zodat het belang van de CSC wordt meegenomen en de CSC van een wijziging **op de hoogte** is.		ISO 27002:2022 8.32
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
procedures	1.	De CSP houdt in het wijzigingsbeheerproces rekening met het bestaan van wijzigingen die een negatief effect kunnen hebben op de CSC.	ISO 27017:2015 12.1.2
op de hoogte	2.	De CSP verstrekt de CSC informatie over wijzigingen aan de clouddienst die een negatief effect kunnen hebben op de clouddienst. Het volgende helpt de CSC bij het bepalen welk effect de wijzigingen kunnen hebben op de informatiebeveiliging: • categorieën van de wijzigingen; • geplande datum en tijd van de wijzigingen; • technische beschrijving van de wijzigingen aan de clouddienst en onderliggende systemen; • melding van de start en voltooiing van de wijzigingen.	ISO 27017:2015 12.1.2
	3.	Wanneer een CSP een clouddienst aanbiedt die afhankelijk is van een keten-CSP, kan het nodig zijn dat de CSP de CSC op de hoogte stelt van wijzigingen die door de keten-CSP worden veroorzaakt.	ISO 27017:2015 12.1.2

4.2.5 *U.05 Intellectuele eigendomsrechten*

Objectdefinitie

De intellectuele eigendomsrechten liggen bij de auteur van de software. Dit kan een natuurlijk persoon zijn dan wel een organisatie namens wie de auteur werkte. Toestemming om de software te mogen gebruiken wordt dan in een licentie vastgelegd. Overigens zijn ook mondelinge of schriftelijke afspraken in bijvoorbeeld een overeenkomst of in algemene voorwaarden mogelijk.

Objecttoelichting

Als een CSP software inzet waarvan de CSC het gebruik in licentie heeft of toestemming heeft die software te gebruiken, dan is het van belang dat de inzet door de CSP nog steeds passend is binnen de licentieovereenkomst van de CSC of de afspraken die zijn gemaakt met degene die de intellectuele eigendomsrechten bezit.

Doelstelling	De naleving bewerkstelligen van eisen van wet- en regelgeving, statutaire en contractuele eisen in verband met intellectuele eigendomsrechten en het gebruik van gepatenteerde producten.		
Risico	Als bij de inzet van software binnen de clouddienst onvoldoende wordt geborgd dat het gebruik door de CSP in overeenstemming is met geldende licentievoorwaarden en intellectuele eigendomsrechten, bestaat het risico dat deze rechten worden geschonden, waardoor de CSC wordt geconfronteerd met juridische claims, sancties en mogelijk gedwongen aanpassing of beëindiging van de dienstverlening.		
Control	De organisatie behoort passende **procedures** te implementeren om intellectuele eigendomsrechten te **beschermen**.		ISO 27002:2022 5.32
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
procedures	1.	De CSC moet beschikken over een procedure voor het identificeren van cloudspecifieke licentievereisten voordat wordt toegestaan dat gelicentieerde software in een clouddienst wordt geïnstalleerd.	ISO 27017:2015 18.1.2
	2.	De CSP informeert de CSC over het clouddienstspecifieke deploymentmodel, zodat duidelijk is wat de impact van de elasticiteit en schaalbaarheid is, waarbij de software op meer systemen of processorkernen kan gaan draaien dan is toegestaan door de licentievoorwaarden.	ISO 27017:2015 18.1.2
beschermen	3.	De CSP moet een proces opzetten voor het reageren op klachten over intellectuele eigendomsrechten.	ISO 27017:2015 18.1.2

4.2.6 *U.06 Kloksynchronisatie*

Objectdefinitie

Kloksynchronisatie betreft het synchroon instellen van systeemklokken op verschillende servers.

Objecttoelichting

Om gebeurtenissen uit verschillende componenten te correleren, worden de klokken van de verschillende systemen gelijkgericht en daarmee de timestamps van gebeurtenissen zijn gesynchroniseerd. Dit synchroniseren is het effect van de juiste instelling van tijd op betreffende componenten.

Het is daarom van belang om kloksynchronisatie te overwegen van de systemen van de CSC, met de systemen van CSP en van andere CSP's, waarop de door de CSC gebruikte clouddiensten draaien. Zonder een dergelijke synchronisatie kan het moeilijk zijn om gebeurtenissen op de systemen van de CSC in overeenstemming te brengen met gebeurtenissen op de systemen van de CSP.

Doelstelling	De correlatie en analyse van beveiligingsgerelateerde gebeurtenissen en andere geregistreerde gegevens mogelijk maken en onderzoeken bij informatiebeveiligingsincidenten ondersteunen.		
Risico	Als systeemklokken van de CSC en de CSP niet consistent en aantoonbaar zijn gesynchroniseerd, bestaat het risico dat beveiligingsgerelateerde gebeurtenissen niet betrouwbaar kunnen worden gecorreleerd en geanalyseerd, waardoor incidenten onvolledig of onjuist worden onderzocht en tijdige en adequate respons wordt bemoeilijkt.		
Control	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, behoren te worden **gesynchroniseerd** met goedgekeurde tijdsbronnen.		ISO 27002:2022 8.17
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
gesynchroniseerd	1.	De CSC moet informatie opvragen over de kloksynchronisatie die wordt gebruikt voor de systemen van de CSP.	ISO 27017:2015 12.4.4
	2.	De CSP moet informatie verstrekken aan de CSC over de klok die wordt gebruikt door de systemen van de CSP, en informatie over hoe de CSC lokale klokken kan synchroniseren met de klok van de clouddienst.	ISO 27017:2015 12.4.4

4.2.7 *U.07 Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen*

Objectdefinitie

De bedrijfsmiddelen van de CSC bevatten de (bedrijfs-)middelen, inclusief de informatie die afkomstig is van de CSC of door het gebruik door de CSC van de clouddienst is verkregen. De bedrijfsmiddelen kunnen de door de CSC gelicentieerde software bevatten. Het labelen is het vastleggen van informatie over de (bedrijfs-)middelen, zoals het vastleggen van de classificatie van de vertrouwelijkheid.

Objecttoelichting

Er zijn clouddiensttoepassingen die functies bieden voor het beheren van door de clouddienst afgeleide gegevens, waarbij deze worden toegevoegd aan de CSC-gegevens. Het identificeren van dergelijke uit clouddiensten afkomstige gegevens als bedrijfsmiddel en het bijhouden ervan in de inventaris van bedrijfsmiddelen kan bijdragen aan het verbeteren van de informatiebeveiliging en het waarborgen van de privacyvereisten vanuit de AVG.

Doelstelling	Het identificeren van de informatie en andere gerelateerde bedrijfsmiddelen van de CSC om de informatiebeveiliging en de vertrouwelijkheid, inclusief de privacy, ervan te behouden en passend eigenaarschap, verwerkings-, verwerkersverantwoordelijkheid toe te wijzen.		
Risico	Als informatie en andere bedrijfsmiddelen die ontstaan of worden gebruikt binnen clouddiensten niet volledig en actueel worden geïdentificeerd, geclassificeerd en geregistreerd, bestaat het risico dat deze middelen buiten de reguliere informatiebeveiligings- en privacyprocessen vallen, waardoor passende bescherming, eigenaarschap en naleving van wettelijke verplichtingen niet zijn geborgd.		
Control	Informatie en andere gerelateerde bedrijfsmiddelen behoren **inzichtelijk** en **overzichtelijk** te zijn gedurende de gehele levenscyclus.		ISO 27002:2022 5.9 en 5.13
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
inzichtelijk	1.	De inventaris van de bedrijfsmiddelen, inclusief de informatie van de CSC, moet rekening houden met hetgeen is opgeslagen in de cloudcomputing-omgeving.	ISO 27017:2015 8.1.1
	2.	De registraties van de inventaris moeten aangeven waar de bedrijfsmiddelen, inclusief de informatie van de CSC, worden bewaard, bijvoorbeeld door de identificatie van de clouddienst.	ISO 27017:2015 8.1.1

	3.	De inventaris van bedrijfsmiddelen van de CSP moet expliciet het volgende identificeren: • CSC-gegevens; • van clouddiensten afgeleide gegevens.	ISO 27017:2015 8.1.1
	4.	De classificatie en labeling weerspiegelt de beschermingsbehoeften van de informatie die het verwerkt, opslaat of verzendt.	BSI C5:2021 AM-06
	5.	De classificatie wordt volgens een uniform schema bepaald. Het schema biedt beschermingsniveaus voor de doelstellingen voor de bescherming van vertrouwelijkheid, integriteit, beschikbaarheid en authenticiteit.	BSI C5:2021 AM-06
	6.	De leveranciersovereenkomst beschrijft de mapping tussen de classificaties van de CSP en de CSC, zodat de CSC kan nagaan of de genomen maatregelen de beschermingsbehoeften van de CSC weerspiegelt.	CIP-netwerk
	7.	De CSP registreert bedrijfsmiddelen met de informatie die nodig is voor het kunnen beheren van informatiebeveiligingsrisico's, inclusief de maatregelen die zijn genomen om deze risico's gedurende de gehele levenscyclus te beheersen. Wijzigingen in deze informatie worden geregistreerd.	BSI C5:2021 AM-01
overzichtelijk	8.	De CSC labelt informatie en bijbehorende bedrijfsmiddelen die in de cloudcomputing-omgeving worden bewaard. Dit in overeenstemming met de door de CSC vastgestelde procedures voor labeling, zodat labeling het automatiseren van het beheer van de informatieverwerking mogelijk maakt.	ISO 27002:2022 5.13
	9.	De CSP documenteert alle servicefunctionaliteiten en maakt deze openbaar, zodat de CSC's hun informatie en bijbehorende bedrijfsmiddelen kunnen classificeren en labelen.	ISO 27017:2015 8.2.2

4.2.8 *U.08 Identiteits- en toegangsmanagement*

Objectdefinitie

Identiteits- en toegangsmanagement betreft het beheer om ervoor te zorgen dat de juiste identiteiten (denk daarbij vooral aan personen of computers) voor de juiste redenen en op het juiste moment toegang krijgen tot de juiste faciliteiten/functies van de clouddienst.

Objecttoelichting

Voor Single Sign-On (SSO) is een eenvoudige integratie en eenvoudig beheer van de gebruikersidentiteit tussen de systemen van de CSC en de clouddienst noodzakelijk. Dit vergemakkelijkt het gebruik van meerdere clouddiensten. Dit is mogelijk wanneer de CSP identiteits- en toegangsbeheertechnologieën van derden ondersteunt voor zijn clouddiensten en de bijbehorende beheerinterfaces.

Bij identiteits- en toegangsmanagement zijn de volgende drie stappen nodig voordat een gebruiker toegang kan krijgen:

1. Identificatie zorgt ervoor dat we weten wie je bent (of in elk geval wat een digitale identiteit van je is).
2. Authenticatie zorgt ervoor dat we met een bepaalde zekerheid weten dat je ook echt degene bent die je digitaal zegt te zijn.
3. Autorisatie zorgt ervoor dat we weten wat je dan mag (al dan niet door een ander gemachtigd) of juist niet mag, ofwel het verstrekken van toegangsrechten.

Doelstelling	Bewerkstelligen dat de toegang tot informatie en andere gerelateerde bedrijfsmiddelen wordt vastgesteld en goedgekeurd, waarbij de toewijzing van toegangsrechten aan de juiste personen en systemen plaatsvindt.		
Risico	Als identiteits- en toegangsmanagement voor clouddiensten onvoldoende is ingericht of niet consequent wordt toegepast, bestaat het risico dat onbevoegden toegang verkrijgen tot informatie en bedrijfsmiddelen of dat handelingen niet herleidbaar zijn tot een specifieke identiteit, waardoor misbruik van gegevens en aanvallen op clouddiensten niet tijdig worden voorkomen of adequaat kunnen worden onderzocht.		
Control	De **identificatie**, het toewijzen van **authenticatie**gegevens en het verstrekken van **toegangsrechten** behoren te worden beheerst door middel van beheerprocessen en passende **identiteits- en toegangsbeheertechnologie**.		ISO 27002:2022 5.16, 5.17 en 5.18
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
identificatie	1.	Om de toegang tot clouddiensten door gebruikers van clouddiensten van een CSC te beheren, moet de CSP gebruikersregistratie- en uitschrijvingsfuncties en specificaties voor het gebruik van deze functies aan de CSC verstrekken.	ISO 27017:2015 9.2.1

authenticatie	2.	De CSC moet verifiëren dat de beheersprocedure van de CSP voor het toekennen van geheime authenticatie-informatie, zoals wachtwoorden, voldoet aan de eisen van de CSC.	ISO 27017:2015 9.2.4
	3.	De CSP moet informatie verstrekken over procedures voor het beheer van de geheime authenticatie-informatie van de CSC, inclusief de procedures voor het toewijzen van dergelijke informatie en voor gebruikersauthenticatie.	ISO 27017:2015 9.2.4
Toegangs-rechten	4.	De CSP moet functies bieden voor het beheer van de toegangsrechten van de gebruikers van de clouddiensten van de CSC, en specificaties voor het gebruik van deze functies.	ISO 27017:2015 9.2.2
identiteits- en toegangs-beheer-technologie	5.	De CSC geeft duidelijkheid over een al dan niet vereiste integratie en in gebruik zijnde, dan wel geplande, voorziening voor identiteits- en toegangsbeheertechnologie.	CIP-netwerk aanvullend op ISO 27017:2015 9.2.2
	6.	Wanneer de CSC al een voorziening voor identiteits- en toegangsbeheertechnologie, al dan niet bij een andere CSP, inzet, moet de CSP voor zijn clouddiensten en de bijbehorende beheerinterfaces een eenvoudige integratie en eenvoudig beheer van de gebruikersidentiteiten tussen de systemen van de CSC en de clouddienst mogelijk maken en zodoende het gebruik van meerdere clouddiensten voor de CSC te vergemakkelijken, inclusief SSO.	CIP-netwerk op basis van ISO 27017:2015 9.2.2

4.2.9 *U.09 Beperking toegang tot informatie en speciale toegangsrechten*

Objectdefinitie

Speciale toegangsrechten zijn toegangsrechten die aan een identiteit, rol of proces worden verleend om activiteiten te kunnen uitvoeren die gewone gebruikers of processen niet kunnen uitvoeren. Gezien de hoge impact van onjuiste handelingen vraagt dit extra aandacht bij het uitgeven van toegangsrechten en om een beperking in de mogelijkheden van de toegang.

Objecttoelichting

Systeembeheerdersrollen eisen, gezien de hoge impact van onjuiste handelingen, meestal speciale toegangsrechten en om een beperking in de mogelijkheden van de toegang. Zo kent de cloudcomputing-omgeving extra aandachtsgebieden voor bijvoorbeeld hypervisorbeheerfuncties en beheerconsoles.

Het monitoren en vastleggen van het gebruik van speciale toegangsrechten wordt gezien als noodzakelijk ter ondersteuning van preventieve en corrigerende maatregelen tegen onjuist gebruik van de bewerkingen met hoge nadelige impact bij een onjuiste handeling.

Doelstelling	Uitsluitend bevoegde toegang bewerkstelligen en onbevoegde toegang tot informatie en andere gerelateerde bedrijfsmiddelen voorkomen, in het bijzonder daar waar het speciale toegangsrechten betreft.		
Risico	Als speciale toegangsrechten niet strikt worden beperkt, toegekend en beheerst, bestaat het risico dat gebruikers of beheerders meer bevoegdheden hebben dan noodzakelijk, waardoor misbruik van deze rechten kan leiden tot ongeautoriseerde toegang, verlies of aantasting van (gevoelige) gegevens en verstoring of uitval van clouddiensten.		
Control	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen behoort te worden **beperkt** overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging, in het bijzonder daar waar het **speciale toegangsrechten** betreft.		ISO 27002:2022 8.2 en 8.3
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
beperkt	1.	De CSC zorgt ervoor dat de toegang tot informatie in de clouddienst wordt beperkt in overeenstemming met zijn toegangscontrolebeleid en dat dergelijke beperkingen worden gerealiseerd. Dit omvat het beperken van de toegang tot clouddiensten, clouddienstfuncties en CSC-gegevens die in de service worden bewaard.	ISO 27017:2015 9.4.1

	2.	De CSP moet toegangscontroles bieden waarmee de CSC de toegang tot zijn clouddiensten, zijn clouddienstfuncties en de CSC-gegevens die in de dienst worden bewaard, kan beperken.	ISO 27017:2015 9.4.1
	3.	De CSP zorgt ervoor dat het rol-gebaseerd uitgeven van toegangsrechten mogelijk is, zodat functiescheiding plaatsvindt, inclusief de scheiding tussen operationele en toezichthoudende functies.	BSI C5:2021 IDM-01 BSI C5:2021 IDM-02
	4.	De CSP zorgt ervoor dat het verlenen en wijzigen van gebruikersaccounts en toegangsrechten op basis van het least privilege-principe mogelijk is, zodat gebruikers precies genoeg toegangsrechten krijgen om hun werk te doen.	BSI C5:2021 IDM-01
	5.	De CSP informeert de CSC, wanneer interne of externe medewerkers van de CSP de gegevens van de CSC lezen of schrijven die in de clouddienst zijn verwerkt, opgeslagen of verzonden of er toegang toe hebben gehad zonder voorafgaande toestemming van de CSC. De informatie wordt verstrekt telkens wanneer de gegevens van de CSC niet zijn gecodeerd, de encryptie is/was uitgeschakeld voor toegang of de contractuele overeenkomsten dergelijke informatie niet expliciet uitsluiten. De informatie bevat de oorzaak, het tijdstip, de duur, het type en de omvang van de toegang. De informatie is voldoende gedetailleerd om materiedeskundigen van de CSC in staat te stellen de risico's van de toegang te beoordelen. De informatie wordt verstrekt conform de contractuele afspraken, dan wel binnen 72 uur na toegang.	BSI C5:2021 IDM-07
speciale toegangs-rechten	6.	De CSC gebruikt voldoende authenticatietechnieken (bijvoorbeeld meervoudige authenticatie) om de beheerders van clouddiensten van de CSC te authenticeren voor de administratieve mogelijkheden van een clouddienst in overeenstemming met de geïdentificeerde risico’s.	ISO 27017:2015 9.2.3
	7.	De CSP gebruikt afdoende authenticatietechnieken, zoals tweefactor- of multifactorauthenticatie, om de beheerders van clouddiensten van de CSC te authenticeren voor de voorzieningen voor het beheer van een clouddienst in overeenstemming met de geïdentificeerde risico’s.	ISO 27017:2015 9.2.3 BSI C5:2021 IDM-01

	8.	Speciale toegangsrechten zijn gepersonaliseerd, beperkt in de tijd op basis van een risicobeoordeling en toegewezen indien nodig voor de uitvoering van taken (need-to-know-principe).	BSI C5:2021 IDM-06 CCM:2020 IAM-10
	9.	Het gebruik van speciale toegangsrechten wordt gelogd om eventueel misbruik van bevoorrechte toegang in verdachte gevallen op te sporen.	BSI C5:2021 IDM-06
	10.	Informatie van het loggen van gebeurtenissen van de gebruikers van de CSC en de toegang tot metadata betreffende de gegevens van de CSC is door de CSP beperkt door: • het beperken van bewaarperiode; • het verwijderen van de gegevens, wanneer verdere bewaring niet langer nodig is voor het doel van de verzameling.	BSI C5:2021 OPS-12

4.2.10 *U.10 Gebruik van cryptografie*

Objectdefinitie

Cryptografie betreft het versleutelen (coderen) van informatie, decryptie voor het ontsleutelen (decoderen) van informatie. Alleen de ontvanger, en eventueel ook de zender, beschikt over de decoderingssleutel om gegevens in hun originele vorm te herstellen.

Objecttoelichting

Het beschermen van bedrijfsgegevens, privacybescherming en identificatiegegevens zijn voor de belangrijke aandachtsgebieden voor cryptografie. Naast de versleuteling is ook het sleutelbeheer en de afspraken daaromtrent onderdeel van cryptografie.

Vanuit wet- en regelgeving kan de CSP mogelijk worden beperkt bij de toepassing van cryptografie.

Gezien de complexiteit en de diversiteit in de toepassing van cryptografie kan desgewenst de CSC in het Programma van Eisen (PvE) de crypto-eisen van het NBV specificeren.

Doelstelling	Correct en doeltreffend gebruik bewerkstelligen van cryptografie om de vertrouwelijkheid, authenticiteit of integriteit van informatie overeenkomstig de bedrijfs- en informatiebeveiligingseisen te beschermen en met inachtneming van de eisen van wet- en regelgeving, statutaire en contractuele eisen met betrekking tot cryptografie.

Risico	Als cryptografie en bijbehorend sleutelbeheer niet correct, consistent of conform wettelijke en contractuele eisen worden toegepast, bestaat het risico dat gegevens tijdens transport of opslag door onbevoegden kunnen worden ingezien of gemanipuleerd, waardoor de vertrouwelijkheid, integriteit en authenticiteit van informatie niet zijn gewaarborgd.		
Control	Regels voor het doeltreffende **gebruik** van cryptografie, met inbegrip van het **beheer** van cryptografische sleutels, behoren te worden gedefinieerd en geïmplementeerd.		ISO 27002:2022 8.24
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
gebruik	1.	De CSC behoort cryptografie te implementeren voor de gebruikte clouddiensten, tenzij anders blijkt uit een risicoanalyse. Cryptografie moet de geïdentificeerde risico's afdoende te beperken, ongeacht of deze cryptografische oplossing door de CSC of door de CSP wordt geleverd.	ISO 27017:2015 10.1.1
	2.	Wanneer de CSP cryptografie aanbiedt, moet de CSC alle door de CSP verstrekte informatie beoordelen om te bevestigen of de cryptografische mogelijkheden: • voldoen aan de beleidsvereisten van de CSC; • compatibel zijn met elke andere cryptografische bescherming die door de CSC wordt gebruikt; • van toepassing zijn op gegevens in rust en in beweging naar, van en binnen de clouddienst.	ISO 27017:2015 10.1.1

	3.	De CSP moet de CSC informatie verstrekken waar cryptografie wordt gebruikt, zodat de CSC kan bepalen of de informatie afdoende is beschermd. Daar waar gegevens van CSC's via openbare netwerken worden overgedragen, geeft de CSP aan op welke wijze sterke encryptie en authenticatie de informatie afdoende beschermd. De informatie moet duidelijkheid geven omtrent: • het gebruik van sterke encryptieprocedures en veilige netwerkprotocollen overeenkomt met de vastgestelde normenkaders; • het gebruik van encryptie aansluit bij de dataclassificatieschema's en rekening houdt met het communicatiekanaal, het type, de sterkte en de kwaliteit van de encryptie; • het roteren van de cryptografische sleutels in overeenstemming is met de berekende cryptoperiode; • het deactiveren van de cryptografische sleutels op het moment van hun vervaldatum of wanneer de entiteit niet langer is gegarandeerd; • voldaan wordt aan de eisen voor het veilig genereren, opslaan, archiveren, opvragen, distribueren, intrekken en verwijderen van de sleutels; • voldaan wordt aan de van toepassing zijnde juridische, regelgevende, zelfopgelegde of contractuele vereisten voor informatiebeveiliging voor zowel CSC als CSP.	ISO 27017:2015 10.1.1 BSI C5:2021 CRY-01 en CRY-02 CCM:2020 CEK-12 CCM:2020 CEK-13 CCM:2020 CEK-17
	4.	De CSP moet de CSC ook informatie verstrekken over alle mogelijkheden die hij biedt die de CSC kan helpen bij het toepassen van zijn eigen cryptografische bescherming.	ISO 27017:2015 10.1.1
	5.	De CSP biedt de CSC de mogelijkheid om eigen cryptografische sleutels te gebruiken en te beheren.	CCM:2020 CEK-08
beheer	6.	De CSC moet de cryptografische sleutels voor elke clouddienst identificeren en procedures voor sleutelbeheer implementeren.	ISO 27017015 10.1.2
	7.	Cryptografische toepassingen voldoen aan passende standaarden van het Forum Standaardisatie. De sterkte van de cryptografie wordt gebaseerd op de actuele adviezen van het NCSC en de Unit Weerbaarheid van de AIVD.	ISO 27002: 8.24

	8.	Wanneer de CSP functionaliteit biedt voor het beheer van sleutels door de CSC, moet de CSC de volgende informatie opvragen over de procedures die worden gebruikt om de door hem gebruikte sleutels te beheren: • type sleutels; • specificaties van het sleutelbeheersysteem, inclusief procedures voor elke fase van de sleutellevenscyclus, d.w.z. genereren, wijzigen of bijwerken, opslaan, buiten gebruik stellen, ophalen, behouden en vernietigen; • aanbevolen sleutelbeheerprocedures voor gebruik door de CSC.	ISO 27017:2015 10.1.2
	9.	De CSC mag de CSP niet toestaan de encryptiesleutels voor cryptografische operaties op te slaan en te beheren wanneer de CSC gebruik maakt van zijn eigen sleutelbeheer of van een afzonderlijke en aparte sleutelbeheerdienst.	ISO 27017:2015 10.1.2
	10.	De privésleutels die voor de versleuteling worden gebruikt, zijn alleen bekend bij de CSC, in overeenstemming met de toepasselijke wettelijke en regelgevende verplichtingen en vereisten. Uitzonderingen volgen een gespecificeerde procedure. De procedures voor het gebruik van private sleutels, inclusief eventuele uitzonderingen, moeten contractueel worden overeengekomen tussen CSC en CSP.	BSI C5:2021 CRY-03

4.2.11 *U.11 Logging en monitoring*

Objectdefinitie

Logging en monitoring betreft de vastlegging van aan informatiebeveiliging gerelateerde gebeurtenissen en het bewaken en onderkennen van afwijkingen op beleidsregels.

Objecttoelichting

Naast het onderkennen van afwijkingen is logging gericht op het vastleggen van gebeurtenissen, als bewijslast en ter verbetering en/of herstel. De bewakingsfunctie is voorbehouden aan de daartoe verantwoordelijke functionaris(sen) en vindt mede plaats op basis van geregistreerde gegevens (logging).

De verantwoordelijkheden van de CSC en de CSP voor het loggen van gebeurtenissen variëren afhankelijk van het type clouddienst dat wordt gebruikt. Met IaaS kan de verantwoordelijkheid van een CSP op het gebied van loggen bijvoorbeeld worden beperkt tot die van componenten van de cloudcomputing-infrastructuur, en kan de CSC verantwoordelijk zijn voor het loggen van de gebeurtenissen van zijn eigen virtuele machines en applicaties.

Doelstelling	Gebeurtenissen registreren, bewijs genereren, synchroniseren, de integriteit van informatie in logbestanden waarborgen, onbevoegde toegang voorkomen, informatiebeveiligingsgebeurtenissen identificeren die tot een informatiebeveiligingsincident kunnen leiden en onderzoeken ondersteunen.		
Risico	Als logging en monitoring van beveiligingsgerelateerde gebeurtenissen onvoldoende zijn ingericht, afgestemd of betrouwbaar worden uitgevoerd, bestaat het risico dat afwijkingen van normaal gedrag niet tijdig worden herkend of onderzocht, waardoor informatiebeveiligingsincidenten langer voortduren en noodzakelijke herstel- en beheersmaatregelen te laat of onjuist worden genomen.		
Control	Er behoren logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden **geregistreerd**, te worden geproduceerd, opgeslagen, **beschermd** en **geanalyseerd**.		ISO 27002:2022 8.15 en 8.16
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
Geregi-streerd	1.	De CSC moet zijn vereisten voor het registreren van gebeurtenissen definiëren en verifiëren dat de clouddienst aan deze vereisten voldoet.	ISO 27017:2015 12.4.1
	2.	De CSC moet informatie opvragen bij de CSP over de monitoringmogelijkheden die voor elke clouddienst beschikbaar zijn.	ISO 27017:2015 CLD.12.4.5
	3.	De CSP heeft applicaties en infrastructuren zodanig geïmplementeerd en geconfigureerd dat gebruikerstoegang van de CSP en de CSC en intra-tenanttoegang worden gemonitord.	CCM:2020 IVS-06
	4.	De CSC moet bepalen of de door de CSP geleverde logmogelijkheden geschikt zijn en of dat de CSC aanvullende logmogelijkheden moet kunnen hebben.	ISO 27017:2015 12.4.3

	5.	De CSP moet mogelijkheden bieden waarmee de CSC specifieke, voor de CSC relevante, aspecten van de werking van de clouddiensten kan monitoren. Bijvoorbeeld om te monitoren en te detecteren of de clouddienst wordt gebruikt als platform om anderen aan te vallen, of dat er gevoelige gegevens uit de clouddienst lekken.	ISO 27017:2015 CLD.12.4.5
Gesynchro-niseerd	6.	De CSC moet informatie opvragen over de kloksynchronisatie die wordt gebruikt voor de systemen van de CSP.	ISO 27017:2015 12.4.4
	7.	De CSP moet informatie verstrekken aan de CSC over de klok die wordt gebruikt door de systemen van de CSP, en informatie over hoe de CSC lokale klokken kan synchroniseren met de klok van de clouddienst.	ISO 27017:2015 12.4.4
beschermd	8.	Als de CSC bewerking op de log mag uitvoeren, moeten die bewerkingen worden geregistreerd.	ISO 27017:2015 12.4.3
	9.	Het gebruik van de monitoringmogelijkheden is voorzien van passende toegangscontroles. De mogelijkheden bieden alleen toegang tot informatie over de eigen clouddienst van de CSC.	ISO 27017:2015 CLD.12.4.5
Geanaly-seerd	10.	De CSP moet de CSC documentatie verstrekken over de mogelijkheden voor servicemonitoring. Monitoring moet gegevens opleveren die consistent zijn met de gebeurtenislogboeken en helpen bij de SLA-voorwaarden.	ISO 27017:2015 CLD.12.4.5

4.2.12 *U.12 Toegangsbeveiliging in een multi-tenant-omgeving*

Objectdefinitie

Toegangsbeveiliging in een multi-tenant-omgeving betreft de toewijzing van fysieke en virtuele middelen, waarbij de tenants (klanten van clouddiensten) en hun gegevens en verwerkingen van elkaar geïsoleerd zijn en daarmee ontoegankelijk voor elkaar. De toegangsbeveiliging in een multi-tenant-omgeving draagt zorg voor beveiligingscontroles om zo te beschermen tegen datalekken en onderlinge nadelige beïnvloeding.

Objecttoelichting

CSC's mogen geen hinder van elkaar ondervinden, zo mogen piekbelastingen bij de ene CSC geen nadelige invloed hebben op de performance van de clouddiensten van de andere CSC.

Doelstelling	Toegang voor bevoegden bewerkstelligen en toegang voor onbevoegden tot informatie en andere gerelateerde bedrijfsmiddelen voorkomen.		
Risico	Als toegangsbeveiliging en isolatie tussen tenants in een multi-tenant-omgeving onvoldoende zijn ingericht of gehandhaafd, bestaat het risico dat andere tenants toegang krijgen tot of invloed uitoefenen op gegevens en verwerkingen van de CSC, waardoor vertrouwelijkheid, integriteit en beschikbaarheid van informatie en dienstverlening worden aangetast.		
Control	Er behoren regels op basis van bedrijfs- en informatiebeveiligingseisen te worden **vastgesteld** en **geïmplementeerd** om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen.		ISO 27002:2022 5.15
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
vastgesteld	1.	Wanneer de clouddienst multi-tenancy omvat, moet de CSP aangeven in welke mate wordt voldaan aan de veilige multi-tenancy en gerelateerde richtlijnen voor een veilige opslag van gegevens, zoals beschreven in ISO/IEC 27040.	ISO 27017:2015 CLD.9.5.2
	2.	De CSP moet rekening houden met de risico's die gepaard gaan met het draaien van door CSC geleverde software binnen de door de CSP aangeboden clouddiensten.	ISO 27017:2015 CLD.9.5.1
geïmplementeerd	3.	De CSP moet passende logische scheiding van CSC-gegevens, (gevirtualiseerde) applicaties, besturingssystemen, opslag en netwerken afdwingen voor: • de scheiding van middelen en gegevens die worden gebruikt door de CSC in een omgeving met meerdere tenants; • de scheiding tussen de beheervoorzieningen van de CSP en de middelen die door de CSC worden gebruikt.	ISO 27017:2015 CLD.9.5.1 CCM:2020 IVS-06
	4.	Wanneer de clouddienst multi-tenancy omvat, moet de CSP informatiebeveiligingscontroles implementeren om te zorgen voor een passende isolatie van bronnen die door verschillende tenants worden gebruikt.	ISO 27017:2015 CLD.9.5.1

	5.	De CSP zorgt voor de hardening van de virtuele machines in de multi-tenant-omgeving, om aan de beveiligingsvereisten van de CSC te voldoen.	ISO 27017:2015 CLD.9.5.2

4.2.13 *U.13 Netwerksegmentatie en koppelvlakken*

Objectdefinitie

Netwerksegmentatie betreft het verdelen van een netwerk in segmenten. Koppelvlakken bieden de mogelijkheid om een veilige en gecontroleerde toegang te bieden tot de onderlinge netwerksegmenten.

Objecttoelichting

Binnen een netwerk dat niet gesegmenteerd is, kunnen alle aanwezige apparaten in dat netwerk met elkaar communiceren. Door netwerksegmentatie en het bieden de mogelijkheid om een veilige en gecontroleerde toegang heeft een beveiligingsincident in een segment alleen impact op dat segment en niet op het gehele netwerk.

Afhankelijk van het type clouddienst kunnen de verantwoordelijkheden voor het configureren van een virtueel netwerk variëren tussen een CSC en een CSP.

Doelstelling	Het netwerk opsplitsen met beveiligingsgrenzen en het verkeer ertussen op basis van de bedrijfsbehoeften beheersen.	
Risico	Als netwerksegmentatie en koppelvlakken niet consistent en correct zijn ontworpen en ingericht, bestaat het risico dat verkeer tussen netwerksegmenten onvoldoende wordt beheerst, waardoor beveiligingsincidenten zich ongehinderd kunnen verspreiden of onbevoegde toegang ontstaat tot systemen en gegevens buiten het beoogde segment.	
Control	Clouddiensten, gebruikers en informatiesystemen **behoren** in de netwerken van de organisatie te worden **gesegmenteerd**, **koppelvlakken** bieden een veilige toegang tot een segment.	ISO 27002:2022 8.22
Conformiteitsindicator, nummer en maatregel		Afgeleid/afkomstig van

behoren	1.	De CSC stelt eisen aan het scheiden van netwerken in de door met meerdere tenants gedeelde cloudomgeving om isolatie van een aangeboden clouddienst te bereiken. De CSC verifieert dat de CSP aan deze vereisten voldoet.	ISO 27017:2015 13.1.3
	2.	De CSP moet scheiding van netwerktoegang afdwingen in de volgende gevallen: • segregatie tussen tenants in een omgeving met meerdere tenants; • scheiding tussen de interne beheeromgeving van de CSP en de cloudomgeving van de CSC.	ISO 27017:2015 13.1.3
	3.	De CSP heeft specifieke beveiligingseisen ontworpen, gepubliceerd en voorzien voor het tot stand brengen van verbindingen binnen het netwerk van de CSP. De beveiligingseisen definiëren voor het verantwoordelijkheidsgebied van de CSP: • in welke gevallen de beveiligingszones gescheiden moeten worden en in welke gevallen CSC's logisch dan wel fysiek gescheiden moeten worden; • welke communicatierelaties en welke netwerk- en applicatieprotocollen per geval zijn toegestaan; • hoe het dataverkeer voor beheer en monitoring van elk netwerkniveau wordt gescheiden; • welke interne, locatieoverschrijdende communicatie is toegestaan, en; • welke netwerkoverschrijdende communicatie is toegestaan.	BSI C5:2021 COS-02
	4.	Waar nodig moet de CSP de CSC helpen bij het verifiëren van de door de CSP geïmplementeerde segregatie.	ISO 27017:2015 13.1.3
Gesegmen-teerd	5.	Bij de configuratie van virtuele netwerken moet er sprake zijn van consistentie van configuraties tussen virtuele en fysieke netwerken geverifieerd op basis van het netwerkbeveiligingsbeleid van de CSP.	ISO 27017:2015 CLD.13.1.4
	6.	De CSP definieert en documenteert informatiebeveiligingsbeleid voor de configuratie van het virtuele netwerk. Dit beleid is consistent met het beveiligingsbeleid voor het fysieke netwerk.	ISO 27017:2015 CLD.13.1.4

	7.	De CSP moet ervoor zorgen dat de virtuele netwerkconfiguratie overeenkomt met het informatiebeveiligingsbeleid, ongeacht de middelen die worden gebruikt om de configuratie te creëren.	ISO 27017:2015 CLD.13.1.4
	8.	De CSP scheidt het dataverkeer van CSC's op netwerkniveau, zodat de vertrouwelijkheid en integriteit van de verzonden gegevens is gegarandeerd.	BSI C5:2021 COS-06
Koppel vlakken	9.	De CSP bewaakt, versleutelt en beperkt de communicatie tussen segmenten/omgevingen tot alleen geverifieerde en geautoriseerde verbindingen. Controleer deze configuraties ten minste jaarlijks en ondersteun deze met een gedocumenteerde rechtvaardiging van alle toegestane services, protocollen, poorten en compenserende controles.	CCM:2020 IVS-03
	10.	Door de CSP zijn op de koppelpunten met externe of onvertrouwde zones 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, zodat (tegen)maatregelen met betrekking tot correlerende gebeurtenissen kunnen worden geïnitieerd.	BIO2 8.21.01 BSI C5:2021 COS-01
	11.	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.	BIO2 8.21.02

4.2.14 *U.14 Beschermen van registraties*

Objectdefinitie

Het beschermen van registraties betreft vertrouwelijkheid en integriteit van CSC-data.

Objecttoelichting

Vanuit het Rijksbreedcloudbeleid worden eisen gesteld aan de opslag van gegevens in de cloud (zie daarvoor de beleidsobjecten). De CSC blijft eindverantwoordelijk voor een veilige opslag, ook nadat besloten is voor een bepaalde CSP te kiezen. Vanuit die verantwoordelijkheid van de CSC is het van belang dat de CSP de CSC informeert over de genomen beveiligingsmaatregelen, zodat de CSC kan nagaan of aan de verplichtingen wordt voldaan.

Doelstelling	De naleving bewerkstelligen van wet- en regelgeving, statutaire en contractuele eisen, alsmede gemeenschaps- of maatschappelijke verwachtingen, met betrekking tot de bescherming en beschikbaarheid van registraties.		
Risico	Als registraties binnen de clouddienst niet aantoonbaar worden beschermd tegen verlies, ongeautoriseerde wijziging of onbeschikbaarheid, bestaat het risico dat gegevens niet betrouwbaar of tijdig beschikbaar zijn, waardoor de CSC haar wettelijke verplichtingen en bedrijfsprocessen niet correct kan uitvoeren.		
Control	Registraties behoren te worden **beschermd** tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.		ISO 27002:2022 5.33
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
beschermd	1.	De CSC heeft voor alle informatie(systemen) in selectielijsten de bewaartermijn vastgelegd, rekening houdend met de eigen bedrijfsdoelstellingen en wet- en regeling, zoals de archiefwet en privacywetgeving. De CSC heeft deze termijnen ook praktisch ingeregeld en toetst periodiek de werking hiervan.	BIO2 5.33.01
	2.	De CSP bewaart, archiveert en verwijdert gegevens in overeenstemming met de vereisten van de CSC en toepasselijke wet- en regelgeving.	CCM:2020 DSP-16
	3.	De CSC moet informatie opvragen bij de CSP over de bescherming van door de CSP verzamelde en opgeslagen gegevens die relevant zijn voor het gebruik van clouddiensten door de CSC.	ISO 27017:2015 18.1.3
	4.	De CSP moet informatie verstrekken aan de CSC over de bescherming van gegevens die door de CSP worden verzameld en opgeslagen met betrekking tot het gebruik van clouddiensten door de CSC.	ISO 27017:2015 18.1.3

4.2.15 *U.15 Inzicht in de beschikbare speciale systeemhulpmiddelen*

Objectdefinitie

Inzicht in de beschikbare speciale systeemhulpmiddelen betreft het inzicht beschikbare programma's in de clouddienst die aan de clouddienst zijn toegevoegd voor functioneel beheer of om de operationele prestaties te verbeteren.

Objecttoelichting

Speciale systeemhulpmiddelen kunnen in staat zijn om gegevens te openbaren, te wissen, te verplaatsen of te veranderen. Verkeerd gebruik van deze middelen kan leiden tot een verlies van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie.

Voorbeelden van speciale systeemhulpmiddelen zijn:

- installatie, wijzigingen en verwijdering van gevirtualiseerde apparaten zoals servers, netwerken en opslag;
- beëindigingsprocedures voor het gebruik van clouddiensten;
- back-up en herstel.

Doelstelling	Bewerkstelligen dat het gebruik van systeemhulpmiddelen geen schade toebrengt aan systeem- en toepassingsbeheersmaatregelen voor informatiebeveiliging.		
Risico	Als het gebruik en de beschikbaarheid van speciale systeemhulpmiddelen binnen de clouddienst onvoldoende inzichtelijk en beheerst zijn, bestaat het risico dat deze hulpmiddelen onjuist of onbevoegd worden gebruikt, waardoor met één handeling grootschalige schade kan ontstaan aan de beschikbaarheid, integriteit en vertrouwelijkheid van systemen en gegevens.		
Control	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, behoort te worden beperkt en nauwkeurig te worden **gecontroleerd**.		ISO 27002:2022 8.18
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
Gecontro-leerd	1.	Wanneer door de CSP het gebruik van systeemhulpmiddelen is toegestaan, moet de CSC de systeemhulpmiddelen identificeren die in zijn cloudomgeving moeten worden gebruikt, en ervoor zorgen dat deze de werking van de clouddienst niet verstoren.	ISO 27017:2015 9.4.4
	2.	De CSP moet de vereisten identificeren voor alle systeemhulpmiddelen die binnen de clouddienst worden gebruikt.	ISO 27017:2015 9.4.4

	3.	De CSP moet ervoor zorgen dat elk gebruik van systeemhulpmiddelen die de normale bedrijfs- of beveiligingsprocedures kunnen omzeilen, strikt beperkt blijft tot bevoegd personeel, en dat het gebruik van dergelijke hulpmiddelen regelmatig wordt beoordeeld en gecontroleerd.	ISO 27017:2015 9.4.4

4.2.16 *U.16 Gedocumenteerde bedieningsprocedures*

Objectdefinitie

Bedieningsprocedures betreft het voorgeschreven gebruik van de speciale systeemhulpmiddelen die direct of indirect kan leiden tot een verlies van de vertrouwelijkheid, integriteit of beschikbaarheid van informatie.

Objecttoelichting

Speciale systeemhulpmiddelen kunnen in staat zijn om gegevens te openbaren, te wissen, te verplaatsen of te veranderen, ook wel aangeduid als kritieke operaties. Verkeerd gebruik van deze middelen kan leiden tot een verlies van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie.

Doelstelling	De correcte en veilige bediening van informatie verwerkende faciliteiten waarborgen.		
Risico	Als bedieningsprocedures voor kritieke systeemhulpmiddelen onvoldoende zijn vastgelegd, begrepen of nageleefd, bestaat het risico dat onjuiste menselijke handelingen leiden tot informatiebeveiligingsincidenten met impact op de vertrouwelijkheid, integriteit en beschikbaarheid van informatie en systemen.		
Control	**Bedieningsprocedures** voor informatie verwerkende faciliteiten behoren te worden gedocumenteerd en **beschikbaar** te worden gesteld aan het personeel dat deze nodig heeft.		ISO 27002:2022 5.37
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
Bedienings-procedures	1.	Procedures voor administratieve handelingen in een cloudcomputing-omgeving moeten worden gedefinieerd, gedocumenteerd en gecontroleerd.	ISO 27017:2015 CLD.12.1.5

Beschikbaar	2.	De CSP moet documentatie over de kritieke operaties en procedures verstrekken aan de CSC's.	ISO 27017:2015 CLD.12.1.5
	3.	De CSC moet procedures documenteren voor kritieke operaties waarbij een storing onherstelbare schade kan veroorzaken aan bedrijfsmiddelen in de cloudcomputing-omgeving.	ISO 27017:2015 CLD.12.1.5
	4.	De CSP heeft in een document vastgelegd dat en hoe toezicht wordt gehouden op kritieke operaties, inclusief de technische maatregelen om detectietools, bedreigingssignaturen en indicatoren van onjuiste handelingen wekelijks of vaker bij te werken.	ISO 27017:2015 CLD.12.1.5 CCM:2020 TVM-04

4.2.17 *U.17 Bewustwording, opleiding en training*

Objectdefinitie

Met bewustwording wordt bij deze maatregel bewustwording van de CSC van de risico's bedoeld. Opleiding en training betreft het ondersteunen van de gebruikers van de CSC om onjuiste bediening van de clouddienst door onvoldoende kennis en ervaring te voorkomen.

Objecttoelichting

Kennis over het veilig gebruik van de clouddienst zit bij de CSP.

Doelstelling	Ervoor zorgen dat personeel en relevante belanghebbenden zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.	
Risico	Als personeel en andere relevante belanghebbenden onvoldoende bewust zijn van hun verantwoordelijkheden en onvoldoende zijn opgeleid in het veilig gebruik van de clouddienst, bestaat het risico dat onjuist handelen plaatsvindt, waardoor beveiligingsmaatregelen niet effectief worden toegepast en informatiebeveiligingsincidenten ontstaan of verergeren.	
Control	Personeel van de CSC die de dienst gebruiken behoren een **passende bewustwording** van en **opleiding en training** in het gebruik van de clouddienst voor zover relevant voor hun functie te krijgen, inclusief de onderwerp specifieke beleidsregels en procedures van de CSC organisatie in relatie tot het geldende regelmatige herijkte informatiebeveiliging en -beleid.	ISO 27002:2022 6.3

Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
passende bewustwor-ding	1.	De CSC moet de volgende items toevoegen aan bewustmakings-, opleidings- en trainingsprogramma's voor bedrijfsmanagers van clouddiensten, beheerders van clouddiensten, integrators van clouddiensten en gebruikers van clouddiensten, inclusief relevante werknemers en contractanten: • normen en procedures voor het gebruik van clouddiensten; • informatiebeveiligingsrisico's met betrekking tot clouddiensten en hoe deze risico's worden beheerd; • systeem- en netwerkomgevingsrisico's bij het gebruik van clouddiensten; • toepasselijke wettelijke en regelgevende overwegingen.	ISO 27017:2015 7.2.2
opleiding en training	2.	Er moeten door de CSC voorlichtings-, onderwijs- en trainingsprogramma's op het gebied van informatiebeveiliging over clouddiensten worden aangeboden aan het management en de toezichthoudende managers, inclusief die van bedrijfsonderdelen.	ISO 27017:2015 7.2.2
	3.	De CSP moet zorgen voor bewustwording, opleiding en training voor werknemers, en CSC's, zoals dienstverleners of leveranciers wier diensten bijdragen aan het aanbieden van de clouddienst, verzoeken hetzelfde te doen, met betrekking tot de juiste omgang met CSC-gegevens en van clouddiensten afgeleide gegevens. Deze gegevens kunnen informatie bevatten die vertrouwelijk is voor een CSC of onderworpen zijn aan specifieke beperkingen, waaronder wettelijke beperkingen, met betrekking tot toegang en gebruik door de CSP.	ISO 27017:2015 7.2.2 BSI C5:2021 SSO-01

4.2.18 *U.18 Beheer van technische kwetsbaarheden*

Objectdefinitie

Technische kwetsbaarheden betreft de zwakke plekken en lekken in de technische beveiliging van informatiesystemen die aanvallers kunnen misbruiken om toegang te krijgen tot deze systemen. Het beheer van technische kwetsbaarheden is een continu proces van actief opsporen van kwetsbaarheden, en het repareren daarvan.

Objecttoelichting

Het beheer van technische kwetsbaarheden is effectief, wanneer de kwetsbaarheden eerder zijn opgepakt en mitigerende maatregelen zijn genomen dan dat er misbruik van is gemaakt. Dit vraagt om een proactieve houding van de CSP. Om verstoring van de clouddienst en daarmee van de bedrijfsvoering van de CSC te voorkomen, is afstemming over de risico's en de aanpak tussen de CSP en de CSC van belang.

Doelstelling	Misbruik van technische kwetsbaarheden voorkomen.		
Risico	Als technische kwetsbaarheden in de clouddienst niet tijdig worden geïdentificeerd, beoordeeld en verholpen, bestaat het risico dat deze kwetsbaarheden door aanvallers worden misbruikt, waardoor beveiligingsincidenten ontstaan met impact op de vertrouwelijkheid, integriteit en beschikbaarheid van informatie en dienstverlening.		
Control	Er behoort informatie te worden **verkregen** over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden behoort te worden **geëvalueerd** en er behoren passende maatregelen te worden getroffen.		ISO 27002:2022 8.8
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
verkregen	1.	De CSC dient informatie op te vragen bij de CSP over het beheer van technische kwetsbaarheden die van invloed kunnen zijn op de geleverde clouddiensten.	ISO 27017:2015 12.6.1
	2.	De CSP moet aan CSC van de clouddienst informatie beschikbaar stellen over het beheer van technische kwetsbaarheden die van invloed kunnen zijn op de geleverde clouddiensten.	ISO 27017:2015 12.6.1
	3.	De CSP informeert de CSC periodiek over de status van incidenten die de CSC raken, of betrekt CSC waar passend en noodzakelijk bij de oplossing. Zodra een incident vanuit het perspectief van de CSP is opgelost, wordt de CSC geïnformeerd over de ondernomen acties.	BSI C5:2021 OPS-21

geëvalueerd	4.	De CSC identificeert technische kwetsbaarheden waar hij verantwoordelijk voor is. De CSC voorkomt nadelige gevolgen en heeft daartoe een proces gedefinieerd en ingericht.	ISO 27017:2015 12.6.1
	5.	Als de kans op misbruik en de verwachte schade beide hoog zijn (bijvoorbeeld met de NCSC-Inschalingsmatrix beveiligingsadviezen of leveranciersbeveiligingsadviezen), worden passende mitigerende maatregelen zo snel mogelijk, maar uiterlijk binnen een week getroffen.	BIO2 8.08.01

4.2.19 *U.19 Melden van informatiebeveiligingsgebeurtenissen*

Objectdefinitie

Onder een informatiebeveiligingsgebeurtenis wordt verstaan een voorval dat wijst op een mogelijke inbreuk van informatiebeveiliging, of op het falen van beheersmaatregelen. Medewerkers moeten incidenten kunnen melden en op deze meldingen moet actie worden ondernomen.

Objecttoelichting

In tegenstelling tot technische kwetsbaarheden kunnen informatiebeveiligingsgebeurtenissen door zowel de CSP als de CSC worden waargenomen. Het kunnen melden en opvolgen ervan moet daarom zowel door de CSP als de CSC worden gedaan.

Doelstelling	Tijdige, consistente en doeltreffende melding ondersteunen van informatiebeveiligingsgebeurtenissen die door personeel kunnen worden geïdentificeerd.	
Risico	Als informatiebeveiligingsgebeurtenissen door medewerkers of leveranciers niet tijdig, eenduidig of consequent worden gemeld en opgevolgd, bestaat het risico dat signalen van falende beheersmaatregelen niet worden herkend of geadresseerd, waardoor beveiligingsincidenten zich herhalen of escaleren met toenemende impact op de organisatie.	
Control	De organisatie behoort te voorzien in een **mechanisme** waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via **passende kanalen** kan **melden**.	ISO 27002:2022 6.8
Conformiteitsindicator, nummer en maatregel		Afgeleid/afkomstig van

mechanisme	1.	De CSP moet de CSC mechanismen bieden voor: • het aan de CSP melden van door de CSC gedetecteerde informatiebeveiligingsgebeurtenissen; • het aan de CSC rapporteren over door de CSP gedetecteerde informatiebeveiligingsgebeurtenissen; • het door de CSC kunnen volgen van de status van gerapporteerde informatiebeveiligingsgebeurtenissen.	ISO 27017:2015 16.1.2
	2.	De CSC moet informatie opvragen bij de CSP over door de CSC te hanteren mechanismen voor: • het aan de CSP melden van door de CSC gedetecteerde informatiebeveiligingsgebeurtenissen; • het door de CSC ontvangen van rapporten over door de CSP gedetecteerde informatiebeveiligingsgebeurtenissen; • het door de CSC kunnen volgen van de status van gerapporteerde informatiebeveiligingsgebeurtenissen.	ISO 27017:2015 16.1.2
passende kanalen	3.	De CSP moet essentiële informatie verstrekken, zoals telefoonnummers, e-mailadressen en servicetijden voor zowel de CSC als de CSP.	ISO 27017:2015 16.1.2
	4.	De CSP beheert en verwijst naar een dagelijks bijgewerkt online register van bekende kwetsbaarheden die van invloed zijn op de CSP en op door de CSP geleverde middelen. Bij iedere kwetsbaarheid wordt aangegeven of er software-updates (bijvoorbeeld een patch of update) beschikbaar zijn, wanneer deze uitgerold worden en of deze door de CSP, de CSC of beiden samen moet worden geïnstalleerd. De bij de kwetsbaarheid opgenomen informatie vormt een geschikte basis voor risicobeoordeling en eventuele vervolgmaatregelen aan de CSC. Het online register is eenvoudig toegankelijk voor elke CSC.	BSI C5:2021 PSS-03
melden	5.	De CSP heeft, in lijn met de toepasselijke wet- en regelgeving, een procedure opgesteld voor het beheren en beantwoorden van verzoeken om openbaarmaking van persoonsgegevens door wetshandhavingsautoriteiten en rapporteert de CSC over de te volgen procedure. De CSP meldt een openbaarmaking aan de CSC, volgens een opgestelde meldingsprocedure, tenzij dit verboden is, zoals bij een strafrechtelijke eis om de vertrouwelijkheid van een rechtshandhavingsonderzoek te bewaren.	CCM:2020 DSP-18

	6.	Wanneer een informatiebeveiligingsgebeurtenis wordt gedetecteerd door de CSC of door de CSP, behoort dit onmiddellijk aan de andere partij te worden gemeld.	ISO 27017:2015 16.1.2

4.2.20 *U.20 Opvolging informatiebeveiligingsincidenten*

Objectdefinitie

De opvolging van een informatiebeveiligingsincident betreft de opvolging van gebeurtenis of een reeks informatiebeveiligingsgebeurtenissen waarvan het waarschijnlijk is dat als er geen opvolging is de informatieveiligheid in gevaar komt en de bedrijfsvoering van de CSC wordt gecompromitteerd.

Objecttoelichting

Voor een effectieve opvolging is duidelijkheid over de rolverdeling tussen de CSC en de CSP en de daarbij te volgen procedures van belang.

Doelstelling	Een snelle, doeltreffende, consistente en geordende reactie op informatiebeveiligingsincidenten, met inbegrip van communicatie over informatiebeveiligingsgebeurtenissen, bewerkstelligen. Tevens in het kader van disciplinaire en gerechtelijke stappen consistent en doeltreffend beheer bewerkstelligen van bewijsmateriaal in verband met informatiebeveiligingsincidenten.		
Risico	Als informatiebeveiligingsincidenten niet snel, consistent en volgens vastgestelde procedures worden opgevolgd en afgehandeld, bestaat het risico dat incidenten onvoldoende worden beheerst en geanalyseerd, waardoor herhaling optreedt, de impact toeneemt en de bedrijfsvoering van de CSC blijvend wordt geschaad.		
Control	De processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten behoren te zijn **gedefinieerd, vastgesteld** en gecommuniceerd, inclusief het identificeren, **verzamelen**, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.		ISO 27002:2022 5.24 en 5.28 NIS:2016
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
gedefinieerd, vastgesteld	1.	De CSC moet de toewijzing van verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten verifiëren en ervoor zorgen dat deze voldoet aan de eisen van de CSC.	ISO 27017:2015 16.1.1

	2.	Als onderdeel van de dienstspecificaties moet de CSP de toewijzing van verantwoordelijkheden en procedures voor het beheer van informatiebeveiligingsincidenten tussen de CSC en de CSP definiëren.	ISO 27017:2015 16.1.1
verzamelen	3.	De CSP moet de CSC documentatie verstrekken over: • de omvang van de informatiebeveiligingsincidenten die de CSP aan de CSC zal rapporteren; • het niveau van openbaarmaking van de detectie van informatiebeveiligingsincidenten en de daarmee samenhangende reacties; • het beoogde tijdsbestek waarbinnen meldingen van informatiebeveiligingsincidenten zullen plaatsvinden; • de procedure voor het melden van informatiebeveiligingsincidenten; • contactgegevens voor de afhandeling van problemen met betrekking tot informatiebeveiligingsincidenten; • alle rechtsmiddelen die van toepassing kunnen zijn als zich bepaalde informatiebeveiligingsincidenten voordoen.	ISO 27017:2015 16.1.1
	4.	Nadat een beveiligingsincident, volgens een responsplan voor beveiligingsincidenten is afgehandeld, wordt door de CSP de rapportage ter definitieve bevestiging naar de CSC gestuurd.	BSI C5:2021 SIM-03 CCM:2020 SEF-03
	5.	De CSP definieert en implementeert processen, procedures en technische maatregelen voor meldingen van beveiligingsinbreuken in de (toeleverings)keten. De CSP rapporteert aan de CSC inbreuken op de beveiliging en veronderstelde inbreuken op de beveiliging, inclusief eventuele relevante inbreuken op de (toeleverings)keten, volgens de toepasselijke SLA's en wet- en regelgeving.	CCM:2020 SEF-07
	6.	De CSP meldt een incident onmiddellijk als een incident aanzienlijke gevolgen heeft voor de continuïteit van zijn essentiële dienst, ook als de CSP niet valt onder de jurisdictie van Nederland, bij de Nederlandse minister van Justitie en Veiligheid en de bevoegde autoriteit. De CSP onderhoudt daartoe contactpunten voor toepasselijke regelgevende instanties, nationale en lokale wetshandhavingsinstanties en andere juridische bevoegde autoriteiten.	NIB:2016 artikel 4, 19e lid en overweging nr. 17 Wbni:2018 artikel 10 CCM:2020 SEF-08

	7.	De CSC en de CSP moeten overeenstemming bereiken over de procedures om te reageren op verzoeken om potentieel digitaal bewijsmateriaal of andere informatie vanuit de cloudcomputing-omgeving.	ISO 27017:2015 16.1.7

4.2.21 *U.21 Waarborgen van de bedrijfscontinuïteit*

Objectdefinitie

Het waarborgen van de bedrijfscontinuïteit betreft die maatregelen, die tijdens normaal bedrijf en bij voorkomende calamiteiten, binnen de in de SLA overeengekomen maximale uitvalduur (RTO), zorgen voor het herstel van de clouddienst, inclusief de gegevens van de CSC, waarbij voor de CSC een normale bedrijfsvoering op een passend niveau (Quality of Service (QoS)) is.

Objecttoelichting

Omdat de CSC voor zijn bedrijfsvoering sterk afhankelijk is van de CSP, zijn door de CSP getroffen bedrijfscontinuïteitsmaatregelen van essentieel belang. Bedrijfscontinuïteitsmaatregelen omvatten het pakket aan maatregelen dat, zowel voor een normaal bedrijf als voor situaties van calamiteiten, zoals natuurrampen, zorgt voor het herstel van gegevens en de dienstverlening, waarbij gegevensverlies beperkt blijft tot het overeengekomen maximale gegevensverlies. Bekende continuïteitsmaatregelen zijn redundantie, disaster recovery en het periodiek aantonen dat herstelfuncties werken.

Doelstelling	De beschikbaarheid van de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie tijdens een verstoring waarborgen.	
Risico	Als bedrijfscontinuïteitsmaatregelen bij de clouddienst onvoldoende zijn ingericht, afgestemd of aantoonbaar werken, bestaat het risico dat bij verstoringen of calamiteiten de clouddienst en de bijbehorende gegevens niet tijdig worden hersteld, waardoor de CSC gedurende korte of langere tijd haar taken geheel of gedeeltelijk niet kan uitvoeren.	
Control	De ICT-gereedheid behoort te worden gepland, **geïmplementeerd**, onderhouden en getest op basis van **bedrijfscontinuïteitsdoelstellingen** en **ICT-continuïteitseisen**.	ISO 27002:2022 5.30
Conformiteitsindicator, nummer en maatregel		Afgeleid/afkomstig van

geïmplemen-teerd	1.	Wanneer de CSC gebruik maakt van meerdere CSP's, dan behoort de CSC ervoor te zorgen dat er een adequate organisatiestructuur is die is voorbereid op een verstoring, deze verzacht en erop reageert, ondersteund door personeel met de nodige verantwoordelijkheid, autoriteit en competentie.	ISO 27002:2022 5.30
	2.	De CSP draagt zorg voor redundantie in middelen en voor een redelijke minimale afstand ervan in overeenstemming met de toepasselijke industrienormen en rekening houdend met calamiteiten, zoals natuurrampen. De CSP informeert de CSC over mogelijke restrisico's in het kader van de BIA van de CSC.	CCM:2020 BCR-11
Bedrijfscon-tinuïteits-doelstellin-gen	3.	De CSC beschrijft de ICT-continuïteitseisen als resultaat van de bedrijfsimpactanalyse (BIA).	ISO 27002:2022 5.30
	4.	Wanneer de CSC gebruik maakt van meerdere CSP's, dan behoort de CSC strategieën voor ICT-continuïteit te identificeren en selecteren waarin opties voor voorafgaand aan, tijdens en na een verstoring in overweging worden genomen. Op basis van de strategieën behoren plannen te worden opgesteld, geïmplementeerd en getest om na een (ver)storing van essentiële processen het vereiste beschikbaarheidsniveau van ICT-diensten binnen de vereiste tijdsbestekken te halen.	ISO 27002:2022 5.30
ICT-continuïteits eisen	5.	De CSP behoort de impact van een storing op de clouddienst of onderneming te bepalen en ervoor te zorgen dat ICT-continuïteitsplannen de volgende ICT-continuïteitsinformatie omvatten: • de maximaal aanvaardbare tijdsperiode (RTO) van elke geprioriteerde ICT-dienst en de procedures voor het herstel van die componenten; • de maximale redelijke periode waarin gegevens verloren kunnen gaan en niet kunnen worden hersteld (RPO) van de als informatie gedefinieerde geprioriteerde ICT-middelen en de procedures om de informatie te herstellen.	ISO 27002:2022 5.30 BSI C5:2021 BCM-02

	6.	De serviceovereenkomst tussen de CSC en de CSP bevat informatie over hoe en in welke mate de continuïteit van de clouddienstverlening is gewaarborgd. In een rampenresponsplan is beschreven hoe te herstellen van natuurrampen en door de mens veroorzaakte rampen.	ISO 27002:2022 5.30 CCM:2020 BCR-09
	7.	De CSC waarborgt dat de in de serviceovereenkomst beschreven informatie over de continuïteit van de clouddienstverlening voldoet aan de continuïteitseisen als resultaat van de BIA.	CIP-netwerk

4.2.22 *U.22 Capaciteitsbeheer*

Objectdefinitie

Capaciteitsbeheer betreft het monitoren van het gebruik van de clouddienst en het voorspellen van verwachte capaciteitseisen om te voldoen aan de vastgestelde prestatiedoelstellingen door de CSP. Ter ondersteuning van de voorspelling is het van belang dat, als onderdeel van het capaciteitsbeheer, het toekomstig verwachte gebruik door de CSC met de CSP wordt afgestemd.

Objecttoelichting

De elastische, schaalbare en on-demand toewijzing van middelen in een clouddienst vergroot over het algemeen de totale capaciteit van de service. De CSC moet zich er echter van bewust zijn dat de ter beschikking gestelde middelen capaciteitsbeperkingen kunnen hebben. Voorbeelden van capaciteitsbeperkingen zijn het aantal processorkernen voor een applicatie, de hoeveelheid beschikbare opslag en de beschikbare netwerkbandbreedte, alsmede de beperkingen in het specifieke abonnement van de CSC of beperkte licentierechten. Als de CSC vereisten heeft die de beperkingen overschrijden, moet de CSC mogelijk de clouddienst of het abonnement wijzigen.

Om ervoor te zorgen dat de CSC capaciteitsbeheer voor clouddiensten kan uitvoeren, moet de CSC toegang hebben tot relevante statistieken over het gebruik van middelen, zoals:

- statistieken voor bepaalde perioden;
- maximale niveaus van het gebruik van de middelen.

Doelstelling	De vereiste capaciteit van de middelen van de clouddienst waarborgen.
Risico	Als het capaciteitsgebruik van de clouddienst onvoldoende wordt gemonitord, voorspeld en afgestemd met de CSP, bestaat het risico dat beschikbare middelen de feitelijke belasting niet aankunnen, waardoor overbelasting optreedt en dit leidt tot onbeschikbaarheid van de clouddienst en verstoring of onjuiste uitvoering van bedrijfsprocessen.

Control	Het gebruik van middelen behoort te worden **gemonitord** en **aangepast** overeenkomstig de huidige en verwachte capaciteitseisen.		ISO 27002:2022 8.6
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
gemonitord	1.	De CSC zorgt ervoor dat de overeengekomen capaciteit die door de clouddienst wordt geleverd, voldoet aan de eisen van de CSC, ook bij capaciteitstekorten of uitval van personeel en IT-middelen.	ISO 27017:2015 12.1.3 BSI C5:2021 OPS-01
	2.	De CSC moet het gebruik van clouddiensten monitoren en hun capaciteitsbehoeften voorspellen om de prestaties van de clouddiensten in de loop van de tijd te garanderen.	ISO 27017:2015 12.1.3
	3.	Afhankelijk van het type clouddienst kan de CSC systeembronnen inzetten die aan hem zijn toegewezen. Daarbij kan de CSP het beheer/gebruik controleren en monitoren om overbelasting van de systeembronnen te voorkomen en een goede performance te bereiken.	BSI C5:2021 OPS-03
aangepast	4.	De CSP moet de totale capaciteit van de middelen monitoren om informatiebeveiligingsincidenten veroorzaakt door tekorten aan middelen te voorkomen. De CSP identificeert daartoe gebruikstrends, zodat de CSP aan toekomstige capaciteitsvereisten kan voldoen.	ISO 27017:2015 12.1.3

4.2.23 *U.23 Back-up van informatie*

Objectdefinitie

Een back-up van informatie is een reservekopie, of een andere vorm van redundante opslag, die een CSP heeft gemaakt van middelen, inclusief de informatie.

Objecttoelichting

De verdeling van de verantwoordelijkheden voor het maken van back-ups in de clouddienst verschilt per type dienst. Bij IaaS ligt de verantwoordelijkheid voor het maken van back-ups doorgaans bij de CSC. Een CSC is zich echter mogelijk niet bewust van zijn verantwoordelijkheid om back-ups te maken van alle CSC-gegevens die in de clouddienst worden geproduceerd, zoals uitvoerbare bestanden die zijn geproduceerd door het gebruik van de ontwikkelingsmogelijkheden van een PaaS-service.

Verschillende niveaus van back-up en herstel kunnen tegen extra kosten als service worden aangeboden en in dit geval kunnen CSC's kiezen wat en wanneer ze een back-up willen maken.

Doelstelling	Herstel mogelijk maken na verlies van gegevens of systemen.		
Risico	Als back-ups van informatie binnen de clouddienst niet volledig, actueel of herstelbaar zijn ingericht, bestaat het risico dat bij verstoringen of calamiteiten gegevens niet (tijdig) kunnen worden hersteld, waardoor de continuïteit van de bedrijfsvoering van de CSC in gevaar komt.		
Control	Back-ups van informatie, software en systemen behoren te worden **bewaard** en regelmatig te worden getest **overeenkomstig** het overeengekomen onderwerpspecifieke **beleid** inzake back-ups.		ISO 27002:2022 8.13
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
bewaard	1.	Het moet duidelijk zijn als de CSC verantwoordelijk is voor het implementeren van back-upmogelijkheden wanneer de CSP deze niet biedt, omdat dit geen onderdeel uitmaakt van het type clouddienst.	ISO 27017:2015 12.3.1
overeenkomstig	2.	De CSP moet de specificaties van zijn back-upmogelijkheden aan de CSC verstrekken. De specificaties moeten, indien van toepassing, de volgende informatie bevatten: • omvang en planning van back-ups; • back-upmethoden en gegevensformaten, inclusief encryptie, indien relevant; • bewaartermijnen voor back-upgegevens; • procedures voor het verifiëren van de integriteit van back-upgegevens; • procedures en tijdschema's voor het herstellen van gegevens vanaf een back-up; • procedures om de back-upmogelijkheden te testen; • opslaglocatie van back-ups.	ISO 27017:2015 12.3.1

	3.	Back-upmaatregelen voor individuele systemen en diensten behoren regelmatig te worden getest om te waarborgen dat ze voldoen aan de doelstellingen van incidentrespons- en bedrijfscontinuïteitsplannen. Dit behoort te worden gecombineerd met een test van de herstelprocedures en te worden gecontroleerd aan de hand van de volgens het bedrijfscontinuïteitsplan vereiste hersteltijd. In het geval van kritische systemen en diensten behoren back-upmaatregelen betrekking te hebben op de informatie, toepassingen en gegevens van alle systemen die nodig zijn om het gehele systeem na een calamiteit te herstellen.	ISO 27002:2022 8.13
beleid	4.	Wanneer de CSP back-upmogelijkheden levert als onderdeel van de clouddienst, moet de CSC de specificaties van de back-upmogelijkheden opvragen bij de CSP.	ISO 27017:2015 12.3.1
	5.	De CSP moet de CSC veilige en gescheiden toegang bieden tot back-ups, zoals virtuele snapshots van een virtuele machine of de opslag, als een dergelijke dienst aan CSC's wordt aangeboden.	ISO 27017:2015 12.3.1

5 Control-domein

5.1 Doelstelling

Het doel van het control-domein is 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 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 voldoen en dat de governance van de clouddiensten toereikend is ingericht. Ook kan niet worden vastgesteld of de gewenste maatregelen worden nageleefd.

5.3 Objecten, controls en maatregelen

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

5.3.1 *C.01 Registratie cloudgebruik en bijhouden risicoanalyses*

Objectdefinitie

Het continu bijhouden van het cloudgebruik en het actualiseren van het overzicht in dreigingen en kwetsbaarheden en het beoordelen van de beheersing van onderkende risico's.

Objecttoelichting

Het bijhouden van het cloudgebruik en het monitoren en het reviewen van de risicoanalyses in relatie tot het gevoerde risicomanagement. Het monitoren en reviewen van risico's is noodzakelijk omdat risicofactoren (waarde van assets, impact, dreigingen, zwakheden en kans op voorkomen en de wet- en regelgeving) steeds veranderen.

Doelstelling	Tijdig nagaan of er veranderingen aanwezig zijn die van invloed zijn op de uitkomst van eerder gemaakte risicoanalyses.

Risico	Als het cloudgebruik en de bijbehorende risicoanalyses niet continu en actueel worden bijgehouden, bestaat het risico dat veranderingen in gebruik, dreigingen, kwetsbaarheden of wet- en regelgeving niet tijdig worden onderkend, waardoor nieuwe of gewijzigde risico's onbeheerst blijven en besluitvorming en bijsturing te laat plaatsvinden.		
Control	De CSC houdt **cloudgebruik** en de risico's daarvan bij, met het doel **risicoanalyses** te actualiseren.		RBC:2022 ISO 27005 2018: 12.2
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
cloudgebruik	1.	De CSC houdt het cloudgebruik en de risico's daarvan bij. Dit wordt bij wezenlijke wijzigingen en ten minste jaarlijks geactualiseerd. 1. De registratie bevat tenminste de volgende zaken: a. het organisatieonderdeel; b. het bedrijfsproces en de verantwoordelijke lijnmanager; c. inzicht in de risico's via een actuele risicoanalyse en DPIA; en d. de leverancier van de public clouddienst en de afgenomen clouddiensten. Dit gebeurt als onderdeel van het rapportageproces voor het IB-beeld, conform de departementale taken en volgens het besluit CIO-stelsel.	RBC:2022 voorwaarde 3 en 5 IK:2023 voorwaarde 13
Risicoanaly-ses	2.	De CSC actualiseert de toegespitste risicoanalyse, exitstrategie en (pre-scan of formele) DPIA bij wezenlijke wijzigingen in de dienstverlening of in de functionaliteit, de technische inrichting, de geografische inrichting of de toeleveranciers, inclusief de te nemen passende acties. Dit vindt ten minste iedere drie jaar plaats of vaker als daar aanleiding toe is. Indien analyses op basis van het cloudbeleid met CIO Rijk moeten worden gedeeld, worden de geactualiseerde analyses opnieuw gedeeld met CIO Rijk.	IK:2023 voorwaarde 9
	3.	Voor bestaande clouddiensten moet conform de BIO2 een risicoanalyse zijn uitgevoerd. Ook deze analyses worden binnen hun huidige levenscyclus en ten minste binnen drie jaar herijkt aan het cloudbeleid en het implementatiekader.	IK:2023 voorwaarde 9
	4.	De CSC 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 wet- en regelgeving, organisatiedoelstellingen, de strategie en het beleid. Daarbij wordt de context van de organisatie steeds in beschouwing genomen.	ISO 27005 2018: 12.2

5.3.2 *C.02 Onpartijdige beoordeling CSP*

Objectdefinitie

Een onpartijdige beoordeling is een beoordeling, bijvoorbeeld in de vorm van een audit, door een derde partij die aantoonbaar onpartijdig is.

Objecttoelichting

Voor het bieden van onpartijdig bewijs zou een relevante onpartijdige audit, zoals geselecteerd door de CSP, een aanvaardbare methode kunnen zijn om tegemoet te komen aan het belang van de CSC bij het beoordelen van de activiteiten van de CSP. Dit op voorwaarde dat er voldoende transparantie wordt geboden. Wanneer de onpartijdige audit onpraktisch is, moet de CSP een zelfevaluatie uitvoeren en het proces en de resultaten ervan aan de CSC bekendmaken.

Doelstelling	Waarborgen dat onpartijdig wordt aangetoond dat de CSP continu een geschikte, toereikende en doeltreffende aanpak voor het beheer van informatiebeveiliging en privacybescherming hanteert.		
Risico	Als het beheer van informatiebeveiliging en privacybescherming bij de CSP niet periodiek en aantoonbaar door een onpartijdige partij wordt beoordeeld, bestaat het risico dat de CSC onvoldoende zekerheid heeft over de daadwerkelijke geschiktheid, toereikendheid en effectiviteit van de genomen maatregelen, waardoor tekortkomingen niet worden onderkend en niet tijdig kunnen worden bijgestuurd.		
Control	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de **implementatie** ervan, met inbegrip van mensen, processen en technologieën, behoren **onpartijdig** en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, te worden beoordeeld en **opgevolgd**.		ISO 27002:2022 5.35
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
implementa-tie	1.	De CSC moet om gedocumenteerd bewijs vragen dat de implementatie van informatiebeveiligingscontroles en richtlijnen voor de clouddienst in overeenstemming is met eventuele beweringen van de CSP. Dergelijk bewijsmateriaal kan certificeringen volgens relevante normen omvatten, zoals ISO 27001, ISAE 3402 en SOC2 (type I of II).	ISO 27017:2015 18.2.1

	2.	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 cloudbeveiligingsbeleid vorm wordt gegeven.	CIP-netwerk
	3.	De CSP moet gedocumenteerd bewijs aan de CSC verstrekken om zijn bewering over het implementeren van informatiebeveiligingscontroles te onderbouwen.	ISO 27017:2015 18.2.1
	4.	Wanneer overeen is gekomen dat er individuele CSC-audits worden gehouden dan zijn het beleid en de instructies (inclusief concepten en richtlijnen) voor het plannen en uitvoeren van audits gedocumenteerd, gecommuniceerd en beschikbaar gesteld en volgens een uniforme structuur gedocumenteerd. Hierbij is er duidelijkheid over de doelstellingen, de verdeling van rollen en verantwoordelijkheden tussen CSC en de CSP, inclusief de kwalificatievereisten voor personeel en de toepasselijke wettelijke en regelgevende vereisten.	BSI C5:2021 COM-02 BSI C5:2021 SP-01
	5.	De CSP zorgt ervoor dat de jaarlijkse rapportage, de uitkomsten van de periodieke servicerapportages en de uitkomsten uit de continue compliance op het cloudbeveiligingsbeleid op elkaar aansluiten.	CIP-netwerk
onpartijdig	6.	Wanneer individuele CSC-audits voor de CSP onpraktisch zijn of de risico's voor de informatiebeveiliging kunnen vergroten, moet de CSP onpartijdig bewijs leveren dat de informatiebeveiliging wordt geïmplementeerd en geëxploiteerd in overeenstemming met het beleid en de procedures van de CSP. Daartoe controleren deskundigen die de toepassing van de relevante en toepasselijke wettelijke, regelgevende, zelfopgelegde en contractuele vereisten op het beleid, de regels en de normen, inclusief de werking van het information security management system (ISMS). Dit gebeurt met regelmatige tussenpozen, ten minste jaarlijks.	ISO 27017:2015 18.2.1 BSI C5:2021 COM-03 CCM:2020 A&A-02
	7.	Het onpartijdige bewijs moet beschikbaar worden gesteld aan potentiële CSC's voordat een contract wordt aangegaan.	ISO 27017:2015 18.2.1

	8.	De CSP behoort periodieke onpartijdige beoordelingen te plannen en te initiëren en hierover te rapporteren aan de CSC.	ISO 27002:2022 5.35
opgevolgd	9.	De CSP behoort zo nodig op basis van de rapportering corrigerende maatregelen te initiëren. Hiertoe worden geïdentificeerde kwetsbaarheden en afwijkingen onderworpen aan een risicobeoordeling en worden vervolgmaatregelen gedefinieerd en opgevolgd. Hiertoe wordt een op risico gebaseerd correctief actieplan gehanteerd, waarbij de herstelstatus beoordeeld kan worden en gerapporteerd wordt aan de relevante belanghebbenden.	ISO 27002:2022 5.35 BSI C5:2021 COM-03 CCM:2020 A&A-03 CCM:2020 A&A-06

5.3.3 *C.03 Beheerorganisatie CSC-CSP inzet clouddiensten*

Objectdefinitie

Een beheerorganisatie voor de inzet van clouddiensten betreft het in de keten CSC-CSP blijvend doelgericht afstemmen en bundelen van kennis en vaardigheden tussen personen voor het inzetten van clouddiensten.

Objecttoelichting

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

In de relatie tussen de CSC en de CSP vormen de taken en verantwoordelijkheden tussen beiden een keten en zijn ze overeengekomen.

Aan de CSC wordt zekerheid geboden over het beoogde beveiligingsniveau van de aangeboden clouddienst.

Doelstelling	Als de beheerorganisatie voor de inzet van clouddiensten tussen CSC en CSP niet duidelijk is ingericht of onvoldoende effectief functioneert, bestaat het risico dat processen, taken en verantwoordelijkheden niet eenduidig worden uitgevoerd, waardoor afspraken niet tijdig of helemaal niet worden opgevolgd en de beheersing van clouddiensten structureel tekortschiet.		
Risico	Ontstaan onduidelijkheid in de processen, waardoor de opvolging van afspraken vertraging oploopt of er zelfs geen opvolging is.		
Control	De CSC en de CSP beoordelen op effectiviteit, zodat hun beheersorganisaties blijvend op elkaar zijn ingericht waarbij 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 tussen de processen van de CSC en van de CSP in een afgestemde processtructuur wordt gecontroleerd op efficiëntie.	NCSC 2015: B.06.07

taken, verantwoordelijkheden en bevoegdheden	2.	De CSC en de CSP houden de taken en verantwoordelijkheden voor de uitvoering van de beheer(s)werkzaamheden bij en de bijbehorende bevoegdheden zijn actueel, zodat deze bijdragen aan de effectiviteit van de ketenafspraken.	CIP-netwerk
functionarissen	3.	De belangrijkste functionarissen (aanspreekpunten) voor de beheerorganisatie in de keten CSC-CSP zijn actueel en de onderlinge relaties zijn met een organisatieschema inzichtelijk onderhouden.	CIP-netwerk

5.3.4 *C.04 Controle op de afhandeling van beveiligingsgebeurtenissen*

Objectdefinitie

De controle op de afhandeling van beveiligingsgebeurtenissen betreft het door de CSP aan de CSC rapporteren over de continue bewaking van beveiligingsgebeurtenissen en de geconstateerde afwijking van het overeengekomen beveiligingsniveau.

Objecttoelichting

In een rapportage van clouddiensten wordt gerapporteerd over bijvoorbeeld de zwakheden, zoals onveilige interfaces en over ongeautoriseerde toegangspogingen, met het doel inzicht en overzicht te krijgen over beveiligingsgebeurtenissen en de opvolging ervan.

Doelstelling	Bewaken dat het monitoren en het opvolgen van beveiligingsgebeurtenissen op niveau blijft en daar waar mogelijk verbeterd kan worden.	
Risico	Als de controle op het monitoren en opvolgen van beveiligingsgebeurtenissen onvoldoende is ingericht of uitgevoerd, bestaat het risico dat geconstateerde zwakheden niet structureel worden opgevolgd, waardoor dezelfde kwetsbaarheden herhaaldelijk kunnen worden misbruikt en de beveiliging van de clouddienst structureel tekortschiet.	
Control	Het monitoren en het opvolgen van beveiligingsgebeurtenissen blijft op niveau of wordt verbeterd doordat de uitvoering regelmatig wordt **bewaakt** en hierover behoort tijdig te worden **gerapporteerd** aan de CSC en **opgevolgd**, terwijl het proces wordt **beoordeeld.**	ISO 27002:2022 8.16 SoGP 2018: SI2.1

Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
bewaakt	1.	Richtlijnen en afspraken voor het monitoren en rapporteren over informatiebeveiliging van de cloudomgeving zijn vastgesteld en worden toegepast conform U.11.	SoGP 2018: S12.1.1
gerapporteerd	2.	Het rapporteren over de informatiebeveiliging is 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 rapporteren vindt plaats op basis van: • 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.	Op vaste tijdstippen worden statistieken vastgesteld, gemonitord en gerapporteerd over de identificatie en het herstel van kwetsbaarheden.	CCM:2020 TVM-10
	5.	Informatiebeveiligingsrapportages worden in samenhang met rapportages uit andere beheerdisciplines (compliance en assurance-management en vulnerability-management) geanalyseerd.	SoGP 2018: S12.6
	6.	Aantoonbaar wordt opvolging gegeven aan verbetervoorstellen uit analyserapportages.	CIP-netwerk
opgevolgd	7.	De beveiligingsplannen van de CSC en de CSP worden periodiek geactualiseerd en toegewezen aan de hiervoor verantwoordelijke functionarissen.	NCSC 2015: 07.11
beoordeeld	8.	Het beleid en de procedures voor het tijdige beheer van beveiligingsincidenten vaststellen, documenteren, goedkeuren, communiceren, toepassen, evalueren en onderhouden. Minstens jaarlijks worden het beleid en de procedures beoordeeld en geüpdatet.	CCM:2020 SEF-02

	9.	De processen, procedures en technische maatregelen ter ondersteuning van bedrijfsprocessen om informatiebeveiligingsgebeurtenissen te beoordelen zijn gedefinieerd, geïmplementeerd en geëvalueerd.	CCM:2020 SEF-06

5.3.5 *C.05 Controle op de afspraken uit leveranciersovereenkomst en SLA*

Objectdefinitie

Controle op de afspraken uit de leveranciersovereenkomst en SLA gaat over de periodieke evaluatie en controle van deze afspraken op effectiviteit en compleetheid.

Objecttoelichting

Door bij het opstellen van de leveranciersovereenkomst en SLA te kijken naar de maatregelen, zoals die in de objecten zijn beschreven, wordt aandacht gegeven aan die aspecten die van belang zijn voor het mitigeren van risico's. Door hier periodiek een evaluatie en controle op uit te voeren en daar waar nodig verbeterplannen door te voeren, blijft de informatieveiligheid en de gegevensbescherming op het vereiste niveau.

Doelstelling	Alle afspraken die in de leveranciersovereenkomst worden geëvalueerd en gecontroleerd op verbeterpunten of het up-to-date zijn.	
Risico	Als de afspraken uit de leveranciersovereenkomst en SLA niet periodiek en aantoonbaar worden geëvalueerd en gecontroleerd, bestaat het risico dat afwijkingen en verouderde afspraken niet tijdig worden onderkend, waardoor de clouddienst niet langer voldoet aan overeengekomen beveiligings- en prestatieniveaus en bijsturing uitblijft.	
Control	De **contractuele vereisten en SLA's** en in het bijzonder **BCM**, **cryptografie**, **software**, veiligheid van de **koppelvlakken**, de **interoperabiliteit & portabiliteit** worden als onderdeel van een **informatiebeveiligingsprogramma** periodiek geëvalueerd en gecontroleerd op verbeterpunten en het up-to-date zijn.	CIP-netwerk
Conformiteitsindicator, nummer en maatregel		Afgeleid/afkomstig van

contractuele vereisten en SLA's	1.	Minimaal jaarlijks worden de contractuele vereisten en SLA's gecontroleerd voor alle diensten die een CSP aan de CSC levert. Wanneer niet aan de contractuele vereisten en SLA's wordt voldaan, wordt dit in samenspraak tussen de CSC en de CSP besproken en worden de problemen opgelost.	CCM:2020 STA-10
BCM	2.	De CSC evalueert het beleid en de procedures voor bedrijfscontinuïteitsbeheer (BCM) en operationele weerbaarheid. De evaluatie van het up-to-date houden van het beleid en de procedures gebeurt minstens jaarlijks.	CCM:2020 BCR-01
	3.	Herstelprocedures worden door de CSP regelmatig getest, tenminste jaarlijks. Met de tests kan worden beoordeeld of zowel de contractuele afspraken met de CSC als de specificaties voor de maximaal toelaatbare downtime (Recovery Time Objective, RTO) en het maximaal toelaatbare dataverlies (Recovery Point Objective, RPO) worden nageleefd (zie U.21). Afwijkingen van de specificaties worden gemeld aan de CSC.	BSI C5:2021 OPS-08
cryptografie	4.	Het beleid en de procedures voor cryptografie, encryptie en sleutelbeheer (zie U.10) worden minstens jaarlijks beoordeeld.	CCM:2020 CEK-01
	5.	Voer een audit uit van encryptie- en sleutelbeheersystemen, encryptiebeleid en bijbehorende processen met een frequentie die evenredig is aan de risicoblootstelling van het systeem, waarbij de audit bij voorkeur continu maar ten minste jaarlijks en na eventuele beveiligingsgebeurtenissen plaatsvindt.	CCM:2020 CEK-09
	6.	Registreer en bewaak belangrijke levenscyclusbeheergebeurtenissen om auditing en rapportage over het gebruik van cryptografische sleutels mogelijk te maken.	CCM:2020 LOG-11
software	7.	Door de CSC worden voor het veilig houden van de applicaties de effectiviteit van de basisvereisten gecontroleerd en de versies van de basisvereisten beheerd. Zo nodig worden de vereisten, de documentatie en de communicatie verbeterd.	BSI C5:2021 SP-01 CCM:2020 AIS-02

koppel vlakken	8.	De CSP bewaakt, versleutelt en beperkt de communicatie tussen segmenten/omgevingen tot alleen geverifieerde en geautoriseerde verbindingen. De CSP controleert deze configuraties ten minste jaarlijks en ondersteunt ze met een gedocumenteerde rechtvaardiging van alle toegestane services, protocollen, poorten en compenserende controles.	CCM:2020 IVS-03
	9.	Als penetratietesten onderdeel zijn van de beveiligingstests, genoemd als onderdeel in de leveranciersovereenkomst, dan worden voor het periodiek uitvoeren van penetratietesten door onpartijdige derde partijen de processen, procedures en technische maatregelen gedefinieerd, geïmplementeerd en geëvalueerd.	CCM:2020 TVM-06
interoperabiliteit & portabiliteit	10.	Het beleid, de procedures en de voorzieningen voor retourneren, verplaatsen en verwijderen van bedrijfsmiddelen, inclusief de daarvoor benodigde interoperabiliteit en portabiliteit worden, in lijn met U.02, minstens jaarlijks beoordeeld en geüpdatet.	CCM:2020 IPY-01
Informatie-beveiligings-programma	11.	De CSC hanteert een informatiebeveiligingsprogramma met daarin de aandachtspunten voor de inzet van de clouddiensten. De afspraken in de leveranciersovereenkomst en de objecten in dit thema-document kan daarvoor input zijn.	CCM:2020 GRC-05