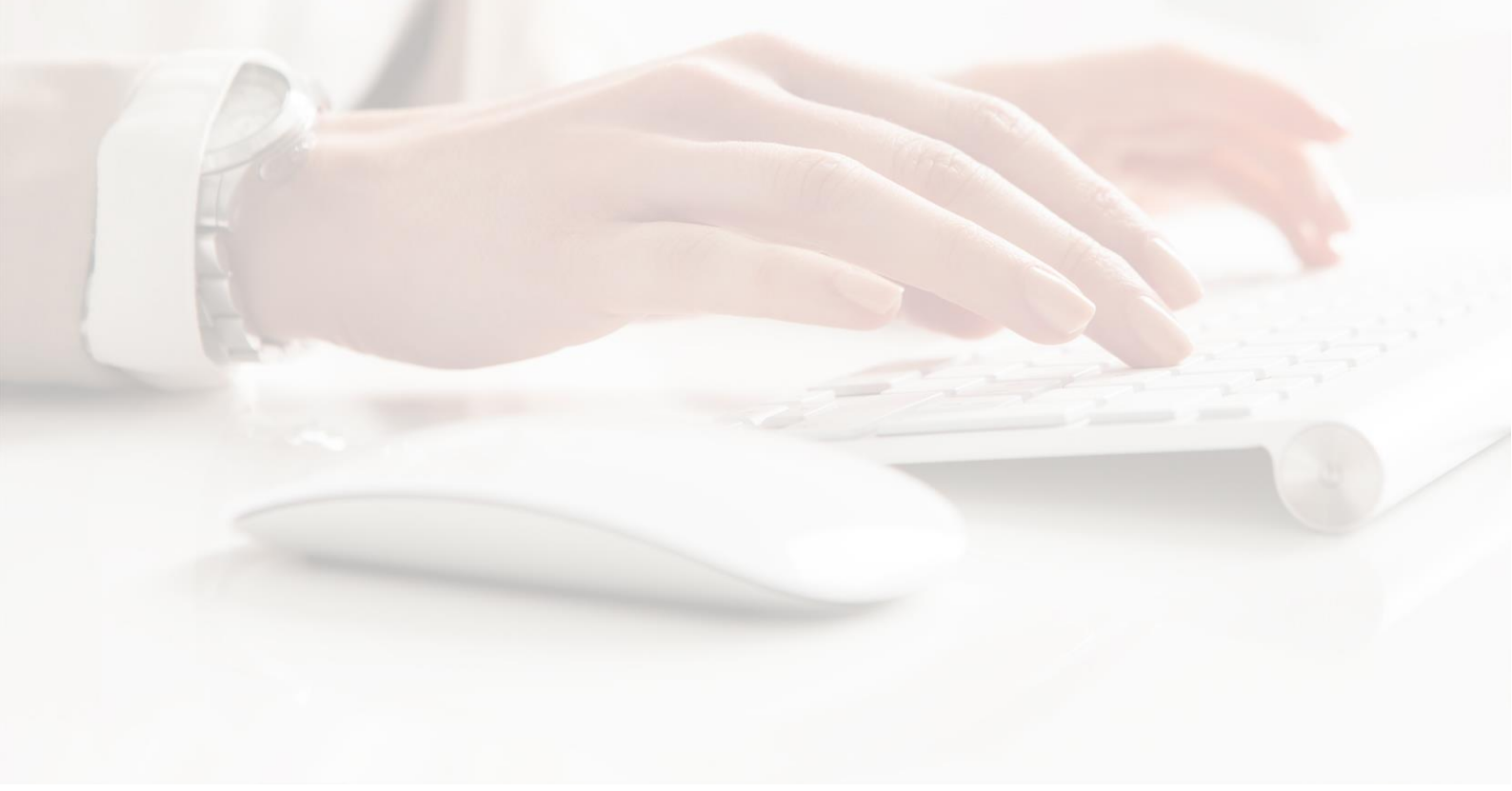
NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

NOREA Handreiking

Handreiking voor SOC 2® en SOC 3® op basis van ISAE3000 / Richtlijn 3000A.

December 2021



Inhoudsopgave

1 Inleiding

1.1 Achtergrond

Deze handreiking is ontwikkeld voor Nederlandse IT auditors (RE's) om hen handvatten te geven voor het uitbrengen van System and Organization Controls 2 rapporten (hierna: SOC 2®) en System and Organization Controls 3 rapporten (hierna SOC 3®) onder ISAE 3000 of het equivalent de NOREA 'Richtlijn 3000A Assurance-opdrachten door IT-auditors'[1]. 'SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy' is een door het American Institute of Certified Public Accountants (AICPA) uitgebrachte guide. Deze Nederlandse publicatie is geen nieuwe richtlijn maar is een handreiking voor Register IT auditors (hierna: auditors) en kan ook nuttige achtergrond informatie geven aan de gebruikers van SOC 2® en SOC 3® assurance-rapporten.

De publicatie van de handreiking speelt in op een groeiend aantal verzoeken vanuit IT serviceorganisaties voor de inzet van auditors bij het uitbrengen SOC 2® en SOC 3® rapporten in Nederland. SOC 2® is geen standaard, maar een specifieke invulling van de Amerikaanse assurance standaard AT-C 205. Deze handreiking geeft handvatten voor het uitbrengen van gelijksoortige rapporten gebaseerd op ISAE 3000. De auditor werkt hierbij niet onder Amerikaanse wet- en regelgeving. Professioneel gezien is er sprake van het opstellen van een ISAE 3000 rapport. Auditors verwijzen daarbij naar het lokale Nederlandse equivalent van ISAE 3000: 'Richtlijn Assurance-opdrachten door IT-auditors (3000A)'. SOC 3® betreft een invulling van dezelfde standaard die leidt tot een beknoptere vorm van het rapport en die een bredere verspreidingskring heeft.

De structuur van het SOC 2® Rapport volgt de structuur van ISAE 3402 (in de Verenigde Staten: SSAE 18 / AT-C section 320, met de service naam 'SOC 1®'). De beheersingsdoelstellingen (de 'Trust Services Criteria') zijn vastgelegd in TSP sectie 100.

Opdrachten die worden uitgevoerd onder deze handreiking vallen uitsluitend onder Nederlandse wet- en regelgeving, waaronder de NOREA-reglementen en -richtlijnen. Deze Nederlandse opdrachten vallen niet onder de Amerikaanse wet- en regelgeving, waaronder AT-C 205. Om duidelijk te maken dat rapporten worden uitgevaardigd onder Nederlandse wet- en regelgeving, dient uit het assurance rapport van de auditor te blijken dat de opdracht is uitgevoerd onder **ISAE 3000 / System and Organization Controls Report** en voor Nederlands gebruik onder **Richtlijn 3000A / System and Organization Controls Rapport**. Het is toegestaan om op het rapport (bijvoorbeeld het voorblad) de aanduiding SOC 2® of SOC 3® te hanteren.

[1] Referenties aan ISAE 3000 in deze publicatie mogen ook worden vervangen door 'Richtlijn Assurance-opdrachten door IT-auditors' (3000A)'. Vanuit het oogpunt van leesbaarheid nemen we geen dubbele referenties op.

1.2 Doelstelling

Het doel van deze handreiking is om auditors inzicht te geven in de toepassing van de Trust Services Criteria in de praktijk. In de handreiking wordt uiteengezet wat SOC 2® en SOC 3® inhoudt en hoe de vereisten omtrent de Trust Services Criteria toegepast kunnen worden. Tevens worden handvatten gegeven voor het opstellen van de rapportage.

Hoewel het niet de hoofddoelstelling is van deze handreiking, geeft deze ook handvatten om te bepalen welk type assurance-rapport het beste past bij de behoeften van de gebruikers in specifieke situaties:

- ISAE 3402-rapport voor IT service organisaties die gebruikende entiteiten zekerheid willen bieden over de beheersingsmaatregelen die relevant zijn voor hun financiële rapportage processen.
- SOC 2® en/of SOC 3® Rapport voor IT service organisaties die zekerheid willen bieden over de beheersingsmaatregelen op het vlak van Beveiliging, Beschikbaarheid, Integriteit van processen, Vertrouwelijkheid en/of Privacy.

Een SOC 2® en SOC 3® Rapport richt zich – in lijn met ISAE 3402 – op de beheersingsomgeving en de beheersingsmaatregelen in een serviceorganisatie en verschaft geen zekerheid over de uitkomsten van processen (zoals bijvoorbeeld het voldoen aan Key Performance Indicators (KPI's) in Service Level Agreements (SLA)).

De voor de Nederlandse auditors opgestelde handreiking is in de Engelse taal, dit om qua terminologie dicht bij de Amerikaanse SOC 2® guide te blijven. De voorliggende handreiking is een vertaling van deze Engelstalige handreiking. Beide zijn nadrukkelijk bedoeld voor gebruik door Nederlandse auditors.

1.3 Vereist kennisniveau

Om deze handreiking goed te begrijpen is kennis nodig van het stramien voor assurance-opdrachten, van de Richtlijn 3402 en Richtlijn 3000A. We verwijzen alleen naar deze richtlijnen waar dat nodig is om de juiste context te verschaffen. De handreiking gaat er vanuit dat de auditors kennis hebben van inhoud van de meest recente versie van de AICPA SOC 2® guide, de Description Criteria (DC sectie 200) en de Trust Services Criteria (TSP sectie 100). Kennisname hiervan is noodzakelijk omdat niet alle details zijn overgenomen in deze Nederlandse handreiking. De lezer moet zich er bewust van zijn dat nieuwe versies van deze basis documenten invloed kunnen hebben op de invulling van de werkzaamheden en / of het rapport.

1.4 Beperkingen

Indien sprake van een SOC 2® of SOC 3® rapport dat wordt gepubliceerd onder de Amerikaanse wet- en regelgeving (inclusief AT-C 205), dan dient dit rapport te worden opgesteld door een CPA die aangesloten is bij de AICPA.

De AICPA heeft logo's ontwikkeld voor gebruik bij het uitvaardigen van een SOC 2®en SOC 3® rapport. De AICPA onderkent geen lokale equivalenten van deze logo's. Verdere details zijn te vinden in hoofdstuk 2.7.

2 System and Organization Controls (SOC) Rapport

2.1 Achtergrond

Een SOC rapport is een assurance-rapport dat zekerheid verschaft over de beheersingsdoelstellingen en -maatregelen die in dat rapport zijn geformuleerd. De AICPA onderscheidt drie geformaliseerde rapporten met betrekking tot service organisaties:

- SOC 1®: dit rapport is gebaseerd op SSAE 18 / AT-C 320, een Amerikaanse standaard afgeleid van de internationale ISAE 3402 standaard[2], en is alleen van toepassing voor assurance met betrekking tot processen die verband houden met financiële verantwoordingen.
- SOC 2®: dit rapport is gebaseerd op de Amerikaanse assurance standaard AT-C 205, die min of meer het equivalent is van ISAE 3000. Het rapport heeft betrekking op de categorieën (in SOC 2® en TSP sectie 100 aangeduid met 'category'): Beveiliging, Beschikbaarheid, Integriteit van processen, Vertrouwelijkheid en Privacy.
- SOC 3®: dit is een beknopt rapport voor een breed publiek gebaseerd op werkzaamheden gelijk aan SOC2®.

De voorliggende handreiking betreft de Nederlandse equivalent voor SOC 2® en SOC 3® onder de richtlijnen en wet- en regelgeving zoals die van toepassing zijn voor bij de NOREA aangesloten register IT auditors.

[2] Voor de volledigheid merken we op dat een SOC 1® rapport onder de regelgeving van de AICPA is gebaseerd op de standaard 'Statement on Standards for Attestation Engagements no. 18' (SSAE 18). Deze verwijst naar AT-C 320, die op zichzelf de Amerikaanse implementatie is van de ISAE 3402 standaard).

2.2 Belangrijkste kenmerken SOC 2®

Het NOREA System and Organization Controls Rapport wordt uitgevoerd in overeenstemming met ISAE 3000. De belangrijkste kenmerken van SOC 2® rapport afgezet tegen een ISAE 3402 of andere invullingen van ISAE 3000 welke niet zijn gebaseerd op SOC 2® zijn:

- De structuur van het rapport is vergelijkbaar met Richtlijn 3402 rapporten (zie ook paragraaf 2.4).
- Alleen een oordeel met een redelijke mate van zekerheid is mogelijk. Dit is een verschil met ISAE 3000, die ook de mogelijkheid biedt voor een oordeel met een beperkte mate van zekerheid.
- Het rapport is gebaseerd op de in TSP sectie 100 gedefinieerde reikwijdte en doelstellingen. De beginselen (categories) bepalen de criteria (beheersingsdoelstellingen). Een serviceorganisatie kan zelf bepalen welke beheersingsmaatregelen van toepassing zijn voor deze beginselen. In TSP sectie 100 zijn onder de doelstellingen (criteria) zogenaamde "Points of Focus" opgenomen. De Points of Focus geven voorbeelden van de aandachtsgebieden waar mogelijk invulling aan gegeven dient te worden middels beheersingsmaatregelen bij de serviceorganisatie.

  De Points of Focus geven details ten aanzien van de belangrijke en minimale karakteristieken van elke Trust Services Criteria en helpen de serviceorganisatie en de auditor om de belangrijkste elementen te adresseren bij het identificeren van beheersingsmaatregelen bij de serviceorganisatie en te zorgen voor een grotere consistentie tussen rapporten. De Point of Focus worden ook niet opgenomen in het rapport. De Points of Focus zijn echter nadrukkelijk geen checklist, dienen ook niet allen geadresseerd te worden en dienen derhalve uitsluitend als leidraad voor de serviceorganisatie en auditor.
- Er is sprake van type I en type II rapporten.
- Er is – in tegenstelling tot Richtlijn 3402 – geen sprake van een minimum review periode. Niettemin wordt geadviseerd dat een type II rapport minimaal betrekking heeft op een periode van drie maanden.
- Evenals bij Richtlijn 3402 en Richtlijn 3000A moet het rapport een beschrijving omvatten van het systeem. Deze wordt opgesteld conform de Description Criteria 200.
- Het rapport is bedoeld voor gebruikers die de inhoud en de doelstelling van het rapport kunnen begrijpen. De gebruikers van wie verwacht mag worden dat ze over deze kennis beschikken zijn:
  - het management van de serviceorganisatie;
  - het management van de gebruikende entiteit;

- potentiële gebruikers die de informatie toepassen bij het selecteren van een serviceorganisatie of om vast te stellen of deze voldoet aan de eisen. Deze gebruikers verkrijgen de kennis daartoe tijdens het uitvoeren van de due diligence;
- accountants en auditors die de beheersingsmaatregelen bij de gebruikende entiteit beoordelen;
- toezichthoudende autoriteiten.

- De rapporten zijn niet bestemd voor een breed publiek en mogen niet worden gepubliceerd op websites of andere publiek toegankelijke media (zie ook hoofdstuk 4).

2.3 Professionele standaarden

De AICPA heeft voor Amerikaanse accountants een handreiking opgesteld voor het uitvoeren van onderzoeken van beheersingssystemen bij een IT serviceorganisatie met betrekking tot de beginselen Beveiliging, Beschikbaarheid, Integriteit van processen, Vertrouwelijkheid en Privacy van de door het systeem verwerkte informatie. Een dergelijk onderzoek wordt aangeduid met de merknaam SOC 2® en SOC 3®. Het rapport over deze opdracht is een SOC 2® en/of een SOC 3® rapport.

SOC 2® en SOC 3® zijn gebaseerd op AT-C 205. Deze Amerikaanse attestation (assurance) standaard wordt gebruikt voor opdrachten waarin een auditor wordt ingeschakeld voor het onderzoeken van een specifiek onderwerp en het daarover afgeven van assurance-rapporten. De standaard gaat over assurance-opdrachten waarin een auditor zich ten doel stelt voldoende bewijsvoering te verzamelen om te komen tot een oordeel die het vertrouwen van de gebruiker – niet zijnde de verantwoordelijke partij – vergroot over het specifieke onderwerp. Het gaat hier om het meten of evalueren van een specifiek onderwerp ten opzichte van criteria. ISAE 3000 is min of meer het internationale equivalent van AT-C sectie 205.

Deze handreiking is gebaseerd op ISAE 3000 (en de Nederlands variant Richtlijn 3000A), een assurance richtlijn met de volgende kenmerken:

- Het onderzoeksobject (de beschrijving van het systeem van de serviceorganisatie en de daarbij horende beheersingsmaatregelen) is afdoende beschreven.
- De uitgangspunten (criteria) die worden toegepast zijn geschikt gegeven de context van de opdracht.
- De normen waarvan de auditor verwacht dat ze zijn toegepast bij het opstellen van de informatie over het onderzoeksobject zijn beschikbaar voor de verwachte gebruikers van het rapport.
- De auditor verwacht voldoende bewijsvoering te kunnen verzamelen om tot een onderbouwd oordeel te komen.

- De conclusie van de auditor, in de vorm van een oordeel met redelijke mate van zekerheid, wordt via een schriftelijk rapport uitgebracht.
- Het rapport dient een redelijk doel (met andere woorden: het heeft waarde voor de gebruikende entiteit).

De tekst in deze handreiking verwijst naar ISAE 3000 aangezien dit de bron is van de Nederlandse NOREA richtlijn en deze aanduiding wordt herkend buiten Nederland.

2.4 Structuur van het SOC 2® rapport

Om aan ISAE 3000 te voldoen en tegelijkertijd duidelijk te maken dat het een volwaardig equivalent is van SOC 2® bevat de titelpagina:

[*Naam van de serviceorganisatie*]
[*Korte beschrijving van de service*]
[*Datum van waarneming in het geval van een type I rapport*]
[*De review periode in geval van een type II rapport*]

SOC 2® RAPPORT

RELEVANT VOOR BEVEILIGING [Gevolgd door een of meer beginselen: BESCHIKBAARHEID, INTEGRITEIT VAN PROCESSEN, VERTROUWELIJKHEID EN/OF PRIVACY.].

De inhoudsopgave omvat doorgaans de volgende elementen:

Sectie I:	Vermelding van het Management[3]
Sectie II:	Assurance-rapport van de onafhankelijke auditor
Sectie III:	Beschrijving van het systeem door de service organisatie
Sectie IV:	De gehanteerde beginselen en criteria en de door de auditor uitgevoerde testwerkzaamheden inclusief de uitkomst daarvan (optioneel bij een type I rapport)
Sectie V:	Overige informatie verschaft door de serviceorganisatie die niet is onderzocht door de auditor. Deze sectie is optioneel.

Hierna gaan we nader in op deze elementen.

Sectie I Vermelding van het management

De schriftelijke vermelding van het management van de serviceorganisatie omvat de volgende onderdelen:

[3] The service organization's "statement" is equivalent to the service organization's "assertion" as defined under AICPA SOC 2® guidance.

- Het management stelt dat de beschrijving van het systeem van de serviceorganisatie een getrouw beeld geeft van het ontwerp en de implementatie op een bepaald moment of gedurende een bepaalde periode (respectievelijk type I en type II), gebaseerd op de criteria [met verwijzing naar hoofdstuk, paragraaf of paginanummers].
- Het management stelt dat de opzet van de beheersingsmaatregelen zoals geformuleerd in de beschrijving van het systeem voldoen aan de van toepassing zijnde criteria (TSP sectie 100) per een bepaalde datum of gedurende een bepaalde periode (type I respectievelijk type II).
- Het management stelt dat de beheersingsmaatregelen zoals opgenomen in de beschrijving van het systeem effectief hebben gewerkt voor de van toepassing zijnde criteria (TSP sectie 100) gedurende een bepaalde periode (type II rapport).

In de bijlage is een voorbeeld opgenomen.

Sectie II Assurance-rapport van een onafhankelijke auditor

Deze sectie omvat (zowel bij een type I als II rapport) onder meer de volgende zaken:

- Gebruik van het woord 'onafhankelijk' in de titel van de paragraaf die het assurance-rapport bevat.
- Het oordeel:
    - In hoeverre de beschrijving een getrouw beeld geeft.
    - In hoeverre de opzet van de beheersingsmaatregelen afdoende is.
    - In een type II rapport: of er sprake is van een effectieve werking van de beheersingsmaatregelen.
- De scope van de opdracht (inclusief sub-serviceorganisaties, verwachtingen ten aanzien van de beheersingsmaatregelen bij de gebruikende entiteit en/of andere informatie).
- De opmerking dat het management verantwoordelijk is voor de beschrijving van het systeem van de serviceorganisatie.
- De opmerking dat de opdracht is uitgevoerd in overeenstemming met **ISAE 3000** en voor Nederlands gebruik in overeenstemming met **Richtlijn 3000A**.

In de bijlage is een voorbeeld opgenomen, dat is gebaseerd op Appendix H van S*OC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*[4].

[4] Deze is te vinden op https://www.aicpastore.com/SOC/PRDOVR~PC-0128210/PC-0128210.jsp

Sectie III Beschrijving van het systeem door de serviceorganisatie

Deze sectie omvat de volgende componenten:

- Het type of de typen services die worden verleend;
- De hoofdzakelijke service commitments en system requirements;
- De componenten van het systeem noodzakelijk voor het verlenen van de dienst(en), bestaande uit:
    - Infrastructuur: de fysieke structuren van de gebruikte IT (zoals faciliteiten, computers, apparatuur, mobiele apparatuur, communicatienetwerken).
    - Software: de applicatiesoftware en de systeemsoftware die deze applicatie software ondersteunt (zoals besturingssystemen, middleware, utilities).
    - Mensen: de medewerkers die betrokken zijn bij de governance, het gebruik en het beheer van systemen (ontwikkelaars, operators, gebruikers en managers).
    - Procedures: de geautomatiseerde en handmatige werkwijzen in en rondom het systeem.
    - Data: de informatie die door het systeem wordt gebruikt en ondersteund (transacties, bestanden, databases, tabellen).
- Indien incidenten geïdentificeerd zijn die het gevolg zijn van (a) interne beheersingsmaatregelen die niet afdoende waren opgezet of niet effectief hebben gewerkt of (b) die hebben geleid tot een significant gebrek in het bereiken van één of meer service commitments dient de volgende informatie te worden opgenomen:
    - Een beschrijving van ieder voorgekomen incident;
    - De timing omtrent het incident;
    - De reikwijdte (of het effect) van het incident.
- De van toepassing zijnde criteria en de gerelateerde interne beheersingsmaatregelen die opgezet zijn om een redelijke mate van zekerheid te verschaffen dat de serviceorganisatie haar service commitments en system requirements te bereiken.
- Indien van toepassing, de Complementary User Entity Controls die noodzakelijk zijn om de service commitments en system requirements te bereiken;
- Indien gebruik wordt gemaakt van een sub-serviceorganisatie en de interne beheersingsmaatregelen bij de sub-service organisatie noodzakelijk zijn om de doelstellingen van de service organisatie te bereiken, het volgende:
    - Indien gebruik wordt gemaakt van de inclusive methode:
        - Een beschrijving van de services die worden verleend door de sub-serviceorganisatie;

        - De interne beheersingsmaatregelen bij de sub-serviceorganisatie die noodzakelijk zijn om de doelstellingen van de serviceorganisatie te bereiken;
        - Relevante aspecten van de infrastructuur, software, mensen, procedures en data bij de sub-serviceorganisatie;
        - De onderdelen van het systeem die toe te kennen zijn aan de sub-serviceorganisatie.
    - Indien gebruik wordt gemaakt van de carve-out methode:
        - Een beschrijving van de services die worden verleend door de sub-serviceorganisatie;
        - Elk van de trust service criteria die bereikt dienen te worden door interne beheersingsmaatregelen bij de sub-serviceorganisatie;
        - De interne beheersingsmaatregelen die bij de sub-serviceorganisatie ingericht dienen te zijn om de doelstellingen van de service organisatie te bereiken.
- Ieder specifiek criterium van de van toepassing zijnde trust service criteria dat niet relevant is met betrekking tot het systeem en daarbij de reden waarom dit criterium niet relevant wordt geacht.
- Indien de beschrijving een tijdsperiode beslaat (type II onderzoek), de relevante details van significante wijzigingen aan het systeem en de interne beheersingsmaatregelen van de serviceorganisatie gedurende de periode.

In aanvulling op deze eisen die specifiek zijn voor IT serviceorganisaties is het mogelijk om de beschrijving weer te geven op basis van internal control componenten:

- Beheersingsomgeving (zoals de filosofie van het management, beleid en management ten aanzien van beveiliging, fysieke beveiliging, beveiliging van medewerkers, beheersing van omgevingsfactoren, monitoring van systemen, problem management, back-up en herstel, systeem account management);
- Het proces van risicobeoordeling.
- Informatie- en communicatiesystemen.
- Monitoring van beheersingsmaatregelen.

Sectie IV De gehanteerde beginselen en criteria en uitgevoerde testwerkzaamheden inclusief de uitkomst daarvan

Deze sectie omvat de criteria die bij de gekozen beginselen behoren, de door de serviceorganisatie uitgevoerde beheersingsmaatregelen, de beschrijving van de testen door de auditor en de uitkomsten van de testen per criterium. De serviceorganisatie kiest het/(de) van

toepassing zijnde beginsel(en) en definieert de beheersingsmaatregelen die samenhangen met de bij de beginsel behorende criteria. De testaanpak en de uitkomsten van de test komen van de auditor. Bij een type II rapport is een omschrijving van de testen en de testuitkomsten uitkomsten een verplicht onderdeel van het rapport. Voor een type I rapport is de beschrijving van de uitgevoerde testen op opzet en bestaan en de uitkomsten van deze tests optioneel.

Sectie V Overige informatie, verstrekt door de serviceorganisatie, die niet is onderzocht door de auditor

Deze sectie is optioneel en kent geen vooraf gedefinieerde inhoudelijke elementen. De inhoud valt niet binnen de scope van het werk van de auditor. De inhoud mag echter niet tegenstrijdig zijn met de inhoud van het rapport of de werkzaamheden die zijn verricht door de auditor. Het is de verantwoordelijkheid van de auditor om dit vast te stellen. De serviceorganisatie kan in deze sectie informatie opnemen die zij van toegevoegde waarde acht voor de gebruiker van het rapport. Voorbeelden zijn:

- Het voornemen om nieuwe systemen te implementeren die relevant zijn voor de gebruikende entiteit of gebruikend systeem.
- Een plan van aanpak ter oplossing van onvolkomenheden die zijn opgenomen in het rapport.
- De reactie van het management op bevindingen die zijn geconstateerd door de auditor in geval deze reactie niet is beoordeeld door de auditor (bijvoorbeeld omdat de actie in de toekomst ligt).
- Andere diensten van de serviceorganisatie die niet binnen de scope van de opdracht vallen, zoals maatregelen gericht op het waarborgen van de continuïteit.

De sectie mag geen informatie bevatten die in tegenspraak is met observaties of oordelen van de auditor. Bovendien dient de inhoud een relatie te hebben met het onderwerp van het rapport.

2.5 SOC 3® rapport

Een SOC 3® rapport heeft dezelfde reikwijdte als een SOC 2® rapport. Echter geldt voor het uitbrengen van een SOC 3® rapport de expliciete vereiste dat het een rapport betreft zonder bevindingen (oordeel zonder enige beperking). Een SOC 3® rapport betreft een beknoptere versie in vergelijking met het SOC 2® rapport en heeft als doel het bereiken van een bredere verspreidingskring dan het SOC 2® rapport. Het SOC 3® rapport mag publiekelijk beschikbaar gesteld worden, bijvoorbeeld op de website van de serviceorganisatie.

Het NOREA System and Organization Controls Rapport dat invulling geeft aan SOC 3® wordt eveneens uitgevoerd in overeenstemming met ISAE 3000. Echter heeft het rapport dat invulling geeft aan SOC 3® een andere opmaak dan het rapport dat invulling geeft aan SOC 2®. Overeenkomst is dat het rapport eveneens een vermelding van het management, een assurance

rapport van een onafhankelijke auditor en een beschrijving van het systeem bevat. De belangrijkste kenmerken van en vereisten voor het rapport zijn:

- De structuur van het rapport is conform de guideline zoals gesteld in 'SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy'.
- Alleen een oordeel met een redelijke mate van zekerheid is mogelijk. Dit is een verschil met Richtlijn 3000A, die ook de mogelijkheid biedt voor een oordeel met een beperkte mate van zekerheid.
- Het rapport is gebaseerd op de in TSP Sectie 100 gedefinieerde reikwijdte en doelstellingen. De beginselen (categories) bepalen de criteria (beheersingsdoelstellingen). Een serviceorganisatie kan zelf bepalen welke beheersingsmaatregelen van toepassing zijn voor deze beginselen. In TSP Sectie 100 zijn onder de doelstellingen (criteria) zogenaamde "Points of Focus" opgenomen. De Points of Focus geven voorbeelden van de aandachtsgebieden waar mogelijk invulling aan gegeven dient te worden middels beheersingsmaatregelen bij de serviceorganisatie. De Points of Focus zijn echter nadrukkelijk geen verplichting en dienen derhalve uitsluitend als leidraad voor de serviceorganisatie en auditor. De Points of Focus geven details ten aanzien van de belangrijke en minimale karakteristieken van elke Trust Services Criteria en helpen de serviceorganisatie en de auditor om de belangrijkste elementen te adresseren bij het identificeren van beheersingsmaatregelen bij de serviceorganisatie en te zorgen voor een grotere consistentie tussen rapporten. De Point of Focus worden ook niet opgenomen in het rapport. De Points of Focus zijn echter nadrukkelijk geen checklist, dienen ook niet allen geadresseerd te worden en dienen derhalve uitsluitend als leidraad voor de serviceorganisatie en auditor.
- Er is uitsluitend sprake van type II rapporten.
- Er is – in tegenstelling tot Richtlijn 3402 – geen sprake van een minimum review periode. Niettemin wordt geadviseerd dat het rapport minimaal betrekking heeft op een periode van drie maanden.
- Evenals bij Richtlijn 3402 moet het rapport een beschrijving omvatten van het systeem. Deze beschrijving betreft een verkorte versie in vergelijking met de beschrijving van een SOC 2® rapport.
- Het rapport mag ongelimiteerd verspreid worden, in tegenstelling tot Richtlijn 3000A rapporten welke een beperkte verspreidingskring kennen.

2.6 Structuur van het SOC 3® rapport

Om aan ISAE 3000 te voldoen en tegelijkertijd duidelijk te maken dat het een volwaardig equivalent is van SOC 3® bevat de titelpagina:

[*Naam van de serviceorganisatie*]
[*Korte beschrijving van de service*]
[*De verslagperiode*]

SOC 3® RAPPORT

RELEVANT VOOR BEVEILIGING [Gevolgd door een of meer beginselen: BESCHIKBAARHEID, INTEGRITEIT VAN PROCESSEN, VERTROUWELIJKHEID EN/OF PRIVACY.].

De inhoudsopgave omvat doorgaans de volgende elementen:

Sectie I: Vermelding van het management[5]
Sectie II: Assurance-rapport van de onafhankelijke auditor
Sectie III: Beschrijving van het systeem door de serviceorganisatie

Hierna gaan we nader in op deze elementen.

Sectie I Vermelding van het management

De schriftelijke vermelding van het management van de serviceorganisatie omvat de volgende onderdelen:

- Het management stelt dat de beschrijving van het systeem van de serviceorganisatie een getrouw beeld geeft van het ontwerp en de implementatie gedurende een bepaalde periode, gebaseerd op de criteria [met verwijzing naar hoofdstuk, paragraaf of paginanummers].
- Het management stelt, per category van toepassing (Beveiliging, Beschikbaarheid, Integriteit van processen, Vertrouwelijkheid en/of Privacy), dat voldoende maatregelen zijn getroffen om invulling te geven aan de category gedurende de verslagperiode.
- Het management stelt dat de beheersingsmaatregelen zoals opgenomen in de beschrijving van het systeem effectief hebben gewerkt voor de van toepassing zijnde criteria (TSP sectie 100) gedurende een bepaalde periode (type II rapport).
- Het management stelt, indien van toepassing, dat interne beheersingsmaatregelen effectief hebben gewerkt indien gebruikers de Complementary User Entity Controls hebben geïmplementeerd en deze effectief hebben gewerkt gedurende de periode.

In de bijlage is een voorbeeld opgenomen.

[5] The service organization's "statement" is equivalent to the service organization's "assertion" as defined under AICPA SOC 2® guidance

Sectie II Assurance-rapport van een onafhankelijke auditor

Deze sectie omvat onder meer de volgende zaken:

- Gebruik van het woord 'onafhankelijk' in de titel van de paragraaf die het assurance-rapport bevat.
- De scope van de opdracht (inclusief sub-serviceorganisaties, verwachtingen ten aanzien van de beheersingsmaatregelen bij de gebruikende entiteit en/of andere informatie).
- De opmerking dat het management verantwoordelijk is voor de beschrijving van het systeem van de serviceorganisatie.
- De opmerking dat de opdracht is uitgevoerd in overeenstemming met **ISAE 3000** en voor Nederlands gebruik in overeenstemming met **Richtlijn 3000A**.
    - Het oordeel.

In de bijlage zijn voorbeelden opgenomen.

Sectie III Beschrijving van de grenzen van het systeem door de serviceorganisatie (description of the boundaries of the system)

Deze sectie omvat minimaal de volgende componenten:

- De achtergrond van het systeem:
    - Scope van de dienstverlening
    - Afbakening van het systeem
    - Subserviceorganisaties
- Een overzicht van het systeem dat ten minste ingaat op:
    - Infrastructuur: de fysieke structuren van de gebruikte IT (zoals faciliteiten, computers, apparatuur, mobiele apparatuur, communicatienetwerken).
    - Software: de applicatiesoftware en de systeemsoftware die deze applicatie software ondersteunt (zoals besturingssystemen, middleware, utilities).
    - Mensen: de medewerkers die betrokken zijn bij de governance, het gebruik en het beheer van systemen (ontwikkelaars, operators, gebruikers en managers).
    - Procedures: de geautomatiseerde en handmatige werkwijzen in en rondom het systeem.
    - Data: de informatie die door het systeem wordt gebruikt en ondersteund (transacties, bestanden, databases, tabellen).
- Processen en procedures

- Interne controle, deze sectie gaat ten minste in op:
    - Beheersingsomgeving.
    - Risico-analyse.
    - Beheersingsmaatregelen.
    - Informatie en communicatie.
    - Monitoring activiteiten.
- Complementary user entity controls.
- Complementary subservice organization controls.

De sectie mag geen informatie bevatten die in tegenspraak is met observaties of oordelen van de auditor. Bovendien dient de inhoud een relatie te hebben met het onderwerp van het rapport.

In tegenstelling tot de inhoud van het SOC 2® rapport bevat het rapport geen verdere uitwerking van beheersingsmaatregelen en de daarbij uitgevoerde werkzaamheden en conclusies van de onafhankelijke service auditor.

2.7 Logo

De AICPA heeft een logo ontwikkeld[6] dat kan worden gebruikt door een serviceorganisatie als deze minstens over een van de genoemde SOC rapporten beschikt, verstrekt door een bij het AICPA aangesloten CPA die zich heeft gebaseerd op de AICPA-standaarden. Een serviceorganisatie kan bekend maken dat assurance-rapporten beschikbaar zijn door deze logo's in drukwerk of online te gebruiken.

In de situatie waarin een System and Organization Controls rapport is gebaseerd op ISAE 3000 (of het lokale equivalent) en is afgeven door een Nederlandse IT auditor, wordt niet voldaan aan de eisen van het AICPA en kan het logo niet worden gebruikt. NOREA heeft geen Nederlands equivalent voor het logo.

Hoofdstuk 4 van deze handreiking gaat verder in op het onderwerp marketing en promotie van een SOC 2® en/of SOC 3® rapport.

[6] http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SOCLogosInfo.aspx

3 Uitvoering van een SOC 2® en/of SOC 3® opdracht

De uitvoering van een SOC 2® en/of SOC 3® opdracht verloopt conform de professionele standaarden zoals beschreven in hoofdstuk 2. Voor een succesvolle uitvoering is het nodig dat de inrichting van de serviceorganisatie voldoende ontwikkeld is. Dit hoofdstuk bevat een aantal belangrijke aandachtspunten voor de verantwoordelijk auditor bij de uitvoering van SOC 2® en/of SOC 3® assurance-opdracht.

3.1 Ervaring en kennis auditor (engagement partner/team)

Er zijn twee hoofdvoorwaarden voor het accepteren of continueren van een SOC 2® en/of SOC 3® opdracht door een auditor: (1) "De personen die de opdracht uitvoeren hebben samen de benodigde professionele competenties" en (2) "De auditor plant de uitvoering van de opdracht zodanig dat deze effectief kan worden uitgevoerd".

ISAE 3000 vereist dat de auditors naast een generiek kennisniveau ook specifieke kennis hebben van processen, technieken, bedrijfstak-specifieke aspecten en rapportering en dat teamleden alleen worden ingezet voor taken die overeenstemmen met hun kennisniveau en hun competenties zodat ze in staat zijn om tot bevindingen te komen en deze te beoordelen.

De auditor kan tijdens de opdracht tot de conclusie komen dat hij/zij op bepaalde onderdelen onvoldoende kennis of ervaring heeft op het vlak van vaktechniek, respectievelijk het onderwerp van de opdracht. De kennis wordt opgedaan door het volgen van onderwijs – waaronder zelfstudie – of door het opdoen van ervaring in de praktijk. Het is niet noodzakelijk dat de auditor persoonlijk alle benodigde kennis heeft om gekwalificeerd te zijn voor het afgeven aan een assurance-rapport. De kenniseisen kunnen deels worden ingevuld door specialisten in te zetten, mits de auditor voldoende kennis heeft om te communiceren met deze specialisten over de doelstellingen van het werk en in staat is om de uitkomsten van het werk van de specialisten te beoordelen om te zien of aan de doelstellingen is voldaan.

De auditor moet voldoende inzicht hebben in het expertisedomein van de specialist om de aard, scope en doelstelling van diens werk te kunnen definiëren en om vast te kunnen stellen of het werk van de specialist in het licht van de doelstellingen adequaat is. De Code of Ethics[7] bepaalt dat een auditor altijd voldoende professionele kennis en competenties moet bezitten. Dit betekent bijvoorbeeld dat het onwaarschijnlijk is dat een registeraccountant met weinig kennis van IT in staat is om een SOC 2® en/of SOC 3® rapport uit te brengen zonder de hulp van een gespecialiseerde auditor.

Verder is het belangrijk dat de auditor begrip heeft van de diensten die door de serviceorganisatie worden ondergebracht bij sub-serviceorganisaties om vast te kunnen stellen of dit invloed heeft op het kunnen voldoen aan de trust services criteria door de service

[7] Reglement gedragscode Register IT-auditors (NOREA) en Verordening gedrags- en beroepsregels accountants (NBA)

organisatie. Daarbij hoort ook het kunnen beoordelen of het management de juiste afwegingen heeft gemaakt over de vraag of een organisatie moet worden gekwalificeerd als een sub-serviceorganisatie (zie ook paragraaf 3.3).

3.2 Onafhankelijkheid

De auditor volgt de van toepassing zijnde standaarden ten aanzien van de professionele onafhankelijkheid. Het gaat hierbij minimaal om de gedragscode register IT auditors van NOREA[8]. Voor de auditors die werken voor accountantskantoren is mogelijk de VIO ('Verordening inzake de onafhankelijkheid van accountants bij assurance-opdrachten') van de NBA van toepassing.

3.3 Opname methode / uitsluitingsmethode

Voor het management van een serviceorganisatie is het belangrijk om vast te stellen of de beheersingsmaatregelen behorende bij activiteiten die zij heeft uitbesteed aan een leverancier nodig zijn om te voldoen aan een of meer van de gedefinieerde criteria (TSP sectie 100). Als dat het geval is, is er sprake van een sub-serviceorganisatie. Het is belangrijk dat al deze sub-service-organisaties tijdens de planning van een SOC 2® en/of SOC 3® opdracht zo vroeg mogelijk worden geïdentificeerd.

Er zijn twee opties voor het omgaan met een sub-serviceorganisatie: de opname methode (inclusive method) en de uitsluitingsmethode (carve-out method). De keuze is een verantwoordelijkheid van de serviceorganisatie. De auditor heeft de verantwoordelijkheid om de argumenten van het management te toetsen.

De opname methode gaat ervanuit dat de werkzaamheden van de auditor ook gericht zijn op de relevante beheersingsmaatregelen bij de sub-serviceorganisatie. De omschrijving van het systeem door de serviceorganisatie omvat dan ook, zover van toepassing alle elementen ten aanzien van de beginselen Beveiliging, Beschikbaarheid, Integriteit van processen, Vertrouwelijkheid en/of Privacy, waar deze liggen bij de sub-serviceorganisatie.

Bij de uitsluitingsmethode is het bovenstaande niet het geval. De betreffende activiteiten van de sub-serviceorganisatie worden niet opgenomen in de beschrijving van het systeem. Als de serviceorganisatie deze methode gebruikt dient dit te worden gemotiveerd door het management. Deze motivatie wordt opgenomen in het rapport. De auditor stelt vast of er – gegeven de uitsluiting – sprake is van een rationele opdracht die hij kan accepteren volgens de voorwaarden van de Code of Ethics.

[8] Hoewel de gedragscode van NOREA niet specifiek ingaat op het aspect onafhankelijkheid is er wel sprake van een fundamenteel beginsel 'Objectiviteit' als cruciale voorwaarde voor onafhankelijkheid. Dit beginsel stelt dat er geen sprake mag zijn van vooringenomenheid, conflicterende belangen of ongewenste invloeden die het oordeel kunnen beïnvloeden.

De beschrijving van het systeem dient in het geval van sub-serviceorganisaties het volgende te omvatten:

- De aard van de services die door de sub-serviceorganisatie worden verleend.
- Waar van toepassing aangeven dat beheersingsmaatregelen (mede) bij de sub-serviceorganisatie liggen.
- De beheersingsmaatregelen die nodig zijn bij een uitgesloten sub-serviceorganisatie om te voldoen aan de beginselen en criteria (TSP sectie 100), al dan niet in combinatie met maatregelen bij de serviceorganisatie zelf.

De sub-serviceorganisatie – evenals de keuze voor een opname of uitsluitingsmethode – moet worden genoemd in de vermelding van het management en in het oordeel van de auditor.

Leveranciers worden vaak gezien als sub-serviceorganisaties. Echter, als de serviceorganisatie zelf de verantwoordelijkheid neemt voor de risico's en de noodzakelijke beheersingsmaatregelen hoeft er geen aanleiding te zijn om deze leverancier te kwalificeren als een sub-serviceorganisatie. Voorbeelden daarvan zijn installatiebedrijven, verhuurders van datacenter-locaties. Indien gebruikt wordt gemaakt van sub-serviceorganisaties, dan dienen in dat geval monitoringsmaatregelen te worden ingericht voor de beheersingsmaatregelen die worden uitgevoerd bij de sub- serviceorganisatie teneinde vast te stellen dat de beheersingsmaatregelen die zijn uitgevoerd door de sub-serviceorganisatie effectief hebben gewerkt gedurende de rapportageperiode.

3.4 Materialiteit en de beoordeling van bevindingen (uitzonderingen)

Een audit wordt uitgevoerd met een bepaald tolerantieniveau ten aanzien van bevindingen, ook wel materialiteit genoemd. Beslissend hierbij is de vraag of een bevinding bepalend is voor door de gebruiker van het rapport te maken afwegingen. Materialiteit heeft in de context van procedure gerichte assurance-rapporten betrekking op het systeem waarover wordt gerapporteerd (kwalitatieve materialiteit) en niet op financiële verantwoording van de gebruikende entiteiten. In de planning en uitvoering hanteert de auditor een materialiteit ten aanzien van drie gebieden: (1) de getrouwe presentatie van de beschrijving van het systeem (2) de opzet van de beheersingsmaatregelen en (3) in geval van een type II rapport de effectieve werking van beheersingsmaatregelen. Bij het bepalen van de materialiteit is het zaak om uit te gaan van de gebruikelijke verwachtingen en wensen van een brede groep gebruikers en hun auditors die begrip hebben van de wijze waarop het systeem van de serviceorganisatie wordt gebruikt.

De beschrijving van het systeem omvat de aspecten die nodig zijn om, met een redelijke mate van zekerheid, te kunnen komen tot inzicht in de uitvoering van transacties, zonder dat belangrijke aspecten ontbreken of zijn vertekend.

Bij het bepalen van de materialiteit spelen onder meer de volgende factoren een rol:

- De complexiteit van het proces dat wordt ondersteund door de beheersingsmaatregelen.
- Het inherente risico op fraude of fouten.
- Acceptabele en waargenomen niveaus van bevindingen.
- De aard en oorzaak van gedane bevindingen.

De initiële vaststelling van de materialiteit wordt door de auditor gedocumenteerd. Het is de basis voor een voorlopig oordeel over de toepasbaarheid van de criteria en voor de geplande testwerkzaamheden, gebaseerd op zijn begrip van het systeem van de service organisatie.

Nadat de werkzaamheden zijn uitgevoerd vindt een herbeoordeling plaats van de materialiteit op basis van de uitkomsten.

De auditor evalueert de bevindingen uit de testwerkzaamheden en onderzoekt de aard en oorzaak van de geconstateerde bevindingen. Op basis daarvan stelt hij vast of de uitkomsten reden zijn om te concluderen dat de beheersingsmaatregel niet voldoende effectief heeft gefunctioneerd in de betreffende periode.

Na het analyseren van de bevindingen en de invloed op de effectiviteit van de beheersings-maatregel stelt de auditor vast wat de impact is op het bereiken van de gedefinieerde beheersingsdoestellingen (criteria) – zowel de afzonderlijke doelstellingen als het geheel van de doelstellingen. De bevindingen kunnen in de volgende vier categorieën vallen. In veel gevallen is er een gedegen professionele afweging nodig om de categorie te bepalen.

- Bevindingen die duidelijk onbelangrijk zijn en waarschijnlijk geen impact hebben op het/(de) beginsel(en) waar het assurance-rapport betrekking op heeft. In dit geval zijn de testwerkzaamheden voldoende basis voor de conclusie dat de beheersingsmaatregelen effectief hebben gewerkt gedurende de gespecificeerde periode.
- Bevindingen die niet tot gevolg hebben dat een beheersingsmaatregel als ineffectief wordt beoordeeld maar die wel relevant kunnen zijn voor een gebruikende entiteit. De relevantie wordt bepaald door de vraag of de auditor van mening is dat de uitzondering impact heeft op het/(de) beginsel(en) waar het assurance-rapport betrekking op heeft.
- Bevindingen die aanleiding geven tot meer testwerk om vast te kunnen stellen of de betreffende beheersingsmaatregelen of andere beheersingsmaatregelen adequaat inspelen op het criterium en daarmee afdoende basis vormen voor een conclusie over de effectieve werking van de beheersingsmaatregelen gedurende de gespecificeerde periode.

- Bevindingen die tot de conclusie leiden dat de beheersingsmaatregel niet afdoende heeft gewerkt gedurende de gespecificeerde periode. De beheersingsmaatregel wordt dan beoordeeld als niet effectief.

Duidelijk onbelangrijke bevindingen zijn bevindingen die geen effect hebben op de organisatie van de gebruiker en de beoordeling van de interne beheersing door de lezer van het rapport. Het gaat dan om unieke of kleine zaken die niet door beheersingsmaatregelen worden afgedekt en slechts in een kleine toename van het controlerisico resulteren. De auditor stelt op basis van de analyse van de bevindingen vast of de doelstellingen van de beheersingsmaatregel(en) zijn gerealiseerd op basis van kwantitatieve en kwalitatieve materialiteit.

Indien sprake is van bevindingen of als naar aanleiding van bevindingen sprake is van een oordeel met beperking(en) van de auditor betekent dit niet dat het rapport geen waarde meer heeft voor de gebruikende entiteit bij het beoordelen van de risico's op materiële onjuistheden. De gebruiker van het rapport gebruikt de informatie uit het rapport immers voor de eigen risico-inschatting.

NB: een opdracht die als doel heeft te resulteren in een SOC 3® rapport kan alleen afgerond worden in het geval dat er geen bevindingen zijn geconstateerd die van zodanige invloed zijn dat de beheersingsdoelstelling(en) niet wordt/(worden) behaald. Een SOC 3® rapport mag uitsluitend uitgebracht worden indien sprak is van een oordeel zonder enige beperkingen.

Het is belangrijk dat de auditor in voldoende detail rapporteert over de bevindingen die voortkomen uit het testwerk, zodat de gebruiker goed inzicht krijgt in deze bevindingen en wat de oorzaak van de bevinding is. Daartoe is de volgende informatie nodig:

- De beheersingsmaatregel die is getest.
- Of het gaat om een test met betrekking tot een deelwaarneming of een test van de gehele populatie.
- De aard van de test.
- Het aantal geteste eenheden per test.
- Het aantal en de aard van de bevindingen.
- De oorzaak van de bevindingen.

Wanneer bij het testwerk bevindingen zijn geïdentificeerd kan het voor de gebruikers van het rapport zinvol zijn als het management, voor zover mogelijk, inzicht verschaft in de oorzaken van de bevindingen, de beheersingsmaatregelen die het effect van de bevinding compenseren, corrigerende acties en andere kwalitatieve factoren die gebruikers helpen om goed te begrijpen wat het effect is van de bevinding.

Deze informatie kan door de serviceorganisatie worden gepresenteerd in de optionele sectie van een type II-rapport getiteld 'Overige Informatie'. Deze sectie valt zoals beschreven in hoofdstuk 2 niet onder de verantwoordelijkheid van de auditor.

Een andere optie is dat het management in de sectie met de beschrijving van het systeem een reactie op de bevinding van de auditor opneemt. In dat geval dient de auditor vast te stellen of er voldoende onderbouwing is voor de reactie van het management door nadere inlichtingen in te winnen in combinatie met andere werkwijzen. Als er daarbij sprake is van toekomstgerichte informatie vanuit het management – zoals het voornemen om beheersingsmaatregelen te implementeren of bevindingen te adresseren – dient deze informatie te worden opgenomen in de sectie 'Overige Informatie'.

3.5 Typen procedures

Het testen of beheersingsmaatregelen effectief zijn heeft als doel om vast te stellen of de verschillende gedefinieerde criteria worden behaald. Het testwerk moet zijn afgestemd op de omstandigheden en richt zich op het verkrijgen van een redelijke mate van zekerheid over het voldoen aan de criteria gedurende de gespecificeerde periode.

Bij het bepalen van het uit te voeren testwerk voor het vaststellen van de werking van de maatregelen beoordeelt de auditor de aard van de beheersingsmaatregelen, de beschikbare documentatie, de te behalen doelstellingen (criteria) en de verwachte efficiency en effectiviteit van de beschikbare test procedures en technieken. Het geheel van het testwerk wordt gebruikt om vast te stellen of de beschrijving van de beheersingsmaatregelen getrouw is en of de maatregelen effectief werken. Er zijn verschillende soorten test procedures, zoals hieronder opgenomen. In veel gevallen zal er sprake zijn van een combinatie.

Test procedure	Omschrijving
Inwinnen inlichtingen	Interviews met relevante medewerkers over de relevante beheersingsmaatregelen.
Observatie	Vaststellen dat specifieke beheersingsmaatregelen worden toegepast
Inspectie	Het lezen van documenten en rapporten die een indicatie geven over het functioneren van de beheersingsmaatregel. Dit omvat ook het lezen van (management) rapporten om te beoordelen of beheersingsmaatregelen adequaat worden gemonitord en of management tijdig actie onderneemt indien dat nodig is.
Herhaalde uitvoering	Het opnieuw uitvoeren van een beheersingsmaatregel om na te gaan of deze correct is uitgevoerd.

De ISAE 3000 geeft meer achtergrond over het uitvoeren van deze test procedures.

Een SOC 2® en/of SOC 3® rapport geeft geen oordeel in de uitkomsten van beheersingsmaatregelen of systemen. De auditor kan niettemin data analyse technieken of andere tooling inzetten om door middel van de output van het proces de effectiviteit van

beheersingsmaatregelen te testen. Dergelijke testprocedures worden ingezet om de effectiviteit van de beheersingsmaatregelen te testen en dienen ter waarborging dat voldoende testwerk is uitgevoerd.

3.6 Typen conclusies

In de bijlage is een voorbeeld opgenomen van een assurance-rapport.

Als de auditor in zijn conclusie beperkingen aanbrengt, dan geeft hij in het auditor's report een duidelijke omschrijving van de redenen daarvoor. Het gaat daarbij onder meer om de volgende gevallen:

- De beschrijving van het systeem door het management geeft in alle materiële opzichten geen getrouw beeld.
- De opzet van de beheersingsmaatregelen is onvoldoende om door onderzoek naar de werking te kunnen komen tot een redelijke mate van zekerheid dat de van toepassing zijnde beheersingsdoelstellingen (criteria) worden gehaald.
- Bij een type II rapport: de beheersingsmaatregelen hebben niet effectief gewerkt gedurende de gespecificeerde periode om de van toepassing zijnde beheersingsdoelstellingen (criteria) te halen.
- Er is sprake van een beperking in de scope die ervoor zorgt dat de auditor onvoldoende bewijs kan verkrijgen.
- De schriftelijke vermelding van het management geeft onvoldoende detail, gaat niet in op bevindingen van de auditor die leiden tot een oordeel met beperkte zekerheid of bevatten onvolkomenheden die het management niet bereid is aan te passen. Hierbij moet de vermelding van het management in lijn zijn met het assurance-report.
- Materiele inconsistentie tussen de overige informatie (sectie V), en de inhoud van het rapport, zoals een verkeerde voorstelling van zaken, waarbij het management weigert om de informatie te corrigeren.

In de afweging over het aanpassen van het auditor's rapport houdt de auditor rekening met de gevolgen van individuele bevindingen ten aanzien van de vermelding van het management en het totaal van die bevindingen. Ook houdt de auditor rekening met de opzet en werking van de beheersingsmaatregelen gedurende de verslagperiode. De auditor weegt onder meer de volgende kwalitatieve en kwantitatieve factoren:

- De aard en oorzaak van de bevinding.
- De tolerantie die de auditor heeft gehanteerd ten aanzien van het aantal bevindingen.
- De alomtegenwoordigheid van de bevinding (bijvoorbeeld of de bevinding meer dan een criterium raakt).

- De waarschijnlijkheid dat de bevinding een indicator is dat er sprake is van tekortkoming die ertoe leiden dat criteria niet worden gehaald.
- De omvang van de fouten die kunnen ontstaan als gevolg van ontoereikende beheersingsmaatregelen.
- De vraag of gebruikers mogelijk misleid worden als het oordeel van de auditor geen beperking bevat.

Als de auditor geen goedkeurend oordeel afgeeft, dan neemt hij in het assurance rapport een duidelijke omschrijving van de redenen op. Het doel is dat gebruikers van het rapport zelf kunnen beoordelen wat het effect is. Als geen goedkeurend oordeel mogelijk is kan de auditor kiezen voor een oordeel met beperking, een oordeelonthouding of een afkeurend oordeel.

In het geval van een SOC 3® rapport leidt een oordeel anders dan een goedkeurend oordeel tot het feit dat het SOC 3® rapport niet uitgebracht mag worden.

4 Het gebruik van een SOC 2® en/of SOC 3® Rapport

Een verschil met ISAE 3402 rapporten is dat de primaire gebruiker van een SOC 2® en/of SOC 3® rapport veelal *niet* de accountant van gebruikende entiteit is, maar het management van de serviceorganisatie en het management van de gebruikende entiteiten (en toekomstige gebruikers en de toezichthouders). Een SOC 2® en/of SOC 3® rapport helpt het management om de uitbestede diensten te monitoren. Als een organisatie bijvoorbeeld back-up services bij een serviceorganisatie inkoopt zonder dat daarbij sprake is van bedrijfsgeheimen, zal dit niet relevant zijn voor de accountant en diens controle van de financiële verantwoording. Maar het management zal wel geïnteresseerd zijn in de beveiliging, beschikbaarheid en vertrouwelijkheid van deze service.

Niettemin kan een SOC 2® en/of SOC 3® rapport nuttig zijn voor de accountant van de entiteit die gebruik maakt van een service organisatie. Sommige beheersingsmaatregelen uit het rapport kunnen gerelateerd zijn aan processen die invloed hebben op de financiële verantwoording. De accountant heeft de verantwoordelijkheid om te beoordelen in hoeverre dit het geval is, aangezien het primaire doel en de scope verschilt van die van een ISAE 3402 rapport.

Het is mogelijk dat er misverstanden ontstaan over een SOC 2® rapport als dit buiten de context wordt gebruikt waarvoor het is bedoeld. Het SOC 2® rapport is dan ook alleen bestemd ter informatie van en voor gebruik door het management van de serviceorganisatie en andere gespecificeerde partijen die voldoende kennis en begrip hebben van:

- De aard van de door de serviceorganisatie verleende diensten.
- Hoe het systeem van de serviceorganisatie samenhangt met de gebruikende entiteit, sub-serviceorganisaties (inclusief complementary subservice organization controls) en andere partijen.
- Interne beheersing en de beperkingen daarvan.
- Aanvullende beheersingsmaatregelen bij de gebruikende entiteit en hoe deze samenhangen met de beheersingsmaatregelen bij de serviceorganisatie om aan de van toepassing zijnde criteria te voldoen.
- De van toepassing zijnde criteria (Trust Services Criteria).
- De risico's die van invloed zijn op het voldoen aan deze criteria en hoe beheersingsmaatregelen deze risico's adresseren.

Gebruikers van het rapport die geacht worden over deze kennis te beschikken zijn:

- het management van de serviceorganisatie
- het management van de gebruikende entiteit
- het management van partijen die overwegen in de toekomst diensten te gaan afnemen van de serviceorganisatie
- auditors die beheersingsmaatregelen beoordelen of erover rapporteren
- toezichthouders.

Het SOC 2® rapport is niet bestemd voor gebruik door andere partijen dan de hiervoor genoemde.

Het SOC 3® rapport betreft een ongelimiteerde verspreidingskring en mag daarmee bijvoorbeeld ook op de website van de service organisatie beschikbaar gesteld worden.

4.1 Marketing en communicatie door de serviceorganisatie

Het SOC 2® rapport is alleen bestemd voor gespecificeerde gebruikers en het is niet toegestaan om generieke kwaliteitsuitingen te doen die inhouden dat het systeem van interne beheersing aan een audit is onderworpen en goedgekeurd door een onafhankelijke service auditor. Ook andere claims (bijvoorbeeld dat een SOC certificaat is verkregen, of dat de serviceorganisatie beschikt over een systeem van interne beheersing van hoge kwaliteit) zijn niet toegestaan. Deze claims zijn niet correct, kunnen verkeerd worden geïnterpreteerd en zijn misleidend. De auditor dient dit bij zijn cliënt onder de aandacht te brengen.

Wat wel kan is dat een serviceorganisatie op haar website toelicht wat de aard is van het rapport, voor wie het rapport beschikbaar is en hoe die organisaties het rapport kunnen verkrijgen.

Het SOC 3® rapport betreft een ongelimiteerde verspreidingskring en mag daarmee bijvoorbeeld ook op de website van de service organisatie beschikbaar gesteld worden.

5 Categorieën en Criteria

5.1 Achtergrond

5.1.1 Introductie

De AICPA Assurance Services Executive Committee (ASEC) heeft een set categorieën en criteria ontwikkeld (Trust Services Criteria) voor het beoordelen van beheersingsmaatregelen op het gebied van Beveiliging, Beschikbaarheid, Integriteit van processen van systemen, Vertrouwelijkheid en Privacy. Deze categorieën en criteria worden van tijd tot tijd herzien. De beschrijving in deze handreiking gaat uit van de versie van 2017, die van toepassing is voor periodes die eindigen op of na 15 december 2018.

Het uitgangspunt van deze beginselen en criteria is de opzet, implementatie en operatie van het systeem van de serviceorganisatie dat bedoeld is om bepaalde zakelijke doelen te bereiken (zoals het verlenen van diensten of de productie van goederen) en dat is ingericht in overeenstemming is met door het management gedefinieerde eisen. Er zijn vijf categorieën van systeem componenten: infrastructuur, software, mensen, processen en data.

Elke categorie heeft een set criteria (in het Nederlands ook wel aangeduid met 'beheersings-doelstellingen'). Deze sets zijn er voor het beoordelen van de effectiviteit van beheersingsmaatregelen voor zover deze relevant zijn voor de Beveiliging, Beschikbaarheid, Integriteit van processen, Vertrouwelijkheid en Privacy van de informatie die door het systeem wordt verwerkt.

5.1.2 Trust Services Criteria

De Trust Services beginselen zijn de volgende:

- *Beveiliging:* Het systeem is beveiligd tegen ongeautoriseerde toegang, gebruik of aanpassing.
- *Beschikbaarheid:* Het systeem is beschikbaar voor gebruik zoals aangegeven door de serviceorganisatie of zoals overeengekomen.
- *Integriteit van processen:* De processen in het systeem zijn volledig, valide, accuraat, tijdig en geautoriseerd.
- *Vertrouwelijkheid:* De informatie is vertrouwelijk zoals overeengekomen.
- *Privacy:* Het verzamelen, gebruiken, opslaan en verstrekken en vernietigen van persoonlijke informatie is in overeenstemming met het privacybeleid van de gebruikende entiteit en met andere criteria.

5.1.3 Criteria (beheersingsdoelstellingen)

Een groot aantal van de criteria die worden gebruikt om een systeem te beoordelen zijn van toepassing op alle beginselen. De criteria zijn georganiseerd in algemene criteria die van toepassing zijn op alle vier de beginselen en in aanvullende criteria die specifiek gelden voor één beginsel:

Beginsel	Aantal criteria
Beveiliging	33 algemene criteria
Beschikbaarheid	33 algemene + 3 aanvullende criteria
Integriteit van processen	33 algemene + 5 aanvullende criteria
Vertrouwelijkheid	33 algemene + 2 aanvullende criteria
Privacy	33 algemene + 18 aanvullende criteria

De algemene criteria vormen een complete set voor het beginsel Beveiliging. Voor de andere vier beginselen is sprake van een combinatie van algemene en aanvullende criteria.

De algemene criteria zijn gegroepeerd in de volgende categorieën:

- *Control environment*. Deze 5 criteria gaan over hoe de organisatie is gestructureerd en hoe een set aan normen, structuren en processen de basis vormen voor het uitvoeren van interne controle binnen de entiteit. De criteria gaan onder meer over verantwoordelijkheden, integriteit, ethiek, en de kwalificaties van de medewerkers en hun werkomgeving.
- *Communication and information*. Deze 3 criteria gaan over hoe de organisatie communiceert over beleid, processen, procedures, afspraken en eisen aan geautoriseerde gebruikers en andere partijen en de verplichtingen die deze gebruikers en partijen hebben ten aanzien van een effectief gebruik van het systeem.
- *Risk assessment*. Deze 4 criteria gaan over hoe de organisatie (i) potentiële risico's identificeert die van invloed kunnen zijn op het bereiken van de doelstellingen; (ii) deze risico's analyseert.
- *Monitoring activities*. Deze 2 criteria gaan over hoe de organisatie het systeem monitort, onder meer op geschiktheid, opzet en operationele effectiviteit van de beheersingsmaatregelen.
- *Control activities*. Deze 3 criteria gaan over hoe de organisatie maatregelen neemt om onvolkomenheden te adresseren en om de risico's voor het behalen van de doelstellingen te beperken.
- *Logical and physical access controls*. Deze 8 criteria gaan over hoe de organisatie voorziet in logische en fysieke toegangsbeveiliging tot het systeem en hoe ongeautoriseerde toegang wordt voorkomen om te voldoen aan de criteria in de assurance-opdracht.

- *System operations*. Deze 5 criteria gaan over hoe de organisatie het systeem uitvoert en daarbij detecteert waar er sprake is van bevindingen, waaronder inbreuken op logische en fysieke beveiliging, en daarmee voldoet aan de criteria in de overeenkomst.
- *Change management*. Dit criterium gaat over hoe de organisatie nagaat of er veranderingen in het systeem nodig zijn, hoe deze veranderingen volgens een beheerst change management-proces worden doorgevoerd en hoe ongeautoriseerde veranderingen in het systeem worden voorkomen om te voldoen aan de criteria waar de assurance-opdracht op gericht is.
- *Risk mitigation*. Deze 2 criteria gaan over hoe de organisatie reageert op de geïdentificeerde risico's, waaronder het ontwerp en de implementatie van beheersingsmaatregelen en andere maatregelen die het risico verlagen en (iv) voortdurend monitort hoe risico's en het risicomanagement-proces zich ontwikkelen.

Voor de categorie Beschikbaarheid gelden drie aanvullende criteria, voor de categorieën Integriteit van processen, Vertrouwelijkheid en Privacy gaat het om respectievelijk 5, 2 en 18 aanvullende criteria. Meer informatie over de algemene en aanvullende criteria is te vinden op de AICPA website[9]. TSP sectie 100 is onderhavig aan updates en het is dan ook aanbevolen om vast te stellen dat gebruik wordt gemaakt van de actuele versie.

5.2 Privacy

Deze sectie beschrijft hoe de Privacy category van de Trust Services Criteria opgenomen kan worden in een SOC 2® en/of SOC 3® rapport.

5.2.1 Privacy Criteria

De criteria die gelden voor de Privacy category in de Trust Services Criteria zijn ingedeeld in de volgende onderwerpen:

1. Notice and communication of objectives;
2. Choice and consent;
3. Collection;
4. Use, retention, and disposal;
5. Access;
6. Disclosure and notification;
7. Quality;
8. Monitoring and enforcement.

9 https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf

De SOC 2® privacy criteria zijn echter niet leidend in de Europese Unie. In de Europese Unie is de Algemene Verordening Gegevensbescherming (AVG) van toepassing, die uitgaat van de volgende privacy principes:

1. Transparantie;
2. Doelbeperking;
3. Gegevensbeperking;
4. Juistheid;
5. Bewaarbeperking;
6. Integriteit en vertrouwelijkheid;
7. Verantwoording.

Een vergelijking van de AVG privacy principes met de SOC 2® privacy criteria laat zien dat veel overeenkomsten bestaan tussen beide raamwerken. Het gebruik van de SOC 2® privacy criteria in de Europese Unie is daarmee niet uitgesloten, mits de onderliggende criteria en 'points of focus' niet conflicterend zijn met de AVG privacy principes.

Om invulling te kunnen geven aan de privacy criteria in SOC 2®, kan het NOREA Privacy Control Framework (PCF) gebruikt worden. Analyse van de SOC 2® privacy criteria en 'points of focus' en het NOREA PCF laat zien dat:

- Het mogelijk is om de SOC 2® privacy categorie binnen de scope van SOC 2® opdrachten te betrekken, omdat de SOC 2® privacy criteria en 'points of focus' niet conflicterend zijn met de AVG privacy principes;
- Het PCF van de NOREA gebruikt kan worden om beheersingsmaatregelen in te richten die de SOC 2® privacy criteria afdekken, rekening houdend met het doel (objective) van de (service)organisatie en de 'points of focus'. Er wordt dan gerapporteerd met de criteria (beheersingsdoelstellingen) uit SOC 2®, welke zijn ingevuld met beheersingsmaatregelen vanuit het PCF;
- Voor het behalen van de control objectives uit het PCF en daarmee de SOC 2® Privacy Criteria kunnen de illustrative controls uit de 'NOREA Guide Privacy Control Framework' als uitgangspunt worden genomen. Hierbij dient rekening gehouden te worden met de specifieke privacy risico's (die van toepassing zijn op de betreffende organisatie waarvoor het SOC 2® rapport wordt afgegeven) die worden gemitigeerd door het inrichten van de interne beheersingsmaatregelen. Er dient daarom door de auditor een beoordeling plaats te vinden of de beheersingsmaatregelen voldoende invulling geven aan het bereiken van de control objective, rekening houdend met de van toepassing zijnde privacy risico's voor de betreffende organisatie;
- Aangezien niet alle onderwerpen uit het PCF terugkomen in de SOC 2® Privacy Criteria, dient de auditor vast te stellen of aanvullende beheersingsmaatregelen met betrekking tot privacy ook relevant zijn om op te nemen onder de overige criteria. Voorbeelden zijn de aanwezigheid van een data protection officer (ook wel functionaris voor de

gegevensbescherming), het uitvoeren van data protection impact assessments (DPIAs), en privacy by design en by default.

5.2.2 Mapping van SOC 2® privacy criteria en het Privacy Control Framework (PCF)

In het kader van de AVG en het aantoonbaar maken van beheersing op het gebied van privacy in Nederland is het PCF ontwikkeld door de NOREA; 'NOREA Guide Privacy Control Framework' d.d. mei 2018. Het primaire doel van het PCF is het bieden van guidance teneinde vast te stellen of de control objectives van een entiteit met betrekking tot beheersing van privacy zijn behaald. Het PCF bevat voorgeschreven control objectives op verschillende privacy onderwerpen, is gebaseerd op de artikelen van de AVG en conform verschillende 'good practices' opgebouwd, waaronder het GAPP raamwerk (waarop TSP sectie 100A-1, 2014 gebaseerd is). Het PCF is gestructureerd op basis van het information lifecycle management model en sluit daarmee aan op de opbouw van de TSP sectie 100 (2017) van de AICPA.

Op de Privacy criteria uit TSP sectie 100 (2017) is een directe mapping gemaakt vanuit het PCF. Hierbij is voor elk criteria uit TSP sectie 100 vastgesteld welke control objectives uit het PCF hierop van toepassing zijn. Op deze wijze is zorg gedragen dat aan elk Privacy criteria uit TSP sectie 100 invulling wordt gegeven op basis van één of meerdere control objectives uit het PCF. Uit de mapping blijkt dat het PCF gebruikt kan worden om invulling te geven aan alle Privacy criteria uit TSP sectie 100 en dat de Privacy categorie niet conflicterend is met de AVG. Door middel van de control objectives uit het PCF kan dus invulling gegeven worden aan de Privacy categorie. Hierbij kan vervolgens gebruik worden gemaakt van de illustrative controls uit het PCF om invulling te geven aan de control objectives uit het PCF en daarmee de SOC2 privacy categorie.

Het gebruik van het PCF (of delen daarvan) binnen een SOC 2® opdracht betekent echter niet dat de organisatie, met het behalen van de Privacy categorie, daarmee ook AVG compliant is. Middels het uitvoeren van de SOC2 opdracht wordt derhalve geen assurance afgegeven over AVG compliance, maar over de beheersing van de ingerichte privacy beheersingsmaatregelen. De mapping van de Privacy Criteria op het PCF is bijgevoegd in Annex 1 – Mapping Privacy categorie – PCF.

Een aantal control objectives (van het PCF) kan niet direct worden gemapt op de SOC 2® Privacy Criteria. Daardoor zal, wanneer enkel privacy controls onder de Privacy Criteria worden opgenomen, geen invulling worden gegeven aan een aantal fundamentele privacy aspecten van de AVG, zoals de aanwezigheid van een data protection officer, het uitvoeren van data protection impact assessments, en privacy by design en by default. Indien de onderwerpen (in het PCF wordt verwezen naar 'topics') en onderliggende beheersingsmaatregelen die niet te mappen zijn naar de SOC 2® criteria van de Privacy categorie niet worden opgenomen, wordt in algemene zin geen volledige invulling gegeven aan alle control objectives uit het PCF. Deze aspecten dienen derhalve onder de common criteria van SOC 2® opgenomen te worden. Onder deze criteria

kunnen dan, ook al betreft het 'common' criteria, privacy gerelateerde beheersingsmaatregelen worden opgenomen door de klant. Ook deze PCF onderwerpen zijn opgenomen in de mapping in Annex 1 – Mapping Privacy category – PCF, als onderdeel van de mapping van het PCF op de SOC 2® common criteria.

5.2.3 Scope van de privacy criteria

Binnen SOC 2® assurance-opdrachten bestaat de mogelijkheid om criteria (beheersingsdoelstellingen) buiten scope te plaatsen als een bepaald risico niet van toepassing is op de (service) organisatie. Bijvoorbeeld: in het geval dat een organisatie zelf niet direct persoonsgegevens van betrokken verzameld, is privacy criteria P3.1 niet van toepassing. Als dit het geval is, dan dient in de volgende secties van het rapport opgenomen te worden aan welke criteria geen invulling gegeven wordt door beheersingsmaatregelen en wat daarvan de reden is (zie punt 7 op pagina 38 van de SOC 2® handreiking NOREA):

- In de vermelding van het management;
- In de systeembeschrijving.

In deze secties dient beschreven te worden welke criteria niet binnen de scope van de assurance-opdracht vallen omdat hiervoor geen beheersingsmaatregelen zijn opgenomen, en wat hiervan de reden is. Hierbij is het van belang dat de auditor een inschatting maakt of de Privacy categorie als geheel wordt behaald in het geval dat bepaalde criteria buiten scope worden geplaatst.

5.2.4 Verwerkingsverantwoordelijke vs. Verwerker

Het aantal criteria en 'points of focus' waaraan invulling wordt gegeven is afhankelijk van de aard van de organisatie. Als de organisatie zich kwalificeert als Verwerkingsverantwoordelijke zijn mogelijk meer criteria van toepassing op de organisatie, dan wanneer zij als Verwerker optreedt. Criteria of delen hiervan kunnen voor een Verwerker niet van toepassing zijn. In het geval dat een criteria deels van toepassing is op de Verwerker dient in de 'user control considerations' verder invulling te worden gegeven aan de verantwoordelijkheid van de Verwerkingsverantwoordelijke.

5.3 Aanwijzingen voor de vermelding van het management en het SOC 2® assurance-rapport

Een SOC 2® rapport geeft een oordeel over:

- De vraag of de beschrijving van het systeem van de organisatie getrouw is en gebaseerd is op de scope van de criteria (TSP sectie 100).
- De vraag of de beheersingsmaatregelen in opzet een redelijke mate van zekerheid geven dat wordt voldaan aan de van toepassing zijnde criteria (TSP sectie 100) als de beschreven maatregelen effectief werken.

- In type II rapporten: de vraag of de beheersingsmaatregelen effectief hebben gewerkt om te voldoen aan de van toepassing zijnde criteria (TSP sectie 100).

Het management van de serviceorganisatie hanteert de aanwijzingen in paragraaf 5.3.1 (in SOC 2® aangeduid met 'criteria') bij het opstellen van hun vermelding (in SOC 2® aangeduid met 'assertion', ISAE 3000 – revised – aangeduid met 'statement') over het systeem en de auditor verwijst ernaar in zijn oordeel. Deze aanwijzingen zijn niet direct beschikbaar voor de gebruikers en om die reden dient het management alle aanwijzingen op te nemen in haar vermelding. Het is mogelijk dat niet alle aanwijzingen van toepassing zijn voor een specifiek geval. De aanwijzing v) in paragraaf 2.4 is bijvoorbeeld niet van toepassing op een serviceorganisatie die geen rapporten of andere informatie verstrekt aan een gebruikende entiteit of andere partijen. De aanwijzing in vii) (2) in paragraaf 2.4 is niet van toepassing bij een serviceorganisatie die geen gebruik maakt van een sub-serviceorganisatie. In dergelijke gevallen vinden gebruikers het doorgaans zinvol dat alle elementen waar de aanwijzingen betrekking op hebben in het rapport worden opgenomen en dat het management aangeeft welke normen om welke redenen niet van toepassing zijn. Dat kan zij doen in de beschrijving van het systeem of in een separate notitie over de uitwerking van de aanwijzingen voor de omschrijving.

5.3.1 Aanwijzingen voor de beschrijving

De aanwijzingen voor een getrouw beeld van de beschrijving van het systeem vereisen dat de volgende informatie in het rapport is opgenomen:

a. Beschrijving omvat alle relevante zaken zoals benoemd in paragraaf 2.4;

b. De beschrijving laat geen relevante zaken weg of geeft geen verkeerde voorstelling van zaken over het systeem en is opgesteld voor de algemene informatiebehoefte van een brede groep gebruikers. De beschrijving hoeft dekt daarom niet alle aspecten af te dekken die een individuele gebruiker belangrijk acht.

Zoals benoemd in paragraaf 2.6 betreft de beschrijving van het SOC 3® rapport een verkorte versie van de beschrijving uit het SOC 2® rapport.

5.3.2 Aanwijzingen voor de opzet

De aanwijzing om vast te stellen of de opzet van de beheersingsmaatregelen voldoet betreft de vraag of de maatregelen, indien deze werken zoals beschreven, een redelijke mate van zekerheid bieden dat aan de van toepassing zijnde criteria wordt voldaan.

5.3.3 Aanwijzingen voor effectieve werking

De aanwijzing om vast te stellen of de beheersingsmaatregelen van het systeem effectief hebben gewerkt om te voldoen aan de van toepassing zijnde criteria (TSP sectie 100) betreft de vraag of deze gedurende de specifieke periode consistent hebben gewerkt overeenkomstig de opzet,

waaronder de vraag of de handmatige beheersingsmaatregelen zijn uitgevoerd door competente en bevoegde personen.

6 SOC 2® en SOC 3® versus andere standaarden

6.1 Het 'mappen' van criteria

Een auditor heeft een norm nodig om in een assurance-rapport te komen tot een conclusie. Er zijn in de praktijk echter meerdere normen zoals ISO 27002 en PCI-DSS. In het geval van een SOC 2® en/of SOC 3® rapport gaat het om de criteria van TSP sectie 100. Indien deze niet worden gehanteerd is er sprake van een rapport dat niet in lijn is met de aanwijzingen van AICPA SOC 2® handreikingen. Ervan uitgaande dat het rapport voldoet aan de eisen van ISAE 3000A is er nog steeds sprake van een valide assurance-rapport wat waarde kan hebben voor een gebruiker. Het is echter geen SOC 2® of SOC 3® rapport. Bij het toepassen van andere raamwerken dan TSP sectie 100 kan het rapport de structuur van een ISAE 3000 / Richtlijn 3000A rapport volgen.

Indien er tevens behoefte is aan een referentie naar een ander normen stelsel dan de TSP is een suggestie om het SOC 2® en/of SOC 3® rapport af te zetten tegen andere raamwerken, een praktijk die in de Verenigde Staten bij SOC 2® populair is. Veel professionals hebben 'mappings' beschikbaar voor hun cliënten van de TSP met ISO 27002, CMM10, PCI-DDS, etc. De Cloud Service Alliance heeft een SOC 2® mapping gepubliceerd met de Cloud Control Matrix (CCM).

Deze handreiking gaat over de toepassing een SOC 2® en/of SOC 3® rapport. Mappings vallen buiten het bestek van dit document.

6.2 SOC 2® en SOC 3® versus ISAE 3402

Zowel een SOC 2® en SOC 3® rapport als een ISAE 3402 assurance-rapport kan zekerheid verschaffen aan de accountant van een gebruikende entiteit. Het verschil is dat een ISAE 3402 altijd is gerelateerd aan processen die verbandhouden met de financiële verslaglegging en waarbij de beheersingsmaatregelen als hoofddoel hebben het bijdragen aan de betrouwbaarheid (juistheid, volledigheid, tijdigheid) van een financiële verantwoording. ISAE 3402 sluit aan op de eisen uit ISA 402 "Audit considerations relating to an entity using a service organization".

Informatie technologie die ondersteunend is aan de administratieve processen kan onderdeel uitmaken van een ISAE 3402 rapport. Het kan ook de scope zijn van een ISAE 3402 rapport van een IT service bureau waar applicaties worden uitgevoerd die een verband houden met de financiële verslaglegging. Echter een SOC 2® en/of SOC 3® rapport over beveiliging zal veelal beter inspelen op de behoefte van de gebruikende entiteit dan een ISAE 3402 rapport.

[10] CCM cloud control matrix, gepubliceerd door de CSA cloud security alliance

7 Bijlage

Deze bijlage bevat een template voor de vermelding van het management en geeft ter illustratie een voorbeeldtekst voor een assurance-rapport van een auditor. Deze bijlage omvat niet alle relevante voorbeelden en er kunnen actuelere versies beschikbaar zijn.

7.1 Vermelding van het management

Deze template voor de vermelding van het management in een SOC 2® rapport heeft de volgende beperkingen:

- Er is geen invulling gegeven aan eventuele overwegingen betreffende beheersingsmaatregelen bij de gebruikende entiteit.
- Er is geen invulling gegeven aan eventuele sub-serviceorganisaties.
- Er is geen invulling gegeven aan een eventueel niet goedkeurend oordeel.

Vermelding van het management van {XYZ Service Organisatie}

Wij hebben de bijgevoegde beschrijving gemaakt met de titel "{Beschrijving van {juridische naam van organisatie}'s {naam of titel van systeem} Systeem over de periode {start datum} tot {eind datum}" (de beschrijving) gebaseerd op de criteria zoals genoemd onder de punten (a)(i)-(ii) hieronder (de criteria voor de beschrijving).

De beschrijving is bedoeld om gebruikers informatie te verschaffen over {type of naam van} systeem, en in het bijzonder beheersingsmaatregelen in het systeem om te voldoen aan de criteria voor {Beveiliging, Beschikbaarheid, Integriteit van processen, Vertrouwelijkheid en/of Privacy} beginselen zoals uiteengezet in TSP sectie 100, "2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy", uitgegeven door het Assurance Services Executive Committee van de AICPA (van toepassing zijnde trust services criteria).

We bevestigen naar eer en geweten dat:

a) de beschrijving een getrouw beeld geeft van {type of name van} systeem gedurende de periode van {start datum} tot {eind datum} (de "gespecificeerde periode"), gebaseerd op de volgende normen voor de beschrijving:

   i. De beschrijving bevat de volgende informatie:

      1. De types dienstverlening.
      2. De componenten van het systeem die worden gebruikt voor de diensten:

         a. Infrastructuur. De fysieke structuren van IT en andere hardware (zoals computers, apparatuur, mobiele telefoons, communicatie netwerken).

b. Software. De toepassingen en de systeemsoftware die deze toepassingen ondersteunt (zoals besturingssystemen, middleware, utilities).

c. Mensen. De medewerkers die betrokken zijn bij de governance, het gebruik en het beheer van systemen (ontwikkelaars, operators, gebruikers en managers).

d. Procedures. De handmatige en geautomatiseerde procedures in en rondom het systeem.

e. Data. De informatie die door het systeem wordt gebruikt en ondersteund (bestanden, databases, tabellen, transacties).

3. De grenzen die in de beschrijving aan het systeem worden gesteld en de aspecten die aan de orde komen.

4. Voor het verschaffen of ontvangen van informatie aan of van sub-serviceorganisaties en andere partijen,

   a. hoe dit gebeurt, wat de rol van de sub-serviceorganisatie of andere partij is

   b. welke procedures er zijn om vast te stellen dat die informatie en de verwerking, onderhoud en opslag daarvan onderworpen zijn aan adequate beheersingsmaatregelen.

5. De van toepassing zijnde trust services criteria en de daarmee samenhangende beheersingsmaatregelen om te voldoen aan de criteria, waaronder:

   a. Aanvullende beheersingsmaatregelen bij de gebruikende entiteit die dienen te worden overwogen in de opzet van het systeem.

   b. In geval van toepassing van de opname methode: de beheersingsmaatregelen bij de sub-serviceorganisatie.

6. Als gebruik wordt gemaakt van de uitsluitingsmethode voor de sub-serviceorganisatie,

   a. de aard van de diensten die worden verleend door de sub-serviceorganisatie;

   b. de van toepassing zijnde trust services criteria die moeten worden afgedekt door beheersingsmaatregelen bij de sub-serviceorganisatie, zelfstandig of in combinatie met beheersingsmaatregelen bij de service organisatie, en de typen beheersingsmaatregelen die naar verwachting nodig zijn bij de sub-serviceorganisatie om te voldoen aan deze criteria.

7. Alle van toepassing zijnde trust services criteria die niet worden afgedekt door een beheersingsmaatregel en de reden daarvan.

8. In de situatie van een type II rapport de relevante veranderingen in het systeem van de organisaties gedurende de betreffende periode.

ii. De beschrijving laat geen relevante zaken weg of geeft geen verkeerde voorstelling van zaken over het systeem en is opgesteld voor de gebruikelijke informatiebehoefte van een brede groep gebruikers. De beschrijving dekt daarom niet alle aspecten af die een individuele gebruiker belangrijk acht.

   a. De beheersingsmaatregelen die in de beschrijving zijn opgenomen zijn toereikend in opzet en bestaan gedurende de periode {start datum} tot {einddatum} om te voldoen aan de van toepassing zijnde trust services criteria

   b. De beheersingsmaatregelen die in de beschrijving zijn opgenomen zijn toereikend in opzet en bestaan en werking gedurende de periode {start datum} tot {einddatum} om te voldoen aan de van toepassing zijnde trust services criteria

{Officiële naam Serviceorganisatie}

{Naam}

{Titel}

{Datum}

7.2 Assurance-rapport SOC 2®

Ter illustratie.

Het assurance-rapport omvat minimaal de volgende elementen	Voorbeeld
a) Een titel die duidelijk aangeeft dat het een onafhankelijk assurance-rapport betreft.	Onafhankelijk Service Auditor Rapport
b) De geadresseerde.	{Geadresseerde}:
c) De conclusie van de auditor. d) Optioneel: Indien oordeel met beperking, oordeelsonthouding of afkeurend oordeel, dient de basis voor het oordeel hier toegevoegd te worden.	Wij hebben onze conclusie gevormd op basis van de zaken die in dit rapport uiteen zijn gezet. Ons oordeel, gebaseerd op de criteria uiteengezet in de vermelding van {Service Organisatie} en de van toepassing zijnde trust services criteria luidt dat: a. De beschrijving een getrouw beeld geeft van ontwerp en implementatie van [{type of naam} gedurende de periode van {Start Datum}, tot {Eind Datum}. b. De beheersingsmaatregelen zoals opgenomen in de beschrijving zijn geschikt om met een redelijke mate van zekerheid te voldoen aan de van toepassing zijnde trust services criteria als deze maatregelen effectief hebben gewerkt gedurende de periode van {Start Datum}, tot {Eind Datum}, en als de gebruikende entiteit de aanvullende beheersingsmaatregelen heeft getroffen zoals verondersteld in het ontwerp van het systeem van {Service Organisatie} gedurende de periode {Start Datum}, tot {Eind Datum}. c. De geteste beheersingsmaatregelen, die samen met de aanvullende beheersingsmaatregelen bij de gebruikende entiteiten, zoals beschreven in de scope-paragraaf van dit rapport, indien deze effectief werken, waren de maatregelen die nodig zijn om een redelijke mate van zekerheid te verschaffen dat de van toepassing zijnde trust services criteria worden behaald. Deze maatregelen werkten effectief gedurende de periode {Start Datum}, tot {Eind Datum}. De specifieke testwerkzaamheden op beheersingsmaatregelen en de aard, timing en resultaten daarvan zijn opgenomen in de sectie van dit rapport met de naam “Criteria, Beheersingsmaatregelen, Test Procedures, en Resultaten.”
e) Een vermelding dat de opdracht is uitgevoerd conform deze handreiking. f) Een vermelding dat de auditor het Reglement Gedragscode ('Code of Ethics') heeft nageleefd.	Wij hebben onze assurance-opdracht uitgevoerd conform Nederlandse wetgeving en de NOREA Richtlijn Assurance-opdrachten door IT-Auditors (3000A). Deze richtlijn vereist dat wij de planning en uitvoering van onze opdracht zo inrichten dat er sprake is van een redelijke mate van zekerheid in ons oordeel. Wij hebben de vereisten van het Reglement Gedragscode (‘Code of Ethics’) van NOREA nageleefd, welke is gebaseerd is op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag.

g)	Een aanduiding of beschrijving van het niveau van zekerheid dat door de auditor is verkregen, de informatie over het onderzoeksobject en, wanneer van toepassing het onderzoeksobject zelf.	We hebben de opdracht gekregen assurance te geven met een redelijke mate van zekerheid over de bijgaande beschrijving getiteld “Beschrijving van {juridische naam van serviceorganisatie}’s {naam of titel van systeem} Systeem” over de periode {start datum} tot {eind datum} (de beschrijving) gebaseerd op de criteria voor een beschrijving zoals weergegeven in DC sectie 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria), (description criteria) en de geschiktheid van de opzet en effectieve werking van beheersingsmaatregelen om te voldoen aan de criteria {Beveiliging, Beschikbaarheid, Integriteit van processen, Vertrouwelijkheid en Privacy} beginselen zoals uiteengezet in TSP sectie 100, “2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy”, uitgegeven door het Assurance Services Executive Committee van de AICPA (van toepassing zijnde trust services criteria) gedurende de periode van {Start Datum}, tot {Eind Datum}. De beschrijving geeft aan dat aan bepaalde van toepassing zijnde trust services criteria alleen kan worden voldaan als de in het ontwerp van het systeem van {juridische naam van serviceorganisatie} veronderstelde aanvullende beheersingsmaatregelen bij {gebruikende entiteit(en)} in opzet adequaat zijn en gedurende de gespecificeerde periode effectief hebben gewerkt, in samenhang met gerelateerde beheersingsmaatregelen bij {juridische naam van serviceorganisatie}. We hebben de opzet en werking van deze aanvullende beheersingsmaatregelen niet onderzocht. {Service Organisatie} gebruikt een serviceorganisatie (sub-serviceorganisatie) {Juridische naam van sub-serviceorganisatie} voor de {Sub-service Functies}. De beschrijving geeft aan dat aan bepaalde trust services criteria alleen kan worden voldaan als de beheersingsmaatregelen bij de sub-serviceorganisatie adequaat zijn in opzet en werking. De beschrijving gaat in op het systeem van {Service Entity}, de beheersingsmaatregelen die relevant zijn voor de van toepassing zijnde trust services criteria en de types beheersingsmaatregelen die de serviceorganisatie verwacht van de sub-serviceorganisatie (opzet en effectieve werking) om te voldoen aan de van toepassing zijnde trust services criteria. [Naam Service Organisatie] gebruikt voor de beschrijving de uitsluitingsmethode. De beschrijving van het systeem gaat dan ook niet in op de beheersingsmaatregelen die zijn getroffen bij de sub-serviceorganisatie. Onze opdracht strekt zich niet uit tot de beheersingsmaatregelen bij de sub-serviceorganisatie. De informatie met de titel "Overige Informatie verstrekt door {naam Service Organisatie} die niet valt onder het Service Auditor's Rapport" is opgenomen door {juridische naam van serviceorganisatie} om additionele informatie te verschaffen en vormt geen onderdeel van de beschrijving van het {type} systeem dat ter beschikking is gesteld aan gebruikende entiteiten. Deze informatie is geen onderdeel van ons onderzoek naar de beschrijving en wij brengen daarover geen oordeel tot uitdrukking.
h)	De beschrijving van de van toepassing zijnde criteria.	De van toepassing zijnde criteria worden aangeduid in de vermelding van de {Service Organisatie}’s in combinatie met de van toepassing zijnde trust services criteria.
i)	Waar van toepassing, een beschrijving van	De beschrijving van de {Service Organisatie} is opgesteld voor de algemene informatiebehoefte van een brede groep gebruikers en hun auditors. De

	de significante inherente beperkingen die verband houden met de meting of evaluatie van het onderzoeksobject ten opzicht van de van toepassing zijnde criteria.	beschrijving dekt daarom niet alle aspecten af die een individuele gebruiker belangrijk acht. Verder is het mogelijk dat beheersingsmaatregelen, vanwege hun aard en inherente beperkingen, niet altijd effectief werkten om te voldoen aan de van toepassing zijnde trust services criteria. Bovendien is de projectie van een eventuele beoordeling van de getrouwheid van de presentatie van de beschrijving of de conclusies omtrent de geschiktheid van de opzet of de effectieve werking naar toekomstige periodes onderhevig aan het risico dat het systeem wordt gewijzigd of dat interne beheersingsmaatregelen bij een serviceorganisatie inadequaat worden of tekortschieten.
j)	Wanneer de van toepassing zijnde criteria voor een bepaald doel zijn gekozen, een vermelding die lezers hierop attent maakt en op het feit dat, als gevolg hiervan, de informatie over het onderzoeksobject mogelijk niet geschikt is voor een ander doel.	Dit rapport en de beschrijving van de testwerkzaamheden en de resultaten daarvan is alleen gericht op gebruik door organisaties die gebruik maken van {Service Entity's Systeem Name} van {Service Organisatie} gedurende de gehele of gedeeltelijke periode van {Start Datum}, tot {Eind Datum} en onafhankelijke auditors die diensten verleen aan deze organisaties voldoende kennis en begrip hebben van: • De aard van de door de serviceorganisatie verleende diensten. • Hoe het systeem van de serviceorganisatie samenhangt met de gebruikende entiteiten, sub-serviceorganisaties en andere partijen. • Interne beheersing en de beperkingen daarvan. • Aanvullende beheersingsmaatregelen bij de gebruikende entiteit en hoe deze samenhangen met de beheersingsmaatregelen bij de serviceorganisatie om de van toepassing zijnde criteria in te vullen. • De van toepassing zijnde criteria (Trust Services Criteria). • De risico's die van invloed zijn op het voldoen aan deze criteria en hoe beheersingsmaatregelen deze risico's adresseren. Dit rapport is niet bedoeld voor gebruik door andere dan de hiervoor genoemde partijen en dergelijk gebruik is niet toegestaan.
k)	Een vermelding van de verantwoordelijke partij en van de evalueerder indien dit een andere partij betreft alsmede een omschrijving van hun verantwoordelijkheden.	{Service Organisatie} heeft de bijgevoegde {Titel Management vermelding} verstrekt, gebaseerd op de daarin geïdentificeerde criteria. {Service Organisatie} is verantwoordelijk voor (1) het opstellen van de beschrijving en de vermelding; (2) de volledigheid, accuratesse en de presentatie van zowel de beschrijving als de vermelding; (3) het verlenen van de diensten zoals in de beschrijving weergegeven; (4) het specificeren van de beheersingsmaatregelen die voldoen aan de van toepassing zijnde trust services criteria en de opname daarvan in de beschrijving; en (5) het opzetten, implementeren en documenteren van de beheersingsmaatregelen om te voldoen aan de van toepassing zijnde trust services criteria.
l) m)	De verantwoordelijkheid van de auditor Een vermelding dat de auditeenheid waar de auditor werkzaam is of aan verbonden is en dat het Reglement Kwaliteitsbeheersing NOREA (RKBN) of regelgeving die ten	Onze verantwoordelijkheid is het uitspreken van een oordeel over de getrouwheid van de presentatie van de beschrijving, gebaseerd op de criteria zoals uiteengezet in de vermelding van {Service Organisatie} en over hoe de opzet en werking van de beheersingsmaatregelen leiden tot het voldoen aan de van toepassing zijnde trust services criteria op basis van procedures die wij hebben gevolgd om een redelijke mate van zekerheid te verschaffen. De auditeenheid past het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe en bijgevolg onderhoudt het een uitgebreid systeem van kwaliteitscontrole met inbegrip van gedocumenteerd beleid en procedures voor de naleving van de

	minste gelijkwaardig is, toepast.	ethische voorschriften, professionele standaarden en de van toepassing zijnde wet- en regelgeving.
n)	Een informatieve samenvatting van de uitgevoerde werkzaamheden als basis voor de conclusie van de auditor.	Onze assurance-opdracht omvat het uitvoeren van procedures die assurance-informatie over de vraag of de presentatie van de beschrijving getrouw is en dat opzet en werking van de beheersingsmaatregelen voldoen aan de van toepassing zijnde trust services criteria. Deze procedures hangen af van beoordelingen door de auditor en de inschatting van het risico dat de beschrijving niet getrouw is en dat de opzet en werking van de beheersingsmaatregelen niet voldoen aan de van toepassing zijnde trust services criteria. De procedures omvatten ook het testen van de effectieve werking van die beheersingsmaatregelen die we noodzakelijk achten om te komen tot een redelijke mate van zekerheid dat wordt voldaan aan de van toepassing zijnde criteria. Onze procedures omvatten ook de beoordeling van de overall-presentatie van de beschrijving. Naar onze mening hebben we voldoende assurance-informatie verkregen om te komen tot een oordeel met een redelijke mate van zekerheid.
o)	Handtekening auditor.	{Handtekening auditor}
p)	Datum van het assurance-rapport.	{Datum van het assurance-rapport}
q)	De locatie in het rechtsgebied waar de auditor werkzaam is.	{Adres van auditor}

7.3 Trust Services Criteria

Gepubliceerd in 2017 door het American Institute of Certified Public Accountants and Chartered Professional Accountants of Canada. Deze set is van toepassing voor periodes die op of na 15 december 2018 eindigen.

- Criteria voor alle categorieën [Beveiliging, Beschikbaarheid, Integriteit van processen, Vertrouwelijkheid en/of Privacy]:
    - Algemene criteria gerelateerd aan 'control environment'.
    - Algemene criteria gerelateerd aan 'communication and information'.
    - Algemene criteria gerelateerd aan 'risk assessment'.
    - Algemene criteria gerelateerd aan 'monitoring activities'.
    - Algemene criteria gerelateerd aan 'control activities'.
    - Algemene criteria gerelateerd aan 'logical and physical access controls'.
    - Algemene criteria gerelateerd aan 'system operations'.
    - Algemene criteria gerelateerd aan 'change management'.
    - Algemene criteria gerelateerd aan 'risk mitigation'.
- A1. Aanvullende criteria voor Beschikbaarheid.
- PI1. Aanvullende criteria voor Integriteit van processen.
- C1. Aanvullende criteria voor Vertrouwelijkheid.
- P1. Aanvullende criteria voor Privacy

Gedetailleerde documentatie is beschikbaar op de AICPA website (https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf).

7.4 SOC 3® rapport – ter illustratie

Een SOC 3® rapportage bevat de volgende elementen	Voorbeeld
a) Een titelpagina die duidelijk aangeeft dat het een SOC 3® rapport betreft.	SOC 3® rapport Rapportage over <systeem/dienst> relevant voor <van toepassing zijnde criteria> <start verslagperiode> tot <einde verslagperiode>.
b) Bewering van het management	Wij zijn verantwoordelijk voor het opzetten, implementeren, en het effectief laten werken van interne beheersingsmaatregelen met betrekking tot <object> gedurende de periode <start verslagperiode> tot en met <einde verslagperiode>, om een redelijke mate van zekerheid te verschaffen dat de serviceverplichtingen en systeemvereisten relevant voor beveiliging, beschikbaarheid, verwerking van integriteit, vertrouwelijkheid en privacy van <klant> werden bereikt. Onze beschrijving van de grenzen van <object> is opgenomen in <bijlage A> en identificeert de aspecten van het <object> die onderdeel zijn van onze bewering. Wij hebben een evaluatie uitgevoerd van de effectieve werking van de interne beheersingsmaatregelen met betrekking tot <object> gedurende de periode <start verslagperiode> tot en met <einde verslagperiode>, om een redelijke mate van zekerheid te verschaffen dat onze serviceverplichtingen en systeemvereisten werden bereikt. Deze evaluatie is uitgevoerd op basis van op de trust services criteria relevant voor beveiliging, beschikbaarheid, integriteit van processen, vertrouwelijkheid en privacy (de van toepassing zijnde 'trust services criteria'), zoals uiteengezet in TSP Sectie 100, 'Trust Services Criteria voor beveiliging, beschikbaarheid, integriteit van processen, vertrouwelijkheid en privacy', van het Amerikaanse Instituut van Public Accountants (AICPA). De doelstellingen van <klant> voor <object> bij het toepassen van de van toepassing zijnde trust services criteria zijn opgenomen in de serviceverplichtingen en systeemvereisten van <klantnaam>. De belangrijkste serviceverplichtingen en systeemvereisten gerelateerd aan de van toepassing zijnde trust services criteria zijn opgenomen in <bijlage B>. Er bestaan inherente beperkingen aan ieder systeem van interne beheersing, waaronder de mogelijkheid tot menselijke fouten en het omzeilen van interne beheersingsmaatregelen. Vanwege deze inherente beperkingen kan een service organisatie redelijke, maar geen absolute zekerheid verschaffen dat de serviceverplichtingen en systeemvereisten worden bereikt. Wij maken gebruik van subservice organisatie(s) <subservice organisatie(s)> om <beschrijving diensten>. De beschrijving van de grenzen van <object> (<bijlage A> van dit rapport) stelt dat bepaalde criteria alleen bereikt kunnen worden indien de beheersingsmaatregelen bij de sub-serviceorganisatie juist zijn opgezet en

	effectief werken. De beschrijving van de grenzen van <object> geeft ook de aanvullende beheersingsmaatregelen van de subservice organisatie weer die zijn verondersteld bij de opzet van de interne beheersingsmaatregelen van <klant>. De beschrijving van de grenzen van <object> geeft niet de feitelijke interne beheersingsmaatregelen bij de subservice organisatie weer. De beschrijving van de grenzen van <object> (bijlage A van dit rapport) stelt dat bepaalde criteria alleen bereikt kunnen worden indien de beheersingsmaatregelen bij de gebruikersorganisatie juist zijn opgezet en effectief werken. De beschrijving van de grenzen van <object> geeft ook de aanvullende beheersingsmaatregelen van de gebruikersorganisatie weer die zijn verondersteld bij de opzet van de interne beheersingsmaatregelen van <klant>. Onze beweringen zijn gevormd op basis van de aangelegenheden die hiervoor zijn uiteengezet. Wij beweren dat de interne beheersingsmaatregelen met betrekking tot <object> effectief hebben gewerkt gedurende de periode <start verslagperiode> tot en met <einde verslagperiode>, om een redelijke mate van zekerheid te verschaffen dat de serviceverplichtingen en systeemvereisten van <klant> werden bereikt gebaseerd op de van toepassing zijnde trust services criteria. <Ondertekening service organisatie>
c) Assurance rapport van de onafhankelijke auditor	1) Scope Wij hebben de management bewering van <klant> getiteld "<Managementbewering van klant>" (bewering) onderzocht. Management van <klant>" beweert hierin dat de interne beheersingsmaatregelen met betrekking tot <object> effectief hebben gewerkt gedurende de periode <start verslagperiode> tot en met <einde verslagperiode>, om een redelijke mate van zekerheid te verschaffen dat de serviceverplichtingen en systeemvereisten van <klant> werden bereikt. Die evaluatie van het management is uitgevoerd op basis van de trust services criteria relevant voor beveiliging, beschikbaarheid, integriteit van processen, vertrouwelijkheid en privacy (van toepassing zijnde trust services criteria) zoals uiteengezet in TSP sectie 100, 'Trust Services Criteria voor beveiliging, beschikbaarheid, integriteit van processen, vertrouwelijkheid en privacy' van het American Institute of Public Accountants (AICPA). 2) Sub-serviceorganisaties <Klant> maakt gebruik van sub-serviceorganisatie(s) <subservice organisatie(s)> om <beschrijving diensten>. De beschrijving van de grenzen van <object> (<bijlage A> van dit rapport) stelt dat bepaalde criteria alleen bereikt kunnen worden indien de beheersingsmaatregelen bij de sub-serviceorganisatie juist zijn opgezet en effectief werken. De beschrijving van de grenzen van <object> geeft ook de aanvullende beheersingsmaatregelen van de subservice organisatie weer die zijn verondersteld bij de opzet van de interne beheersingsmaatregelen van <klant>. De beschrijving van de grenzen van <object> geeft niet de feitelijke interne beheersingsmaatregelen bij de subservice organisatie weer. Onze opdracht bevat geen toetsing van de dienstverlening en de interne beheersingsmaatregelen van de sub-serviceorganisatie. 3) Beheersingsmaatregelen bij de gebruikende entiteit (Complementary User Entity Controls)

	De beschrijving van de grenzen van <object> (<bijlage A> van dit rapport) stelt dat bepaalde criteria alleen bereikt kunnen worden indien de beheersingsmaatregelen bij de gebruikersorganisatie juist zijn opgezet en effectief werken. De beschrijving van de grenzen van <object> geeft ook de aanvullende beheersingsmaatregelen van de gebruikersorganisatie weer die zijn verondersteld bij de opzet van de interne beheersingsmaatregelen van <klant>. Wij hebben de opzet of effectieve werking van deze beheersingsmaatregelen bij de gebruikersorganisatie niet geëvalueerd. 4) Verantwoordelijkheden van de serviceorganisatie <Klant> is verantwoordelijk voor haar serviceverplichtingen en systeemvereisten, en voor het opzetten, het implementeren en het effectief laten werken van interne beheersingsmaatregelen in het systeem om een redelijke mate van zekerheid te verschaffen dat de serviceverplichtingen en systeemvereisten van <klant> werden bereikt. <Klant> heeft tevens de bijgaande bewering gedaan met betrekking tot de effectieve werking van interne beheersingsmaatregelen met betrekking tot <object>. In het opstellen van deze bewering is <klant> verantwoordelijk voor het selecteren en identificeren van de relevante trust services criteria in haar vermelding, en voor het hebben van een redelijke onderbouwing voor het doen van de bewering door het uitvoeren van een beoordeling van de effectiviteit van de interne beheersingsmaatregelen met betrekking tot <object>. 5) Verantwoordelijkheden van de service auditor Onze verantwoordelijkheid is het verschaffen van een oordeel, gebaseerd op ons onderzoek, of de beweringen van het management dat interne beheersingsmaatregelen met betrekking tot <object> effectief werkten gedurende de periode om een redelijke mate van zekerheid te verschaffen dat de serviceverplichtingen en systeemvereisten van de service organisatie werden bereikt gebaseerd op de van toepassing zijnde trust services criteria. Wij hebben onze assurance-opdracht uitgevoerd conform Nederlandse wetgeving en NOREA Richtlijn Assurance-opdrachten door IT-Auditors (3000A). Deze opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid voor ons oordeel. Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd is op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag. De IT-auditeenheid past het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe en bijgevolg onderhoudt het een uitgebreid systeem van kwaliteitscontrole met inbegrip van gedocumenteerd beleid en procedures voor de naleving van de ethische voorschriften, professionele standaarden en de van toepassing zijnde wet- en regelgeving. Naar onze mening hebben wij voldoende assurance-informatie verkregen om te komen tot een oordeel met een redelijke mate van zekerheid. Ons onderzoek omvatte onder andere: • Het verkrijgen van inzicht in het <object> en de serviceverplichtingen en systeemvereisten van de service organisatie. • Het maken van een inschatting van de risico's dat interne beheersingsmaatregelen niet effectief werkten om de

	serviceverplichtingen en systeemvereisten van <klant> te bereiken, gebaseerd op de van toepassing zijnde trust services criteria. • Het uitvoeren van procedures om assurance-informatie te verkrijgen over de vraag of interne beheersingsmaatregelen met betrekking tot <object> effectief werkten om de serviceverplichtingen en systeemvereisten van <klant> te bereiken, gebaseerd op de van toepassing zijnde trust services criteria. Ons onderzoek omvatte ook het uitvoeren van overige procedures die wij noodzakelijk achtten op basis van de omstandigheden. 6) Inherente beperkingen De beschrijving van de grenzen van <object> van <klant> is opgesteld voor de algemene informatiebehoefte van een brede groep gebruikers en hun auditors. De beschrijving van de grenzen van <object> dekt daarom niet alle aspecten af die een individuele gebruiker belangrijk acht. Vanwege hun aard en inherente beperkingen is het mogelijk dat interne beheersingsmaatregelen niet altijd effectief werkten om een redelijke mate van zekerheid te verschaffen dat de serviceverplichtingen en systeemvereisten van <klant> werden bereikt gebaseerd op de van toepassing zijnde trust services criteria. Bovendien is de projectie van de conclusies omtrent de effectieve werking van interne beheersingsmaatregelen naar toekomstige periodes onderhevig aan het risico dat <object> wordt gewijzigd of dat interne beheersingsmaatregelen bij een serviceorganisatie inadequaat worden of tekortschieten. 7) Oordeel Ons oordeel is gebaseerd op de aangelegenheden die in dit assurance-rapport zijn uiteengezet. Naar ons oordeel zijn de beweringen van het management, waarin is vermeld dat de interne beheersingsmaatregelen met betrekking tot <object> effectief werkten gedurende de periode <start verslagperiode> tot en met <einde verslagperiode> om een redelijke mate van zekerheid te verschaffen dat de serviceverplichtingen en systeemvereisten van <klant> werden bereikt gebaseerd op de van toepassing zijnde trust services criteria, in alle materiële opzichten, getrouw weergegeven. [Datum] [Handtekening auditor]
d) Bijlage A <klant>'s beschrijving van de grenzen van het systeem.	*De beschrijving betreft een ingekorte versie van de beschrijving uit het SOC 2® rapport. De beschrijving dient ten minste de hieronder genoemde onderdelen te bevatten:* - *Achtergrond (algemene informatie)* - *Systeem overzicht (inclusief de paragrafen infrastructuur, software, mensen, procedures en data)* - *Interne controle (inclusief de paragrafen controle omgeving, risk assessment, controle activiteiten, informatie & communicatie, monitoring activiteiten)* - *Scope van de service / afbakening van het systeem / sub-serviceorganisaties* - *Complementary user entity controls* - *Complementary subservice organization controls*
e) Bijlage B	*Bijlage B geeft een overzicht van de belangrijkste serviceverplichtingen en systeemvereisten. Deze kunnen bijvoorbeeld gebaseerd zijn op verantwoordelijkheden die zijn opgenomen in interne beleidsstukken en*

Belangrijkste serviceverplichtingen en systeemvereisten	*procedures, Service Level Agreements of op basis van relevante wet- en regelgeving.*

7.5 Belangrijkste verwijzingen naar handreikingen, professionele standaarden, richtlijnen artikelen en brochures

De DC Sectie 200 – Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (Description Criteria 200) is te vinden op: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/dc-200.pdf

De 'TSP Sectie 100 – 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy' zijn te vinden op de AICPA website: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf

De standard ISAE 3000 (Revised), Assurance Engagements Other than Audits or Reviews of Historical Financial Information is te vinden op: https://www.ifac.org/system/files/publications/files/ISAE%203000%20Revised%20-%20for%20IAASB.pdf

De NOREA richtlijn Assurance-opdrachten door IT-auditors (3000) is te vinden op: https://www.norea.nl/download/?id=5640

De NOREA richtlijn 3402 – Assurance rapporten betreffende interne beheersingsmaatregelen bij een serviceorganisatie is te vinden op: https://www.norea.nl/download/?id=474

Het NOREA Privacy Control Framework is te vinden op: https://www.norea.nl/download/?id=6317

7.6 Auteurs

Voorzitter	René Ewals	ACS
Kernteam	Jeroen Francot	BDO
Kernteam	Carlijn Frins	BDO
Kernteam	Dennis Houtekamer	EY
Kernteam	Milan van Helden	EY
Teamlid	Jan Matto	Mazars
Teamlid	Robert Boon	Deloitte
Teamlid	Jeroen Meulendijks	VanderBeecken

7.7 Mapping Privacy category – PCF

In deze annex is de mapping opgenomen tussen de Privacy criteria uit TSP sectie 100 (2017) en de PCF control objectives ('NOREA Guide Privacy Control Framework' d.d. mei 2018), welke ter ondersteuning kan bieden voor het inrichten van controls onder de SOC2 Privacy Criteria. Voor de uitgeschreven SOC 2 Privacy criteria wordt verwezen naar de Trust Services Criteria 2017 (TSP sectie 100) van de AICPA Assurance Services Executive Committee (ASEC). De PCF control objectives zijn in zijn geheel opgenomen. Omdat de mapping met het PCF slechts ter ondersteuning dient, is het niet benodigd deze op te nemen in het rapport. Om aan te sluiten bij de SOC2 richtlijnen, dienen de criteria zoals opgenomen in TSP sectie 100 opgenomen te worden in het rapport.

A. Mapping Privacy criteria – PCF Control objectives

Privacy Criteria – TSP sectie 100 (2017)	PCF Tag	PCF Topic	PCF Control objective
P1.1	PPO (01.1)	Privacy policy	The entity has established and communicated a policy that states its objectives and responsibilities regarding privacy and is in line with accepted privacy principles and applicable laws and regulations.
	PST (02.1)	Privacy statement	The entity transparently informs data subjects of the entity's policy, requirements, and practices regarding the collection, use, retention, disclosure and disposal of personal data.
P2.1	CFR (03.1)	Consent framework	The entity obtains data subject's consent for processing personal data where required or necessary.
P3.1	PDI (01.3)	Personal data identification and classification	The entity understands and documents which personal data is stored and processed and identifies and treats personal data appropriately. Measures to safeguard personal data take into account the differences in sensitivity in personal data, leading to identification of risks and compliance with laws and regulations.
	DMI (04.1)	Data minimisation	Personal data is adequate, relevant, and limited to what is necessary in relation to the legitimate purposes for which it is processed.
P3.2	CFR (03.1)	Consent framework	The entity obtains data subject's consent for processing personal data where required or necessary.
P4.1	ULI (05.1)	Use limitation	Personal data is not disclosed, made available or otherwise used for other purposes than those specified in the entity's privacy statement except: a) with the consent of the data subject; or b) by the authority of law.
P4.2	DRE (05.3)	Data retention	Personal data is retained no longer than the minimum time needed, as required by applicable laws and regulations, or for the purposes for which it was collected.
P4.3	DDA (05.4)	Disposal, destruction and anonymisation	Personal data is anonymised and/or disposed of within the entity where required. Identities should not be identifiable and personal data should not be available once it is past its retention date.

Privacy Criteria – TSP sectie 100 (2017)	PCF Tag	PCF Topic	PCF Control objective
	DDR (06.3)	Data deletion requests	Data deletion requests are responded to adequately and data subjects are able to have their personal data deleted if applicable criteria are met.
P5.1	DAR (06.1)	Data access requests	Data subject access requests are responded to adequately, and data subjects are able to determine which personal data relating to her/him is processed and in what way.
	DPR (06.3)	Data portability requests	Data portability requests are responded to adequately and data subjects are able to have their personal data transferred to another entity if applicable criteria are met.
P5.2	DCR (06.2)	Data correction requests	Data subject correction requests are responded to adequately, and data subjects are able to determine whether their personal data is correct/up-to-date, and are able to correct their personal data.
	ACD (09.1)	Accuracy and completeness of data	Documented procedures for validation, editing and update of personal data assure accurate and complete personal data processing and the ability to access it when needed.
P6.1	TPD (07.1)	Third party disclosure and registration	Personal data is not disclosed to third parties, or further processed for purposes for which the individual has not consented to.
	DTR (07.3)	Data transfers	Personal data is not transferred (i.e. movement, viewing, or printing of data in another location) internationally to countries that have an inadequate legal privacy regime.
	TPA (07.2)	Third party agreements	Privacy considerations and requirements are adequately covered when procuring (personal data related) solutions or services from third parties resulting in appropriate handling or protection of personal data.
P6.2	TPD (07.1)	Third party disclosure and registration	Personal data is not disclosed to third parties, or further processed for purposes for which the individual has not consented to.
P6.3	PIB (01.6)	Privacy incident and breach management	The entity adequately detects and handles privacy-related incidents; privacy-related incidents are responded to appropriately as to limit the consequences and to take measures to prevent future breaches.
P6.4	TPA (07.2)	Third party agreements	Privacy considerations and requirements are adequately covered when procuring (personal data related) solutions or services from third parties resulting in appropriate handling or protection of personal data.
P6.5	PIB (01.6)	Privacy incident and breach management	The entity adequately detects and handles privacy-related incidents; privacy-related incidents are responded to appropriately as to limit the consequences and to take measures to prevent future breaches.
	TPA (07.2)	Third party agreements	Privacy considerations and requirements are adequately covered when procuring (personal data related) solutions or services from third parties resulting in appropriate handling or protection of personal data.

Privacy Criteria – TSP sectie 100 (2017)	PCF Tag	PCF Topic	PCF Control objective
P6.6	PIB (01.6)	Privacy incident and breach management	The entity adequately detects and handles privacy-related incidents; privacy-related incidents are responded to appropriately as to limit the consequences and to take measures to prevent future breaches.
P6.7	DAR (06.1) PDI (01.4)	Data access requests Personal data identification and classification	Data subject access requests are responded to adequately, and data subjects are able to determine which personal data relating to her/him is processed and in what way. The entity understands and documents which personal data is stored and processed and identifies and treats personal data appropriately. Measures to safeguard personal data take into account the differences in sensitivity in personal data, leading to identification of risks and compliance with laws and regulations.
P7.1	ACD (09.1) DMI (04.1)	Accuracy and completeness of data Data minimisation	Documented procedures for validation, editing and update of personal data assure accurate and complete personal data processing and the ability to access it when needed. Personal data is adequate, relevant, and limited to what is necessary in relation to the legitimate purposes for which it is processed.
P8.1	REV (10.1) MON (10.2) URE (05.5)	Review of privacy compliance Periodic monitoring on privacy controls Use and restriction	Adequate oversight of the internal organisation and third parties ensures compliance with applicable privacy laws and regulatory requirements and decreases the risk of data breaches or loss of personal data. The entity systematically and periodically assesses privacy processes and controls, as to establish that they operate as designed, resulting in ongoing compliance with applicable laws and regulatory requirements. Personal data is not used in case of the restriction of the data subject or in case of specific legal restrictions by local government. Objections to processing by data subject will be handled adequately.

B. Mapping privacy points of focus onder Common Criteria – PCF Control objectives

Naast de controls onder de Privacy Criteria zijn er een aantal Common Criteria waarbij privacy dient te worden meegenomen in de controls, wanneer de privacy category wordt gehanteerd binnen een SOC2 opdracht. Dit zijn de volgende Common Criteria:

Common Criteria – TSP sectie 100 (2017)	TSP Topic	PCF Tag	PCF Topic	PCF Control objective
CC2.3	Communication of objectives related to privacy	PST (02.1)	Privacy statement	The entity transparently informs data subjects of the entity's policy, requirements, and practices regarding the collection, use, retention, disclosure and disposal of personal data.

Common Criteria – TSP sectie 100 (2017)	TSP Topic	PCF Tag	PCF Topic	PCF Control objective
CC7.3	Assessment of impact of security events on personal information	PIB (01.6)	Privacy incident and breach management	The entity adequately detects and handles privacy-related incidents; privacy-related incidents are responded to appropriately as to limit the consequences and to take measures to prevent future breaches.
CC7.3	Identification of affected information after unauthorized use or disclosure of personal information	PIB (01.6)	Privacy incident and breach management	The entity adequately detects and handles privacy-related incidents; privacy-related incidents are responded to appropriately as to limit the consequences and to take measures to prevent future breaches.
CC7.4	Communication of affected information after unauthorized use or disclosure of personal information	PIB (01.6)	Privacy incident and breach management	The entity adequately detects and handles privacy-related incidents; privacy-related incidents are responded to appropriately as to limit the consequences and to take measures to prevent future breaches.
CC7.4	Evaluation and, if appropriate, sanctioning of individuals involved in the unauthorized use or disclosure of personal information	PIB (01.6)	Privacy incident and breach management	The entity adequately detects and handles privacy-related incidents; privacy-related incidents are responded to appropriately as to limit the consequences and to take measures to prevent future breaches.
CC8.1	Protection of personal information during the change processes	PBD (05.2)	Privacy architecture (Privacy by Design and Privacy by Default)	The entity takes into account solid privacy policies, principles, and/or applicable laws and regulations when designing or changing products, services, business systems or processes.
CC9.2	Obtaining privacy commitments from vendors and business partners with access to personal information	TPA (07.2)	Third party agreements	Privacy considerations and requirements are adequately covered when procuring (personal data related) solutions or services from third parties resulting in appropriate handling or protection of personal data.
CC9.2	Assessing compliance by vendors and business partners with the entity's privacy	TPA (07.2)	Third party agreements	Privacy considerations and requirements are adequately covered when procuring (personal data related) solutions or services from third parties resulting in appropriate handling or protection of personal data.

Common Criteria – TSP sectie 100 (2017)	TSP Topic	PCF Tag	PCF Topic	PCF Control objective
	commitments and requirements			

C. Mapping missende PCF Control objectives – Common Criteria

De onderwerpen (topics) uit het PCF welke niet direct te mappen zijn naar de SOC 2 criteria van de privacy category, dienen te worden opgenomen onder de Common Criteria van SOC 2. Onder deze criteria kunnen dan, ook al betreft het 'common' criteria, privacy gerelateerde controls worden opgenomen door de klant. Deze mapping ziet er als volgt uit:

PCF Tag	PCF Topic	PCF Control objective	Common Criteria SOC 2
DRR	Definition of roles and responsibilities	The entity has established and implemented clear roles and responsibilities regarding the safeguarding of personal data and the achievement of privacy objectives.	CC1.3
RMA	Risk management	The entity systematically and periodically identifies, assesses, and mitigates factors that endanger the achievement of privacy objectives.	CC3.1 CC3.2
PIA	Data Protection Impact Assessments	The privacy-related impact of new products and services and their use within the entity is systematically identified, assessed and addressed.	CC3.4
SCO	Staff competences	Staff in positions with access to or control over personal data and personal data processes have the necessary privacy competences to adequately perform their duties.	CC1.4
SAT	Staff awareness and training	Staff is sufficiently aware of privacy laws, regulations and organisational privacy policies and guidelines, and their individual responsibilities with regard to privacy, and the entity engages in programs to establish and maintain awareness.	CC1.4 CC2.2
LRC	Legal review of changes in regulatory or business requirements	Privacy risks associated with changes to the entity (structure and strategy) and to regulatory requirements are adequately considered.	CC3.4
ISP	Information security program	Personal data is adequately secured from accidental errors or loss, or from malicious acts such as hacking or deliberate theft, disclosure or loss.	CC5.1
IAM	Identity and access management	Assignment of appropriate access rights, appropriate changes to access rights and timely removal of access rights decreases the likelihood of unauthorised access to, or inappropriate handling of personal data, or data breaches by internal employees, third parties or hackers.	CC6.1 CC6.2 CC6.3 CC6.6
STR	Secure transmission	Restricted access to personal data during transmission adequately prevents unauthorised disclosure, breach, altering or destruction of personal data.	CC6.7
ENC	Encryption and end-point security	Encryption assures the prevention of a breach of personal data (accidental loss of personal data, or malicious acts such as deliberate theft, disclosure or loss).	CC6.1 CC6.7
LOG	Logging of access	The entity detects and investigates access or access attempts to personal data by staff, third parties or hackers that could	CC7.2

		result in a breach, sabotage of systems, insertion of malicious code, theft of personal data, etc.	