2016

SOC 2: TOEPASSING EN UITVOERING

AFSTUDEERONDERZOEK MET BETREKKING TOT DE TOEPASBAARHEID EN MARKTBESTENDIGHEID VAN DE SOC 2-ASSURANCERICHTLIJN

C.J. NIELD

FEBRUARI 2016 – JUNI 2016

auditconnect

SOC 2: TOEPASSING EN UITVOERING

"I alone cannot change the world, but I can cast a stone across the waters to create many ripples."
- Mother Teresa

Auteur:
C.J. (Christopher) Nield

Praktijkcoach:
M.J. (Mark) van Zitteren RE

Praktijkorganisatie:
AuditConnect B.V. (Apeldoorn)

Schoolcoach:
R.P.M.L.C (René) van den Nieuwenhoff

Onderwijsinstelling:
Saxion (Apeldoorn)

Gepubliceerd op 6-6-2016

VERSIEBEHEER

Datum:	Wijziging:
4-4-16	Structuur van scriptie vastgesteld.
7-4-16	Inrichting versiebeheer.
8-4-16	Samenvoeging onderzoeksvraag twee en drie (in overleg met school- en praktijkcoach).
15-4-16	Wijzigingen gemaakt op basis van de NOREA presentatie over de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100.
17-4-16	Beantwoording deelvraag één en twee herschreven.
21-4-16	Deelvraag vijf geschrapt (geen verdere toevoeging aan het onderzoek).
22-4-16	Eerste concept aangeleverd aan schoolcoach en praktijkcoach.
25-4-16	Revisie o.b.v. opmerkingen collega (AuditConnect).
2-5-16	Afronding hoofdstuk vijf.
3-5-16	Beantwoording deelvraag drie en vier.
5-5-16	Beantwoording probleemstelling.
10-5-16	Formulering conclusie en aanbevelingen.
13-5-16	Formulering abstract.
17-5-16	Verwerking opmerkingen dhr. van Zitteren.
19-5-16	Status gewijzigd van concept naar definitief.
27-5-16	Feedback dhr. van den Nieuwenhoff verwerkt.

tabel 1: versiebeheer

Colofon:

Gegevens afstudeeronderzoeker:

Naam:	Dhr. C.J. (Christopher) Nield
E-mailadres:	cjnield@gmail.com
Telefoonnummer:	+31(0)64 59 29 066
Opleiding:	HBO Security Management te Saxion Apeldoorn
Studentnummer:	312985
Leerjaar:	4

Gegevens praktijkcoach:

Bedrijf:	AuditConnect B.V.
Praktijkcoach:	Dhr. M.J. (Mark) van Zitteren RE
Telefoonnummer:	+31(0)61 58 88 560
E-mailadres:	m.vanzitteren@auditconnect.nl
Bezoekadres:	Meester van Rhemenslaan 7
Postcode:	7316 AK
Plaats:	Apeldoorn
Postadres:	Postbus 4355, 7320 AJ te Apeldoorn

Gegevens schoolcoach:

Bedrijf:	Saxion
Schoolcoach:	Dhr. R.P.M.L.C (René) van den Nieuwenhoff
Telefoonnummer:	+31(0)62 95 95 194
E-mailadres:	r.p.m.l.c.vandennieuwenhoff@saxion.nl
Adres:	Kerklaan 21
Postcode:	7311 AA
Plaats:	Apeldoorn

VOORWOORD

Deze scriptie beschrijft de opzet, resultaten en conclusie van het afstudeeronderzoek “SOC 2: toepassing en uitvoering”. Dit onderzoek is uitgevoerd om het toepassingsbereik van de SOC 2-assurancerichtlijn vast te stellen, alsmede het verkrijgen van inzicht over de beste methode van uitvoering.

Mijn dank gaat uit naar dhr. Mark van Zitteren, voor zijn begeleiding en het gegeven vertrouwen. Ook dhr. Mischa van der Vliet wil ik bedanken voor de mogelijkheid om een bijdrage te leveren aan het productportfolio van AuditConnect B.V. Tevens zou ik dhr. René van den Nieuwenhoff willen bedanken voor zijn betrokkenheid en flexibiliteit. Afrondend wil ik aan het voltallige team van AuditConnect B.V. mijn dank kenbaar maken voor de ervaring, toewijding en ondersteuning in het vormgeven van dit onderzoek alsmede voor de opgedane praktijkervaring.

Ik wens u lering en inzicht bij het lezen van deze scriptie.

Christopher Nield

AFKORTINGENLIJST

AICPA	American Institute of Certified Public Accountants
CICA	Canadian Institute of Chartered Accountants
CPA	Certified Public Accountant
EDP	Electronic Data Processing
GAPP	Generally Accepted Privacy Principles
IFAC	International Federation of Accountants
IP	Intellectual Property
ISAE	International Standards on Assurance Engagements
ISM	Information Security Management
ISO	International Standards Organisation
NOREA	Nederlandse Orde van Register EDP-Auditors
MVO	Maatschappelijk Verantwoord Ondernemen
RE	Register EDP(-auditor)
SAS	Statement on Auditing Standards
SOC	Service Organisation Control
TPM	Third Party Mededeling/Memorandum
TSP	Trust Services Principles
WBP	Wet Bescherming Persoonsgegevens

DEFINITIES

Term:	Definitie:
Service Organisation Control	*Service Organisation Controls (SOC) reports are designed to help service organisations, organisations that operate information systems and provide information system services to other entities, build trust and confidence in their service delivery processes and controls through a report by an independent Certified Public Accountant. Each type of SOC report is designed to help service organisations meet specific user needs.* **(AICPA, Service Organisation Controls (SOC) Reports for Service Organizations, z.j.)**
Serviceorganisatie	*An organisation or segment of an organisation that provides services to user entities, which are likely to be relevant to those user entities' internal control over financial reporting.* **(AICPA, 2010)**
Gebruikersorganisatie	*An entity that uses a service organisation.* **(AICPA, 2010)**

tabel 2: definities

ABSTRACT

Het onderzoek “SOC 2: toepassing en uitvoering” is uitgevoerd in opdracht van AuditConnect B.V. SOC (Service Organisation Control) 2 is een assurancerichtlijn ontwikkeld in Amerika, gericht op het verstrekken van een redelijke mate van assurance over de beheersing van uitbestede IT-processen. De richtlijn is vernieuwend vanwege de scoping en werkwijze: assuranceverklaringen geven weinig mogelijkheid om te bepalen wat en hoe er getoetst wordt. SOC 2 daarentegen biedt de mogelijkheid om modulair een verklaring samen te laten stellen op basis van enkele thema’s. Deze thema’s, principles genoemd, zijn:

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

Deze thema’s geven een organisatie de mogelijkheid om gericht te toetsen. Zo kan een organisatie kiezen om confidentiality achterwege te laten omdat er geen relevantie is met de te toetsen materie. Deze “principles” zijn ontleend aan de Trust Services Principles and Criteria (TSP) Sectie 100, het geïntegreerde normenkader van SOC 2. SOC 2 toetst exclusief op basis van de TSP Sectie 100, waar andere richtlijnen geen normenkader verplicht stellen. De principles die de TSP Sectie 100 aanreikt bestaan uit controls (beheersmaatregelen) gerelateerd aan het principle, met indien nodig enkele aanvullende controls. Zodoende wordt er diepgaand getoetst op de beheersing van de systeembeveiliging, systeembeschikbaarheid, integriteit van de verwerking van gegevens, vertrouwelijkheid van informatie en privacyaspecten van de verwerking van data of informatie.

De aanleiding van het onderzoek komt voort uit de introductie van de SOC 2-richtlijn in Nederland. De toepasbaarheid en uitvoering van de richtlijn zijn gedurende het onderzoek inzichtelijk gemaakt om zo een advies te kunnen formuleren aan AuditConnect B.V. en de IT-auditbranche als geheel. Voor het onderzoek is de volgende probleemstelling gehanteerd:

Welk type organisatie heeft baat bij een SOC 2-rapportage en hoe kan de SOC 2-richtlijn het meest effectief geïmplementeerd en/of getoetst worden, op basis van welke uitvoeringscriteria en leidt dit tot een algemeen toepasbare oplossing?

Het doel van het onderzoek betreft het opstellen van een algemeen toepasbare implementatieaanpak waarin een zo breed mogelijk toepassingsgebied wordt behouden. Om deze aanpak te ontwikkelen is er tijdens het onderzoek uitgebreid aandacht besteed aan hoe assurancerapporten en -opdrachten werken, wat een organisatie stimuleert om te kiezen voor een bepaald assurancerapport en hoe de markt kan worden aangemoedigd om te kiezen voor een SOC 2-rapportage.

Gedurende het onderzoek is inzichtelijk gemaakt hoe SOC 2 de markt kan beïnvloeden: de rapportage biedt organisaties mogelijkheden op de gebieden van standaardisatie en vereenvoudiging. Daarnaast zijn er voor organisaties met internationale aspiraties kansen om onderhandelingen te versoepelen met een SOC 2-rapportage vanwege de internationale acceptatie van de verklaring.

Een rapport conform de SOC 2-richtlijn brengt echter ook nieuwe uitdagingen met zich mee. Nederlandse en Amerikaanse wet- en regelgeving zijn op het gebied van privacy sterk uiteenlopend, waardoor dit niet conform de TSP Sectie 100 “Privacy”-criteria kan worden getoetst. Het American Institute of Certified Public Accountants (AICPA) heeft ook meerdere trademarks belegd op SOC 2 waardoor de toepassing van de Amerikaanse SOC 2-richtlijn niet mogelijk is zonder lid te zijn van het AICPA en conform de Amerikaanse eisen een SOC 2-opdracht uit te voeren.

Als antwoord hierop heeft de Nederlandse Orde van Register EDP-Auditors (NOREA) de Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 uitgebracht, om Nederlandse organisaties en auditors de mogelijkheid te bieden een SOC 2-rapport te laten ontwikkelen op basis van Nederlandse wet- en regelgeving en de internationale ISAE 3000-richtlijn. De ISAE 3000 is een richtlijn die gebruikt wordt voor assuranceopdrachten waarbij geen historische financiële gegevens onderzocht worden. Hierdoor kan deze richtlijn worden gebruikt als kapstok voor een Nederlandse SOC 2-assurancerapportage.

Momenteel is de markt nog niet volwassen genoeg om de overstap naar SOC 2 te kunnen maken. Veel bedrijven en auditors hanteren (al dan niet vrijwillig) de ISAE/NOREA Richtlijn 3402, een financieel georiënteerde assuranceverklaring verwant aan de ISAE 3000. Deze richtlijn wordt veel gebruikt door zijn bekendheid, maar dit heeft met zich meegebracht dat de rapportage door de jaren heen is gebruikt in situaties waarvoor de richtlijn niet ontworpen is. Momenteel heeft de NOREA Richtlijn 3402 een groot marktaandeel waar SOC 2 zich mee tracht te concurreren. De verwachting is dat dit pas over enkele jaren (in enige mate) lukt. Organisaties wensen vereenvoudiging en standaardisatie maar momenteel is de richtlijn niet bekend genoeg en is de (inkoop)vraag naar de ISAE/NOREA Richtlijn 3402 te groot.

Er kunnen initiatieven worden gestart om de bekendheid en acceptatie te vergroten. Dit berust primair bij IT-auditors, de NOREA en accountants van klantorganisaties. Via deze kanalen kan de bekendheid van SOC 2 worden vergroot om de kans op adoptie te vergroten. Zonder bekendheid is de kans klein dat SOC 2 in Nederland toegepast zal worden.

SOC 2 is een kansrijke assurancerichtlijn die voor organisaties mogelijkheden biedt met betrekking tot kostenbesparing en efficiëntieverhoging. Uit de resultaten van het onderzoek kan worden geconcludeerd dat de Nederlandse markt in zijn huidige staat nog niet volwassen genoeg is voor het adopteren van de SOC 2-richtlijn.

INHOUD

VERSIEBEHEER 2
VOORWOORD 4
AFKORTINGENLIJST 5
DEFINITIES 5
ABSTRACT 6
INLEIDING 9
LEESWIJZER 10
HOOFDSTUK 1 ALGEMENE INFORMATIE 11
HOOFDSTUK 2 ONDERZOEKSOPZET 14
HOOFDSTUK 3 THEORETISCH KADER 17
HOOFDSTUK 4 VERANTWOORDING METHODEN 29
HOOFDSTUK 5 ONDERZOEKSRESULTATEN 35
5.1 INTERVIEWRESULTATEN 35
HOOFDSTUK 6 BEANTWOORDING DEELVRAGEN EN PROBLEEMSTELLING 40
6.1 DEELVRAAG 1 41
6.2 DEELVRAAG 2 46
6.3 DEELVRAAG 3 48
6.4 DEELVRAAG 4 50
6.5 PROBLEEMSTELLING 52
HOOFDSTUK 7 CONCLUSIE EN AANBEVELINGEN 55
7.1 SAMENVATTING 55
7.2 CONCLUSIE 59
7.3 AANBEVELINGEN 60
7.4 DISCUSSIE 62
BIBLIOGRAFIE 64
BIJLAGE 1 GESPREKSVERSLAG & VRAGENLIJST INTERXION 66
BIJLAGE 2 GESPREKSVERSLAG & VRAGENLIJST EBPI 70
BIJLAGE 3 GESPREKSVERSLAG & VRAGENLIJST KPN 74
BIJLAGE 4 ONDERBOUWING DEELVRAAG 1 78
BIJLAGE 5 ONDERBOUWING DEELVRAAG 2 84
BIJLAGE 6 ONDERBOUWING DEELVRAAG 3 91
BIJLAGE 7 ONDERBOUWING DEELVRAAG 4 94
BIJLAGE 8 ONDERBOUWING PROBLEEMSTELLING 97

INLEIDING

Deze scriptie heeft als thema de SOC 2-assurancerichtlijn en hoe deze richtlijn de assurancebranche beïnvloedt. Deze richtlijn bestaat al enkele jaren en wordt primair in Amerika gebruikt. Naarmate SOC 2 internationale bekendheid heeft gekregen zijn er bewegingen in gang gezet om deze richtlijn ook in Nederland te introduceren. In deze scriptie zal onderzocht worden wat de SOC 2-richtlijn is, wat voor ontwikkelingen dit met zich meebrengt en hoe deze richtlijn het meest effectief ten uitvoer kan worden gebracht.

SOC is een richtlijn die gebruikt wordt in organisaties (momenteel vooral in Amerika) om een assurancerapport af te geven over de beheersing van uitbestede diensten en processen. De SOC-richtlijn is ontwikkeld om audit- en assurance richtlijnen aan te vullen en internationaal op één lijn te trekken. Binnen de SOC-richtlijn worden meerdere niveaus onderkend, namelijk SOC 1, 2 en 3.

Het onderzoek zal zich richten op de SOC 2-richtlijn, waarbij specifiek aandacht wordt besteed aan de toepasbaarheid voor organisaties en het ontwikkelen van een plan om een SOC 2-opdracht zo effectief en efficiënt mogelijk uit te laten voeren.

LEESWIJZER

In deze leeswijzer is de structuur van de scriptie beschreven. De scriptie bestaat uit de volgende onderdelen:

- Hoofdstuk één betreft algemene informatie over de opdracht, organisatie en (beroeps)producten;
- Hoofdstuk twee zal ingaan op de onderzoeksopzet, de deelvragen en de probleemstelling;
- Hoofdstuk drie bevat het theoretisch kader, uitgewerkt aan de hand van literatuurstudie;
- Hoofdstuk vier verantwoordt de te gebruiken onderzoeksmethoden;
- Hoofdstuk vijf behelst de resultaten van het onderzoek;
- Hoofdstuk zes beantwoordt de deelvragen en probleemstelling;
- Hoofdstuk zeven sluit af met een conclusie en aanbevelingen;
- Bijlagen, bevattende relevante teksten of resultaten welke niet in de hoofdtekst behoren.

Vanaf hoofdstuk vijf zal worden gewerkt met bijlagen om te voorkomen dat de hoofdtekst onnodig groot wordt. In hoofdstuk vijf zijn de interviewresultaten samengevat, waarbij de volledige resultaten terug te vinden zijn in bijlagen één tot en met drie. Voor de onderzoeksvragen in hoofdstuk zes is hetzelfde gedaan waar de onderbouwing per vraag terug te vinden is in de bijlagen.

HOOFDSTUK 1 ALGEMENE INFORMATIE

In dit hoofdstuk is algemene informatie met betrekking tot de opdracht gegeven. De praktijkorganisatie, onderzoeksopdracht en de te ontwikkelen beroepsproducten (producten ten behoeve van de opdrachtgever) zijn hier beschreven. Afrondend zijn de gegevens van de begeleiders gedocumenteerd.

De onderzoeksopdracht en de daaruit voortvloeiende beroepsproducten zullen worden ontwikkeld in opdracht van AuditConnect B.V. AuditConnect B.V. verleent diensten op de (IT-)gebieden van keteninformatisering, audits, penetratietesten en assessments voor privacy en security. AuditConnect B.V. is een kleine organisatie gericht op in het verbeteren van de IT-dienstverlening van klanten. In deze paragraaf zal worden toegelicht wat de productgroepen zijn, wat de missie en visie van AuditConnect B.V. zijn en hoe de organisatie vormgegeven is.

Productgroepen
AuditConnect B.V. heeft de volgende productgroepen in zijn portfolio:

- IT-audits en penetratietesten;
- IT-privacy (compliance) adviesdiensten;
- Informatiebeveiligingsadviesdiensten;
- IT-audit-, security- en privacytrainingen.

Bovenstaande productgroepen geven klanten op basis van wet- en regelgeving, normen en richtlijnen een betrouwbaar inzicht in de kwaliteit van de ICT-dienstverlening en waar voor een organisatie nog verbeterpunten liggen. Daarnaast vallen onder de noemer “informatiebeveiligingsadviesdiensten” ook processen als keteninformatisering, begeleide aansluiting op, en auditing van, het DigiD alsmede identiteits- en toegangsbeheer.

IT-audits worden uitgevoerd door Register EDP (Electronic Data Processing) auditors wat de kwaliteit en betrouwbaarheid van de verrichte werkzaamheden ondersteunt. Dit zijn auditors die geregistreerd staan bij de NOREA, de beroepsorganisatie voor IT-auditors. Tevens vervullen medewerkers de functie van projectleider en/of consultant, afhankelijk van de opdracht.

Visie en missie
AuditConnect B.V. heeft de volgende missie en visie (AuditConnect B.V., 2016):

Visie:

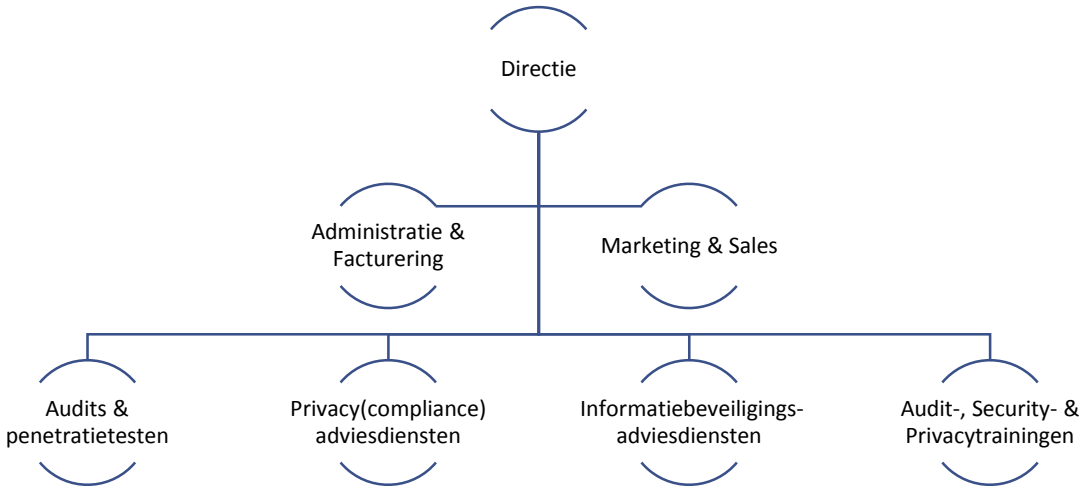
Goed advies, betaalbaar, kernachtig, op een prettige manier, met kennis van zaken en pragmatisch. Daar staan wij voor!

Missie:

Onze professionele IT-auditors, projectleiders en consultants kunnen zich snel in uw bedrijfsprocessen inleven en kunnen u daardoor in een kort tijdsbestek deskundig bijstaan. Daarmee biedt AuditConnect u de instrumenten voor het optimaliseren van de prestaties van uw organisatie.

Zoals hierboven beschreven is, stuurt AuditConnect B.V. op kwalitatief hoge dienstverlening zonder daarbij de visie van de klant uit het oog te verliezen. Scherp geprijsde, betrouwbare dienstverlening staat centraal.

Organogram
De structuur van AuditConnect B.V. is hieronder schematisch weergegeven (figuur één).



figuur 1: organigram AuditConnect B.V.

De invulling van de teams kan verschillen, afhankelijk van de opdracht. Verschillende opdrachten kunnen verschillende specialismen vereisen. Daarnaast wordt verwacht dat de organisatie de komende maanden gestaag zal groeien. Deze groei zal voor een deel de staffuncties zijn en voor de rest in de lijnteams.

Gedurende de afstudeerstage wordt er meegedraaid binnen de teams “informatiebeveiligingsadviesdiensten” en “audits en penetratietesten”. Dit heeft als doel het overbrengen van praktische kennis met betrekking tot auditing om dit te kunnen verwerken in de beroepsproducten.

Onderzoeksopdracht
De onderzoeksopdracht heeft betrekking op assurancerichtlijnen, specifiek de SOC 2-richtlijn. Het externe doel van het onderzoek is om een implementatieplan op te stellen voor deze richtlijn. Het interne doel van het onderzoek draait om het inzichtelijk maken van SOC 2, wanneer deze richtlijn het beste toe te passen is voor welke organisaties en hoe de uitvoering het beste plaats kan vinden.

Voor de bovenstaande onderzoeksopdracht zijn onderzoeksvragen geformuleerd. Uit de resultaten van deze onderzoeksvragen is de beantwoording van de probleemstelling voortgevloeid. De theoretische kennis in de scriptie zal in de praktijk gebracht worden door de oplevering van beroepsproducten, zoals een werkprogramma en benodigde documentatie. Voor de onderzoeksopdracht zal de focus worden gelegd op veldonderzoek bij organisaties en onderzoek naar relevante richtlijnen. De resultaten hiervan zullen gebruikt worden om de SOC 2-aanpak te ontwikkelen. Hierbij wordt ook uitgebreid onderzoek gedaan naar criteria voor de toepassing en wat voor randvoorwaarden organisaties stellen voordat SOC 2 ten uitvoer wordt gebracht.

Beroepsproduct
Het beroepsproduct is de ontwikkeling van een productlijn (offerte tot eindrapport) te gebruiken voor de uitvoering van een SOC 2-opdracht binnen een serviceorganisatie. Om dit mogelijk te maken zullen de onderzoeksresultaten toegepast worden zodat de benodigde mate van verfijning aanwezig is in de documentatie. Daarnaast zal er ook een werkprogramma ontwikkeld worden voor de auditrapporten, bij voorkeur (zo) geautomatiseerd (mogelijk). Deze documentatie wordt gebruikt om het proces te structureren, bevindingen vast te leggen en biedt tevens de basis voor het eindrapport. De praktijkkennis om deze documenten te ontwikkelen zal worden opgedaan door in de praktijk mee te werken

Het beroepsproduct zal bestaan uit alle benodigde producten (offerte, werkprogramma, rapportages en het implementatieplan) om de uitvoering en afronding mogelijk te maken. De doelstelling is om producten te ontwikkelen waarmee SOC 2 kan worden getoetst bij organisaties op basis van een zo generiek mogelijk toepasbare methodiek.

Gegevens begeleiders
Hieronder zijn de gegevens van zowel praktijk- als schoolcoach bijgevoegd (tabel drie)

	Gegevens praktijkcoach	**Gegevens schoolcoach**
Organisatie:	AuditConnect B.V.	Saxion
Naam:	M.J. (Mark) van Zitteren RE	R.P.M.L.C (René) van den Nieuwenhoff
Telefoonnummer:	+31(0)61 58 88 560	+31(0)62 95 95 194
E-mailadres:	m.vanzitteren@auditconnect.nl	r.p.m.l.c.vandennieuwenhoff@saxion.nl
Adres:	Meester van Rhemenslaan 7	Kerklaan 21
Postcode:	7316 AK	7311 AA
Plaats:	Apeldoorn	Apeldoorn

tabel 3: gegevens begeleiders

HOOFDSTUK 2 ONDERZOEKSOPZET

In dit hoofdstuk is de onderzoeksopzet geformuleerd. De aanleiding voor het vraagstuk zal worden beschreven evenals de probleemstelling, doelstelling, onderzoeksvragen en de betrokkenen bij het onderzoek.

Aanleiding
De aanleiding voor het onderzoek komt voort uit ontwikkelingen in de IT-auditbranche. Er zijn meerdere assurancerichtlijnen die internationaal gehanteerd worden (SSAE16, ISAE 3000 & 3402). Deze richtlijnen maken het mogelijk om een internationaal geaccepteerd rapport te publiceren over auditbevindingen die voortkomen uit de beoordeling van de beheersing over een IT-proces. Deze richtlijnen worden continu doorontwikkeld op basis van veranderingen in de markt. Zo is de val van ENRON in 2001 de start geweest voor ontwikkelingen in de auditbranche die ervoor moeten zorgen dat financiële verslaglegging niet meer gemanipuleerd en/of vervalst kan worden.

SOC 1 is hieruit voortgevloeid als een verdere uitwerking van eerdere maatregelen, richtlijnen en de Sarbanes-Oxley Act (SOX). Waar in de financiële branche dus al maatregelen genomen zijn om de integriteit van informatie te borgen, gebeurt dit nu ook verder in de IT-sector met behulp van SOC 2. Er is momenteel nog geen richtlijn met een eigen normenkader die naar volledigheid de aspecten van SOC 2 betrekt bij een audit. Dit betekent dat, afhankelijk van de scope, een dienst of proces gedurende een audit geen bevindingen hoeft op te leveren, maar dat bijvoorbeeld wachtwoorden in plain tekst opgeslagen kunnen zijn (wat beveiligingstechnisch extreem onverantwoord is en een risico op zichzelf is). Deze bevindingen hoeven niet naar voren te komen als er niet naar relevante criteria wordt gekeken, zoals SOC 2 zal doen (Boer, 2013).

SOC 2 toetst privacy- en beveiligingsaspecten van een IT-proces, opdat het proces en de informatie (ongeacht of de informatie als input, throughput of output fungeert) aantoonbaar voldoen aan vastgestelde “trust services principles”. Deze principles sturen op beschikbaarheid, beveiliging, privacy, vertrouwelijkheid en integriteit van data. Dit betekent dat data wordt onderzocht op (Boer, 2013):

- Privacygevoeligheid.
- Het juiste rubriceringsniveau met bijbehorende beheersmaatregelen.
- Beschikbaarheid van de data op basis van de IT-infrastructuur van een organisatie.
- Beveiligingsmaatregelen, zowel fysiek als logisch.
- De integriteit van de informatie waarmee wordt bedoeld of informatie zonder verlies of mutatie van data verwerkt wordt.

Daarnaast is het ook zo dat de ISAE 3402-richtlijn momenteel niet altijd gebruikt wordt zoals bedoeld door de auteurs van de richtlijn (in voorkomende gevallen: het is niet dat de richtlijn per definitie onjuist wordt toegepast). Een voorbeeld hiervan is het toetsen van beheersmaatregelen die niet in relatie staan tot de financiële verslaglegging. Dergelijke opdrachten vallen buiten de scope van de richtlijn en dienen niet getoetst te worden op basis van de NOREA Richtlijn 3402 maar de NOREA Richtlijn 3000. De NOREA Richtlijn 3402 kijkt naar de interne controle van de serviceorganisatie en de genomen beheersmaatregelen. Deze richtlijn is de opvolger van de SAS 70 en bouwt voort op de criteria welke in de SAS 70 zijn opgenomen. De ISAE 3402 en de SAS 70 zijn assurancerichtlijnen welke kijken naar de beheersmaatregelen van een serviceorganisatie met betrekking tot de financiële verslaglegging van een organisatie. Echter is het zo dat organisaties een ISAE 3402-verklaring in enige mate (kunnen) misbruiken (Anderson, 2012) (Boer, 2013). De verklaring kijkt niet naar de aspecten van SOC 2 maar kan wel worden gebruikt om een signaal af te geven dat internal control op orde is, terwijl er geen aandacht geschonken wordt aan bijvoorbeeld privacyaspecten.

Tevens kan er bij deze richtlijn als het ware modulair worden gewerkt: organisaties kunnen een eigen normenkader samenstellen op basis van eigen wensen en behoeften. Dit brengt met zich mee dat organisaties kunnen kiezen (op basis van voorkennis) om bepaalde aspecten bij een audit buiten beschouwing te laten omdat deze aspecten niet voldoende beheerst worden.

Zodoende heeft de auditee invloed op de scope en de diepgang en kan gestuurd worden op het buiten scope laten van specifieke punten , als klanten van de serviceorganisatie hiervan overtuigd kunnen worden. Dit levert de organisatie (indien de rest van de audit geen bevindingen oplevert) een verklaring op dat conform de ISAE 3402-richtlijn wordt gewerkt, zonder dat de statement alle relevante beheersprocessen van de serviceorganisatie in scope heeft genomen.

Naar aanleiding van grote datalekken bij o.a. Sony, Adobe en Ashley Madison hebben organisaties een betrouwbaar, internationaal geaccepteerd raamwerk nodig waarmee getoetst en aangetoond kan worden (aan partners en mogelijke afnemers) dat de IT-processen en informatie van de organisatie aantoonbaar beveiligd zijn. Dit uit zich als een maatschappelijk belang vanuit meerdere perspectieven: klanten willen zekerheid dat hun informatie veilig is, en organisaties willen klanten winnen door veiligheid en beveiliging te garanderen.

Van belang is ook dat de richtlijn niet gebruikt kan worden om verschillende signalen af te geven zoals met de ISAE 3402. Momenteel is er nog geen eenduidige richtlijn voor de toetsingsaspecten van SOC 2 wat tevens het rapporteren van bevindingen bemoeilijkt. Zodra deze richtlijn ontwikkeld is, wordt op internationaal gebied één lijn getrokken voor IT-auditing en het rapporteren hiervan. Op basis van deze herdefiniëring kan een organisatie efficiënter omgaan met IT-auditing en het vastleggen (en opvolgen) van bevindingen. Daarnaast hebben organisaties die met SOC 2 werken een onafhankelijke audit van de procesintegriteit en betrokken informatie, wat een organisatie kan helpen klanten te werven en behouden door aantoonbare beheersing van IT-diensten.

AuditConnect B.V. onderkent meerwaarde te zien in de SOC 2-richtlijn. Door een implementatiemodel toe te voegen aan hun portfolio verwacht AuditConnect B.V. een sterke(re) positie te kunnen verwerven in de markt, gezien er naar verwachting vraag zal zijn naar (de uitvoering van) deze richtlijn.

Probleemstelling
Voor dit onderzoek is de volgende probleemstelling gehanteerd:

Welk type organisatie heeft baat bij een SOC 2-rapportage en hoe kan de SOC 2-richtlijn het meest effectief geïmplementeerd en/of getoetst worden, op basis van welke uitvoeringscriteria en leidt dit tot een algemeen toepasbare oplossing?

De probleemstelling zal gedurende het onderzoek uitgewerkt worden.

Onderzoeksvragen
Voor het beantwoorden van de probleemstelling zijn de volgende vragen geformuleerd:

1. Wat zijn de meest gebruikte assurancerichtlijnen en wat voegt de SOC 2-richtlijn hier aan toe?
2. Wat zijn de juridische overwegingen bij de uitvoering en het onderhoud van SOC 2 voor organisaties?
3. Welke criteria zijn van belang voor organisaties om een SOC 2-opdracht te starten?
4. Wat ondersteunt de succesvolle uitvoering van een SOC 2-opdracht?

Doelstelling
De doelstelling is om een productlijn (van offerte tot eindrapport) te ontwikkelen waarmee SOC 2 kan worden uitgevoerd bij organisaties op basis van een algemeen toepasbare methodiek. De producten dienen dusdanig flexibel te worden opgezet dat zij algemeen toepasbaar zijn en effectief toegepast kunnen worden. Flexibel heeft hier de context dat het beroepsproduct niet te star wordt opgezet, wat als effect zou kunnen hebben dat minder organisaties gebruik kunnen maken van een SOC 2-richtlijn door een te strakke scoping. Een te strakke scoping zou zorgen dat het profiel te nauw wordt opgesteld, waardoor veel organisaties er niet aan zouden voldoen.

Dit betekent dat een rapportagestructuur, implementatiemodel en andere producten ontwikkeld moeten worden zoals offertes en rapportages. De implementatie zal projectmatig verlopen, via bijvoorbeeld de Prince 2-methodiek. De toetsing zal gebeuren aan de hand van de TSP Sectie 100. Het laatste, maar belangrijkste, is dat de producten dermate flexibel ingericht zijn dat SOC 2 kan worden toegepast in alle mogelijke verschillende serviceorganisaties die er baat bij kunnen hebben (ongeacht primaire proces of mate van automatisering).

Betrokkenen
De volgende betrokkenen worden onderkend in de onderzoeksopdracht (tabel vier):

Betrokkene:	**Toelichting:**
C.J. (Christopher) Nield	Afstudeeronderzoeker.
Dhr. M.J. (Mark) van Zitteren RE	Senior IT-auditor/consultant. Praktijkcoach en contactpersoon AuditConnect B.V.
Dhr. R.P.M.L.C (René) van den Nieuwenhoff	Docent Security Management, eerste lezer en contactpersoon Saxion.
Drs. J.J.H. (Jelle) Hooiveld.	Tweede lezer.
AuditConnect B.V.	Stageverlenende organisatie. Wenst een SOC 2-implementatieplan wat algemeen toepasbaar is, ongeacht branche, grootte of mate van automatisering.
Organisaties die SOC 2 geïmplementeerd hebben	Deze organisaties zullen worden gebruikt om best practices, uitvoeringscriteria en randvoorwaarden voor een succesvolle implementatie vast te stellen.
Organisaties die SOC 2 niet geïmplementeerd hebben	In kaart brengen op basis van uitvoeringscriteria welke organisaties SOC 2 kunnen implementeren en onderzoek naar welke organisaties baat hebben bij de implementatie van SOC 2.
NOREA (Nederlandse Orde van Register EDP-Auditors)	Beroepsvereniging Register EDP-auditors. Informatievoorziening en indien nodig het plaatsen van enquêtes.

tabel 4: betrokkenen

HOOFDSTUK 3 THEORETISCH KADER

Het theoretisch kader zal de onderzoeksvragen en centrale begrippen die gebruikt worden gedurende het onderzoek voor zover mogelijk verklaren. De volgende centrale begrippen worden behandeld:

- Assurance;
- Audit;
- IT-auditing;
- IT-auditor;
- Auditcriteria;
- SOC;
- Uitvoeringscriteria;
- Flexibiliteitscriteria;
- Implementatieplan.

Dit afstudeeronderzoek richt zich op externe IT-audits op basis van de SOC 2-richtlijn. In dit theoretisch kader zijn de bovengenoemde begrippen uiteengezet om een weergave van het onderzoeksthema te schetsen waarna het onderzoeksthema summier zal worden samengevat.

Assurance versus audit

In eerste aanzet moet er een onderscheid worden gemaakt tussen twee termen, die soms foutief worden gebruikt omdat men ze aanziet voor dezelfde termen: assurance(opdracht) en audit. CPA Australia (2014) definieert "assurance" als volgt:

> *"The term assurance refers to the expression of a conclusion that is intended to increase the confidence that users can place in a given subject matter or information. For example, an auditor's report is a conclusion that increases the confidence that users can place in a company's financial statements."*
>
> **(CPA Australia, 2014)**

Assurance heeft het doel om het vertrouwen in een bepaald onderwerp of over bepaalde informatie te vergroten. Echter kan worden gesteld dat een audit hetzelfde doet. Er is één verschil wat maakt dat een audit een assurance opdracht is, maar niet alle assurance opdrachten een audit zijn: audits moeten altijd een mate van "reasonable assurance" behalen (CPA Australia, 2014). In figuur twee wordt een overzicht gegeven van wat "reasonable assurance" inhoudt:

Type of assurance	For example	Nature of key work performed	Example form of conclusion
Reasonable assurance	An audit of financial statements	Detailed testing, evidence gathering and substantiation to support the conclusion.	"We believe the financial statements *present* a true and fair view".
Limited assurance	A review of financial statements	Primarily enquiries and analysis, less detailed procedures.	"We have *not* become aware of any matter to cause us to believe the financial statements *do not* present a true and fair view".
No assurance	Preparing financial statements (compilation)	Preparation of the financial statements	No conclusion provided

figuur 2: levels of assurance (CPA Australia, 2014)

Op basis van deze informatie kan worden gesteld dat een audit diepgaande validatie is van informatie en daadwerkelijk bewijst of iets kloppend is. Assurance daarentegen is minder gedetailleerd en diepgaand, waardoor aan de conclusie minder waarde kan worden verbonden.
Een assuranceverklaring zal op het niveau van "limited assurance" zitten, wat wel enige mate van assurance schept, maar wat niet dezelfde diepgaande validiteit vertoont als een audit.

Hierdoor geldt dat een audit een geaccepteerd middel is om een niveau van "reasonable assurance" te scheppen binnen een organisatie voor stakeholders. Voor het onderzoek zal gekeken worden naar assurance opdrachten welke een niveau van "reasonable assurance" behalen. Dit betekent dat er enkel naar audits zal worden gekeken, conform figuur twee**Fout! Verwijzingsbron niet gevonden.**.

Auditing: een verkenning
Het onderzoek staat in het teken van auditing: maar wat is auditing? Zoals in de vorige paragraaf gesteld is, is assurance een term waar verschillende niveaus van vertrouwen mee kunnen worden behaald. Waar assurance over het algemeen een niveau van "limited assurance" afgeeft, zal een audit altijd het niveau van "reasonable assurance" behalen, doordat er sprake is van een diepgaand onderzoek met een bewijslast vanuit de opdrachtgever. Assurance is niet diepgaand genoeg om het onderzoeksthema naar volledigheid uit te werken.

Met betrekking tot auditing zijn er verschillende definities te vinden wat deze term betekent. Hanson stelt in "Auditing: theory and its application" (1942) dat auditing betrekking heeft op het volgende proces:

> *"In the present complex state of affairs it is necessary for institutions, businesses, and individuals to keep records of their condition and progress. Whether these records are reliable is often a question. An audit is an examination of such records to establish their reliability and the reliability of statements drawn from them. Opinion as to the reliance to be placed upon the statements is usually given in a report, the short form of which is often referred to as a certificate."*
>
> **(Hanson, 1942)**

Waar deze definitie ruim zeventig jaar oud is, behelst de definitie wel de kern van het proces: het controleren en toetsen van bedrijfsgegevens en de totstandkoming ervan zodat toetsing van het systeem en/of de werkwijze plaats kan vinden zoals financiële verslagen. Daarnaast wordt ook terecht een kanttekening geplaatst bij de betrouwbaarheid van deze gegevens. Zoals tegenwoordig ook nog gebeurt, wordt een audit afgerond met een rapportage met bevindingen of een verkorte rapportage, bekend als een "certificate".

De ISO 9000:2005 schept de volgende definitie voor een (interne) audit:

> *"The definition of an audit is: a systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled."*
>
> **(European Certification Group, 2016)**

Bovenstaande definitie gaat verder dan de definitie van Hanson (1942). Waar Hanson zijn definitie relatief vaag is over hoe een audit afgenomen wordt, is de ISO 9000:2005 scherper. Er wordt duidelijk gesteld dat een audit een proces is waarin onafhankelijk en systematisch bewijs wordt verkregen om te kunnen bepalen in welke mate een organisatie voldoet aan auditcriteria, zijnde een normenkader.

In auditing wordt er een verder onderscheid gemaakt tussen een interne en een externe audit. In tabel vijf is een definitie van beide typen weergegeven:

Interne audit	Externe audit
"Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes." **(Instituut van Internal Auditors, z.j.)**	*"An external audit, defined as a company audit which is performed by a party which is not a department or employed by business to be audited, are very commonly performed. The external audit approach has two main purposes: The company believes an outside party will be more efficient at the work or because a governmental entity, such as the IRS, is auditing the business."* **(Wilkinson, 2013)**

tabel 5: verschil interne en externe audit

Een interne audit wordt door de organisatie zelf afgenomen met als doel het verbeteren van interne processen. De organisatie bezit interne auditors welke aan de hand van een normenkader toetsen of de organisatie voldoet aan een richtlijn en een certificaat kan blijven voeren. Voorbeeld van een interne audit is de ISO 9000:2005 voor kwaliteitsmanagement. De externe audit wordt uitgevoerd door een onafhankelijke, externe partij zoals een accountantskantoor of adviesbureau. Het werkgebied is hetzelfde, enkel het perspectief van de auditor is verschillend.

Een organisatie kan besluiten om de voorkeur te geven aan een externe audit ten opzichte van een interne audit. Dit kan voortkomen uit meerdere redenen:

- Het voorkomen van belangenverstrengeling, wat bij een interne audit sneller voor kan komen.
- De organisatieovertuiging dat een externe partij efficiënter/effectiever is.
- Een verplichte audit vanuit de overheid, waarbij interne auditors geen bijdrage mogen leveren.

Het onderzoek richt zich op externe audits, gezien de wens van AuditConnect B.V. dit aan te bieden als onafhankelijke partij en de bovengenoemde redenen die de voorkeur geven aan een externe, onafhankelijke partij. Voor het onderzoek zal de volgende samengestelde definitie van een audit worden aangehouden:

Een audit is een proces waarbij op basis van een bewijslast vanuit de opdrachtgever en (veld)onderzoek van de (externe) auditors een organisatie zichzelf laat toetsen op basis van een normenkader opdat inzichtelijk en zonder ambiguïteit wordt bewezen hoe een organisatie het betreffende normenkader naleeft, aan de hand van vastgestelde criteria, zodat waar nodig verandering in naleving van de criteria kan worden aangebracht.

Auditing: het proces

Waar een audit zo kan worden gedefinieerd, geeft dit nog geen inzicht in het proces van een audit. Een audit bestaat uit enkele stappen die doorlopen moeten worden. In figuur drie is op hoofdlijnen een weergave van processtappen geschetst op basis van een NOREA Richtlijn 3402-audit (AuditConnect B.V., 2016).

figuur 3: proces van een NOREA Richtlijn 3402-audit (AuditConnect B.V., 2016)

Zoals in figuur 3figuur drie is weergegeven behelst de NOREA Richtlijn 3402-audit meerdere stappen. Dit proces kan verschillen van de weergave in figuur drie, maar in essentie blijft het proces hetzelfde: een organisatie huurt externe auditors in die de organisatie, zijn risico's en zijn beheersmaatregelen onderzoeken om vervolgens een onafhankelijk oordeel te vormen en een rapportage te
schrijven.

Binnen een audit valt nog een dieper onderscheid te maken in de vorm van de audit: vaak benoemd als een type I of type II-audit. Afhankelijk van het gekozen type heeft dit invloed op de scope en doorlooptijd van het proces. Dit heeft geen betrekking op het afnemen van een interne of een externe audit, maar heeft betrekking op de scope van de audit. Hieronder is weergegeven op basis van de SAS 70-richtlijn wat de verschillen tussen de rapportages zijn (tabel zes):

Type I audit & rapportage	**Type II audit & rapportage**
"A Type I report includes the service organisation's description of its controls and objectives, and an auditor's opinion on the controls' suitability for meeting the specified objectives." **(Intralinks, 2009)**	*"A Type II report, in addition to the Type I components, includes a test and evaluation of the effectiveness of the internal controls. The Type II attests to the effectiveness of the controls in meeting the specified objectives over a period of time, typically six months."* **(Intralinks, 2009)**

tabel 6: type auditrapportages

Aangezien de SAS 70 vervangen is door de ISAE 3402 kan gesteld worden dat bovenstaand onderscheid niet volledig relevant meer is. Dit onderscheid is doorgezet in de ISAE 3402, maar de bovenstaande beschrijving is diepgaander, waar de informatie over dit onderscheid in de ISAE 3402 wat aan de summiere kant is (Duijnborgh audit b.v., z.j.). Op basis hiervan is ervoor gekozen de SAS 70 definitie aan te houden. Voor een audit heeft dit betrekking op het tijdsbestek waarin een audit plaatsvindt. Een type II zal over een periode van minimaal zes maanden tot een jaar kijken naar de effectiviteit van de aanwezige beheersmaatregelen (opzet, bestaan en werking), waar een type I audit een momentopname betreft welke alleen kijkt naar de aanwezigheid (opzet en bestaan) van beheersmaatregelen.

Het onderzoek zal zich richten op type II-audits op basis van de bovenstaande definitie. Een type II-audit is voor een organisatie zwaarder, maar geeft meer duidelijkheid over de interne controle van een serviceorganisatie en het functioneren van beheersmaatregelen.

IT-audits & IT-auditors

Nu verduidelijkt is wat een audit precies inhoudt, wordt verder ingezoomd op IT-audits. Enkel IT-audits zijn relevant voor het onderzoek. Een IT-audit is een audit specifiek gericht op IT-beheersingsaspecten van een organisatie. De volgende definitie geeft dit weer:

> *"IT Audit is the process of collecting and evaluating evidence to determine whether a computer system has been designed to maintain data integrity, safeguard assets, allows organisational goals to be achieved effectively, and uses resources efficiently. Data integrity relates to the accuracy and completeness of information as well as to its validity in accordance with the norms. An effective information system leads the organisation to achieve its objectives and an efficient information system uses minimum resources in achieving the required objectives. An IT Auditor must know the characteristics of users of the information system and the decision making environment in the auditee organisation while evaluating the effectiveness of any system."*
>
> **(INTOSAI, z.j.)**

Waar een "gewone" audit kan kijken naar de verschillende aspecten van een organisatie met betrekking tot o.a. financiële verslaglegging, kijkt een IT-audit naar de verschillende aspecten van een IT-omgeving. Hierbij wordt specifiek gelet op de criteria welke betrekking hebben op de beschikbaarheid, beveiliging, etc. van de te auditen elementen (AICPA, 2015).

Op basis van deze criteria wordt getoetst of een organisatie voldoet aan de gestelde eisen. Een IT-audit werkt (op hoofdlijnen) hetzelfde als een niet-IT-gerelateerde audit, maar betreft een ander toepassingsgebied. Daarnaast wordt in de definitie ook duidelijk gesteld wat een IT-auditor moet weten over de (IT)-organisatie. Voor een IT-audit zijn er specifiek opgeleide IT-auditors. Binnen het vakgebied is het mogelijk certificeringen te behalen op het gebied van IT-auditing. Dit zijn in Nederland auditors geregistreerd bij de NOREA, de Nederlandse Orde van Register EDP Auditors. IT-auditors aangesloten bij de NOREA zijn geregistreerd als RE (Register EDP).

Dit geeft een keurmerk van kennis, kunde en betrouwbaarheid af gezien de IT-auditor in staat is deskundig advies te leveren op het gebied van IT-assurance en auditprojecten (De IT-Auditor, z.j.).

Onderstaande definitie geeft het profiel van een IT-auditor weer.

> *"Een IT-auditor oordeelt en adviseert over IT in bedrijven en organisaties. Als professional is hij de aangewezen deskundige om een onafhankelijke beoordeling uit te voeren. Het vakgebied werd aanvankelijk aangeduid als EDP-auditing (Electronic Data Processing). Tegenwoordig geven we de voorkeur aan de aanduiding "IT-auditing"."*
>
> **(De IT-Auditor, z.j.)**

Hetzelfde geldt voor de IT-auditor als voor de IT-audit: waar een "gewone" auditor naar aspecten kijkt met betrekking tot de o.a. financiële verslaglegging van een organisatie, kijkt de IT-auditor naar de IT-beheersingsaspecten van een organisatie, bijvoorbeeld op basis van de vastgestelde principes in de TSP Sectie 100 (AICPA, 2015) of COBIT.

Zoals beschreven betreft een IT-audit een ander werkgebied dan een financiële audit. Hierdoor is het van belang dat er deskundig personeel aanwezig is om een IT-audit uit te kunnen voeren. AuditConnect B.V. bewaakt dit door RE-auditors te leveren. Voor het onderzoek zal hier rekening mee worden gehouden.

Auditcriteria

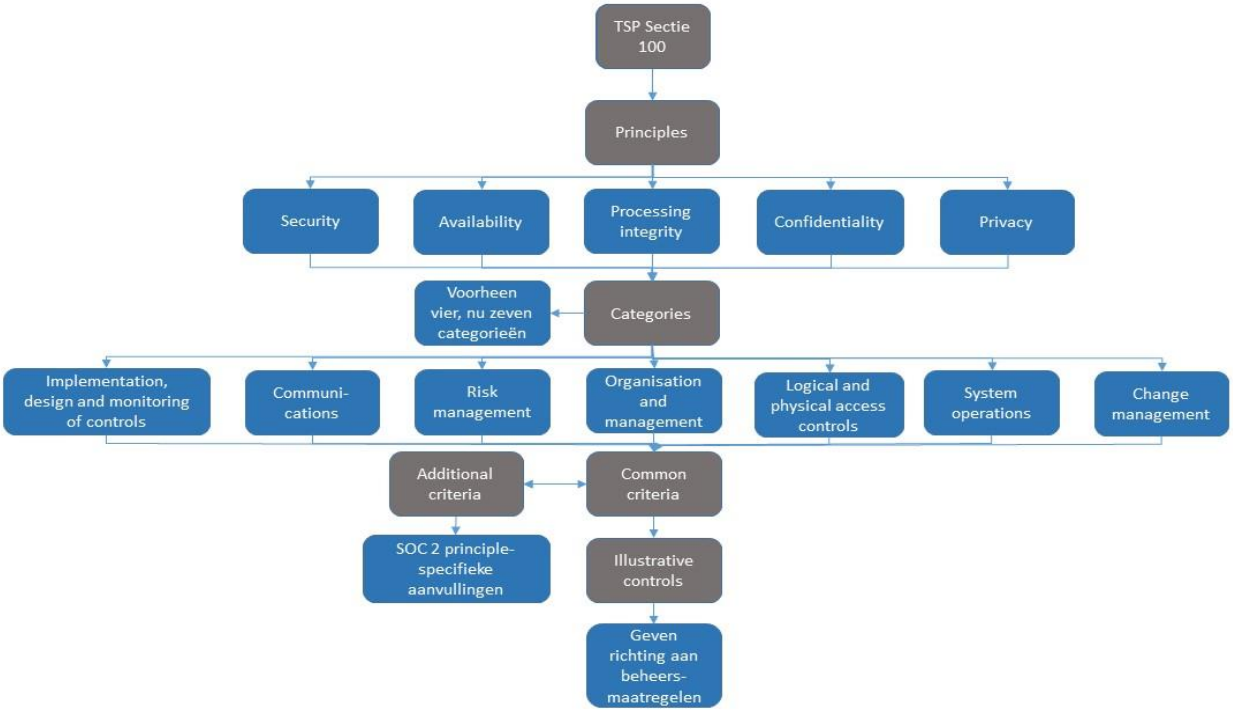
Zoals eerder aangegeven wordt een (IT-)audit afgenomen aan de hand van auditbare criteria. Deze criteria gelden als de aspecten waarop een organisatie getoetst wordt. Een voorbeeld hiervan is de "trust services principles" ("TSP" Sectie 100), een lijst met criteria waar de IT-organisatie van een bedrijf op getoetst kan worden. SOC 2 werkt op basis van deze lijst, waardoor deze lijst specifiek toegelicht zal worden.

Het doel van deze lijst is om een organisatie te toetsen op de volgende principles:

> *.13 The following are the trust services principles:*
>
> *a. Security. The system is protected against unauthorized access, use, or modification.*
> *b. Availability. The system is available for operation and use as committed or agreed.*
> *c. Processing integrity. System processing is complete, valid, accurate, timely, and authorized.*
> *d. Confidentiality. Information designated as confidential is protected as committed or agreed.*
> *e. Privacy. The privacy principle address the system's collection, use, retention, dis-closure, and disposal of personal information in accordance with the entity's commitments and system requirements.*
>
> **(AICPA, Exposure Draft: Proposed Revision of Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy, 2016)**

Oftewel: op basis van opgestelde criteria, zoals de TSP Sectie 100 wordt een IT-auditor in staat gesteld een systeem of omgeving te toetsen opdat inzichtelijk wordt of beheersmaatregelen naar behoren functioneren en een organisatie al dan niet voldoet aan gestelde criteria. Deze criteria zijn internationaal geaccepteerd en gehanteerd, wat de betrouwbaarheid en validiteit ten goede komt. Zonder een dergelijk raamwerk zou het auditproces bemoeilijkt worden, doordat auditfirma onderling andere criteria zouden kunnen naleven. Dit is momenteel het geval met de ISAE 3402 richtlijn, wat eenduidigheid bemoeilijkt.

De TSP Sectie 100 is als volgt vormgegeven (figuur vier):



figuur 4: TSP Sectie 100 (AICPA, Exposure Draft: Proposed Revision of Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy, 2016)

Voor het onderzoek zal de meest recente versie van de TSP Sectie 100 gebruikt worden. Naar aanleiding van de ontwikkeling welke de SOC-richtlijn teweeg brengt, is de TSP Sectie 100:2009 herschreven. Vervolgens is de TSP Sectie 100:2015 herschreven naar een exposure draft, welke als leidend wordt aangehouden voor het onderzoek. SOC 2 draagt bij aan een beter auditbaar klimaat voor uitbestede diensten, waarbij het van belang is dat er een raamwerk is wat de correcte diepgang in toetsing heeft. Door de herontwikkeling van de TSP Sectie 100 en de samenhang die er nu is met SOC 2, is er nu een optimaal raamwerk beschikbaar zonder overbodige criteria. De voorgaande publicaties van de TSP Sectie 100 miste deze samenwerking waardoor de toepasbaarheid in mindere mate aanwezig was. SOC 2 heeft wel sinds de ontwikkeling van de SOC 2-richtlijn getoetst op basis van de TSP Sectie 100.

Service Organisation Control-richtlijn

Op basis van de behandelde termen is een beeld geschept van een audit, externe audit, auditproces, IT-audit, IT-auditor en auditcriteria. Het onderzoek is toegespitst op een auditbare IT-richtlijn, namelijk de SOC-richtlijn. SOC staat voor "Service Organisation Control" en is op te delen in drie sub-richtlijnen: SOC 1, SOC 2 en SOC 3. In figuur vijf is hier een schematische uiteenzetting van weergegeven (Boer, 2013).

figuur 5: uiteenzetting SOC 1, 2 & 3

Op basis van de uiteenzetting in figuur vijf wordt duidelijk dat het onderscheid in de rapportages en werkwijzen binnen enkele punten te vinden is, namelijk:

- Scope van de audit.
- De rapportage-inhoud.
- De verspreiding van de rapportage.

SOC 2 heeft de volgende doelstelling:

> *The primary focus of this guide is on examining and reporting on a description of a service organisation's system and the suitability of the design and operating effectiveness of the controls over its system relevant to security, availability, processing integrity, confidentiality, or privacy using the trust services criteria. Such an engagement is known as a SOC 2 engagement, and a report on such an engagement is known as a SOC 2 report.*
>
> **(AICPA, 2015)**

SOC 2 dient gebruikt te worden om een rapport te ontwikkelen over de opzet, bestaan (en werking) van een systeem van beheersmaatregelen van een serviceorganisatie. Van belang hierbij is de systeembeschrijving met bijbehorende boundaries, de te auditen principles en criteria alsmede de wijze van rapporteren.

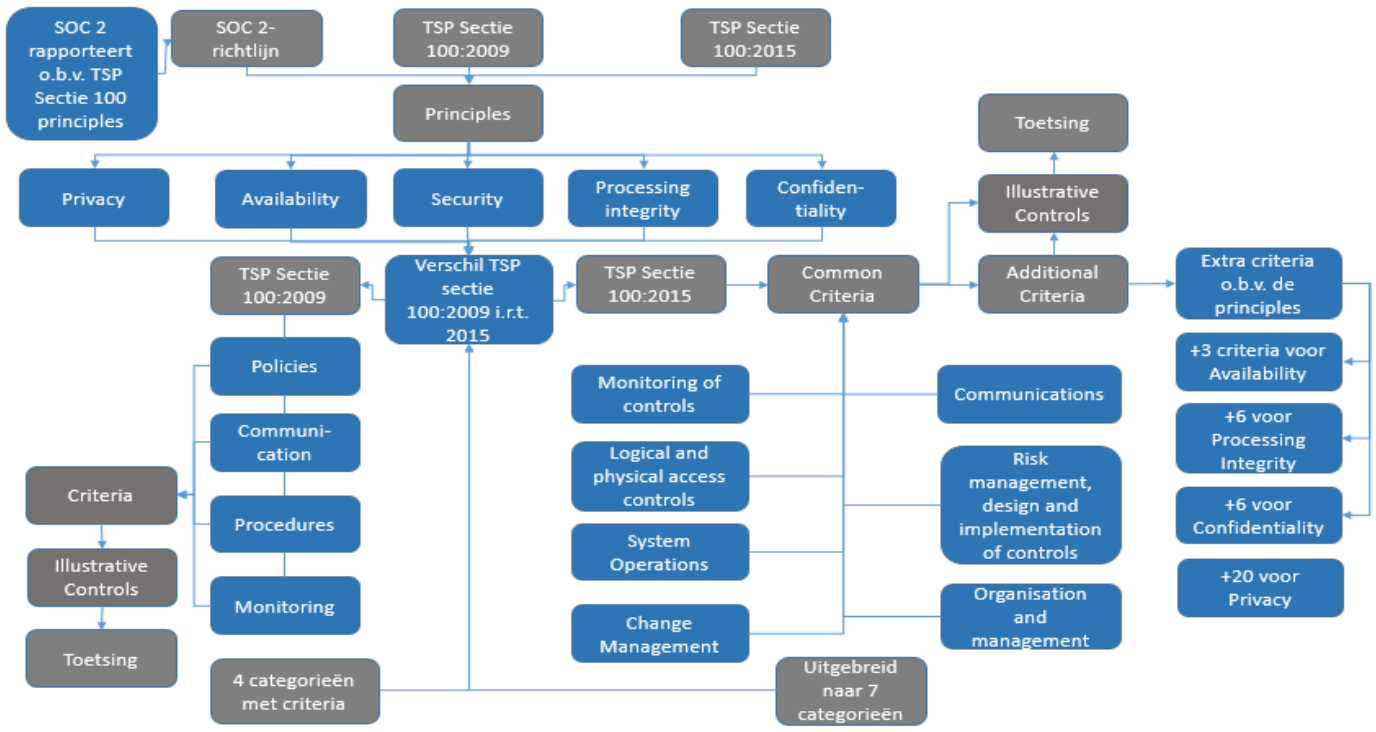
Inhoudelijk wordt in een SOC 2-rapportage op hoofdlijnen de volgende structuur aangehouden (KPMG Advisory N.V., 2012):

- Sectie I: Management bewering;
- Sectie II: Auditorsrapport;
- Sectie III: Systeembeschrijving;
- Sectie IV: Beheersingsdoelstellingen en -maatregelen aangevuld met testinformatie;
- Sectie V: Overige informatie die niet door het rapport van de auditor gedekt wordt.

Zowel een type I als type II-rapportage zal op deze wijze opgebouwd zijn. Bij een type II rapportage zal er gedurende een periode (3 maanden tot een jaar volgens SOC 2) beoordeeld worden hoe een te auditen dienst gepresteerd heeft waarbij eventueel accountants en toezichthouders van gebruikers bij betrokken worden (Boer, 2013).

SOC 2 zal tijdens het onderzoek nader onderzocht worden. SOC 2 maakt het voor een organisatie mogelijk om uitbestede diensten of processen te auditen op basis van de criteria als gedefinieerd in de TSP sectie 100. De samenhang tussen SOC 2 en de TSP Sectie 100 heeft bijgedragen aan de herontwikkeling van de TSP Sectie 100 door overbodige criteria te verwijderen en beter leesbare rapportage op te leveren.

SOC 2 en de TSP Sectie 100 zijn naast elkaar toe te passen gezien deze (in enige mate van elkaar afhankelijke) structuur. Dit zorgt ervoor dat SOC 2 eerder als internationaal te hanteren raamwerk geaccepteerd zal worden, gezien de afstemming tussen beide richtlijnen. Hier zal tijdens het onderzoek uitgebreid aandacht aan worden besteed. Van belang om te weten is dat waar de ISAE 3402 spreekt over beheersmaatregelen, de SOC 2 en TSP Sectie 100 werken in termen van trust principles, controls en criteria. Om de wijzigingen van de TSP Sectie 100 in relatie te brengen met SOC 2 is in figuurfiguur 6 zes een schematische weergave van de verschillende richtlijnen opgenomen.



figuur 6: verschillen TSP Sectie 100 2009 i.r.t. TSP Sectie 100 2015

De wijzigingen zijn resulteren in meer subcategorieën en criteria per trust service principle. Dit betekent dat er een betere dekking is van de relevante criteria en categorieën waardoor een organisatie effectiever geaudit kan worden.

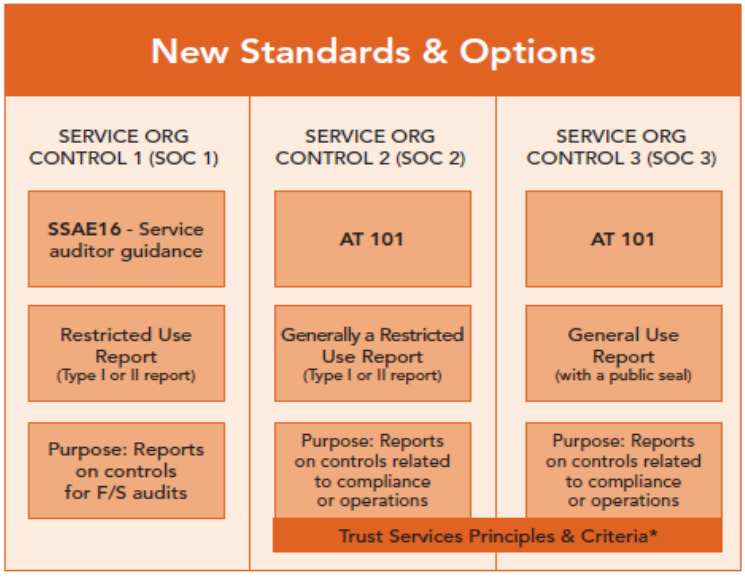
SOC 2 en SOC 3 zijn gelijk voor een auditor: er wordt getoetst op basis van de TSP Sectie 100. Het verschil tussen de richtlijnen is te vinden in de inhoud van de rapportage en verspreidingskring. SOC 3 is geen detailrapportage en is vrij te verspreiden. SOC 3 geeft daarnaast een "seal" wat op een website kan worden geplaatst en doorverwijst naar de SOC 3-rapportage, wat voor bezoekers van een website inzichtelijk maakt zonder onnodige diepgang hoe een organisatie de SOC 3-audit is doorgekomen (figuur 7figuur zeven).

figuur 7: SOC 3-zegel

SOC 2 daarentegen is beschikbaar voor een beperkte gebruikerskring, zoals experts van organisaties die gebruik hebben gemaakt van de te auditen dienst. Van belang is dat degene die de rapportage lezen kennis hebben van de materie waarover gerapporteerd wordt.

Tevens zal gedurende het onderzoek aandacht besteed worden aan de juridische overwegingen van een SOC 2-rapportage met betrekking tot vereisten, voorwaarden voor herkeuring en wettelijke voorschriften. Een voorbeeld hiervan is de naam "SOC 2". Deze naam is door het AIPCA ontworpen en is een trademark. Een Nederlandse interpretatie van deze richtlijn zal dus anders genoemd moeten worden. Daarnaast zal de Nederlandse vertaling waarschijnlijk geen privacy-analyse omvatten, omdat de Amerikaanse definitie van privacy wezenlijk verschilt van de Nederlandse definitie (Sikkema, 2015). Door dit te onderzoeken moet inzichtelijk worden wat voor juridische gevolgen er aan een SOC 2-opdracht zitten en waaraan voldaan moet worden eer een opdracht gestart mag worden.

SOC 2 toetst, zoals eerder beschreven in hoofdstuk twee, op basis van vijf principles. Zodoende kan een organisatie zich laten toetsen op basis van een geaccepteerd raamwerk wat de validiteit en betrouwbaarheid van de audit ten goede komt. Tevens zorgt de SOC 2 ervoor dat de ISAE 3402 (of in verouderde gevallen de SAS 70) niet meer misbruikt worden om een assuranceverklaring af te geven, terwijl niet in alle gevallen de richtlijn correct toegepast wordt door de mogelijkheid tot een relatief vrije scope. Afrondend draagt de SOC 2-richtlijn bij aan het internationaal op één lijn trekken van assurance opdrachten voor IT-serviceorganisaties doordat er in Amerika al acceptatie voor deze richtlijn is; verwacht wordt dat dit in Nederland binnen enkele jaren ook zal groeien (Sikkema, 2015).



figuur 8: onderscheid SOC-rapporten

Het onderscheid tussen de SOC-rapporten is weergegeven in figuur acht (Katcher, 2014).

Zoals in figuur acht weergegeven is, valt SOC 2 onder de AT 101 in Amerika. De AT 101 is de basis voor “Attest Engagements”, opdrachten waarbij een object getoetst wordt wat resulteert in een oordeel over het object (AICPA, 2015). Dit betekent dat de rapportage wordt opgeleverd volgens de AT 101-standaard. Op basis van dit framework wordt een “practitioner” (beroepsbeoefenaar) in staat gesteld een assurance opdracht uit te voeren. De AT 101 geldt als het ware als basis qua structuur, werkwijze en ethiek. Binnen Nederland zal gelden dat de SOC 2 richtlijn gebaseerd zal worden op de ISAE 3000, die dezelfde richtlijnen stelt (op hoofdlijnen) als de AT 101.

SOC 1, met zijn afwijkende scope, valt onder een aparte richtlijn gericht op financiële assurance statements (NDB LLP Accountants & Consultants, z.j.). Tijdens het onderzoek zal uitgebreid aandacht worden besteed aan het uiteenzetten van de meest gebruikte richtlijnen en waar SOC 2 de hiaten vult. SOC 1 zal hierin summier aan bod komen.

Voor het onderzoek zal op basis van de gedefinieerde typen audits en auditors onderzoek worden gepleegd. Het onderzoeksthema kan als volgt worden gedefinieerd:

Tijdens het onderzoek zal er enkel worden gekeken naar externe IT-audits welke een niveau van “reasonable assurance” (figuur twee) opleveren op basis van het gebruik van de kennis en kunde van (RE-geregistreerde) IT-auditors die bij AuditConnect B.V. werkzaam zijn, die zorg kunnen dragen voor de implementatie van SOC 2 en correcte toetsing ervan aan de hand van de TSP Sectie 100.

Afsluitend worden enkele termen verklaard welke tijdens het onderzoek veelvuldig gebruikt zijn.

De eerste van deze termen is uitvoeringscriteria. Met uitvoeringscriteria wordt gedoeld op eisen welke de SOC 2-richtlijn stelt om geïmplementeerd te kunnen worden. Ook wordt hiermee bedoeld wat een organisatie moet hebben eer SOC 2 geïmplementeerd kan worden. Hiermee wordt bedoeld, maar niet uitsluitend:

- Klantwens (wat willen ze met SOC 2 doen/mogelijk maken);
- Mate van aanwezige ICT;
- Primaire proces;
- Omvang;
- Andere voorkomende “randvoorwaarden” vanuit organisaties;
- Baseline welke SOC 2 stelt voordat de richtlijn toegepast mag worden.

Uitvoeringscriteria wordt als volgt gedefinieerd:

De criteria welke SOC 2 stelt aan een organisatie die SOC 2 wil toepassen op zijn dienstverlening en de randvoorwaarden vanuit een organisatie om baat te hebben bij de uitvoering van een SOC 2-opdracht.

Tevens zal de term “leervermogen” tijdens het onderzoek gebruikt worden. Het leervermogen van een organisatie refereert naar óf en hoe een organisatie leert. Tabel zeven geeft weer welke vormen van leren toegepast kunnen worden:

Leerslag	Domein van leren	Categorie van leren	Resultaat van leren	Vraag
Nulslag	Uitkomsten	Reflectieloos doen	Continuering	Geen
Enkelslag	Regels	Moeten vs. Mogen	Verbetering	Hoe?
Dubbelslag	Inzichten	Weten vs. Begrijpen	Vernieuwing	Waardoor/ waarom?
Drieslag	Principes	Willen vs. Zijn	Ontwikkeling	Waartoe?
Metaleren	Leren	Reflecteren	Leren te leren	Waartoe en hoe?

tabel 7: leerslagen (Bennink, 2015)

Afhankelijk van welke leerslagen aanwezig zijn in een organisatie, is een organisatie wel of niet geschikt voor een bepaalde activiteit. Een organisatie waar nulslagleren plaatsvindt, is niet in staat om zijn dienstverlening te verbeteren. Een organisatie waar drieslagleren plaatsvindt zoekt actief naar ontwikkelkansen en stelt een punt aan de horizon op om naar te werken. Afhankelijk van de relevantie van het leervermogen van een organisatie voor het onderzoek zal een advies worden uitgegeven over een minimaal aanwezige leerslag voor een SOC 2-opdracht gestart wordt.

Als laatste wordt de term implementatieplan toegelicht. In eerste aanzet zal de term implementeren worden toegelicht:

> *Implementatie is een procesmatige en/of planmatige invoering van een vernieuwing of verandering. Dit met als smal doel dat de vernieuwing of verandering is geïntegreerd in het beroepsmatige handelen, in het functioneren van organisatie(s) of in de structuur van de sector. En als breed doel dat de vernieuwing of verandering verbetering oplevert.*
>
> **(NJI.nl, z.j.)**

Daarnaast kan een verder onderscheid worden aangebracht in de methode van implementatie. Voor de implementatie (en het onderzoek) kan of een ontwerpbenadering, danwel een ontwikkelbenadering aangehouden worden (tabel acht) (Bennink, 2015).

Ontwikkelingsaanpak:	Ontwerpaanpak:
▪ Samen met “elkaar” taken oppakken ▪ Medewerkers staan centraal; worden om input gevraagd, kunnen meebeslissen ▪ Procesbegeleiding ▪ Als er veel weerstand heerst ▪ Als er veel tijd beschikbaar is	▪ Dwingend opgelegd, zo doen we het en niet anders ▪ Expertrol: vertrouwen op expertise ▪ Als je weinig tijd hebt ▪ Als er weinig weerstand heerst ▪ Medewerkers worden niet meegenomen met het besluit

tabel 8: ontwerp- en ontwikkelaanpak

Beide methoden hebben raakvlak met de manier van implementeren. Bij een ontwerpaanpak zal er veelal dwingend worden gewerkt op basis van een managementwens (organisatie wil voldoen aan standaard x) waar een beperkt tijdsbestek voor beschikbaar is. Daarnaast wordt deze methode gehanteerd wanneer er weinig weerstand heerst in de organisatie waarbij medewerkers weinig tot geen inspraak hebben.

Ter illustratie: organisatie x wil een ISAE 3402 type I-verklaring om te voldoen aan een klantwens. Gezien de klant een kort tijdsbestek beschikbaar heeft voor de uitvoering (en oplevering van een type I rapportage) is het van belang dat de auditor meteen met steun van het management kan beginnen met het auditproces, om de organisatie op korte termijn te voorzien van een ISAE 3402 type I-rapportage. Voor medewerkers van organisatie x betekent dit dat hen dwingend wordt opgelegd medewerking te verlenen en de auditor te steunen waar mogelijk. Indien er weerstand heerst kan dit door gerichte interventies weggenomen worden, maar vanwege de dwingende aanpak zal dit waarschijnlijk niet het geval zijn (Metselaar, 2011). Door deze methode is een auditfirma in staat op korte termijn een type I-rapportage af te leveren wat de mogelijkheid tot een type II-rapportage voor organisatie x mogelijk maakt. In ieder geval kan organisatie x zo aantonen aan hun klant dat ze medewerking verlenen en zodra een type II mogelijk is, dit zullen overwegen.

Bij een ontwikkelbenadering wordt er meer ingezet op het in samenspraak ontwikkelen en uitvoeren van een implementatie. Medewerkers dragen bij aan het schrijven en meedenken van de implementatie waarbij de route van implementatie wordt vastgesteld. Indien in een organisatie veel weerstand heerst en er veel tijd beschikbaar is, is dit de beste methode om een implementatie plaatst te laten vinden.

Ter illustratie: organisatie y wil een ISO 27001 behalen. Organisatie y stelt hier meerdere maanden voor beschikbaar, om na de implementatie direct een audit te kunnen afnemen. Zodoende kan de auditor in samenwerking met personeel van organisatie y een ontwerp te maken voor de implementatie, waar de tijd voor kan worden genomen. In samenwerking met het personeel kan zo de meest effectieve route van implementatie ontwikkeld worden. In deze situaties is vaak veel weerstand aanwezig en door de beschikbare tijd kan hier effectief mee worden omgegaan (Metselaar, 2011). Medewerkers krijgen het gevoel dat ze betrokken worden en zodoende ontstaat er veranderbereidheid. De deskundigheid van het personeel van organisatie y zorgt ervoor dat de implementatie effectief kan verlopen door hun diepgaande kennis over de organisatie en zijn processen. Na afronding van de implementatie, een proces wat zo enkele maanden duurt, is op een organische wijze een ISO 27001 geïmplementeerd welke daarna geaudit kan worden.

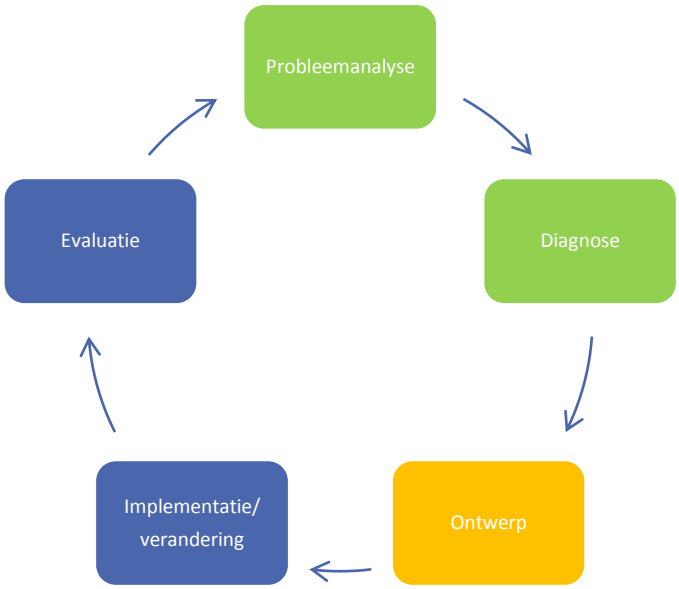
Oftewel implementeren is het procesmatig al dan planmatig invoeren van een verandering welke betrekking heeft op de bedrijfsvoering of werkwijze waardoor verandering danwel verbetering mogelijk wordt gemaakt. Een implementatieplan wordt, eerdergenoemde definitie en mogelijke aanpakken in het oog houdend, dan als volgt gedefinieerd:

Een plan gericht op de gefaseerde implementatie van een project, plan of verandering waar het implementatieplan inzichtelijk maakt wat de (sub)doelen, verantwoordelijk(hed)en, randvoorwaarden en planning voor het implementatieproces zijn waarbij medewerkers en management in (minimaal) enige mate betrokken worden.

HOOFDSTUK 4 VERANTWOORDING METHODEN

In dit hoofdstuk is de onderzoeksmethode verantwoord. Er is sprake van ontwerpgericht onderzoek voor de afstudeeropdracht. Deze methode geeft richting aan het op te leveren product (het ontwerpen van) en stuurt op bruikbaarheid en toepasbaarheid van resultaten. Dit hoofdstuk bevat verder de onderzoekspopulatie, eenheden, variabelen en een mindmap welke voor het onderzoek van toepassing zijn.

Zoals in figuur 9figuur negen is weergegeven, is de interventiecyclus van een onderzoek een cyclisch proces (Hezemans, 2015). Afhankelijk van het instapmoment van een onderzoek heeft dit invloed op welk perspectief gekozen wordt om het onderzoek ten uitvoer te brengen.



figuur 9: interventiecyclus van onderzoek (Hezemans, 2015)

Voor het onderzoek is als instapmoment de ontwerpfase gehanteerd. De probleemanalyse en diagnosefase zijn al afgerond (zie hoofdstuk twee en hoofdstuk drie). Het onderzoek richt zich op de ontwerpfase, waar op basis van vergaarde kennis uit de literatuurstudie gekeken zal worden naar een passend ontwerp opdat SOC 2 voor zoveel mogelijk organisaties, danwel het juiste type organisatie, te implementeren is.

Voor het onderzoek is gekozen een inductieve methode aan te houden. Deze methode is gericht op flexibiliteit, kwaliteit, het begrijpen van de context en het ontwikkelen van theorieën. Tevens hanteert deze methode de aangemelde problematiek (hoofdstuk twee) als uitgangspunt. Voor het onderzoekonderwerp is het minder geschikt om te kijken naar kwantitatief onderzoek, gezien het een maatwerkoplossing betreft. Echter is er ook weinig te onderzoeken op het gebied van kwantitatief onderzoek. Weinig organisaties hebben SOC 2 toegepast (in Europa/Nederland) dus er kan nog niet op een dergelijke mate onderzoek worden gedaan in de maatschappij.

Om tot een geschikte implementatieaanpak te komen moeten de volgende deelvragen beantwoord worden, op basis van de kennis die als relevant wordt gezien:

Onderzoeksvragen
Voor het beantwoorden van de probleemstelling zijn de volgende vragen geformuleerd:

1. Wat zijn de meest gebruikte assurancerichtlijnen en wat voegt de SOC 2-richtlijn hier aan toe?
2. Wat zijn de juridische overwegingen bij de uitvoering en het onderhoud van SOC 2 voor organisaties?
3. Welke criteria zijn van belang voor organisaties om een SOC 2-opdracht te starten?
4. Wat ondersteunt de succesvolle uitvoering van een SOC 2-opdracht?

In tabel negen is beschreven wat per vraag onderzocht moet worden en met welk doel.

Onderzoeks-vraag:	Benodigde informatie/data/ kennis:	Doel:
1	Literatuurstudie naar de meest gebruikte assurancerichtlijnen inclusief SOC 2, overeenkomsten en verschillen en de mate van toepasbaarheid. Daarnaast zal ook gekeken worden of deze richtlijnen "misbruikt" kunnen worden om organisaties onterecht te certificeren.	Het in kaart brengen van de meest gebruikte assurancerichtlijnen en inzicht krijgen in de structuur, toepassingen en het gebruik/misbruik van deze richtlijnen. Tevens het in kaart brengen van organisaties die baat hebben bij SOC 2 op basis van vastgestelde overeenkomsten en verschillen tussen SOC 2 en de overige assurancerichtlijnen.
2	Verplichtingen vanuit SOC 2 en andere vereiste richtlijnen. Relevante wetgeving en jurisprudentie.	In kaart brengen wat de juridische gevolgen (indien aanwezig) zijn van een SOC 2-implementatie en het onderhoud hiervan. Advies geven met betrekking tot omgang met deze (mogelijke) overwegingen.
3	Gegevens over de SOC 2-implementatie bij organisaties. Denk hierbij aan motivatie en werkwijze voor de implementatie en wat voor wijzigingen de implementatie in de bedrijfsvoering heeft aangebracht en welke gevolgen dit met zich mee brengt.	Een overzicht scheppen van criteria welke voor organisaties van belang zijn om SOC 2 uit te laten voeren. Op zoek gaan naar gedeelde criteria zodat er een profiel van een organisatie kan worden ontwikkeld die baat heeft bij SOC 2. Tevens wordt zo vastgesteld wat de uitvoeringscriteria zijn voor organisaties en wordt er op zoek gegaan naar best practices. (*Kanttekening: dit blijft in enige mate afhankelijk van de eisen die SOC 2 stelt voordat SOC 2 geïmplementeerd mag worden*.)
4	Op basis van het profiel uit vraag drie verder onderzoek plegen naar organisaties die baat hebben bij SOC 2 door het profiel te toetsen aan verwachtingen en wensen van klanten. Daarnaast verdere literatuurstudie over het ontwikkelen van een betrouwbaar profiel en de toetsing ervan.	Het ontwerpen van een profiel waardoor AuditConnect B.V. gericht klanten kan benaderen en toetsen of zij binnen het profiel van organisaties vallen die baat hebben bij een SOC 2-implementatie. Daarnaast kan zo het profiel worden getoetst, wat de onderzoeksresultaten verder valideert.

tabel 9: benodigde informatie en doel per onderzoeksvraag

Als eerste worden de deelvragen beantwoord. Hierna wordt de probleemstelling beantwoord.

> *Hoe kan de SOC 2-richtlijn het meest effectief binnen een nader vast te stellen type organisatie geïmplementeerd en/of getoetst worden, op basis van welke uitvoeringscriteria en leidt dit tot een algemeen toepasbare oplossing voor organisaties?*

Op basis van het ontwikkelde implementatieplan en organisatieprofiel (gebaseerd op de uitvoeringscriteria) kan zo een flexibele rapportagestructuur ontworpen worden. Alle onderzoeksgegevens zullen verder gebruikt worden om de probleemstelling te beantwoorden.

Waarborg

Om zorg te dragen voor de validiteit en betrouwbaarheid van gegevens en conclusies, worden de gespreksverslagen van interviews toegevoegd. Zodoende wordt het proces van hypothese - interview – resultaat – conclusie duidelijk in kaart gebracht, om te voorkomen dat de conclusies niet reproduceerbaar zijn of ongefundeerd lijken te zijn. Bij de interviews wordt gebruik gemaakt van open vragen en worden de antwoorden gewogen op de waarde die er aan gehecht kan worden, om te voorkomen dat subjectiviteit meegenomen wordt in het beantwoorden van de onderzoeksvragen. Op basis van de waarde en de aan- of afwezigheid van subjectiviteit van de antwoorden worden resultaten meegenomen in het vormen van een conclusie. Op deze wijze wordt gedurende het onderzoekstraject de validiteit en betrouwbaarheid van de gegevens en conclusies geborgd. Voor de reproduceerbaarheid kan zo op basis van dezelfde werkwijze in combinatie met literatuuronderzoek gelijksoortige conclusies getrokken worden.

Populatie

De populatie voor het onderzoek bestaat uit twee onderzoeksgroepen: organisaties die SOC 2 wel hebben geïmplementeerd en organisatie die SOC 2 niet hebben geïmplementeerd.

Eenheden en variabelen

Binnen het onderzoek worden variabelen en eenheden onderkend. Om een juiste operationalisatie te kunnen maken, is het van belang dat deze begrippen juist worden toegepast. Eenheden kunnen als volgt worden gedefinieerd:

> *De eenheden zijn in een onderzoek de mensen of zaken waarover het onderzoek een uitspraak doet, zoals gemeenten, slachtoffers, cliënten, besluitvormingsprocessen, etc.*
>
> **(Losse, 2012)**

Variabelen hebben de volgende definitie:

> *De variabelen van een onderzoek zijn kenmerken van de eenheden die in kaart gebracht moeten worden, zoals aantal inwoners, werkdruk, leeftijd, managementtype, etc.*
>
> **(Losse, 2012)**

De volgende eenheden worden onderkend:

- Assurancerichtlijnen (inclusief SOC 2) — tabel tien
- Organisaties die SOC 2 geïmplementeerd hebben — tabel elf**Fout! Verwijzingsbron niet gevonden.**
- Organisaties die SOC 2 niet geïmplementeerd hebben — tabel twaalf
- Uitvoeringscriteria — tabel dertien

Per tabel is één eenheid behandeld, met de daarbij relevante variabelen en onderzoekshandelingen (Hezemans, 2015). De eenheden hangen samen met de onderzoeksvragen.

Hieronder is een overzicht gegeven van de samenhang tussen de onderzoeksvragen en de eenheden:

- Onderzoeksvraag 1: tabel tien
- Onderzoeksvraag 2: tabel tien, elf en twaalf
- Onderzoeksvraag 3: tabel elf en twaalf
- Onderzoeksvraag 4: tabel elf, twaalf en dertien

De volgende tabellen zijn gebruikt voor het onderzoek:

Eenheid	Variabelen	Dataverzamelings-methode	Meetinstrument
Assurance-richtlijnen (inclusief SOC 2)	Scoping van richtlijnen. Vereisten voor implementatie van richtlijn. Auditcriteria per richtlijn. Overeenkomsten en verschillen. Baseline voor certificering. Invloed SOC 2 in relatie tot andere richtlijnen. Toepasbaarheid SOC 2.	Literatuurstudie: de richtlijnen zelf, theorie over de implementatie van de richtlijnen, vergelijkend onderzoek naar de richtlijnen.	▪ Wat is de scoping? ▪ Welke vereisten stellen de richtlijnen? ▪ Heeft elke richtlijn eigen auditcriteria of kan dit op basis van de TSP Sectie 100? ▪ Welke overeenkomsten en verschillen zijn er tussen de richtlijnen? ▪ Stellen de richtlijnen een baseline voor de implementatie, en zo ja, wat voor baseline? ▪ Welke invloed heeft SOC 2 op de richtlijnen? ▪ Hoe toepasbaar is SOC 2?

tabel 10: eenheid assurancerichtlijnen (inclusief SOC 2)

Eenheid	Variabelen	Dataverzamelings-methode	Meetinstrument
Organisaties die SOC 2 geïmplementeerd hebben	SOC 2 implementatie. Criteria als randvoorwaarden vanuit organisatie voor SOC 2-implementatie. Wijzigingen bedrijfsvoering voor implementatie SOC 2. Implementatie SOC 2. Samenhang SOC 2 in relatie tot geïmplementeerde richtlijnen. SOC 2 in relatie tot een aanmerkelijke stijging in beveiligingsbewustzijn. Ontwikkeling en behoud klantenbestand door SOC 2.	Diepte-interviews met interne kennishouders (ISM-verantwoordelijke, interne auditors, security managers). Indien mogelijk/praktisch verspreiden van een enquête.	▪ Welke randvoorwaarden had uw organisatie voor de implementatie van SOC 2? ▪ Hoe ging de implementatie? ▪ Moest de bedrijfsvoering aangepast worden voor, na of tijdens de implementatie? ▪ Hoe hangt SOC samen andere geïmplementeerde richtlijnen (ISO 27001 etc.)? ▪ Merkt u een stijging in het beveiligingsbewustzijn bij betrokken medewerkers na de implementatie?

			▪ Is het klantenbestand gegroeid naar aanleiding van de implementatie? ▪ Wat is de branding value van SOC 2?

tabel 11: eenheid organisaties die SOC 2 hebben geïmplementeerd

Eenheid	Variabelen	Dataverzamelings-methode	Meetinstrument
Organisaties die SOC 2 niet geïmplementeerd hebben	Criteria om SOC 2 niet te implementeren. Uitgevoerde richtlijnen. Assuranceproces. Organisatie-volwassenheid. Ontwikkeling en behoud klantenbestand door SOC 2. Zijn er eerder TPM's afgegeven?	Diepte-interviews met interne kennishouders (ISM-verantwoordelijke, interne auditors, security managers). Indien mogelijk/praktisch verspreiden van een enquête. Waar mogelijk deskresearch naar behaalde certificeringen, audits en afgegeven statements.	▪ Waarom is de keuze gemaakt SOC 2 niet te implementeren? ▪ Welke andere richtlijnen heeft uw organisatie geïmplementeerd? ▪ Hoe is het assuranceproces binnen uw organisatie vormgegeven? ▪ Hoe zou u de volwassenheid van de organisatie omschrijven? ▪ Bent u van mening dat SOC 2 kan bijdragen aan het behouden en verbreden van het klantenbestand? ▪ Zijn er eerder TPM's afgegeven?

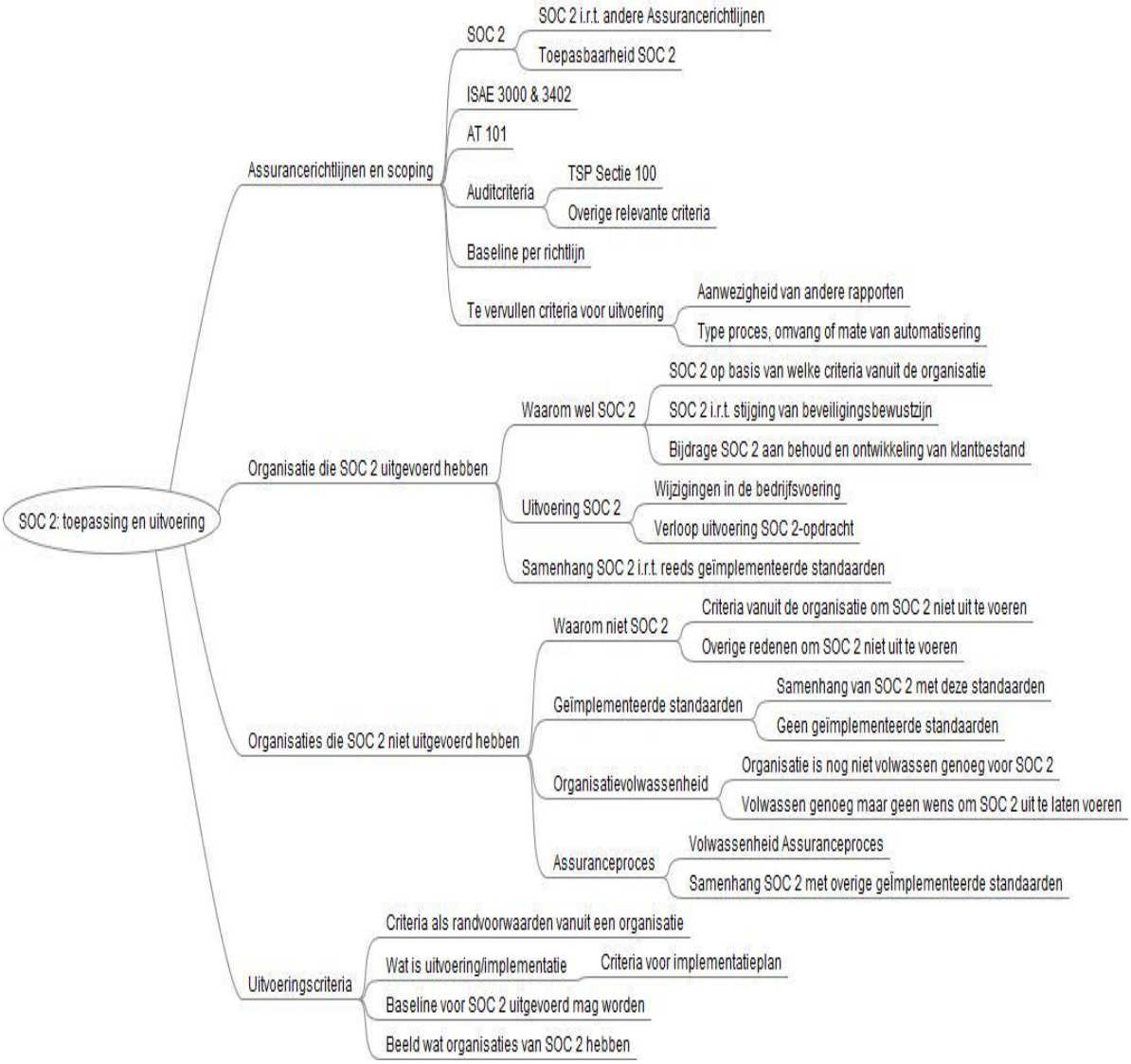
tabel 12: eenheid organisaties die SOC 2 niet hebben geïmplementeerd

Eenheid	Variabelen	Dataverzamelings-methode	Meetinstrument
Uitvoeringscriteria	Wat is implementatie? Uitvoeringscriteria als randvoorwaarden voor een organisatie. Baseline SOC 2-implementatie. Beeld van SOC 2.	Literatuurstudie, Diepte-interviews met interne kennishouders (ISM-verantwoordelijke, interne auditors, security managers) en externe specialisten. Indien mogelijk/praktisch verspreiden van een enquête.	▪ Hoe kan implementatie het beste gedefinieerd worden? ▪ Welke uitvoeringscriteria stellen organisaties? ▪ Welke baseline stelt SOC 2 voor zijn implementatie? ▪ Hoe kijken organisaties tegen SOC 2 aan?

tabel 13: eenheid uitvoeringscriteria

Mindmap

In **Fout! Verwijzingsbron niet gevonden.**figuur tien is de mindmap opgenomen. Deze mindmap geeft de o nderlinge structuur en verbanden tussen de eenheden en variabelen verder aan.



figuur 10: mindmap eenheden en variabelen

HOOFDSTUK 5 ONDERZOEKSRESULTATEN

In dit hoofdstuk worden de onderzoeksresultaten beschreven. Voor het onderzoek is gebruik gemaakt van de volgende dataverzamelingsmethoden:

- Interviews;
- Literatuuronderzoek.

In dit hoofdstuk zijn de interviewresultaten samengevat weergegeven met een beschrijving van de resultaten. Het literatuuronderzoek en de resultaten ervan zijn verweven in de deelvragen zelf en zullen hier niet benoemd worden wegens omvang. Voor de volledige gespreksverslagen en vragenlijsten wordt doorverwezen naar bijlage één tot en met drie.

5.1 INTERVIEWRESULTATEN

Voor het onderzoek zijn enkele interviews uitgevoerd. Deze interviews benaderen de materie van SOC 2 vanuit verschillende perspectieven, namelijk vanuit een organisatie die SOC 2 heeft uitgevoerd en jaarlijks laat auditen, een organisatie die SOC 2 niet heeft uitgevoerd en een deskundige opinie over de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 en de toepasbaarheid hiervan. Op basis van de vergaarde informatie wordt vanuit verschillende standpunten gekeken naar SOC 2, de implementatie, het onderhoud en de toepasbaarheid. Tevens zal worden onderzocht hoe organisaties assurance benaderen en of de visie op informatiebeveiliging in relatie staat tot hoe er omgegaan wordt met assurance.

Gezien de vertrouwelijkheid van informatie is het niet mogelijk gespreksverslagen volledig aan te leveren. In bijlagen één tot en met drie zijn de geaccordeerde gespreksverslagen opgenomen, zoals overlegd met de geïnterviewden. Op basis van deze verslagen worden algemene conclusies getrokken over SOC 2.

De volgende interviews zijn uitgevoerd (tabel 14tabel veertien):

Interview:	**Geïnterviewde(n):**
Organisatie die SOC 2 ten uitvoer heeft gebracht en jaarlijks audit;	Theo Buurman (Quality Manager) en Hans Metz (Security Manager), InterXion
Organisatie die SOC 2 niet ten uitvoer heeft gebracht;	Stefan van den Broek (Information Risk and Quality Manager), EBPI
Deskundige opinie over de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 (NOREA, 2016).	René van de Hesseweg (Client assurance Manager en teamlid ontwikkeling NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100.), KPN

tabel 14: geïnterviewden

Interview 1: Theo Buurman en Hans Metz, InterXion
InterXion is een organisatie gespecialiseerd in het leveren van dataservices aan klanten. InterXion is een datacenter met eind 2016 zeven locaties. InterXion levert zijn klanten ruimte, connectiviteit en koeling. InterXion bedient een breed scala aan klanten, waaronder ook internationale klanten. Mede hierdoor is InterXion gestart met het auditen van SOC 2. Internationale klanten vragen vaker om een SOC 2, wat bijdraagt aan het realiseren van internationale ambities. Gezien InterXion jaarlijks een SOC 2-opdracht laat uitvoeren is voor het interview gekeken hoe SOC 2 toegepast kan worden, wat voorkomende uitdagingen zijn en hoe SOC 2 zich verhoudt tot andere audits. Voor het gehele verslag en de vragenlijst, zie bijlage één.

Aan het gespreksverslag kunnen de volgende observaties worden ontleend:

- Er is een significante reductie in de mate van klantaudits doordat SOC 2 (internationale) klanten de gewenste assurance levert (één rapport wat meerdere klanten voorziet in hun behoefte);
- Minder tijdverlies door minder voorbereiding voor audits;
- Een hogere efficiency in het auditproces door minder audits;
- Een hogere effectiviteit binnen de processen. De controls binnen de TSP Sectie 100 brengen de juiste focus aan op de operationele processen.
- Eigen initiatief en continue verbetering als filosofie wat zich uit in proactief handelen, het inzetten van nieuwe middelen en flexibiliteit;
- Trends liggen op het gebied van connectiviteitsontwikkelingen, het verankeren van controls in processen, informatiebeveiligingsstandaarden en de implementatie hiervan;
- Assurance als “business enabler”: een manier om proceskwaliteit te borgen en aantoonbaar te maken;
- Een SOC 2-audit is stringenter dan andere audits. Het concretiseren van normen en het ontsluiten van de juiste bewijslast kan lastig zijn;
- De interne auditfunctie kan bijdragen aan een succesvol verloop van de audit;
- Bedrijfsvoering had geen aanpassingen nodig om te voldoen aan een SOC 2-audit;
- Er wordt een grote meerwaarde toegekend aan SOC 2 op het gebied van internationale betrekkingen.

Op basis van deze punten is het volgende beeld samengesteld voor een organisatie die SOC 2 wil implementeren (los van alle complicaties die SOC 2 met zich meebrengt, zoals wet- en regelgeving):

- Er is sprake van een lerende organisatie (Bennink, 2015);
- Continue verbetering van (de kwaliteit van) de dienstverlening;
- Assurance is geen kwestie van vinkjes zetten, maar een proces met diepgaande meerwaarde wat in alle lagen van de organisatie dien te leven;
- Behoud en vergroting van het klantenbestand als een pijler voor assurance, naast procesverbetering;
- Een reden (wens/eis/noodzaak) om te voldoen aan de eisen van internationale klanten, of het aantrekken hiervan;
- De wens om een efficiëntieslag te plegen m.b.t. het assuranceproces.

Op het hoogste niveau kan het type organisatie gedefinieerd worden als een organisatie met een wens om processen en dienstverlening te verbeteren en deze verbeteringen op een internationaal geaccepteerde wijze te borgen. Assurance is een integraal proces waar heel de organisatie aan deelneemt. Internationale aspiraties zijn aanwezig. De organisatie heeft leervermogen en gebruikt dit om verbetering en vernieuwing in de organisatie te stimuleren. Er is sprake van een familiecultuur, wat bijdraagt aan flexibiliteit en betrouwbare interne samenwerking.

Interview 2: Stefan van den Broek, EBPI
EBPI (European Business Process Institute) is een organisatie gespecialiseerd in massale berichtenverwerking. EBPI verzorgt berichtenuitwisseling van de overheid richting burgers en ondernemers. EBPI beheert deze keteninformatie-uitwisseling en is verantwoordelijk voor de diensten en infrastructuur die deze uitwisseling mogelijk maakt. EBPI heeft geen SOC 2-opdracht laten uitvoeren en daardoor stond het interview in het teken van de redenen waarom er geen SOC 2 uitgevoerd is, hoe het assuranceproces is vormgegeven en wat de verwachtingen voor de toekomst zijn. Voor het gehele interview en de vragenlijst, zie bijlage twee.

Aan het gespreksverslag kunnen de volgende observaties worden ontleend:

- Informatiebeveiliging is een hoge prioriteit voor EBPI. Meerdere certificeringen zijn behaald en worden onderhouden, op verzoek van klanten alsmede door eigen initiatieven;
- De organisatie is niet bekend met SOC 2. Dit geldt naar verwachting voor het merendeel van de organisaties in Nederland, doordat het vakgebied assurance niet snel verandert, mede door de ISAE/NOREA Richtlijn 3402;
- De abstractie van de normen van de TSP Sectie 100 staan open voor interpretatie, afhankelijk van hoever de organisatie gaat in het plaatsen van controls en de diepgang van de auditor zijn testen;
- Een vastgesteld normenkader zou een tijdsbesparing opleveren en de complexiteit van het assuranceproces verminderen;
- Normenkaders ontwikkelen vaak niet mee doordat eisen contractueel zijn vastgesteld. Het is van belang voor de adoptie van SOC 2 dat de TSP Sectie 100 mee evolueert op basis van hedendaagse dreigingen;
- Klanten moeten bekend worden gemaakt met de SOC 2-richtlijn en meegroeien in het veranderende assurancelandschap. De NOREA moet hierin een leidende rol aannemen.

Op basis van de bovenstaande observaties wordt duidelijk dat SOC 2 in zijn toepassing enkele uitdagingen met zich meebrengt. Voordat organisaties zullen overstappen is het van belang dat er:

- Kennis is over SOC 2 bij zowel klanten als auditors;
- De juiste mate van abstractie is vastgesteld;
- Klanten meegroeien met veranderingen in het assurancevakgebied;
- Organische groei zeker is gesteld en plaats vindt;
- De NOREA een leidende rol neemt met betrekking tot het delen van informatie over SOC 2.

Samenvattend kan worden gesteld dat de kennis over SOC 2 moet groeien, klanten moeten inzien wat voor assuranceproduct passend is en dat de NOREA zowel klanten als auditors moet begeleiden in het juist toepassen van de handreiking. Wanneer klanten de meerwaarde van SOC 2 inzien, zal ontwikkeling aan het normenkader plaats blijven vinden waardoor organisaties weerbaar blijven tegen toekomstige dreigingen. Indien dit niet gebeurt, is de waarde van SOC 2 laag en de kans op adoptie laag.

Interview 3: René van de Hesseweg, KPN
Het primaire proces van KPN is het leveren van geïntegreerde telecom- en IT-diensten zoals telefonie, connectiviteit en proceshosting of -ondersteuning. KPN bedient internationale klanten en dient te voldoen aan een breed scala van wet- en regelgeving, maar ook aan verschillende (audit)eisen van haar klanten. Door de complexiteit die dit met zich meebrengt in het assuranceproces heeft KPN (en voorheen Getronics) een integraal assuranceframework ontworpen wat niet alleen toepasbaar is op haar eigen processen, maar ook op de processen van sub-serviceorganisaties. Zodoende kan er door de keten heen assurance verkregen worden op een wijze waarin effectiviteit en efficiëntie niet verloren gaan.

Daarnaast is dhr. van de Hesseweg teamlid geweest van de werkgroep verantwoordelijk voor het publiceren van de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100. Het gehele gespreksverslag is terug te vinden in bijlage drie, inclusief de vragenlijst.

Aan het interview kunnen de volgende observaties worden ontleend:

- Complexiteit in het aantal normenkaders dat klanten eisen en de toepassing ervan;
- Klanten weten niet wat voor hen de juiste assurance is en gebruiken hierdoor vaak enkel bekende verklaringen zoals de ISAE 3402;
- Klanten moeten worden meegenomen in het assuranceproces om inzichtelijk te krijgen wat voor welke klant nodig is qua assurance;
- Verschuiving in de doelgroep van een assurancerapport (kennishouders naar management);
- SOC 2 brengt eenduidigheid door een vastgesteld kader wat problemen met de ISAE 3402 kan verhelpen en de veelvuldigheid van normenkaders kan laten verkleinen;
- Scheidingslijn tussen SOC 1 en SOC 2 is voor klanten niet duidelijk, dit biedt de mogelijkheid tot toepassingsonduidelijkheid zoals bij de ISAE 3000 en 3402;
- Marktwaarde van SOC 2 is momenteel laag door onbekendheid en onbekendheid van klanten en auditors;
- NOREA kan de marktwaarde vergroten door bijscholing en initiatieven inzetten om SOC internationaal te laten publiceren in samenwerking met andere partijen wat bepaalde obstakels van SOC 2 kan verhelpen;
- Kans op adoptie onder auditors is momenteel laag doordat er geen verplichting is volgens de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 te handelen (NOREA, 2016);
- Het verlies van elementen zoals zegels en toetsing op het gebied van “Privacy” verkleint de kans op adoptie;
- Indien de NOREA geen aandacht schept voor de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 is de kans klein dat auditors en klanten deze zullen gaan gebruiken.

Uit het gespreksverslag kan worden geconcludeerd dat er meerdere uitdagingen zijn voor SOC 2. Het verlies van enkele elementen maakt dat het minder aantrekkelijk is voor klanten om zich te laten auditen op basis van de NOREA Guidance to Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 (NOREA, 2016). De onbekend- en onvolwassenheid van klanten op het gebied van assurance is een reden waarom assuranceverklaringen “misbruikt” worden; doordat men niet weet welk type assurance geschikt is voor hen. Accountants e.d. kunnen op basis van de (vaak contractueel vereiste) NOREA Richtlijn 3402-rapportage een jaarrekening wel controleren, maar dit geeft geen assurance over andere elementen van een organisatie die ook gecontroleerd dienen te worden. De NOREA moet een actieve rol spelen in het promoten van de handreiking en zijn toepassing

om zowel klanten als auditors bekend te maken met de mogelijkheden van de handreiking. Momenteel is de marktwaarde laag en de kans op adoptie klein, echter kan de NOREA hier wel een grote rol in spelen.

SOC 2 biedt een versimpelde rapportage die voor een verschuivende doelgroep leesbaar is en het vastgestelde normenkader komt de eenduidigheid van audits ten goede. Afrondend kan er een vereenvoudiging ontstaan in het landschap van te hanteren frameworks (bijvoorbeeld voor KPN) doordat organisaties over stappen van eigen of andere normenkaders op de TSP. Indien er geen stappen worden ondernomen om deze uitdagingen te overkomen, blijft de kans op adoptie laag.

HOOFDSTUK 6 BEANTWOORDING DEELVRAGEN EN PROBLEEMSTELLING

In dit hoofdstuk zullen de deelvragen beantwoord worden. De volgende onderzoeksvragen zijn benoemd in de onderzoeksopzet en -verantwoording:

1. Wat zijn de meest gebruikte assurancerichtlijnen en wat voegt de SOC 2-richtlijn hier aan toe?
2. Wat zijn de juridische overwegingen bij de uitvoering en het onderhoud van SOC 2 voor organisaties?
3. Welke criteria zijn van belang voor organisaties om een SOC 2-opdracht te starten?
4. Wat ondersteunt de succesvolle uitvoering van een SOC 2-opdracht?

Elke onderzoeksvraag wordt behandeld. (zie paragraaf 6.1 tot en met 6.4.)

Daarnaast zal ook de probleemstelling beantwoord worden. Deze luidt:

Welk type organisatie heeft baat bij een SOC 2-rapportage en hoe kan de SOC 2-richtlijn het meest effectief geïmplementeerd en/of getoetst worden, op basis van welke uitvoeringscriteria en leidt dit tot een algemeen toepasbare oplossing?

Per deelvraag is enkel de samenvatting benoemd in de paragraaf. Dit is wegens omvang besloten opdat de hoofdtekst niet onnodig groot wordt. In de bijlagen één tot en met vijf zijn de onderbouwingen van de deelvragen opgenomen.

Na de beantwoording van de deelvragen volgt de beantwoording van de probleemstelling, opgenomen in paragraaf 6.5.

De onderzoeksmethoden beschreven in hoofdstuk vier en de onderzoeksresultaten zoals beschreven in hoofdstuk vijf zijn gebruikt om de onderzoeksvragen te beantwoorden. Op basis van deze resultaten en methodieken is een context gegeven per onderzoeksvraag waarmee een passend antwoord is geformuleerd.

6.1 DEELVRAAG 1

WAT ZIJN DE MEEST GEBRUIKTE ASSURANCERICHTLIJNEN EN WAT VOEGT DE SOC 2-RICHTLIJN HIER AAN TOE?

Voor de beantwoording van deze onderzoeksvraag is gebruik gemaakt van de onderzoeksmethodieken zoals beschreven in hoofdstuk vier, tabel tien. Op basis van de geoperationaliseerde eenheden en variabelen is de beantwoording tot stand gekomen.

Inleiding
Voor het onderzoek is een selectie gemaakt van de relevante assurancerichtlijnen. Internationaal zijn er meerdere partijen die richtlijnen ontwerpen en laten toetsen door hun (geregistreerde) leden. Een voorbeeld hiervan is het AICPA (American Institute of Certified Public Accountants) of haar Nederlandse tegenhanger, de Nederlandse Orde van Register EDP-Auditors (NOREA).

Deze partijen ontwerpen en creëren richtlijnen op basis van vragen en ontwikkelingen uit de markt of wet- en regelgeving en best practices danwel verbeteringen vanuit hun ledenbestand. Een assurancerichtlijn is een strak geheel van vereisten, voorwaarden en afhankelijkheden wat een organisatie in staat stelt om processen, diensten of de bedrijfsvoering te laten toetsen op meerdere vlakken. Een assurancerichtlijn kan meerdere aspecten van een organisatie onderzoeken of buiten beschouwing laten. Afhankelijk van de scoping van de richtlijn wordt bepaald wat relevant is voor de richtlijn en waarop de organisatie zal worden getoetst. Zodoende is het van belang een selectie te maken van de relevante assurancerichtlijnen. Hiervoor is het onderzoeksthema gebruikt, beschreven in het theoretisch kader (hoofdstuk drie):

Tijdens het onderzoek zal er enkel worden gekeken naar externe IT-audits welke een niveau van "reasonable assurance" (figuur twee) opleveren op basis van het gebruik van de kennis en kunde van (RE-geregistreerde) IT-auditors die bij AuditConnect B.V. werkzaam zijn, die zorg kunnen dragen voor de implementatie van SOC 2 en correcte toetsing ervan aan de hand van de TSP Sectie 100.

Enkel IT-audits met een werkgebied gericht op het testen van IT-controls zijn relevant voor het onderzoek waardoor bijvoorbeeld IT-audits met een financieel werkgebied niet als relevant geacht worden. Hetzelfde geldt voor audits die als scope maatschappelijk verantwoord ondernemen, milieuvriendelijkheid en andere werkgebieden behelzen waarbij geen link is met een (ondersteunend) IT-landschap en het verkrijgen van assurance hierover. Onderstaande richtlijnen zijn tevens gekozen op basis van uitbesteding van processen: al deze richtlijnen hebben als scope uitbestede IT-processen, diensten en de beheersing hierover. Waar Amerikaanse richtlijnen vertaald zijn door de NOREA, wordt de NOREA-variant aangehouden. Enkel de SOC-richtlijn zal als Amerikaanse richtlijn gebruikt worden. De NOREA heeft een vertaling gepubliceerd, maar voor de volledigheid moeten de Amerikaanse SOC-richtlijnen onderzocht worden.

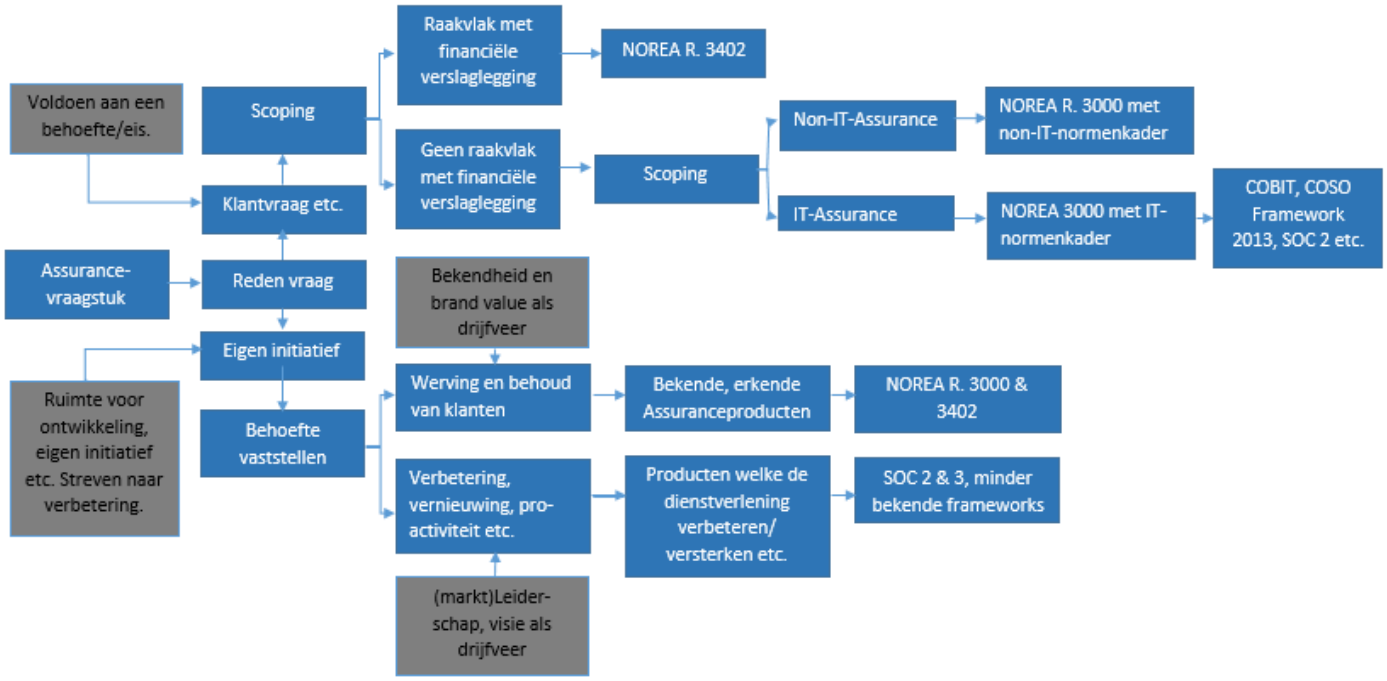
De volgende richtlijnen zijn gekozen:

- ISAE 3000 op basis van de herziene NBA Standaard 3000 en NOREA Richtlijn 3000 (NBA, 2016) (NOREA, 2009);
- ISAE 3402 op basis van de NOREA Richtlijn 3402 (NOREA, 2011);
- SOC 1, 2 en 3((AICPA, 2013), (AIPCA, 2015));
- NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 (NOREA, 2016).

Deze richtlijnen zijn gekozen omdat de NOREA Richtlijn 3000 en 3402 tot de ontwikkeling van de SOC-richtlijn golden als “het best beschikbare middel” om assurance te verkrijgen over de beheersing van uitbestede IT-diensten en processen. Daarnaast is er een scope welke overeenkomt met een SOC 1 danwel een SOC 2-rapport.

De NOREA Richtlijn 3000 i.c.m. het SOC 2-rapportmodel en de TSP Sectie 100 is de uitwerking van de NOREA voor de SOC 2-richtlijn, op basis van Nederlandse wet- en regelgeving en beroepsreglementen. Alle richtlijnen zullen uiteen worden gezet en de toevoeging van SOC 2 (op basis van de NOREA Richtlijn 3000 en de TSP Sectie 100) zal vast worden gesteld. Overige richtlijnen hebben niet de juiste scope om relevant te zijn voor het onderzoek (richtlijnen met betrekking tot MVO, milieuverantwoord ondernemen etc.) en worden niet behandeld.

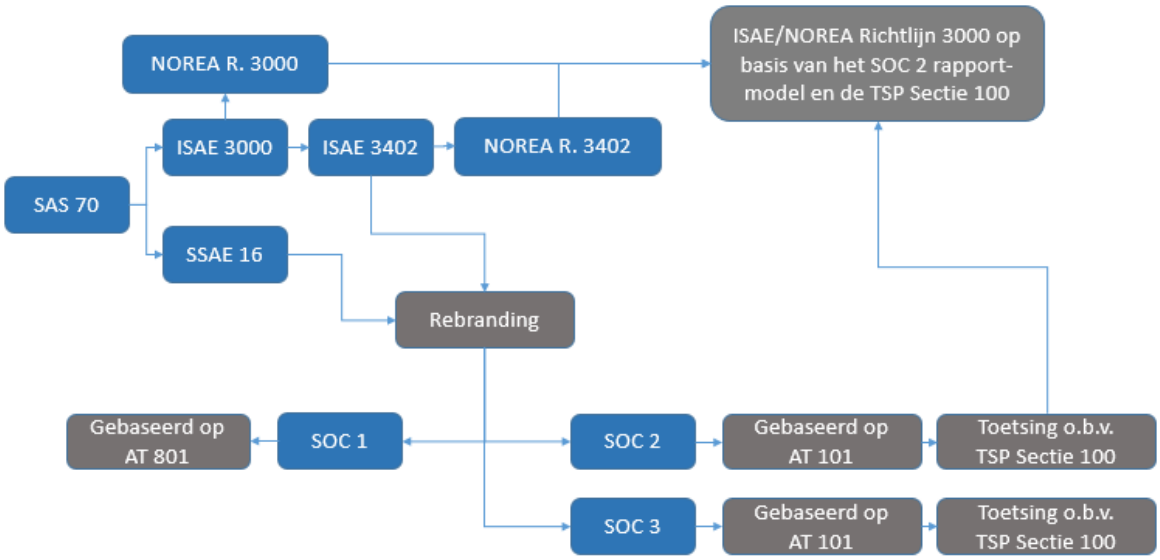
Afhankelijk van de behoefte van een serviceorganisatie of de wens van een gebruikersorganisatie kan een bepaald product gekozen worden. Dit hangt verder samen met waarover assurance verkregen dient te worden. Het kiezen van een passende rapportage of verklaring kan een lastig proces zijn: bepaalde richtlijnen geven duidelijk weer waarvoor ze toegepast mogen worden, maar het kan lastig zijn om in te schatten of de organisatie danwel de beheersmaatregelen binnen de ene richtlijn of de andere richtlijn getoetst dient te worden. Hieronder is schematisch weergegeven hoe een assurancevraagstuk leidt tot een bepaald product (figuur elf):



figuur 11: bepaling van de juiste assurancerapporten per vraagstuk

Afhankelijk van de reden van de vraag, is er ruimte om een richtlijn te kiezen. Wanneer een klant echter een specifiek rapport wenst, kan de serviceorganisatie hier echter weinig aan wijzigen en dient het rapport opgeleverd te worden door de serviceorganisatie. Indien er wel sprake is van eigen initiatief kan er onderzocht worden waar de behoefte van de serviceorganisatie ligt. Is er sprake van klantbehoud, dan is de beste keus een geaccepteerde assuranceverklaring. Als verbetering, vernieuwing of ontwikkeling de beweegreden is, kan er gekeken worden naar minder bekende richtlijnen (zoals SOC 2) om de dienstverlening verder te ontwikkelen en een degelijk fundament voor assurance in te richten.

Voor het kiezen van het juiste assuranceproduct is het van belang om te weten hoe de richtlijnen zich hebben ontwikkeld door de jaren heen en vanuit welke richtlijnen uiteindelijk SOC 2 is voortgekomen. Hieronder is een schematische weergave gegeven van de onderlinge samenhang en ontwikkeling van de gekozen richtlijnen (figuur twaalf):



figuur 12: schematische weergave ontwikkeling assurancerichtlijnen

De ontwikkelingen die hebben geleid tot de NOREA-vertaling van SOC 2 zijn complex en vereisen de nodige uitleg: voor de volledigheid wordt hier verder in de volgende onderzoeksvraag op ingegaan. Voor nu is van belang om kennis te nemen van het feit dat de SOC 2 in de NOREA 3000 is geplaatst door de NOREA (NOREA, 2016). Dit betekent dat het rapport aan de grondslag de NOREA Richtlijn 3000 heeft, welke de regels en werkwijze stelt voor een auditor. Het rapport is ingedeeld naar het rapportmodel van SOC 2, omdat de NOREA Richtlijn 3000 geen verplichte indeling voorschrijft. De resterende richtlijnen zijn doorontwikkeld vanaf de SAS 70, welke als gevolg van onder andere de SOX-wetgeving is ontwikkeld. De “rebranding” heeft betrekking op de publicatie van de SOC-richtlijnen. Op basis van bestaande richtlijnen zijn deze richtlijnen onder een nieuwe naam gepubliceerd.

Om een antwoord te kunnen formuleren op deze deelvraag is het van belang om verder de diepte in te gaan. Zoals eerder aangegeven zijn er veel richtlijnen met verschillende toepassingsgebieden. Om de toevoeging van SOC 2 vast te stellen zijn alleen vergelijkbare richtlijnen gekozen. Deze richtlijnen met hun toepassingsgebied zijn (tabel vijftien):

Richtlijn:	**Scope:**
NOREA Richtlijn 3000	Gericht op opdrachten waarin *geen* sprake is van beheersmaatregelen welke enige relatie hebben met de financiële verslaglegging. **(NBA, 2016)**
NOREA Richtlijn 3402	Gericht op opdrachten waarin sprake is van een *waarschijnlijke* relatie tussen beheersmaatregelen van uitbestede processen en financiële verslaglegging van een organisatie. **(NOREA, 2011)**
SOC 1	Gericht op opdrachten waarin sprake is van een *directe* relatie tussen beheersmaatregelen van uitbestede processen en financiële verslaglegging van een organisatie. **(AICPA, 2013)**

SOC 2	Gericht op het toetsen van controls welke in relatie staan tot de security, availability, processing integrity, confidentiality en privacy van een organisatie haar uitbestede processen. **(AIPCA, 2015)**
SOC 3	Gericht op het toetsen van controls welke in relatie staan tot de security, availability, processing integrity, confidentiality en privacy van een organisatie haar uitbestede processen. **(AIPCA, 2015)**
Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC-rapportmodel en de TSP Sectie 100	Gericht op het toetsen van controls welke in relatie staan tot de security, availability, processing integrity, confidentiality en privacy van een organisatie haar uitbestede processen. Ingericht op basis van het Amerikaanse SOC 2-rapportmodel en opgesteld conform Nederlandse wet- en regelgeving in plaats van Amerikaanse wet- en regelgeving. **(NOREA, 2016)**

tabel 15: relevante richtlijnen inclusief scoping

Zoals hierboven is weergegeven, hebben de verschillende richtlijnen een verschillende scoping. Het aanwezig zijn van een (directe) relatie, al dan niet met beheersmaatregelen die van invloed zijn op de financiële verslaglegging van een organisatie bepaalt voor een groot deel of er sprake is van een Richtlijn 3402 of een Richtlijn 3000. Hetzelfde geldt voor SOC 1 en SOC 2, waarbij een vergelijkbare scope is gesteld.

Zodoende is vastgesteld welke richtlijnen gekozen zijn, wat voor bereik deze richtlijnen hebben en hoe de best passende richtlijn gekozen kan worden. Vervolgens zal de toevoeging van SOC 2 worden vastgesteld. De toevoeging van SOC 2 op deze richtlijnen bestaat uit de volgende punten:

- Vereisten SOC 2 in combinatie met de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 (NOREA, 2016);
- Het wegnemen van toepassingsonduidelijkheid tussen de NOREA Richtlijnen 3000 en 3402
- Het stimuleren van eenduidigheid tussen audits;
- Internationale betrekkingen op het gebied van assurance standaardiseren.

Deze punten zijn individueel onderzocht. In deze paragraaf is enkel de samenvatting van de beantwoording opgenomen en niet de volledige onderbouwing. Deze is terug te vinden in bijlage vier.

Samenvatting
Er kan worden gesteld dat er momenteel meerdere assurancerichtlijnen in gebruik zijn. Afgezet tegen SOC 2 komen enkel de NOREA Richtlijnen 3000 en 3402 naar voren als relevante richtlijnen. Binnen deze richtlijnen zijn problemen onderkend zoals (een gebrek aan of over-)bekendheid, afwijkende normenrichtlijnen en onjuiste toepassing.

Zowel de NOREA Richtlijnen 3000 en 3402 als SOC 2 hebben vergelijkbare vereisten. SOC 2 zal op basis van de NOREA Richtlijn 3000 afgenomen worden. Dit levert geen problemen op zoals tegenstrijdige vereisten en ook geen verreikende nieuwe verplichtingen voor de auditor. Doordat beide verklaringen dezelfde vereisten hebben, is er ook een mogelijkheid om dezelfde markt te benutten.

Door de publicatie van de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 is er ook de mogelijkheid gekomen om een einde te maken aan de toepassingsonduidelijkheid tussen de NOREA Richtlijnen 3000 en 3402 (NOREA, 2016). Doordat SOC-richtlijnen een strakke scheiding in hun scope hanteren, wordt het eenvoudiger om een organisatie te plaatsen in een passende verklaring. Waar SOC 1 zich richt op controls met een directe relatie tot de financiële verslaglegging, richt SOC 2 zich op het toetsen van de TSP Sectie 100. Zodoende kan niet langer een verklaring worden afgegeven over financieel gerelateerde controls terwijl een richtlijn is gebruikt die hiervoor niet is gemaakt.

SOC 2 brengt nog een ander voordeel met zich mee: werken met een geïntegreerd normenkader brengt standaardisatie in de toepassing van SOC 2 teweeg. Zodoende heeft elke organisatie die een SOC 2-rapport heeft laten opleveren hetzelfde normenkader voor toetsing. Dit voorkomt onduidelijkheid en zorgt voor meer draagvlak voor de verklaring. Daarnaast zorgt dit ervoor dat het normenkader van SOC 2, de TSP Sectie 100, gedurende de levensloop van SOC 2 bijgewerkt zal worden om dekking te verlenen over relevante trends en dreigingen.

SOC 2 kan de toepassingsproblemen met de NOREA Richtlijnen 3000 en 3402 verhelpen, maar brengt nieuwe uitdagingen met zich mee op het gebied van internationale wetgeving. De verschillen tussen wetgevingen werpen barrières op voor een internationaal gestandaardiseerde assuranceverklaring met een geïntegreerd normenkader. Momenteel kan SOC 2 in Nederland worden gebruikt en in Amerika, maar wordt het toetsen op basis van Amerikaanse eisen afgeraden door deze verschillen. Hierdoor wordt een uitwisseling van de SOC 2-verklaring tussen Amerika en Nederland bemoeilijkt. Hierdoor raken enkele sterke punten van de richtlijn ook verloren, zoals het toetsen op het principle “Privacy”, het publiceren van logo’s en het afnemen van een SOC 2-verklaring op basis van Amerikaanse wet- en regelgeving, alsmede beroepsreglementen (dit wordt afgeraden, tenzij een organisatie zeker is dat zij voldoen aan de relevante eisen).

Afrondend kan worden gesteld dat SOC 2 een toevoeging is voor de Nederlandse assurancebranche. Het rapport brengt voordelen met zich mee met betrekking tot bestaande verklaringen, maar heeft ook nieuwe uitdagingen door een internationaal werkgebied en de verschillen in wet- en regelgeving die dit met zich mee brengt. Hierdoor gaan helaas enkele voordelige aspecten van het rapport verloren totdat een organisatie met zekerheid kan stellen te voldoen aan de Amerikaanse eisen.

6.2 DEELVRAAG 2

WAT ZIJN DE JURIDISCHE OVERWEGINGEN BIJ DE UITVOERING EN HET ONDERHOUD VAN SOC 2 VOOR ORGANISATIES?

Voor de beantwoording van deze onderzoeksvraag is gebruik gemaakt van de onderzoeksmethodieken zoals beschreven in hoofdstuk vier, tabel tien, elf en twaalf. Op basis van de geoperationaliseerde eenheden en variabelen is de beantwoording tot stand gekomen.

Inleiding
Zoals in de vorige vraag al kort beschreven is, heeft een SOC 2-rapport meerdere juridische overwegingen. Deze deelvraag gaat in op de juridische overwegingen die er zijn voor het uit laten voeren van een SOC 2-opdracht en hoe deze van invloed zijn op een SOC 2-rapport.

Onderzoek heeft aangetoond dat er de volgende overwegingen van toepassing zijn op een SOC 2-rapport. Dit zijn:

- Trademark;
- Plaatsing in de NOREA Richtlijn 3000;
- Verlies van toetsing op het gebied van privacy;
- Geldigheid van een rapportage;
- SOC 3.

Per punt is toegelicht wat de overweging is en wat dit betekent voor de organisatie danwel de SOC 2-rapportage. Wederom is in deze paragraaf enkel de samenvatting opgenomen en wordt voor de volledige onderbouwing verwezen naar bijlage vijf.

Samenvatting
Er zijn meerdere overwegingen voor het starten, begeleiden en afronden van een SOC 2. De publicatie van de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 draagt bij aan het verminderen van het effect van deze overwegingen, maar kan ze niet volledig wegnemen en presenteert tegelijkertijd nieuwe uitdagingen (NOREA, 2016).

Het trademark van het AICPA is geen obstakel voor het uitvoeren van een SOC 2-opdracht in Nederland, mits dit gebeurt op basis van de NOREA Guidance to Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 (NOREA, 2016). Er kan geen gebruik worden gemaakt van materiaal waarop het AIPCA zijn trademark heeft gelegd, zonder dat hier kosten aan verbonden zijn (licensing) of gelieerd te zijn aan het AICPA als CPA.

Doordat de NOREA het rapportmodel van SOC 2 heeft geplaatst in de NOREA Richtlijn 3000 kan er worden gewerkt volgens de SOC 2-rapportagemethodiek zonder dat trademark hier verder van invloed is. De plaatsing in een Nederlandse richtlijn betekent wel dat de rapportage opgesteld is op basis van Nederlandse wet- en regelgeving en zodoende niet per definitie voldoet aan de Amerikaanse eisen. Voordat een SOC 2-rapport op basis van de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 aangemerkt kan worden als een rapport dat in lijn is met Amerikaanse vereisten, moet hier grondig onderzoek naar worden gepleegd (NOREA, 2016). Grotere accountancykantoren zullen hier wel aan voldoen doordat zij internationaal opereren en al CPA's in dienst hebben.

De verschillen in wet- en regelgeving hebben ook als gevolg dat er in Nederland niet getoetst kan worden op het “Privacy” principle. De Amerikaanse en Nederlandse definitie van privacy verschillen enorm, maar ook de wijze van dataclassificatie is niet hetzelfde. Hierdoor zou in de toepassing een verschil ontstaan. Een Nederlandse toetsing op privacy zou niet hetzelfde zijn voor een Amerikaan en vice versa. De kloof tussen de wet- en regelgeving is groot en wordt de komende tijd alleen groter door o.a. de nieuwe Europese Privacy Verordening. Op basis hiervan is gekozen door de NOREA om “Privacy” niet mee te nemen in de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 (NOREA, 2016). Zodoende is ook voor het onderzoek besloten om “Privacy” buiten scope te plaatsen.

Een voordeel van de SOC 2-rapportage is dat deze onbeperkt geldig is. Een organisatie kan zijn SOC 2-rapportage jaren lang geldig laten zijn, mits zij relevante systeemwijzigingen (changes) hebben benoemd in de rapportage. De gebruikersorganisatie is verantwoordelijk voor het aanmerken van de relevantie van een change, om zo de objectiviteit te bewaren. Indien deze changes benoemd zijn kan een organisatie zijn SOC 2-rapportage theoretisch onbeperkt geldig laten zijn. Echter kan een klantorganisatie wel uiten dat er geen vertrouwen meer is in de SOC 2-rapportage, doordat er bijvoorbeeld lange tijd audit heeft plaatsgevonden. In dit geval is de serviceorganisatie verantwoordelijk voor het herauditen van SOC 2. Tijdens dit proces kan het management een bridge letter afgeven richting klanten om kenbaar te maken dat er ontwikkelingen gaande zijn en assurance bewaakt wordt. Als een organisatie zijn changes niet benoemt, of niet kan benoemen vervalt de SOC 2-raportage nadat de eerste niet-benoemde change heeft plaatsgevonden. Voor organisaties is het dus van belang een change kalender te hebben welke ook nageleefd wordt.

Nadat een organisatie een SOC 2-rapportage op heeft laten leveren kan een organisatie een SOC 3-opdracht starten. SOC 3 heeft ten opzichte van SOC 2 een publicitaire meerwaarde doordat er geen gebruikerskring is: de rapportage is vrij te verspreiden. Meestal wordt deze op een website geplaatst voor bezoekers van de website. SOC 3 levert geen details over de audit maar benoemt kort welke principles getoetst zijn en of er voldaan is aan de principles. Er zijn geen systeembeschrijving of testresultaten opgenomen een SOC 3. SOC 3 levert volgens de Amerikaanse richtlijn een zegel op, op te vragen bij het AICPA. In de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 komt dit te vervallen doordat er niet volgens Amerikaanse wet- en regelgeving alsmede beroepsreglementen wordt gewerkt (NOREA, 2016). Dit betekent dat er geen zegel kan worden afgegeven aan NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100-rapporten (NOREA, 2016).

Afrondend kan worden gesteld dat SOC 2 meerdere overwegingen heeft op juridisch vlak. Doordat er grote verschillen zijn in de wet- en regelgeving ziet de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 er niet hetzelfde uit als de Amerikaanse SOC 2-richtlijn (NOREA, 2016). Hierdoor gaan enkele elementen zoals een zegel en toetsing over privacy verloren, maar is er wel zekerheid dat er conform Nederlandse wet- en regelgeving wordt gehandeld.

6.3 DEELVRAAG 3

WELKE CRITERIA ZIJN VAN BELANG VOOR ORGANISATIES OM EEN SOC 2-OPDRACHT TE STARTEN?

Voor de beantwoording van deze onderzoeksvraag is gebruik gemaakt van de onderzoeksmethodieken zoals beschreven in hoofdstuk vier, tabel elf en twaalf. Op basis van de geoperationaliseerde eenheden en variabelen is de beantwoording tot stand gekomen.

Inleiding
Waar de vorige deelvragen uitgebreid onderzocht hebben wat SOC 2 is en wat de overwegingen van een SOC 2-rapport zijn, gaat deze deelvraag in op de redenen die een organisatie heeft om een SOC 2-opdracht ten uitvoer te laten brengen.

Op basis van de vergaarde informatie in hoofdstuk vijf en de gespreksverslagen in bijlagen één tot en met drie is een selectie gemaakt van de criteria welke voor organisaties van belang zijn om te starten met een SOC 2-opdracht. De volgende criteria zijn geformuleerd:

- Aantoonbare meerwaarde richting gebruikersorganisaties;
- De NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 is bij gebruikers- en serviceorganisaties bekend;
- Duidelijkheid in de toepassing van SOC 2 en de TSP Sectie 100;
- Duidelijkheid met betrekking tot de internationale geldigheid van een SOC 2-rapport;
- Vereenvoudiging in het assuranceproces;
- Klantwens of eigen initiatief;
- Organische groei van SOC 2 en de TSP Sectie 100.

Bovenstaande punten zijn individueel uiteengezet in bijlage drie.

Samenvatting
Er zijn meerdere criteria voor organisaties waaraan voldaan moet worden voordat er gestart wordt met een SOC 2-opdracht. SOC 2 voldoet momenteel maar aan één van deze criteria: SOC 2 kan vereenvoudiging brengen. De NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 is echter niet bekend en kan zijn meerwaarde niet aantonen. Daarnaast kan de TSP Sectie 100 een uitdaging zijn door de abstractie van de normen. Deze staan open voor interpretatie en het is van belang dat er afstemming tussen de auditor en de serviceorganisatie plaatsvindt voordat er geaudit wordt. Ook de geldigheid van de rapportage op internationaal vlak dient verder onderzocht te worden om inzichtelijk te krijgen waar een organisatie aan moet voldoen voordat de SOC 2-rapportage internationaal geldig is.

Op basis hiervan kan worden gesteld dat er niet wordt voldaan aan de criteria die organisaties stellen. Indien SOC 2 wel voldoet aan deze criteria, zal deze eerder geadopteerd worden. Wanneer SOC 2 deze criteria niet kan vervullen blijft de kans op adoptie laag. Om de kans op adoptie te verhogen is het van belang dat er onderzoek plaatsvindt naar de Amerikaanse eisen en hoe de TSP Sectie 100 juist geïnterpreteerd dient te worden. Tegelijkertijd dient de NOREA bekendheid van de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 te vergroten en de meerwaarde aantoonbaar te maken (door bijvoorbeeld kennissessies, whitepapers of andere maatregelen). Afrondend dient er zorg gedragen te worden voor de doorontwikkeling van de TSP Sectie 100.

Als kanttekening moet er worden gesteld dat nog niet inzichtelijk is vanuit welk perspectief de meeste SOC 2-opdrachten zullen voortkomen, namelijk de klant of de organisatie zelf. Bekendheid van SOC 2 is relevant voor het klantperspectief, waar voor de organisatie SOC 2 als middel voor organisatieontwikkeling kan worden gepositioneerd. Dit dient verder onderzocht te worden.

6.4 DEELVRAAG 4

WAT ONDERSTEUNT DE SUCCESVOLLE UITVOERING VAN EEN SOC 2-OPDRACHT?

Voor de beantwoording van deze onderzoeksvraag is gebruik gemaakt van de onderzoeksmethodieken zoals beschreven in hoofdstuk vier, tabel elf, twaalf en dertien. Op basis van de geoperationaliseerde eenheden en variabelen is de beantwoording tot stand gekomen.

Inleiding
In deze deelvraag zal een overzicht worden gemaakt van de ondersteunende voorwaarden voor een succesvolle uitvoering van een SOC 2-opdracht. Uit de voorgaande deelvragen zijn randvoorwaarden naar voren gekomen om een SOC 2-opdracht succesvol uit te laten voeren. Waar de audit volgens hetzelfde proces gaat als bijvoorbeeld een NOREA Richtlijn 3402-audit, zijn er echter wel enkele aspecten bij een SOC 2-audit welke invloed hebben op het (succesvolle) verloop van de opdracht.

Deze randvoorwaarden geven aan wanneer organisaties zouden starten met een SOC 2-opdracht, wat gebruikt kan worden om adoptie te stimuleren. De randvoorwaarden zijn gebaseerd op invloeden die bepalen wanneer het aannemelijk zou zijn dat organisaties zouden met SOC 2-opdrachten.

De volgende randvoorwaarden worden onderkend voor de succesvolle uitvoering van een SOC 2-opdracht:

- Afstemming met de auditor;
- Kennis over SOC 2 bij zowel auditors als klanten;
- Het inrichten van een audit trail dat voldoet voor een SOC 2-audit;
- Draagvlak met betrekking tot assurance;
- Gebruikersorganisaties dienen mee te groeien met ontwikkelingen op het gebied van assurance;
- Ondersteuning vanuit de NOREA;
- Afnemen van een nulmeting;
- Duidelijkheid over mogelijke aanpassingen op de bedrijfsvoering;
- Het leervermogen van de organisatie wordt gestimuleerd.

Een internationaal geaccepteerde SOC 2-rapportage kent er de volgende randvoorwaarden:

- Kennis van de toepasselijke wet- en regelgeving;
- Een CPA ondertekent de rapportage.

Bovenstaande punten zijn individueel uiteengezet. Deze paragraaf bevat enkel de samenvatting, voor de onderbouwing wordt verwezen naar bijlage zeven.

Samenvatting
Er zijn meerdere randvoorwaarden welke van belang zijn voor het uitvoeren van een SOC 2-opdracht. De auditor en serviceorganisatie dienen uitgebreid af te stemmen wat de scope is, of er controls zijn die niet relevant en wat een juiste interpretatie van de normen van de TSP Sectie 100 is. Dit hangt nauw samen met de benodigde kennis over SOC 2 voor klanten en auditors. Zonder deze kennis kan de afstemming niet plaatsvinden op een wijze die de audit ten goede komt. De NOREA dient hierin een leidende rol aan te nemen door materiaal en informatie beschikbaar te stellen en auditors te informeren over ontwikkelingen. Tevens kan een nulmeting veel verrassingen voorkomen en wordt het afnemen hiervan ook geadviseerd.

Klanten dienen echter ook mee te groeien in de ontwikkelingen op het gebied van assurance. Als gebruikersorganisaties vast blijven houden aan rapportages op basis van de NOREA Richtlijn 3402 is de kans klein dat er geaccepteerd wordt dat hun serviceorganisatie een SOC 2-rapport laat publiceren.
Alle betrokken organisaties dienen draagvlak te hebben voor assurance, maar vooral de serviceorganisatie dient dit draagvlak te hebben. De audit is stringent en brengt vooral de eerste keer uitdagingen met zich mee, zoals het audit trail en de interpretatie van de normen. Zonder dit draagvlak en een stimulatie van het leervermogen van de organisatie is de kans klein dat de organisatie zich opnieuw zou laten auditen volgens SOC 2. Indien aanpassingen aan de bedrijfsvoering noodzakelijk zijn door nieuwe controls dient dit duidelijk te zijn zodat de organisatie zich hier tijdig op kan aanpassen.

Afrondend kan worden gesteld dat communicatie van groot belang is voor het uitvoeren van een SOC 2-opdracht en dat zowel auditor als de serviceorganisatie een gedeelde verantwoordelijkheid hebben in het succesvolle verloop ervan. Zonder samenwerking is de kans op succes laag.

6.5 PROBLEEMSTELLING

Welk type organisatie heeft baat bij een SOC 2-rapportage en hoe kan de SOC 2-richtlijn het meest effectief geïmplementeerd en/of getoetst worden, op basis van welke uitvoeringscriteria en leidt dit tot een algemeen toepasbare oplossing?

In deze paragraaf zal de probleemstelling van het onderzoek “SOC 2: toepassing en uitvoering” beantwoord worden. De probleemstelling zal per onderdeel van de stelling uiteen worden gezet om vervolgens tot een samenvatting en beantwoording te komen. De volgende onderdelen worden hierin onderkend:

- Welk type organisatie heeft baat bij een SOC 2-rapportage;
- Hoe kan de SOC 2-richtlijn het meest effectief geïmplementeerd en/of getoetst worden;
- Welke uitvoeringscriteria zijn relevant;
- Leidt dit tot een algemeen toepasbare oplossing?

In deze paragraaf wordt enkel de samenvatting en beantwoording beschreven. Onderbouwing van de samenvatting is opgenomen in bijlage acht.

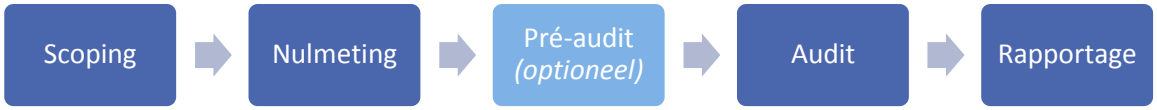
Samenvatting
De SOC 2-richtlijn en uitvoering ervan, zowel de Amerikaanse als de Nederlandse publicatie, is niet voor elke organisatie een reële mogelijkheid. Voordat er gestart kan worden met een opdracht moet duidelijk zijn wat de organisatie wil bereiken met de rapportage, welke scope wordt aangehouden en hoe dit de rapportage beïnvloedt, etc. Het starten van de opdracht brengt veel overwegingen met zich mee die directe invloed hebben op (de kwaliteit van) de uitvoering.

Het type organisatie dat baat heeft bij SOC 2 zijn grotere organisaties die intensief klantcontact hebben met partijen die ieder een normenkader voorschrijven. Voorbeelden van organisaties die baat zouden hebben bij SOC 2-rapporten zijn datacenters, telecombedrijven of internationaal georiënteerde organisaties. Door het complexe assurancelandschap dat ontstaat door alle normenkaders is er een sterke wens voor vereenvoudiging, wat SOC 2 kan bieden door het vastgestelde normenkader. Interne ontwikkeling en groei zijn pijlers van de organisatiefilosofie. Men ziet in dat assurance ten positieve bijdraagt aan de bedrijfsvoering en proceskwaliteit. Bovenal zijn vereenvoudiging, verbetering en (internationale) groei herkenbare signalen bij organisaties die SOC 2 zouden kunnen toepassen.

Tijdens het onderzoek zijn ook enkele best practices naar voren gekomen. Deze best practices kunnen organisaties helpen bij het uit laten voeren van een SOC 2-opdracht en auditors helpen om de theorie van SOC 2 effectief toe te kunnen passen. Wat betreft deze best practices wordt geadviseerd deze te volgen en verder te ontwikkelen. Deze best practices betreffen:

- Afstemming tussen klant en auditor;
- Het uitvoeren van een nulmeting;
- Betrokken partijen zijn bekend met de SOC 2-richtlijn;
- Het inrichten van een audit trail voor SOC 2;
- Werkwijze conform de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100;
- Ondertekening door een CPA (indien een internationaal geldige SOC 2-rapportage is gewenst);
- Betrokken partijen zijn bekend met de juridische overwegingen van een SOC 2-rapportage.

Dit uit zich in de volgende implementatieaanpak zoals weergegeven in figuur dertien:



figuur 13: SOC 2-implementatieaanpak

Tijdens de scoping worden de te toetsen principles vastgesteld en de afstemming met de organisatie gezocht voor de interpretatie van de normen. Zodra de afstemming en scoping afgerond is, wordt een nulmeting afgerond om inzicht in de stand van zaken te scheppen voor auditor en organisatie. Op basis van (mogelijke) bevindingen kan gekozen worden voor het nodige tijdsbestek voor herstelwerkzaamheden. Indien gewenst kan er een pré-audit plaatsvinden, bijvoorbeeld door een ander adviesbureau om de objectiviteit of voorbereiding te optimaliseren. De volgende stap is het afnemen van de daadwerkelijke audit om vervolgens een concept rapportage op te leveren ter afstemming. Na afstemming wordt de rapportage definitief ondertekend en overlegd.

Ook zijn tijdens het onderzoek uitvoeringscriteria in kaart gebracht: de criteria die bepalen wanneer een organisatie naar verwachting zou starten met het uit laten voeren van een SOC 2-opdracht en welke invloeden hierop onderkend worden. Deze criteria helpen organisaties bij het starten van een opdracht, geven inzicht in de ontwikkeling van de markt en sturen op ondersteuning voor de uitvoering. Deze criteria zijn:

- Afstemming met de auditor;
- Kennis over SOC 2 bij zowel auditors als klanten;
- Het inrichten van een audit trail dat voldoet voor een SOC 2-audit;
- Draagvlak met betrekking tot assurance;
- Gebruikersorganisaties dienen mee te groeien met ontwikkelingen op het gebied van assurance;
- Ondersteuning vanuit de NOREA;
- Afnemen van een nulmeting;
- Duidelijkheid over mogelijke aanpassingen op de bedrijfsvoering;
- Het leervermogen van de organisatie wordt gestimuleerd.

Deelvraag vier gaat uitgebreid in op deze criteria. Onderbouwing per criterium is te vinden in paragraaf 6.4. Deze criteria geven aan wanneer organisaties zouden starten met een SOC 2-opdracht, wat de adoptie ten goede zou komen. De criteria zijn gebaseerd op invloeden die bepalen wanneer het aannemelijk zou zijn dat organisaties starten met SOC 2-opdrachten. Zoals uit de opsomming blijkt, is er vooral meer kennis en ondersteuning nodig voordat een organisatie een SOC 2-opdracht gunt aan een externe partij. Men is niet bekend met de materie en zal niet starten totdat de toevoeging en meerwaarde op de bedrijfsvoering bekend zijn. Indien deze ondersteuning en kennis wel beschikbaar zijn, in combinatie met ondersteuning en kennisdeling vanuit de NOREA, is de verwachting dat dit proces versneld kan worden.

Door de flexibiliteit in de toepassing van SOC 2 is er sprake van een algemeen toepasbare oplossing. Opdrachten kunnen verschillen, zoals in de scope, maar dit levert geen situaties op waar dit ten koste zou gaan van de flexibiliteit van het assuranceproduct SOC 2. De scope is veranderlijk maar de rest van het proces staat vast: er is een standaard werkwijze, normenkader en rapportagemodel wat uiteindelijk een gestandaardiseerde rapportage oplevert.

Dit is ook de kracht van SOC 2 (zowel de Amerikaans en Nederlandse publicatie): standaardisatie wordt gestimuleerd door de oplevering van rapportages gebaseerd op dezelfde normenkaders volgens dezelfde richtlijnen. Door de verschillen in wet- en regelgeving kan dit helaas niet volledig tot uiting komen.

Beantwoording
In conclusie kan het volgende worden gesteld: er is geen duidelijk organisatietype dat baat heeft bij SOC 2, maar er is meer sprake van een wens voor verbetering, vereenvoudiging en/of standaardisatie bij organisaties die baat zouden kunnen hebben bij SOC 2. De SOC 2-richtlijn kan hieraan bijdragen door een effectieve implementatie op basis van enkele best practices, zoals afstemming met de auditor. Het is noodzakelijk voor organisaties dat er (in enige mate) voldaan wordt aan de uitvoeringscriteria omdat deze de marktontwikkelingen weerspiegelen met betrekking tot de adoptie van SOC 2. Zolang hier niet of nauwelijks aan wordt voldaan, zullen organisaties niet overstappen op een SOC 2-rapport. Er is wel sprake van een algemeen toepasbare oplossing (waarin enkel de scope verandert) wat als eindproduct een gestandaardiseerd assurancerapport oplevert.

SOC 2 kan de Nederlandse assurancemarkt helpen ontwikkelen, maar van belang hierbij is dat de markt meegroeit. Momenteel is het kennisniveau over assurance niet voldoende wat de onjuiste toepassing van assurancerapporten onderhoudt. Indien de markt gestimuleerd kan worden om kennis te nemen van SOC 2 stijgt de kans dat SOC 2 binnen Nederlandse organisaties toegepast wordt. Er is geen sprake van een onbruikbaar assuranceproduct, maar wel sprake van een onvolwassen markt op het gebied van assurance.

HOOFDSTUK 7 CONCLUSIE EN AANBEVELINGEN

In dit hoofdstuk zijn de conclusie en aanbevelingen opgenomen met betrekking tot het afstudeeronderzoek “SOC 2: toepassing en uitvoering”. Dit hoofdstuk bevat een samenvatting van het onderzoek, een conclusie, een selectie van aanbevelingen en een discussie.

7.1 SAMENVATTING

De onderzoeksopdracht is aangereikt door AuditConnect B.V. Het interne doel van het onderzoek is het inzichtelijk krijgen van de toepasbaarheid van het SOC 2-assurancerapport en een weerspiegeling te geven van de uitvoering van een SOC 2-opdracht. Het externe doel van het onderzoek is het ontwikkelen van een implementatieaanpak voor een SOC 2-opdracht. De aanleiding voor het onderzoek komt voort uit ontwikkelingen in de IT- en auditbranche. Door een hoge ontwikkelsnelheid en een stijgende mate van procesuitbesteding is de vraag ontstaan hoe het beste assurance kan worden verkregen over de beheersing van uitbestede IT-processen. Veel bedrijven besteden processen uit en dit zal blijven stijgen (figuur negentien). Bestaande assuranceverklaringen trachten de juiste mate van assurance af te geven over uitbestede processen, maar dit past niet altijd binnen de scope van de verklaring. assurance wordt soms ten onrechte afgegeven door een verkeerde toepassing van een richtlijn, zoals onderkend wordt met betrekking tot de NOREA Richtlijn 3402.

Niet alleen de IT ontwikkelt zich; ook assurance ontwikkelt zich. Dit heeft als resultaat dat in 2011 Amerika de SOC-richtlijnen gepubliceerd heeft. Deze richtlijnen zijn gebaseerd op oudere assuranceproducten zoals SAS 70 en de ISAE 3000 en 3402, maar vernieuwd om huidige IT-omgevingen weerbaar te maken tegen hedendaagse dreigingen. De NOREA heeft hiervan een Nederlandse versie gepubliceerd: de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100. Deze handreiking beschrijft hoe een IT-auditor een SOC 2-opdracht kan uitvoeren conform met Nederlandse wet- en regelgeving en de beroepsreglementen van een IT-auditor.

SOC 2 is een assurancerapport dat toetst op basis van de TSP Sectie 100. SOC 2 levert het rapportmodel, op basis waarvan de rapportage opgeleverd dient te worden. Dit model ziet er als volgt uit:

- Sectie I: Vermelding van het management;
- Sectie II: Assurancerapport van de onafhankelijke auditor;
- Sectie III: Beschrijving van het systeem door de serviceorganisatie;
- 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.

De serviceorganisatie is verantwoordelijk voor het aanleveren van Sectie I, Sectie III en Sectie V. De auditor is verantwoordelijk voor Sectie II en Sectie IV. Sectie II bevat het rapport van de auditor en Sectie IV bevat de onderbouwing met testresultaten.

De toetsing geschiedt op basis van de TSP Sectie 100 die vijf principles aanreikt voor toetsing. Deze principles zijn: Security, Availability, Processing Integrity, Confidentiality en Privacy. Organisaties kunnen één of meerdere principles kiezen voor toetsing om zo een flexibele scoping mogelijk te maken. Per principle zijn er relatief abstracte controls geformuleerd. Het is aan de organisatie om beheersmaatregelen te implementeren (indien dit nog niet plaats heeft gevonden) om te voldoen aan deze controls.

Op basis van de controls en geïmplementeerde beheersmaatregelen zal de auditor vervolgens de organisatie toetsen op de naleving van de controls en of er voldaan wordt aan de normen. Het abstractieniveau van deze controls kan het inschatten van de juiste maatregelen bemoeilijken doordat er ruimte voor interpretatie is. Na afronding van de toetsing wordt de rapportage afgestemd met de serviceorganisatie om vervolgens de rapportage definitief op te leveren.

SOC 2 kan voor de assurancebranche een stimulans zijn voor standaardisatie en vereenvoudiging. Het normenkader, de TSP Sectie 100, is gekoppeld aan SOC 2 waardoor er niet van afgeweken kan worden. Dit betekent ook dat het auditen gebeurt op basis van dezelfde normen, wat tot op heden niet altijd gebeurt doordat organisaties eigen ontwikkelde normenkaders mogen hanteren in bestaande assurancerapporten. Tevens zijn de internationale mogelijkheden van een SOC 2-rapport kansen voor de markt: het rapport is in Amerika geaccepteerd en wordt veel opgevraagd, dus voor organisaties met internationale klanten of ambities is een SOC 2-rapport daardoor een manier om internationaal sneller tot afstemming te komen tussen betrokken partijen. Door de grote verschillen in wet- en regelgeving gaat deze stap in standaardisatie deels verloren omdat de Nederlandse publicatie af moet wijken van de Amerikaanse publicatie om in lijn te blijven met Nederlandse wet- en regelgeving.

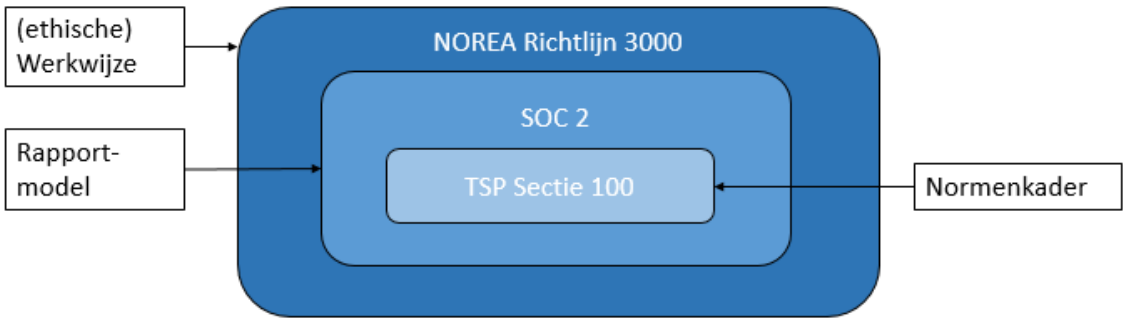
Meerdere richtlijnen zijn als relevant bestempeld voor het onderzoek:

- ISAE 3000 op basis van de herziene NBA Standaard 3000 en NOREA Richtlijn 3000 (NBA, 2016) (NOREA, 2009);
- ISAE 3402 op basis van de NOREA Richtlijn 3402 (NOREA, 2011);
- SOC 1, 2 en 3 (AICPA, 2013) (AIPCA, 2015);
- NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 (NOREA, 2016).

De toevoeging van SOC 2 op deze richtlijnen bestaat uit enkele punten, zoals het stimuleren van eenduidigheid, het voorkomen van toepassingsonduidelijkheid en het standaardiseren van internationale betrekkingen op het gebied van assurance. SOC 2 kan dit bewerkstelligen doordat er een vastgesteld normenkader is. Men wordt gedwongen de TSP Sectie 100 te gebruiken omdat er anders niet conform SOC 2 is gewerkt. Dit stimuleert de eenduidigheid tussen auditresultaten en organisaties, maar het stuurt ook op internationale standaardisatie van assurancerapporten. Dit ondersteunt internationale relaties doordat rapportages niet vertaald hoeven te worden en normenkaders één-op-één overeenkomen. Dit was voorheen niet mogelijk doordat er geen specifieke normenkaders verplicht werden gesteld in de ISAE/NOREA Richtlijn 3000 of 3402. Doordat SOC 1, 2 en 3 een strakke scheiding hebben in hun scope is de kans op toepassingsonduidelijkheid zoals aanwezig is bij de NOREA Richtlijn 3000 en 3402 sterk verkleind. SOC 2 mag niet gebruikt worden voor rapporten die een uitspraak doen over beheersmaatregelen die in relatie staan tot de financiële verslaglegging, enkel over de vijf eerder genoemde principles en hoe de beheersmaatregelen presteren.

Het IP van SOC 2 ligt bij het AIPCA. Als ontwikkelaar van deze richtlijn beheert het AICPA de evolutie en wijziging van de richtlijn. Gezien het AICPA gevestigd is in Amerika, is SOC 2 gebaseerd op Amerikaanse wet- en regelgeving. Dit brengt enkele overwegingen met zich mee voor een SOC 2-rapport gebaseerd op de Nederlandse handreiking van de NOREA. Privacy kan niet worden getoetst door te grote verschillen in de wet- en regelgeving en er kunnen geen zegels worden afgegeven door het AICPA, doordat er niet met de Amerikaanse richtlijn wordt gewerkt. Wanneer er wel met de Amerikaanse richtlijn wordt gewerkt kan dit wel. Het kost echter tijd om te onderzoeken wat nodig is om te voldoen aan de eisen voor een Amerikaanse SOC 2-rapportage.

Door het trademark mag de Nederlandse publicatie geen standaard SOC-rapport zijn: hiervoor is een andere constructie ontworpen zodat er wel met de SOC 2-richtlijn kan worden gewerkt, maar dat er geen inbreuk op het IP van het AICPA plaatsvindt. Door SOC 2 te plaatsen in de NOREA Richtlijn 3000 is dit mogelijk gemaakt. Dit ziet er als volgt uit (figuur veertien):



figuur 14: vormgeving SOC 2-rapport conform de NOREA Guidance to Richtlijn (ISAE) 3000 Service Organisation Control Reports for IT Organisations Based on the AICPA SOC 2 Report Model and the Trust Services Principles and Criteria

Tevens dient een Nederlandse SOC 2-rapportage ondertekend te worden door een RE-geregistreerde IT-auditor. Een Amerikaanse SOC 2-rapportage moet door een CPA ondertekend worden.

Voor organisaties levert het voordelen op om assurance door SOC 2 af te laten geven. Het interview met InterXion in bijlage één benadrukt voordelen zoals efficiency, tijdsbesparing en een scherpstelling op de dagelijkse operatie door TSP Sectie 100 controls. Daarentegen zijn er ook factoren die SOC 2 complex maken, zoals de abstractie van de TSP Sectie 100 normen en trademarking vanuit het AICPA. Uit onderzoek zijn de volgende criteria naar voren gekomen die bepalen of organisaties willen en kunnen gaan starten met een SOC 2-opdracht:

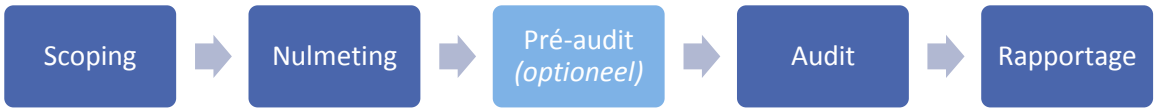
- Aantoonbare meerwaarde richting gebruikersorganisaties;
- De NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 is bij gebruikers- en serviceorganisaties bekend;
- Duidelijkheid in de toepassing van SOC 2 en de TSP Sectie 100;
- Duidelijkheid met betrekking tot de internationale geldigheid van een SOC 2-rapport;
- Vereenvoudiging in het assuranceproces;
- Klantwens of eigen initiatief;
- Organische groei van SOC 2 en de TSP Sectie 100.

Momenteel is het marktanimo voor SOC 2 laag en de kans op adoptie klein. Het rapport is niet bekend bij auditors en (mogelijke) klanten, waardoor de rapportage niet opgevraagd zal worden. Service- en gebruikersorganisaties zijn onvolwassen en niet bekend op het gebied van assurance: men levert over het algemeen een ISAE/NOREA Richtlijn 3402 op omdat dit vereist is voor de jaarrekeningcontrole van een gebruikersorganisatie. Dit geeft niet per definitie de gewenste mate van assurance over uitbestede processen die niet gerelateerd zijn aan de financiële verslaglegging. Ook is vaak contractueel bepaald wat voor assurancerapport opgeleverd dient te worden. De NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 is niet dwingend opgelegd (het is een handreiking en geen richtlijn), waardoor auditors zelf kunnen bepalen of zij hier kansen in zien. Zolang niet voldaan wordt aan bovenstaande criteria voor een organisatie, zal er niet gekozen worden voor een SOC 2-opdracht. Hierin kan de NOREA een actieve rol gaan spelen door promotie, studie en ontwikkeling en verder onderzoek naar de mogelijkheid van een internationale SOC 2.

Voor het effectief ten uitvoer brengen van een SOC 2-opdracht zijn enkele best practices opgesteld op basis van het onderzoek. Op basis van vragen van service- en gebruikersorganisaties en onderzoek naar implementatietrajecten zijn de volgende best practices geformuleerd:

- Afstemming met de auditor;
- Kennis over SOC 2 bij zowel auditors als klanten;
- Het inrichten van een audit trail dat voldoet voor een SOC 2-audit;
- Draagvlak met betrekking tot assurance;
- Gebruikersorganisaties dienen mee te groeien met ontwikkelingen op het gebied van assurance;
- Ondersteuning vanuit de NOREA;
- Afnemen van een nulmeting;
- Duidelijkheid over mogelijke aanpassingen op de bedrijfsvoering;
- Het leervermogen van de organisatie wordt gestimuleerd.

SOC 2-opdrachten kunnen volgens het proces in figuur vijftien uitgevoerd worden.



figuur 15: SOC 2-implementatieaanpak

Door de aanpak in figuur vijftien te volgen kunnen de eerder genoemde practices verwerkt worden in het proces, zoals de afstemming en de nulmeting.

SOC 2 biedt wel een flexibele, algemeen toepasbare methodiek wat een voordeel is. Door de aangegeven criteria, ondersteunende voorwaarden en de implementatieaanpak kan er in elke organisatie die een mate van uitbestede IT bezit conform de eisen van de TPS Sectie 100 een SOC 2-opdracht ten uitvoer worden gebracht.

SOC 2 is als assurancerapportage een bruikbaar stelsel in combinatie met de TSP Sectie 100 en de NOREA Richtlijn 3000. Door de samenwerking tussen deze richtlijnen is het mogelijk om SOC 2 in Nederland te implementeren zonder dat hiervoor trademarks overtreden worden.

7.2 CONCLUSIE

Zoals in de samenvatting uitgebreid beschreven is biedt SOC 2 kansen voor de assurancebranche en het kennisniveau van auditors en organisaties. De praktijk wijst echter uit dat het bewustzijn te laag is om op dit moment gebruik te kunnen maken van de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100. De vraagzijde van de markt is nog niet volwassen genoeg om over te stappen op een nieuwe assuranceverklaring: men houdt vast aan de ISAE/NOREA Richtlijn 3402 en ziet geen noodzaak om over te stappen. Dit geldt ook voor accountants waardoor het (onterechte) gebruik van deze rapportage in stand gehouden wordt. Er is meer onderzoek nodig naar de eisen voor een Amerikaanse SOC 2-rapportage alsmede de toetsing van privacy op basis van Nederlandse wet- en regelgeving.

In conclusie kan het volgende worden gesteld: er is geen duidelijk organisatietype dat baat heeft bij SOC 2, maar er is eerder sprake van een wens voor verbetering, vereenvoudiging en/of standaardisatie. De SOC 2-richtlijn kan hieraan bijdragen door een effectieve implementatie op basis van enkele best practices, zoals afstemming met de auditor of het afnemen van een nulmeting. Noodzakelijk is het echter dat organisaties (in enige mate) voldoen aan de uitvoeringscriteria omdat deze de marktontwikkelingen weerspiegelen. Zolang hier niet of nauwelijks aan voldaan wordt, zullen organisaties niet overstappen op een SOC 2-rapport. Er is wel sprake van een algemeen toepasbare oplossing (waarin enkel de scope verandert) wat als eindproduct een gestandaardiseerd assurancerapport oplevert.

Naar verwachting zal de Nederlandse markt over enkele jaren pas klaar zijn voor de toepassing van SOC 2. SOC 2 kan nu al overal uitgevoerd worden maar door een gebrek aan kennis bij organisaties en auditors zou een SOC 2-rapportage nu niet geaccepteerd worden als een geldige rapportage. Voordat dit wijzigt moet SOC 2 meer bekendheid verwerven en een reputatie als betrouwbare en doeltreffende assuranceverklaring opbouwen. Voor nu kan worden gesteld dat de Nederlandse markt niet volwassen genoeg is om de overstap te maken naar de volgende generatie assurancerapporten.

7.3 AANBEVELINGEN

In deze afrondende paragraaf zijn enkele aanbevelingen geformuleerd voor AuditConnect B.V. en IT-auditors belast met het uitvoeren van SOC 2-opdrachten. Zoals beschreven is de markt nog niet klaar voor de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 en de toepassing ervan. Het onderzoek heeft wel zijn doel kunnen behalen: de toevoeging van SOC 2 is onderzocht en de meest effectieve manier van implementatie is bepaald.

De volgende aanbevelingen zijn geformuleerd:

- Stimuleer het gebruik van de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 door het aanbieden van kennissessies aan klanten, auditors en geïnteresseerden;
- Verder onderzoek is nodig naar de Amerikaanse eisen en de invulling ervan om internationaal geaccepteerde SOC 2 -rapporten te publiceren. Het aanbieden van rapportages die voldoen aan de Amerikaanse eisen is een sterk marketing tool;
- Verder onderzoek is nodig om een concreet organisatieprofiel vast te stellen. Het huidige profiel kon wegens tijdsgebrek en beschikbare informatie niet gekoppeld worden aan managementmodellen. Voor een accuraat profiel wordt nader onderzoek geadviseerd;
- Verder onderzoek is nodig naar de rol die de NOREA kan spelen in het promoten van dan wel het bijdragen aan een internationaal SOC 2-rapport waarop geen trademarks rusten die de effectiviteit van de rapportage verminderen;
- Het ontwikkelde materiaal zoals de aanpak en het werkprogramma dienen mee te ontwikkelen met (mogelijke) wijzigingen aan de TSP Sectie 100 en SOC 2;
- Het is aan te raden personeel bekend te maken met de TSP Sectie 100 en SOC 2, de uitvoering hiervan en de beschikbare middelen;
- De eerste SOC 2-opdrachten en audits kunnen moeizaam verlopen doordat er minder ervaring beschikbaar is op het gebied van SOC 2. Richt offertes hierop in zodat er tijd is om met klanten de juiste afstemming te bereiken om te voorkomen dat later in het proces onduidelijkheden ontstaan;
- Een aanbeveling is om gebruik te maken van de nulmeting om zo kennis op te doen over de gemiddelde stand van zaken in organisaties. Dit schept een beeld over de volwassenheid van de organisatie en of er extra begeleiding nodig is voordat de SOC 2-audit gestart kan worden;
- Totdat klanten volwassen worden op het gebied van assurance zal SOC 2 niet geaccepteerd worden in de Nederlandse markt. Voordat SOC 2 geaccepteerd is, heeft het weinig nut om het product actief te gaan vermarkten. De nadruk dient te liggen op publiciteit, kennisdeling en het inzichtelijk maken van de kansen die SOC 2 biedt;
- SOC 2 kan gepositioneerd worden voor organisaties die op eigen initiatief assurancetrajecten willen starten voor verbetering of ontwikkeling. Andere partijen hebben weinig baat bij SOC 2 totdat SOC 2 bekend wordt en de ISAE/NOREA Richtlijn 3402 wordt minder geëist door klanten.
- Het leervermogen van de organisatie is relevant voor de kans op toepassing van SOC 2. Organisaties met een hoger leervermogen, wat zich uit in minimaal twee- of drieslag leren (tabel zeven), zullen sneller bereid zijn te starten met een SOC 2-opdracht. Dit wordt uitgedragen door wensen voor verbetering, integraal kwaliteitsmanagement en een werkwijze die ontwikkeling stimuleert. Dit kan gebruikt worden om voor bestaande klanten het leervermogen in te schatten en indien dit voldoende wordt geacht, de verbeterkansen van SOC 2 aan te kaarten.

Deze aanbevelingen zijn gebaseerd op onderzoeksresultaten. Op basis van deze aanbevelingen kunnen AuditConnect B.V. en IT-auditors zich voorbereiden op de adoptie van SOC 2, deze adoptie stimuleren en hier effectief op inspelen zodra SOC 2 bekend genoeg is. De SOC 2-richtlijn biedt kansen en geadviseerd wordt om hierop in te spelen zodra de markt volwassen genoeg is.

7.4 DISCUSSIE

De SOC 2-assurancerichtlijn biedt door zijn scoping en werkwijze kansen voor organisaties om meer zekerheid te verkrijgen over de beheersing van uitbestede IT-dienstverlening. Dit betekent voor zowel auditors als de vraagzijde van de markt dat er een verandering plaatsvindt in hoe assurance afgegeven kan worden: dit hoeft niet meer alleen via bijvoorbeeld de ISAE 3402 en er kan gerichter onderzocht worden hoe de beheersing van IT-diensten op de gebieden van Security, Availability, Processing Integrity, Confidentiality en Privacy is belegd.

Dit betekent dat er een kentering moet plaatsvinden. Gezien ontwikkelingen en trends op het gebied van IT is de huidige wijze van assuranceverstrekking niet altijd afdoende. Processen leunen sterk op (uitbestede) IT-diensten waarvan duidelijk moet zijn hoe de beheersing is geregeld om dreigingen af te kunnen weren. Het onderzoek concludeert dat de vraagzijde van de markt nog niet klaar is voor de SOC 2-assurancerichtlijn. Hiervoor zijn verschillende redenen benoemd die allen van belang zijn voor de adoptie van de verklaring.

Maar hoe kan dit dan veranderen? Als de markt niet bij kan of wil draaien heeft het ontwikkelen van assuranceverklaringen geen nut. Als er geen gebruik wordt gemaakt van de mogelijkheden stimuleert dit niet tot kennisgroei en een vergroting van de toepassing van SOC 2.

De NOREA heeft de mogelijkheid om leidend te zijn in het starten van initiatieven om de adoptie te vergroten. De vraagzijde van de markt dient bekend te worden met de mogelijkheden op het gebied van assurance, die verder gaan dan alleen een ISAE 3402-rapport. SOC 2 biedt de markt de mogelijkheid om assurance af te geven met betrekking tot hedendaagse dreigingen in een internationaal perspectief. IT-dreigingen veranderen continu, maar assurance als proces is relatief statisch: richtlijnen en normenkaders worden wel herzien, maar blijven veelal ongewijzigd in hun scope of toepassing. Hierdoor ontstaat de mogelijkheid dat een assurancerapport kan worden afgegeven wat niet in lijn staat met huidige IT-dreigingen.

De markt is momenteel niet volwassen genoeg om SOC 2 in de praktijk te kunnen laten slagen. Er wordt ook wel gesproken over “opvoeden”: men moet leren over assurance en snappen wat relevant is voor welke assurancevraag. Indien het bewustzijn uitblijft, wordt de ontwikkeling van dit vakgebied ook geremd. Doordat richtlijnen niet worden gebruikt is er geen noodzaak of stimulans tot de verdere ontwikkeling van deze richtlijnen. Assurance wordt afgegeven volgens het principe van “het meest gebruikte” en niet “het best passende”.

Groei en de bijbehorende stimulatie zijn niet alleen van belang voor het bedrijfsleven: ook de assurancebranche heeft dit nodig, maar die is afhankelijk van de volwassenheid van de markt. Zolang de vraagzijde vast blijft houden aan “het meest gebruikte” kunnen beide partijen niet groeien omdat vanuit de markt de noodzaak tot ontwikkeling niet wordt onderkend. Immers; iedereen vraagt om een ISAE/NOREA Richtlijn 3402, dus dan zal het wel goed zijn.

Hier moeten de NOREA en IT-auditors individudeel de handen ineenslaan. De vraagzijde van de markt moet opgevoed worden. Kennisdeling is hier van vitaal belang. Adviesbureaus kunnen kennissessies organiseren en klanten stimuleren onderzoek te plegen naar de mogelijkheden.
De NOREA kan voorzien in de vraag over informatie met betrekking tot SOC 2, het begeleiden van uitvoeringstrajecten door tips op te stellen en bovenal de toepassing van SOC 2 stimuleren.

Zolang de markt niet bijgeschoold wordt in het maken van keuzes met betrekking tot assurance zal er vast worden gehouden aan hetgeen wat voor organisaties bekend is, ongeacht of dit de juiste dekking levert. Pas nadat blijkt dat de dekking niet voldoende is zal de markt gaan kijken naar alternatieven. Daarom moet er bewustwording geschept worden, om te voorkomen dat de put gedempt wordt nadat het kalf verdronken is.

BIBLIOGRAFIE

AICPA. (2010). *AT 801.* New York: AICPA.

AICPA. (2013). *An Executive Overview of GAPP.* New York: AICPA.

AICPA. (2013). *Service Organisations: Reporting on Controls at a Service Organisation Revelant to a User Entities' Internal Control over Financial Reporting.* New York: AICPA.

AICPA. (2015). *AT 101.* New York: AICPA.

AICPA. (2015). *TSP Section 100.* New York: AICPA.

AICPA. (2015). *TSP Section 100 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.* New York: AICPA.

AICPA. (2016). *Exposure Draft: Proposed Revision of Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy.* New York: AICPA.

AICPA. (z.j.). *Service Organisation Controls (SOC) Reports for Service Organizations*. Retrieved from AICPA.org: http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/serviceorganization's management.aspx

AIPCA. (2015). *Reporting on Controls at a Service Organisation Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy (SOC2).* New York: AICPA.

Anderson, C. (2012). *Understanding SOC 2.* Onbekend: Baker Tilly Virchow Krause. Retrieved from http://www.bakertilly.com/uploads/Financial-Services-Understanding-SOC-2_Webinar.pdf

AuditConnect B.V. (2016). *ISAE 3402 audit en advies*. Retrieved from AuditConnect.nl: http://www.auditconnect.nl/nl/it-audits/isae-3402/

AuditConnect B.V. (2016). *Over AuditConnect*. Retrieved from AuditConnect.nl: http://www.auditconnect.nl/nl/

Bennink, H. (2015). *Organisatieadvisering: het mooie en het moeilijke.* Nijmegen: Hogeschool van Arnhem en Nijmegen.

Boer, J. &. (2013). *Nieuwe ontwikkelingen IT-gerelateerde Service Organisation Control rapportages*. Retrieved from Compact.nl: http://www.compact.nl/artikelen/C-2013-2-Boer.htm

Coopers, Pricewaterhouse. (2013). *10 Minutes on Service Provider Transparency.* Onbekend: Pricewaterhouse Coopers.

CPA Australia. (2014). *A Guide to Understanding Auditing and assurance.* Southbank: CPA Australia ltd.

De IT-Auditor. (z.j.). *Wat is een IT-auditor?* Retrieved from deITauditor.nl: https://www.deitauditor.nl/wat-is-een-it-auditor/

Dimov, D. (2013, 1 10). *Differences between the Privacy Laws in the E.U. and the US*. Retrieved from INFOSECInstitute.com: http://resources.infosecinstitute.com/differences-privacy-laws-in-eu-and-us/

Duijnborgh audit b.v. (z.j.). *ISAE 3402 verklaring type 1 en 2.* Nieuwegein: Duijnborgh audit b.v.

European Certification Group. (2016). *What is an Audit and What is the Audit Process?* Retrieved from eurcert.com: http://www.eurcert.com/en/iso-certification-the-audit-process.html

Haes, d. A. (2015, 4 21). *Reis door de privacy-kloof tussen Europa en Amerika*. Retrieved from Computerworld.nl: http://computerworld.nl/security/85999-reis-door-de-privacykloof-tussen-europa-en-amerika

Hanson, A. (1942). Definition of Auditing. In A. Hanson, *Auditing: Theory and its Application* (p. 3). New York: McGraw Hill Book Company Inc.

Hezemans, C. (2015). *Plan van Aanpak.* Apeldoorn: Saxion.

Instituut van Internal Auditors. (z.j.). *Vakgebied*. Retrieved from IIA.nl.

INTOSAI. (z.j.). *Information Technology Audit: General Principles.* Onbekend: INTOSAI. Retrieved from INTOSAI.com: http://intosaiitaudit.org/publication_and_resources/3

Intralinks. (2009). *SAS 70 Type II Audits.* New York: Intralinks.

Katcher, A. P. (2014). *Service Organization Controls: Managing Risks by Obtaining a Service Auditor's Report.* Onbekend: AICPA.

KPMG Advisory N.V. (2012). *KPMG Praktijkgids 4 Service Organisatie Control-rapport, ISAE 3402.* Amstelveen: KPMG Advisory N.V.

Losse, M. (2012). *Syllabus Probleemanalyse.* Enschede: Saxion .

Metselaar, E. C. (2011). *Van weerstand naar veranderbereidheid.* Heemstede: Holland Business Publications.
NBA. (2016). *ISAE 3000 Herzien: assurance-opdrachten anders dan opdrachten tot controle of beoordeling van historische financiële informatie.* Amsterdam: NBA.
NDB LLP Accountants & Consultants. (z.j.). *AT 101 SOC 2 | Important Points to Know*. Retrieved from SSAE16.org: http://www.ssae16.org/what-is-ssae-16/at-101-and-soc-2.html
NJI.nl. (z.j.). *Wat is implementeren?* Retrieved from NJI.nl: http://www.nji.nl/nl/Implementatie/Implementeren-met-effect/Wat-is-implementeren
NOREA. (2009). *Richtlijn assurance-opdrachten door IT-Auditors.* Amsterdam: NOREA.
NOREA. (2011). *NOREA Richtlijn 3402.* Amsterdam: NOREA.
NOREA. (2015). *Privacy Impact Analyse (PIA).* Amsterdam: NOREA.
NOREA. (2016). *Guidance to Richtlijn (ISAE) 3000 Service Organisation Control Reports for IT Organisations Based on the AICPA SOC 2 Report Model and the Trust Services Principles and Criteria.* Amsterdam: NOREA.
NOREA. (2016, 4 14). *Presentatie SOC 2 Handreiking*. Retrieved from NOREA: http://www.norea.nl/Norea/Actueel/Activiteiten+en+evenementen/Presentatie+SOC-2+Handreiking.aspx
Sikkema, T. (2015, 2 19). Auditors meeting SOC & assurance. (C. Nield, Interviewer)
Wilkinson, J. (2013, 7 23). *External Audit Definition*. Retrieved from StrategicCFO.com: http://strategiccfo.com/wikicfo/external-audit-definitio/
WIPO. (2016). *Global Brand Database*. Retrieved from WIPO.int: http://www.wipo.int/branddb/en/
WIPO. (2016). *Global Brand Database*. Retrieved from WIPO.int: http://www.wipo.int/branddb/en/

BIJLAGE 1 GESPREKSVERSLAG & VRAGENLIJST INTERXION

Inleiding
In deze bijlage is het gespreksverslag opgenomen van het interview met Theo Buurman en Hans Metz van InterXion. Dhr. Buurman is verantwoordelijk voor compliance en quality management en dhr. Metz zijn verantwoordelijkheden liggen op het vlak van security management. Conclusies van het verslag zijn opgenomen in hoofdstuk vijf. Omwille van de omvang van het gespreksverslag is besloten het verslag in de bijlage op te nemen. Het gespreksverslag is ingezien door beide geïnterviewden en wijzigingen zijn aangebracht waar gewenst. Afrondend is ook de gebruikte vragenlijst opgenomen in deze bijlage.

Gespreksverslag
Aanwezig: Theo Buurman, Hans Metz
Locatie: InterXion

Afspraken
Voorafgaand aan het interview is vastgesteld dat er geen verbatim van het interview mag worden toegevoegd aan de scriptie vanwege vertrouwelijke gespreksonderwerpen. In overleg met de geïnterviewden is besloten een gespreksverslag op te leveren, dat vóór plaatsing in de scriptie door de geïnterviewden gecontroleerd zal worden alvorens goedkeuring verleend wordt. Tijdens het gesprek is de vragenlijst aangehouden zoals beschreven in bijlage één.

Verslag
Aanwezig bij het gesprek waren Theo Buurman, Quality Manager en Hans Metz, Security Manager. Dhr. Buurman is verantwoordelijk voor compliance en proceskwaliteit waar dhr. Metz verantwoordelijk is voor de beveiliging van InterXion. InterXion levert “dataservices”, wat betekent dat er ruimte, koeling, stroom en connectiviteit geleverd wordt aan klanten. Hierin kunnen klanten zelf bepalen bij welke leverancier diensten worden afgenomen, aangezien InterXion zijn klanten deze vrijheid biedt. Momenteel zijn er zes datacentra operationeel, waar er rond het einde van 2016 een zevende in gebruik zal worden genomen. InterXion bedient een scala aan klanten met verschillende wensen en eisen. Hieronder vallen ook klanten buiten de EU. Gezien de groei in voorgaande jaren en de stijgende vraag naar dataopslag is de verwachting dat InterXion ook de komende jaren sterk zal blijven groeien. Sinds 2013 laat InterXion SOC 2-audits uitvoeren.

InterXion bedient zijn klanten zoals veel datacentra doen op het gebied van informatiebeveiliging: wat er op de servers staat, is de verantwoordelijkheid van de klant. De nodige maatregelen zijn getroffen om te voorkomen dat er ongeautoriseerde wijzigingen of toegang tot InterXion en/of klantruimten plaats kan vinden. Voor InterXion kan informatiebeveiliging worden gezien als een business enabler. Klanten kunnen naar eigen inzicht aan InterXion maatregelen verzoeken ter implementatie, naast de bestaande maatregelen. Bestaande maatregelen zijn vergelijkbaar met maatregelen welke in datacentra van andere providers toegepast zijn. Op het gebied van informatiebeveiliging heeft op IT-gebied de interne organisatie de focus. Voor datacentra ligt de focus op fysieke beveiliging met de nodige IT-maatregelen maar uiteindelijk is de klant verantwoordelijk voor dit aspect van de beveiliging. InterXion beveiligt platforms, ruimte en nutsvoorzieningen maar niet de digitale inhoud van de serverracks. Sleutelbeheer vindt wel plaats, indien klanten dit wensen. Fysieke en logische toegang zijn voor InterXion de zwaartepunten van de beveiliging van de datacentra. Personen in de datacentra kunnen te alle tijden gevolgd worden en alle activiteiten wordt gelogd.

Onderscheidend is de klantgerichte werkwijze van InterXion: de klant en zijn wensen staan centraal. Er is een baseline van maatregelen aanwezig, maar indien een klant aanvullende eisen heeft kunnen deze ook geïmplementeerd worden. Trends voor InterXion zijn “cloud connect” (het via InterXion verbinden van meerdere cloud service providers om in de cloud applicaties te kunnen beheren), en veelvoorkomende eisen op het gebied van standaarden zoals PCI DSS en ISO 50001.

Er worden risico’s onderkend door InterXion maar in de branche worden geen ontwikkelingen gezien welke als zorgelijk ervaren worden. Voor InterXion zelf ligt de nadruk zeer op “traceability” (het kunnen loggen en ontsluiten van bewijs) van beveiligingsmaatregelen. Het moet inzichtelijk zijn wanneer bijvoorbeeld data is verwijderd zodat het bewezen kan worden aan klanten.

Daarnaast heeft InterXion een eigen visie op assurance. Dit kan worden gedefinieerd als het borgen van het kwaliteitsniveau in processen. Door een snelle groei van de organisatie is het van belang dat de processen meegroeien met de organisatie. Waar eerst sprake was van reactief handelen, ligt nu de nadruk op preventie. InterXion is van mening dat assurance niet draait om het behalen van een certificering of voldoen aan een normenkader, maar dat het gaat om de achterliggende meerwaarde. Door een audit met goed gevolg te behalen wordt voldaan aan bijvoorbeeld een klantwens (een rapportage) maar door de meerwaarde ervan op procesniveau toe te passen kan de organisatie er voor zorgen dat beheersmaatregelen ook worden nageleefd. Een voorbeeld hiervan is het zoveel mogelijk integreren van controls in de dagelijkse operatie. Voor zowel bewijslast als naleving betekent dit een stijging in de effectiviteit en werkbaarheid. Het gedachtegoed draait enerzijds om flexibiliteit in de dagelijkse operatie wanneer en waar mogelijk en anderzijds om conform regels en beheersmaatregelen de dagelijkse operatie te sturen.

InterXion start op eigen initiatief assurancetrajecten. De intrinsieke motivatie hier is dat dit het mogelijk maakt om processen continu te verbeteren en de kwaliteitsborging te versterken. Daarnaast vinden er veel audits plaats vanuit klanten op verschillende kaders, welke door SOC 2 gedeeltelijk worden gedekt. Voor InterXion is het van belang dat een assurancerichtlijn of certificering bij kan dragen aan verbetering en niet wordt gebruik om enkel klanten te behouden. Voor InterXion zijn de redenen om voor SOC 2 te kiezen als volgt:

- 75% reductie in audits van klanten doordat SOC 2 (internationale) klanten de gewenste assurance biedt;
- Minder tijdverlies van tijd door de voorbereiding voor audits;
- Een hogere efficiency in het auditproces.
- Een hogere effectiviteit binnen de processen. De controls binnen de TSP Sectie 100 brengen de juiste focus aan op de operationele processen.

InterXion legt de nadruk op Security en Availability van de TSP Sectie 100, wat inhoudt dat de standaard normen voor Security worden getoetst, maar ook de aanvullende normen van Availability. Voor InterXion is het afnemen van de SOC 2-audit een continu leerproces. Tegenwoordig ligt de nadruk op het ontsluiten van het juiste bewijs en niet op het begrijpen van de TSP Sectie 100 of implementeren van de juiste maatregelen: deze fases heeft InterXion gepasseerd. InterXion heeft geen aanpassingen moeten doorvoeren in zijn bedrijfsvoering voor de uitvoering van een SOC 2-audit. De interne auditfunctie levert een sterke bijdrage aan het hoog houden van de kwaliteit van processen, controls en dienstverlening met als gevolg heeft dat de audit geen (grote) bevindingen oplevert. Steekproeven worden door de interne auditfunctie afgenomen wat logische access controls versterkt. Het gedachtegoed van continue verbetering komt hierin terug. Voor InterXion is het van belang dat de lat hoog ligt en dat hier naar gepresteerd wordt. Van belang is wel dat de organisatie bekend gemaakt wordt met het normenkader, aangezien de audit stringenter is dan andere audits. Aangegeven wordt wel dat het creëren van een duidelijk audit trail lastig is en dat hieraan veel aandacht besteed moet worden. InterXion onderkent geen ontwikkelingen waarover intern assurance verkregen moet worden. Cloud connect wordt echter wel gezien als een ontwikkeling waarover assurance moet worden verkregen.

Op internationaal vlak is SOC 2 van belang voor InterXion. Nieuwe klanten komen bij InterXion terecht door de SOC 2-rapportage. Niet alleen draagt deze audit bij aan het behouden van klanten, maar worden er ook aantoonbaar nieuwe klanten aangetrokken. Daarnaast heeft de SOC 2-rapportage nog een voordeel: waar eerst veel klantaudits plaatsvonden nemen klanten nu genoegen met de SOC 2-rapportage. Dit betekent een stijging in efficiency door significant minder audits en daardoor een besparing in tijd en geld. SOC 2 brengt voor InterXion nieuwe verbeterpunten in kaart waarop gehandeld kan worden. Security awareness stijgt door de SOC 2-rapportage en het feit dat controls waar mogelijk ingebed zijn in processen en procedures zorgt ervoor dat processen zich automatisch conformeren aan de eisen van een SOC 2-audit.

Vragenlijst

Algemeen:

- Naam, functie;
- Organisatiebeschrijving met primair proces;

Informatiebeveiliging:

- Wat betekent informatiebeveiliging voor uw organisatie?
- Hoe geeft u of uw organisatie hier invulling aan? (proces(volwassenheid))
- Wat ziet u als trends binnen uw branche op het gebied van informatiebeveiliging? (dreiging/ positieve ontwikkelingen)

Assurance:

- Wat betekent assurance voor uw organisatie?
- Hoe geeft uw organisatie hier invulling aan? (proces(volwassenheid))
- Start uw organisatie op eigen initiatief assurancetrajecten, of komt dit voort uit een klant/leverancierswens? Zijn er andere redenen voor uw organisatie om een assurancetraject te starten?
- Ziet u binnen uw branche ontwikkelingen waarover assurance verkregen dient te worden?
- Waarom is voor SOC 2 gekozen? Is uw SOC internationaal toepasbaar dat wil zeggen op basis van Amerikaanse wet- en regelgeving?
- Heeft u verbeteringen gemerkt in uw IT-infrastructuur naar aanleiding van de uitvoer van een SOC 2-audit?
- Was uw organisatie al bekend met het normenkader en de toetsing hiervan alvorens een SOC 2-opdracht werd uitgevoerd? Bracht deze nieuwe audit uitdagingen met zich mee door de controls en gewenste bewijslast?
- Kan een SOC 2-audit als stringenter dan normaal worden aangemerkt?
- Merkt u verbetering bij het aangaan van internationale onderhandelingen door de SOC 2-rapportage?
- Bent u van mening dat een assurancerapport bijdraagt aan het vergroten of behouden van uw klantenbestand?
- Bent u van mening dat een assurancerapport bijdraagt aan het verhogen van het beveiligingsbewustzijn onder uw collega's?

Afronding

- Vaststellen wat uitgesloten moet worden.

BIJLAGE 2 GESPREKSVERSLAG & VRAGENLIJST EBPI

Inleiding
In deze bijlage is het gespreksverslag van het interview met dhr. van den Broek opgenomen. Dhr. van den Broek is verantwoordelijk voor het managen van informatiebeveiligingsrisico's en het bijbehorende kwaliteitsmanagement. Omwille van de omvang van het verslag is het gespreksverslag in de bijlage geplaats. In hoofdstuk vijf zijn conclusies getrokken op basis van het verslag. Het gespreksverslag is ingezien door dhr. van den Broek en wijzigingen zijn aangebracht waar gewenst. Afrondend is ook de gebruikte vragenlijst opgenomen in deze bijlage.

Gespreksverslag
Aanwezig: Stefan van den Broek
Locatie: EBPI, Den Haag

Afspraken
Voorafgaand aan het interview is vastgesteld dat er geen verbatim van het interview mag worden toegevoegd aan de scriptie vanwege vertrouwelijke gespreksonderwerpen. In overleg met de geïnterviewde is besloten een gespreksverslag op te leveren, dat vóór plaatsing in de scriptie door de geïnterviewde gecontroleerd zal worden alvorens goedkeuring verleend wordt.
Tijdens het gesprek is de vragenlijst aangehouden zoals beschreven in XXXX.

Verslag
EBPI (European Business Process Institute) is een organisatie gespecialiseerd in massale berichtenverwerking. EBPI verzorgt berichtenuitwisseling van de overheid richting burgers en ondernemers. EBPI beheert deze keteninformatie-uitwisseling en is verantwoordelijk voor de diensten en infrastructuur die deze uitwisseling mogelijk maakt. Verwacht wordt dat de organisatie de komende jaren een grote groei zal doormaken, zoals ook over de afgelopen jaren heeft plaatsgevonden.

Geïnterviewd is Stefan van den Broek, Information Risk & Quality Manager. Dhr. van den Broek is verantwoordelijk voor het beheer van informatiebeveiligingsrisico's en kwaliteitsborging binnen de organisatie. Dit uit zich onder andere in procesbeheersing, het managen van (audit)kwaliteit en de beheersing van risico's.

Informatiebeveiliging is voor EBPI een wezenlijk onderdeel van de dagelijkse operatie. Personeel moet voldoen aan eisen met betrekking tot communicatie, handelingen en informatie-uitwisseling. De organisatie zoekt geen publieke bekendheid en handelt discreet richting klanten. De achterliggende filosofie van informatiebeveiliging benadrukt proactiviteit en handelingsbewust werken. Gezien de gegevens die verwerkt worden is ook de integriteit van de berichten van groot belang. Om te zorgen dat processen naar behoren functioneren en risico's gemitigeerd worden vinden er op regelmatige basis (interne) audits plaats. Geconstateerde afwijkingen worden verholpen om de IT-infrastructuur continu te verbeteren. ISO-certificeringen benadrukken de focus op de beheersbaarheid en integriteit van processen. Organisatiegroei wordt gestimuleerd, maar dit moet niet ten koste gaan van informatiebeveiliging.

Gezien de klanten die EBPI bedient, wordt er onderkend dat er een zekere complexiteit op het gebied van de te hanteren normenkaders aanwezig is. Klanten wensen hun normenkaders waar mogelijk toegepast te zien, zodat op basis van de eisen van de klant bewezen kan worden hoe de processen functioneren. Dit heeft als gevolg dat verschillende klanten gelijke eisen hebben (bijvoorbeeld op het gebied van beschikbaarheid) maar dat deze eisen wel separaat getoetst dienen te worden. Een wenselijke ontwikkeling zou zijn dat er meer gebruik wordt gemaakt van integrale normenkaders door klanten, zodat auditing zo efficiënt mogelijk plaats kan vinden. De voorberei-

ding en audit zelf kosten veel tijd en een generiek normenkader zou besparing met zich meebrengen. Klanten stellen normenkaders of eisen echter contractueel vast waardoor het bemoeilijkt wordt om hierin een wijziging te bewerkstellen. Dit remt echter ook de evolutie van de normenkaders van de klant, doordat normen niet herzien worden naar mate de tijd verstrijkt. Marktstandaarden daarentegen evolueren mee, om te borgen dat ook nieuwe dreigingen meegenomen worden in een audit. Hier wordt benadrukt dat de NOREA initiatieven zou kunnen starten om deze ontwikkeling te bewerkstelligen. Klanten moeten inzien dat verandering niet per sé slecht is en dat het de weerbaarheid ten goede komt. Ook wordt virtualisatie en de mogelijkheden hiervan onderkend. Zodoende kan oude infrastructuur uitgefaseerd worden maar kunnen verouderde applicaties virtueel gedraaid worden. Organisaties kunnen zo effectiever beheren wat waar draait en kunnen sneller acteren op end-of-life software en de benodigde migraties.

Dhr. van den Broek is bekend met de SOC 2-richtlijn. Als oud-RE is er ruime kennis aanwezig over auditing, richtlijnen en de uitdagingen voor een audit(or). SOC 2 kan worden gezien als een product met kansen doordat er sprake is van een geïntegreerd normenkader, maar een gevaar is de mate van abstractie. Doordat er de normen op hoog niveau zijn geformuleerd en niet als concrete technische eisen, brengt de audit uitdagingen met zich mee. De organisatie moet zelf interpreteren wat de norm voor hen betekent waarop vervolgens de auditor zijn eigen inschatting maakt of de getroffen maatregelen voldoende zijn. Daarnaast maken klanten niet altijd de juiste inschattingen voor assurance: vaak wordt gekozen voor de bekende weg (ISAE/NOREA Richtlijn 3402) waar deze richtlijn niet per definitie het meest geschikt is voor de situatie. Het is van belang klanten hier mee te laten groeien en in te laten zien welk assuranceproduct geschikt is voor welke scope. Wederom brengt dit voor de NOREA verantwoordelijkheid met zich mee. Auditors als klanten moeten weten wat waarvoor geschikt is. De mogelijkheden van SOC 2 worden onderkend en er worden kanttekeningen gezet bij de bruikbaarheid. Doordat de verschillen tussen de Amerikaanse en Nederlandse richtlijn groot zijn, raken enkele elementen verloren die de waarde van SOC 2 en SOC 3 vergroten.

Klanten zijn hedendaags op zoek naar zekerheid omtrent complexe producten: dit wordt verkregen door normenkaders te hanteren waaraan serviceorganisaties dienen te voldoen. Door eisen te stellen aan processen, beheersmaatregelen en beleid garandeert een gebruikersorganisatie zich dat zijn serviceorganisatie voldoet aan de eisen die de gebruikersorganisatie stelt. Echter kunnen deze eisen de groei van één of beide organisaties remmen, doordat de normenkaders niet mee ontwikkelen (doordat eisen contractueel zijn vastgelegd) of niet gereviseerd worden (om huidige dreigingen mee te nemen). Dit betreft assurance in een vorm die een belemmering stelt aan het functioneren van de organisatie. Voor zowel gebruikers- als serviceorganisatie is het van belang een balans te vinden tussen wat nodig is om assurance te verkrijgen, zonder dat dit ten koste gaat van ontwikkelmogelijkheden.

Gesteld wordt dat adoptie in de huidige vorm een uitdaging is. Echter kan ontwikkeling en bewustwording bijdragen aan de marktadoptie van SOC 2. Normenkaders moeten blijven ontwikkelen om bestendigheid tegen hedendaagse dreigingen te kunnen bieden. Dit is een voordeel van de TSP Sectie 100, doordat het normenkader regelmatig gereviseerd wordt. Door de hoge snelheid van IT-ontwikkelingen is het van belang dat normenkaders meegroeien, omdat er anders een mismatch ontstaat tussen dreiging en geïmplementeerde maatregelen.

Gezien de abstractie van de normen van de TSP Sectie 100 (geen concrete technische eisen bijvoorbeeld) kan het correct interpreteren van deze normen een uitdaging zijn voor zowel auditor als auditee. De NOREA kan hierin bijdragen door het vergroten van het klantbewustzijn. De NOREA kan de markt hierin steunen door SOC 2-audits op basis van de TSP Sectie 100 aan te prijzen. De NOREA zou op deze wijze een “keurmerk” af kunnen geven: dit zou klanten en gebruikers zekerheid geven over de betrouwbaarheid van het product SOC 2 en de toetsing ervan. Op deze wijze zou de NOREA een waardevolle toevoeging zijn en zou de kans groter zijn dat SOC 2 geadopteerd wordt door de markt en auditors.

Vragenlijst

Algemeen:

- Naam, functie;
- Organisatiebeschrijving met primair proces;

Informatiebeveiliging:

- Wat betekent informatiebeveiliging voor uw organisatie?
- Hoe geeft u of uw organisatie hier invulling aan? (proces(volwassenheid))
- Wat ziet u als trends binnen uw branche op het gebied van informatiebeveiliging? (dreiging/ positieve ontwikkelingen)
- Hoe wilt u hier op reageren?
- Bent u van mening dat u weerbaar genoeg bent tegen hedendaagse dreigingen?
- *Indien nee: hoe gaat uw organisatie hier mee om?*

Assurance:

- Wat betekent assurance voor uw organisatie?
- Hoe geeft uw organisatie hier invulling aan? (proces(volwassenheid))
- Start uw organisatie op eigen initiatief assurancetrajecten, of komt dit voort uit een klant/leverancierswens? Zijn er andere redenen voor uw organisatie om een assurancetraject te starten?
- Ziet u binnen uw branche ontwikkelingen waarover assurance verkregen dient te worden?
- Bent u bekend met het SOC 2-assurancerapport?
- Heeft u verbeteringen gemerkt in uw IT-infrastructuur naar aanleiding van de uitvoer van een audit?
- Werkt u op basis van een eigen normenkader of een marktontwikkeld normenkader? Indien eigen normenkader, brengt dit complicaties met zich mee?
- Bent u van mening dat een assurancerapport bijdraagt aan het vergroten of behouden van uw klantenbestand?
- Bent u van mening dat een assurancerapport bijdraagt aan het verhogen van het beveiligingsbewustzijn onder uw collega's?

Afsluiting:

- Aangeven wat niet opgenomen dient te worden in het verslag, indien van toepassing.

BIJLAGE 3 GESPREKSVERSLAG & VRAGENLIJST KPN

Inleiding
In deze bijlage is een gespreksverslag opgenomen van het interview met dhr. René van de Hesseweg van KPN. Tevens was dhr. van de Hesseweg een teamlid van de werkgroep die verantwoordelijk is voor de publicatie van de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 (NOREA, 2016). Deze bijlage bevat enkel het verslag. De conclusies van het verslag zijn opgenomen in hoofdstuk vijf, om de hoofdtekst niet onnodig groot te maken. Het gespreksverslag is ingezien door dhr. van de Hesseweg en wijzigingen zijn aangebracht waar gewenst. Afrondend is ook de gebruikte vragenlijst opgenomen in deze bijlage.

Gespreksverslag
Aanwezig: René van de Hesseweg
Locatie: KPN, Apeldoorn

Afspraken
Voorafgaand aan het interview is vastgesteld dat er geen verbatim van het interview mag worden toegevoegd aan de scriptie. Dit is bepaald vanwege vertrouwelijke gespreksonderwerpen. In overleg met de geïnterviewden is besloten een gespreksverslag op te leveren, wat vóór plaatsing in de scriptie door de geïnterviewden gecontroleerd zal worden alvorens goedkeuring verleend wordt. Tijdens het gesprek is de vragenlijst aangehouden zoals beschreven in bijlage drie.

Verslag
Het interview heeft plaatsgevonden bij KPN te Apeldoorn met dhr. René van de Hesseweg. Verantwoordelijk voor Client assurance is dhr. van de Hesseweg ondergebracht in de interne auditfunctie, welke deel is van de afdeling Security and Compliance van de unit Business Operations. Tevens heeft dhr. van de Hesseweg bijgedragen aan de ontwikkeling van de NOREA Handreiking Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC-rapportmodel en de TSP Sectie 100, wat de Nederlandse invulling is van het SOC 2-rapportmodel in combinatie met Nederlandse wet- en regelgeving. Voor het interview is gebruik gemaakt van deze kennis om een deskundige opinie in te winnen over de assurancebranche en de toevoeging die SOC 2 met zich mee brengt.

KPN haar primaire proces is het leveren van geïntegreerde telecom- en IT-diensten zoals telefonie, connectiviteit en proceshosting of -ondersteuning. KPN bedient internationale klanten en dient te voldoen aan een breed scala van wet- en regelgeving, maar ook aan verschillende (audit)eisen van haar klanten. Door de complexiteit die dit met zich meebrengt in het assuranceproces heeft KPN (en voorheen Getronics) een integraal assuranceframework ontworpen wat niet alleen toepasbaar is op haar eigen processen, maar ook op de processen van sub-serviceorganisaties. Zodoende kan er door de keten heen assurance verkregen worden op een wijze waarin effectiviteit en efficiëntie niet verloren gaan. Het afnemen van veel verschillende audits voor klanten over verschillende processen levert door deze integrale aanpak een efficiëntieslag op. Momenteel werkt KPN met gestandaardiseerde ISAE 3000 assurance rapportages voor een groot deel van haar diensten. Deze rapporten hebben als normenkader het integrale assuranceframework maar dit geldt wel als een eigen ontwikkeld normenkader. Hierdoor is dit kader een discussiepunt, doordat het geen marktontwikkelde standaard betreft.

Het framework is samengesteld op basis van zoveel mogelijk normenkaders en richtlijnen waaraan KPN dient te voldoen en de eisen die haar klanten stellen. SOC 2 is hier nog niet aan toegevoegd. Dit komt doordat zowel de markt als het KPN management nog niet bekend is met SOC 2. Daar-

naast kan niet zonder overleg met klanten grote wijzigingen aangebracht worden in beheersingsdoelstellingen en -maatregelen doordat klanten willen weten waarom er iets gewijzigd wordt. Er moet voorkomen worden dat klanten het idee krijgen dat de wijziging plaatsvindt om een bevinding weg te werken. Eén sub-serviceorganisatie (in India) heeft een SOC 2-opdracht laten uitvoeren, maar de vraag naar SOC 2 is verder beperkt omdat klanten nog niet bekend zijn met SOC 2. SOC 1 wordt internationaal vaker gevraagd als assurancerapport. Trends voor KPN liggen op het gebied van embedded controls, continuous auditing en traceability ten behoeve van een audit trail.

Dit framework dient als basis voor alle assuranceopdrachten voor KPN. KPN heeft daarnaast ook besloten om af te stappen van ISAE 3402 rapporten, doordat dit rapport niet altijd de juiste toepasbaarheid of klantreactie heeft. Bepaalde klanten willen het rapport maar maken hier verder geen gebruik van. Dit komt deels door onbekendheid vanuit klanten over wat een ISAE 3402 rapport is en hoe het toegepast dient te worden. Door contractuele vereisten is een ISAE 3402 rapport vaak verplicht, zonder dat dit de juiste mate van assurance afgeeft over de scope van de opdracht. Een ander rapport kan beter van toepassing zijn maar door onbekendheid wordt hier niet naar gevraagd. Daarnaast is het 3402-rapport wat eigenlijk enkel bedoeld is voor auditor naar auditor verkeer en andere personen met de benodigde kennis, tegenwoordig ook bedoeld voor management van een organisatie. De managementbewering is een belangrijk onderdeel van het rapport en zodoende neemt het management het rapport ook tot zich. Dit brengt met zich mee dat het jargon van de auditor voor verwarring kan zorgen omdat lezers niet genoeg kennis hebben van de materie.

De oplossing hiervoor zou een versimpelde rapportage zijn. Door een groei in het aantal vragen om assurancerapporten kan er gesteld worden dat dit steeds belangrijker zal worden. Momenteel sluit een 3402-rapport (of een 3000-rapport) niet aan op de gebruikersgroep doordat wordt gewerkt met vaktermen die niet bekend zijn bij lezers. SOC 2 draagt hier aan bij, maar compliceert dit ook. De rapportage werkt met een vastgesteld kader wat de eenduidigheid en betrouwbaarheid van de rapporten ten goede komt maar de scheidingslijn tussen SOC 1 en SOC 2 wordt als problematisch ervaren. Een accountant kan SOC 2 ook gebruiken in het kader van jaarrekeningcontrole mits daarin de criteria ten aanzien van de integriteit van de verwerking is opgenomen en de beheersingsmaatregelen in relatie staan met de financiële verslaglegging. Op basis van de principles van SOC 2 kan een accountant een passende rapportage opvragen, maar dit is gescheiden in SOC 1 en SOC 2. Dit kan verwarring met zich mee brengen voor serviceorganisaties die een rapportage op dienen te leveren. Van belang is dat er samen wordt gewerkt tussen de service- en klantorganisatie om vast te stellen wat er precies geaudit moet worden om zo een passend rapport te kiezen.

De marktwaarde van SOC 2 is momenteel laag. Accountants, vooral van kleinere kantoren, zijn onvoldoende op de hoogte van de richtlijn. IT-auditors zijn ook niet allemaal op de hoogte van het rapport. Hierdoor blijft er gevraagd worden naar ISAE 3402-rapporten terwijl deze niet per sé toepasbaar zijn. Dit wordt gezien als een hiaat tussen security, accountants en IT-auditing: een accountant heeft niet de kennis die een IT-auditor heeft, maar is wel bevoegd om een rapportage te ondertekenen. Hierdoor wordt ook niet per definitie gevraagd om de juiste rapportages terwijl security in situaties van groot belang is. De IT-auditor heeft deze kennis wel maar is afhankelijk van de visie van de accountant op welke rapportage gewenst is. Het overtuigen van een accountant is niet altijd mogelijk doordat contractueel vastgelegd kan zijn welke rapportage opgeleverd dient te worden. Als dit vastgelegd is zien klanten en accountants vaak geen reden om dit te wijzigen.

Daarnaast wordt er niet gestimuleerd te werken met de NOREA Handreiking Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 omdat dit geen richtlijn of standaard is: het is aan de auditor zelf om te bepalen of er met de handreiking wordt gewerkt. De NOREA zou hierin een actievere rol

op zich kunnen nemen door een organische groei van de handreiking te stimuleren zodat IT-auditors en klanten de meerwaarde van de rapportage inzien. Met organische groei wordt de ontwikkeling van de handreiking bedoeld naar aanleiding van ontwikkelingen in de IT-sector (big data etc.).

SOC 2 kan een grote meerwaarde betekenen voor de betrouwbaarheid en eenduidigheid tussen audits. Doordat de scoping bestaat uit enkele principles kan er geen verschil ontstaan tussen audits die getoetst zijn op basis van dezelfde principles, waar dit wel het geval is met eigen ontwikkelde normenkaders. Dit remt internationale samenwerking doordat audits voor organisaties niet dezelfde scope en normenkaders hanteren. Van belang voor adoptie van SOC 2 is ook dat verkoopafdelingen van organisaties weten wat de door hun organisatie vastgestelde assuranceproducten zijn en wanneer welk product beter geschikt is. Momenteel is dit niet zo wat de adoptie van SOC 2 ondermijnt en de ontwikkeling in de assurancebranche remt. Idealiter vindt er afstemming plaats tussen de verkooporganisatie van een klant en de IT-auditor om vast te stellen welk rapport het beste past bij de vraag. Bij KPN is dit ingericht wat positieve resultaten behaalt.

Van belang voor adoptie van de NOREA Handreiking Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 is dat er binnen de NOREA aandacht wordt geschept voor de handreiking en zijn toepassing. De beroepsgroep moet leidend zijn in het faciliteren van bruikbare assuranceproducten.

Momenteel is SOC 2 vooral voor Amerikaanse klanten van belang gezien het een Amerikaans product betreft, maar idealiter verschuift SOC 2 van het AICPA naar bijvoorbeeld de IFAC (International Federation of Accountants). De IFAC zou de mogelijkheid hebben om een internationaal geaccepteerd product te ontwerpen, zoals de ISAE-richtlijnen, om SOC 2 niet als Amerikaans product maar als internationaal product te publiceren. Door een officiële internationale publicatie zonder obstakels als trademarking en wet- regelgeving zou een internationaal gestandaardiseerd assurancerapport een betere kans krijgen geaccepteerd te worden. Dit is echter een langdurig proces en er is geen garantie dat dit plaats zal vinden. Hierin zou de NOREA wel een rol kunnen spelen.

Voor de adoptie van SOC 2 is wel van belang dat er sprake is en blijft van een organische groei. Doordat o.a. “Privacy” niet getoetst worden in de NOREA-publicatie maar dit wel van belang is (o.a. door de Wet Meldplicht Datalekken) is de verwachting dat er ontwikkeld zal worden aan de handreiking om deze elementen weer toe te voegen op basis van Nederlandse wet- en regelgeving. Dezelfde organische groei is van belang voor zowel SOC 2 als de TSP Sectie 100 om ontwikkeling mogelijk te maken en adoptie verder te stimuleren. Onbekendheid en onvolwassenheid op het gebied van assurance zijn momenteel de grootste obstakels voor adoptie van SOC 2. Dit moet verholpen worden. Hierin kan de NOREA een rol spelen door auditors en accountants te onderwijzen en ondersteunen in de toepassing van SOC 2. Daarnaast is er tijd nodig om de markt kennis te laten maken met SOC 2. Zonder bekendheid zal de markt SOC 2 niet adopteren, ongeacht hoe de richtlijn functioneert.

Afrondend onderkent dhr. van de Hesseweg versnippering van procesbeheer als een zorgelijke trend. Veel partijen zijn betrokken bij het managen van uitbestede processen en het beheer verschuift van een centraal punt naar meerdere partijen die elk een deel ten uitvoer brengen. Het kan lastig zijn om in kaart te brengen wie waarvoor verantwoordelijk is en daarnaast zijn er voorschriften die bepalen dat er niet altijd op een andere auditor zijn werkzaamheden kan worden gesteund. Het auditen van deze processen wordt zo complexer en tijdrovender dan nodig is. SOC 2 kan dit verhelpen door over de gehele keten assurance eenduidig te rapporteren. De vastgestelde inhoud reduceert de complexiteit wat de efficiëntie ten goede komt. Van belang is dat organisaties zich gaan richten op assurance als onderdeel van kwaliteitsmanagement en dit ook inbedden in hun procesgang.

Vragenlijst

Algemeen:

- Naam, functie;
- Organisatiebeschrijving met primair proces;

SOC 2:

- NOREA en SOC 2; het resultaat?
- Zal SOC 2 bijdragen aan een vermindering van “misbruik” van de ISAE/NOREA 3402 richtlijn?
- Welke overwegingen zijn er voor het starten van een SOC 2-opdracht?
- Welke kansen zijn er voor SOC 2 en hoe zouden deze benut kunnen worden?
- Wat is SOC 2 zijn grootste aandachtspunt/zwakte?
- Wat zijn de verwachtingen voor SOC 2 in zijn gebruik, bekendheid en waarde richting klanten?
- Welke best practices zijn er om een SOC 2-audit te doorlopen?
- Hoe kan een organisatie er het beste voor zorgen dat hun SOC 2-rapport voldoet aan Amerikaanse wet- en regelgeving?
- Bent u van mening dat SOC 2 kan bijdragen aan internationale onderhandelingen door zijn internationale draagvlak? Of verwacht u geen veranderingen ten opzichte van de ISAE-richtlijnen en hun draagvlak?
- Wat zijn verdere ontwikkelingen op het gebied van IT-assurance?
- Bent u van mening dat SOC 2 kan bijdragen aan het versterken of verbeteren aan de beheersing van de gemiddelde organisatie zijn IT-infrastructuur?
- Wat onderkent u als trends binnen het assurance-vakgebied?
- Wat zie u als zorgelijke ontwikkelingen binnen uw branche waarover assurance dient verkregen te worden?

Afronding

- Vaststellen wat uitgesloten moet worden.

BIJLAGE 4 ONDERBOUWING DEELVRAAG 1

Inleiding
In deze bijlage wordt de onderbouwing behandeld van deelvraag één “wat zijn de meest gebruikte assurancerichtlijnen en wat voegt de SOC 2-richtlijn hier aan toe?”. Wegens de omvang is besloten dit niet in de hoofdtekst op te nemen. In paragraaf 6.1 is de samenvatting van de beantwoording van de deelvraag opgenomen.

Beantwoording
Vereisten SOC 2 in combinatie met de NOREA Richtlijn 3000
Assurancerichtlijnen stellen vereisten voordat er gestart kan worden met een opdracht. Deze vereisten zijn gesteld om te voorkomen dat een opdracht de waarde van een oordeel verandert, ondeskundige opinies gegeven worden en een auditor opties te geven wanneer zijn objectiviteit, scepsis en ethische verantwoordelijkheid in het geding dreigen te komen. De SOC 2 richtlijn stelt enkele vereisten voordat dat een SOC 2-opdracht gestart kan worden. Deze vereisten kunnen worden verdeeld in twee categorieën:

- Toepasbaarheidsvereisten;
- Opdrachtvereisten.

De verschillende vereisten zullen hieronder benoemd worden.

De TSP Sectie 100 kan worden gebruikt voor toetsing wanneer voldaan is aan de volgende voorwaarden (AIPCA, 2015):

- Er is sprake van te auditen *uitbestede* processen;
- De te toetsen controls hebben *geen* direct verband met de financiële verslaglegging;
- Er is sprake van een *toetsbare* IT-infrastructuur;
- De te auditen elementen betreffen *operational (IT-)controls*.

Daarnaast onderkent SOC 2 de volgende opdrachtvereisten (AIPCA, 2015):

- AT 101 aan de grondslag van de opdracht;
- Het management van de service organisation dient te voldoen aan hun verplichting tot informatievoorziening;
- Het management levert de systeembeschrijving en scope van de opdracht aan;
- De auditor schat in of de opdracht wordt aangenomen op basis van de scope, te onderzoeken diensten en criteria;
- De opdracht wordt enkel aangegaan wanneer de auditor tevreden is over de kennis en kunde van betrokken partijen met betrekking tot de te onderzoeken diensten en de auditor zeker is dat hij gedurende de opdracht sceptisch en onafhankelijk kan blijven;
- De opdracht wordt enkel aangegaan wanneer het management van de opdrachtgevende organisatie als integer kan worden beschouwd en er geen klantrelatie ontstaat welke voor de auditor schade aan zijn reputatie kan berokkenen;
- De auditor hoeft niet onafhankelijk te zijn van elke gebruikende entiteit van de service organisation;
- De aan te leveren systeembeschrijving dient opgebouwd te zijn uit de volgende aspecten: infrastructure, software, people, procedures en data;
- Het vaststellen van de materialiteit (inhoudelijke juistheid) van de aangeleverde informatie door de auditor;
- Verspreiding van de rapportage is enkel toegestaan binnen een kleine gebruikerskring. De rapportage is niet bedoeld voor (aankomende) klanten, tenzij er vooraf vastgestelde personen in deze organisaties benoemd zijn.

SOC 2 stelt wel vereisten voor zijn gebruik zoals beschreven, maar geen eisen met betrekking tot voorgaande implementatietrajecten, zoals een ISO 27001-certificaat. Het is van belang dat de auditor kan vertrouwen op de aangeleverde informatie, het management en zijn eigen kennis en kunde tijdens een SOC 2-opdracht. De NOREA Richtlijnen stellen geen vereisten met betrekking tot voorgaande implementatietrajecten en zijn vergelijkbaar qua vereisten met SOC 2. Op deze wijze blijft hetzelfde werkgebied beschikbaar voor SOC 2, zonder dat serviceorganisaties hiervoor nieuwe of extra certificeringen moeten behalen. Door deze werkwijze aan te houden blijft SOC 2 beschikbaar voor alle soorten organisaties.

De NOREA 3000, waarin het SOC 2-rapportmodel geplaatst zal worden voor Nederlandse opdrachten, stelt ook enkele relevante vereisten voordat de richtlijn toegepast mag worden (NBA, 2016):

- De beroepsbeoefenaar zal zich houden aan de voorschriften als beschreven in de richtlijn. Indien er afgeweken wordt van de richtlijn zal de beroepsbeoefenaar zijn oordeel beschrijven als non-compliant met de NOREA 3000;
- De beroepsbeoefenaar dient de gehele richtlijn te begrijpen, inclusief toepassing en ondersteunend materiaal;
- De beroepsbeoefenaar dient te handelen naar de relevante ethische voorschriften danwel andere relevante wet- en regelgeving welke minstens even veeleisend is;
- De beroepsbeoefenaar dient tevreden te zijn met de acceptatie en continuatie van de klantrelatie en assurance opdracht en zal concluderen wanneer dit voldoende is;
- De beroepsbeoefenaar zal alleen de opdracht vervolgen wanneer er:
    i) Er geen reden is om te vermoeden dat de onafhankelijkheid of ethische positie van de beroepsbeoefenaar in het geding komt;
    ii) Er onder de personen die de opdracht zullen voeren de benodigde kennis en kunde aanwezig is;
    iii) De voorwaarden van de opdracht en verantwoordelijkheden zijn besproken tussen de partijen.
- Indien er informatie beschikbaar tijdens het proces welke ervoor zou zorgen dat de klant niet akkoord was gegaan met de overeenkomst zal dit tijdig gecommuniceerd worden opdat er handelingen ondernomen kunnen worden tussen de klant en beroepsbeoefenaar;
- De beroepsbeoefenaar dient de aanvaardbaarheid van het object van onderzoek te beoordelen
- De opdracht voldoet aan gestelde volgende criteria met betrekking tot het ontwerp, normenkader en de beroepsbeoefenaar. Indien deze vereisten niet aanwezig zijn zal hierover gecommuniceerd worden tussen de beroepsbeoefenaar en de betrokken partijen. Indien de vereisten niet toegevoegd kunnen worden, zal de beroepsbeoefenaar de opdracht afwijzen. Echter zal een opdracht zo non-compliant zijn met de NOREA 3000 en mag er niet gesteld worden gewerkt te hebben op basis van de NOREA 3000;
- Indien er een scope wordt vastgesteld door de klant waarvan de beroepsbeoefenaar vermoedt dat er geen oordeel gevormd kan worden, zal de opdracht afgewezen worden, mits dit door de wet verplicht wordt;
- Klant en beroepsbeoefenaar zullen instemmen met de voorwaarden voor de opdracht, welke schriftelijk vastgelegd zullen worden. Bij herhalende opdrachten zal de beroepsbeoefenaar vaststellen of de voorwaarden nog gelden, gewijzigd moeten worden en of de noodzaak er is om de klant te herinneren aan de voorwaarden. De beroepsbeoefenaar zal niet instemmen met een wijziging in de voorwaarden tenzij hier een geldige reden voor is. Bewijs wat voor de wijziging verkregen is, wordt echter niet nietig verklaard door de wijziging;
- In voorkomende omstandigheden kan wet- en regelgeving voorschrijven hoe het rapport geschreven dient te worden. In dit geval zal de beroepsbeoefenaar vaststellen of:
    i) De rapportage geen misverstanden schept;
    ii) Een verdere uitleg mogelijke misverstanden kan voorkomen.

Afrondend kan er worden gesteld dat een SOC 2-opdracht meerdere vereisten met zich mee brengt. Doordat SOC 2 binnen een NOREA-richtlijn is geplaatst brengt dit ook de beroepsregels van de NOREA met zich mee. Daarentegen zijn Amerikaanse regels niet meer van toepassing. Zo zal een SOC 2-rapportage niet berusten op de AT 101, maar op de NOREA Richtlijn 3000.

Waar dit als veel of lastig te realiseren vereisten over kunnen komen, is dit voor IT-auditors niet ongewoon: IT-auditor is een beschermd beroep waarbij onafhankelijkheid, scepsis en ethisch handelen van belang zijn. Daarnaast stelt het beroep ook strakke regels aan het rapporteren en volbrengen van opdrachten om de kwaliteit van audits gelijk te trekken.

Er is geen sprake van conflicterende, onduidelijke of onrealiseerbare vereisten voor een SOC 2-opdracht wanneer deze geplaatst is in een NOREA 3000-richtlijn. Voor een IT-auditor is het haalbaar een SOC 2-opdracht ten uitvoer te brengen op basis van de in Nederland geldende wet- en regelgeving in combinatie met de geldende beroepsreglementen.

Het wegnemen van toepassingsonduidelijkheid tussen de NOREA Richtlijnen 3000 en 3402
Binnen het vakgebied van IT-auditors wordt regelmatig aangehaald dat een Richtlijn 3402-verklaring onjuist toegepast wordt (Sikkema, 2015). Dit heeft meerdere oorzaken. Zo is de Richtlijn 3402 het eerste assuranceproduct wat naar behoren functioneerde binnen de markt. Een 3402-verklaring heeft door de jaren heen waarde gekregen als een betrouwbaar rapport wat voor veel accountants voldoende is om een jaarrekeningcontrole mee af te kunnen ronden. Twee jaar voor de Richtlijn 3402 is ook de Richtlijn 3000 uitgebracht. Deze richtlijn is beduidend minder succesvol, terwijl deze richtlijn voor situaties waar een Richtlijn 3402 voor wordt gebruikt in bepaalde gevallen beter geschikt is.

Zoals eerder aangegeven is een Richtlijn 3402-verklaring een verklaring die ingaat op de beheersmaatregelen die een waarschijnlijke relatie hebben met de financiële verslaglegging. Voor accountants van klanten of partners van organisaties is het van belang om aan te kunnen tonen dat de jaarrekening juist en volledig is. Een Richtlijn 3402-verklaring was en is het middel voor de accountant om hierop te kunnen steunen. Organisaties bepalen zelf het normenkader, wat betekent dat het kader door de organisatie kan worden ontwikkeld of dat er een vastgesteld kader aan wordt gehouden. De Richtlijn 3000 daarentegen was bedoeld voor alle situaties waarin geen relatie was met beheersmaatregelen die van invloed zijn op de financiële verslaglegging, bijvoorbeeld voor een verklaring over het functioneren van een geïmplementeerd COBIT-normenkader.

De Richtlijn 3402 (tevens de ISAE 3402) is als het ware slachtoffer geworden van zijn eigen succes (Sikkema, 2015) (Boer, 2013). Doordat het product veel gevraagd werd (en wordt) door accountants, zoals de SAS 70 hiervoor, kreeg het product bekendheid. Deze bekendheid zorgde ervoor, in combinatie met de onbekendheid over de toepassing van de Richtlijn 3000, dat de Richtlijn 3402 is toegepast op situaties waarin geen sprake was van financieel gerelateerde beheersmaatregelen. Dit is niet toegestaan omdat de Richtlijn 3402 ontwikkeld is om juist financieel gerelateerde beheersmaatregelen te auditen. Door de bekendheid van het product is de Richtlijn 3000, die voor bepaalde opdrachten beter geschikt was het veld uit geslagen en wordt de Richtlijn 3402 gezien als hét assuranceproduct voor (zo goed als) alle situaties.

Het vakgebied is zich bewust van de verschillen tussen de richtlijnen, maar klanten niet. Een opdracht komt vaak voort uit de wens van een klant van een serviceorganisatie die inzicht wil hebben in de beheersing van de uitbestede diensten. Deze klanten hebben vaak geen kennis van de verschillen tussen de richtlijnen en willen het “bekende” product, ook al levert een ander product betere dekking of assurance. Door deze onbekendheid wordt het vakgebied gedwongen de Richtlijn 3402 ten onrechte aan te houden. Het succes van de Richtlijn 3402 dwingt het vakgebied deze verklaringen af te blijven geven.

Door een strikte scheiding in de scope van SOC 1 en SOC 2 kan de onduidelijkheid tussen de NOREA Richtlijnen 3000 en 3402 verholpen worden. Beide richtlijnen hebben een eigen werkgebied. Het kan lastig zijn een serviceorganisatie exact te plaatsen binnen SOC 1 of SOC 2. Echter hoeft een organisatie dit niet alleen te bepalen: een IT-auditor kan een organisatie hierbij adviseren op basis van de aanwezige controls en hoe deze zich verhouden (al dan niet) tot de financiële verslaglegging (De IT-Auditor, z.j.). De naleving van de rapportagescheiding zal naar verwachting zonder problemen verlopen wat SOC 2 een betrouwbaar product maakt met een helder toepassingsgebied.

SOC 2 komt hierin een frisse wind brengen: het betreft hier een gestandaardiseerd rapport met een uniform normenkader dat geen dekking levert voor de financiële verslaglegging (indien uitgevoerd op basis van de SOC 2-richtlijn). Daarvoor is een SOC 1-rapport opgesteld wat toetst op basis van andere richtlijnen, eisen en wet- en regelgeving. Zodoende wordt door het naleven van de SOC-rapportagescheiding gezorgd voor een einde aan toepassingsonduidelijkheid doordat zeer duidelijk wordt gesteld waarvoor een rapport bedoeld is. Het naleven van deze scheiding is voor alle betrokken partijen (klant, serviceorganisatie en auditor) cruciaal in het voorkomen van toepassingsonduidelijkheid, maar naar verwachting zal dit geen probleem vormen. De richtlijn schept een duidelijk beeld van zijn toepassingsgebied, waar bij afwijking kan worden gesteld dat een verklaring non-compliant is met de richtlijn. Afrondend is de scheiding vele malen duidelijker dan dit tussen de Richtlijn 3000 en Richtlijn 3402 is, wat de naleving ten goede komt. Waar dit niet duidelijk is voor een klant of serviceorganisatie, is het aan een (RE-geregistreerde) IT-auditor om hierover te adviseren.

Het stimuleren van eenduidigheid tussen audits
Zoals in figuur twaalf weergegeven is, zijn er meerdere richtlijnen voor audits. SOC 2 is een voorbeeld hiervan, maar ook de NOREA Richtlijnen 3000 en 3402 worden veelvuldig gebruikt.

Waar SOC 2 toetst op basis van een geïntegreerd normenkader (de TSP Sectie 100, welke inzichtelijk maakt hoe de IT-infrastructuur van een uitbesteed proces of dienst functioneert en beheerd wordt), is dit niet zo bij de NOREA Richtlijnen 3000 en 3402. Deze verschillen kunnen leiden tot een gebrek aan eenduidigheid tussen audits, ook al zijn deze gebaseerd op dezelfde richtlijnen.

Binnen de NOREA Richtlijn 3402 en 3000-verklaringen kan een eigen normenkader (door de organisatie ontwikkeld) of een marktontwikkeld normenkader geplaatst worden (COBIT, SOC 2, COSO Framework 2013 etc.). SOC 2 neemt deze mogelijkheid weg door te werken met een geïntegreerd normenkader, waarin wel bepaald kan worden wat binnen of buiten de scope van de opdracht valt, maar waarin verder geen beheersmaatregelen gewijzigd kunnen worden (tenzij dit degelijk onderbouwd kan worden). Dit is van belang omdat het voor organisaties zo mogelijk wordt gemaakt meer waarde te hechten aan de assuranceverklaring van een leveranciersorganisatie. Een door de serviceorganisatie ontwikkeld normenkader kan bepaalde aspecten die de gebruikersorganisatie wel relevant vindt, buiten beschouwing laten. Indien de gebruikersorganisatie dit getoetst zou willen zien, is het aannemelijk dat de kosten ook voor de gebruikersorganisatie zijn. Vooral aankomende klanten kunnen hier problemen mee hebben, doordat bijvoorbeeld niet inzichtelijk is hoe de databeveiliging is geregeld omdat beheersmaatregelen vaag of onduidelijk zijn geformuleerd. Een geïntegreerd normenkader geeft deze mogelijkheden (en problemen) niet.

Daarnaast kan er zo uniforme, eenduidige toetsing plaatsvinden wat de kwaliteit van audits ten goede komt. Doordat een normenkader verplicht gebruikt wordt krijgt de verdere ontwikkeling van een kader meer aandacht, dan wanneer het normenkader niet verplicht was.

Kinderziektes, best practices en tijdsgebonden ontwikkelingen zoals big data kunnen beter worden verwerkt in het kader doordat de noodzaak er is het normenkader bij te houden. Wie een SOC 2-opdracht uitvoert, moet tenslotte met een verplicht normenkader werken (TSP Sectie 100). Wanneer dit kader niet up-to-date zou zijn, of niet meer passend voor en door een snel veranderende IT-omgeving zouden er geen SOC 2-opdrachten meer uitgevoerd worden doordat de dekking van het normenkader en de verleende assurance niet meer voldoende zijn voor klanten en serviceorganisaties.

Oftewel: het ontwikkelen en vermarkten van een SOC 2-assurancesrapport komt niet alleen de kwaliteit van audits ten goede, maar ook de verdere ontwikkelingen van de TSP Sectie 100 wat SOC 2 een langere levensverwachting geeft met een sterke basis voor IT-assurance.

Internationale betrekkingen op het gebied van assurance standaardiseren
SOC brengt op internationaal gebied ook veranderingen met zich mee: sinds zijn ontwikkeling en toepassing in 2011 werkt Amerika met de SOC-richtlijnen (Boer, 2013). Voor organisaties die meer aanspraak willen maken op klanten die buiten Europa vallen, is een SOC-rapport een mogelijkheid meer klantrelaties op te bouwen buiten de EU. Waar kan worden gesteld dat een ISAE 3000 of 3402 ook internationaal geaccepteerd zijn, bieden zij niet dezelfde eenduidigheid en scope als een SOC 2-rapport.

Tijdens onderhandelingen of aanbestedingen kan dit in het voordeel werken van de aanbieder, doordat er geen onduidelijkheid is over de inhoud van een SOC-rapport: er is geen ruimte voor een eigen ontwikkeld normenkader (wat voor de volledigheid vertaald zou moeten worden eer het toegelicht kan worden) en beide partijen werken op basis van dezelfde principles, criteria en toetsingsmogelijkheden. Tegenwoordig geldt een ISAE/NOREA 3402-verklaring vaak al als knock-out criterium bij aanbestedingen en dit zal naar verwachting ook voor SOC 2-rapporten zal gaan gelden (Sikkema, 2015).

De publicatie van de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations (NOREA, 2016) gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 heeft echter enkele overwegingen met zich meegebracht voor een internationale georiënteerde SOC 2-rapportage. Zo wordt er afgeraden volgens Amerikaanse wet- en regelgeving te werken, totdat inzichtelijk is hoe hier aan voldaan kan worden. Dit betekent bijvoorbeeld dat het principle Privacy van de TSP is komen te vervallen, doordat er andere definities worden gehanteerd door Amerika en Nederland. Het rapport zal echter wel in het Engels gepubliceerd worden om te voorkomen dat verschillen tussen definities ontstaan tijdens de vertaling (NOREA, 2016).

De toepassing van SOC 2 binnen Nederland zou zorgen voor een eenduidige aanpak met betrekking tot het auditen van uitbestede processen en diensten, op basis van een (inter)nationaal toegepast normenkader. Zoals eerder aangegeven wordt zo de eenduidigheid gestimuleerd en hebben gebruikersorganisaties meer inzicht in wat het betekent als een serviceorganisatie een SOC 2-opdracht volbrengt en wat de resultaten betekenen (mits zij benoemd zijn in de vooraf bepaalde gebruikerskring van de rapportage). De ontwikkeling van het normenkader zal gedurende het leven van SOC 2 gedragen worden doordat er een verplichting is met het kader te werken. Hierdoor is het van belang dat het kader bestand is tegen huidige dreigingen en op de hoogte is van relevante trends.

Deze ontwikkelingen stoppen niet binnen Nederland: samenwerking met Amerika verloopt beter doordat een geïntegreerd normenkader wordt gebruikt, in combinatie met een richtlijn die al enkele jaren actief in gebruik is in Amerika. Zodoende kan effectiever en efficiënter benoemd worden wat de sterke punten zijn van een serviceorganisatie, maar kan een aankomende klant dit ook beter inschatten dan wanneer er met een eigen ontwikkeld normenkader gewerkt wordt.

De wet- en regelgeving verschilt sterk tussen de landen. De SOC 2-rapportage wordt in Nederland toegepast binnen de NOREA Richtlijn 3000, welke in Amerika niet (h)erkend hoeft te worden. Er kan voor internationaal georiënteerde verklaringen gewerkt worden met de ISAE 3000, mits er zekerheid is dat voldaan is aan alle relevante wet- en regelgeving alsmede de Amerikaanse beroepsreglementen.

Afrondend blijkt dat SOC 2 een grote stap is in standaardisering. Echter is er geen sprake van een grote stap voor internationale standaardisatie. Dit wordt tegengewerkt door verschillen in de heersende wet- en regelgeving en beroepsreglementen van de beroepsorganisaties van IT-auditors. SOC 2 kan worden gebruikt als assuranceproduct, maar aangeraden wordt geen rapportages voor internationaal gebruik op te stellen tenzij er zekerheid is dat er voldaan is aan alle relevante vereisten.

BIJLAGE 5 ONDERBOUWING DEELVRAAG 2

Inleiding
In deze bijlage is de onderbouwing opgenomen van deelvraag twee “wat zijn de juridische overwegingen bij de uitvoering en het onderhoud van SOC 2 voor organisaties?”. In paragraaf 6.2 is de samenvatting van de deelvraag opgenomen.

Beantwoording
Trademark*:*
Het AICPA is verantwoordelijk voor de ontwikkeling van de SOC-richtlijn. Daarnaast heeft het AICPA in het verleden meerdere assurancerichtlijnen ontwikkeld en kan zij worden gezien als Amerikaanse marktleider op het gebied van ontwikkelen en vermarkten van deze richtlijnen. Om haar intellectual property (IP) te beschermen, heeft het AICPA meerdere trademarks geregistreerd met betrekking tot SOC-rapporten, zoals hieronder weergegeven (tabel zestien) (WIPO, 2016):

#	Brand	Source	Status	Origin	Holder	Number	App. Date
1	SERVICE ORGANISATION CONTROL REPORTS	US TM	Active	US	American Institute of Certified Public Accountants	85136882	23-9-2010
2	AICPA SOC AICPA SERVICE ORGANIZATION CONTROL REPORTS SERVICE ORGANIZATIONS FORMERLY SAS 70 REPORTS AICPA.ORG/SOC	US TM	Active	US	American Institute of Certified Public Accountants	85323337	17-5-2011
3	AICPA SERVICE ORGANIZATION CONTROL REPORTS FORMERLY SAS 70 REPORTS AICPA SOC AICPA.ORG/SOC	US TM	Active	US	American Institute of Certified Public Accountants	85324955	19-5-2011
4	AICPA SOC AICPA.ORG/SOC AICPA SERVICE ORGANIZATION CONTROL REPORTS FORMERLY SAS 70 REPORTS	US TM	Inactive	US	American Institute of Certified Public Accountants	85323340	17-5-2011
5	SOC 3 SysTrust For Service Organizations	IL TM	Active	IL	American Institute of Certified Public Accountants	235025	16-1-2011
6	SOC³ SYSTRUST FOR SERVICE ORGANIZATIONS	CA TM	Inactive	CA	American Institute of Certified Public Accountants	1512319	24-1-2011
7	SOC3 SysTrust for Service Organizations	EM TM	Active	EM	American Institute of Certified Public Accountants	9674078	20-1-2011
8	SOC3 SYSTRUST FOR SERVICE ORGANIZATIONS	MX TM	Active	MX	American Institute of Certified Public Accountants	119851148242	18-1-2011
9	soc 3 sys trust for service organizations	SG TM	Active	SG	American Institute of Certified Public Accountants	T1103397Z	18-3-2011
10	SOC3 SYSTRUST FOR SERVICE ORGANIZATIONS	US TM	Active	US	American Institute of Certified Public Accountants	85137763	24-9-2010
11	SOC3 SysTrust for Service Organizations	CH TM	Active	CH	American Institute of Certified Public Accountants	533782011	12-9-2012
12	SOC3 SYS TRUST FOR SERVICE ORGANIZATIONS	AU TM	Inactive	AU	American Institute of Certified Public Accountants	1404514	17-1-2011

tabel 16: geregistreerde trademarks op zoektermen “Service Organisation Control, American Institute of Certified Public Accountants”

De volgende termen zijn eveneens voorzien van een trademark (tabel zeventien) (WIPO, 2016):

#	Brand	Source	Status	Origin	Holder	Number	App. Date
11	SOC 3	CA TM	Active	CA	American Institute of Certified Public Accountants	1518402	9-3-2011
12	SOC 2	CA TM	Active	CA	American Institute of Certified Public Accountants	1518403	9-3-2011
13	SOC 1	CA TM	Active	CA	American Institute of Certified Public Accountants	1518401	9-3-2011
14	SOC 1	US TM	Active	US	American Institute of Certified Public Accountants	85918623	30-4-2013
15	SOC 2	US TM	Active	US	American Institute of Certified Public Accountants	85918626	30-4-2013
16	SOC 3	US TM	Active	US	American Institute of Certified Public Accountants	85918631	30-4-2013
17	SOC 2	US TM	Inactive	US	American Institute of Certified Public Accountants	85136849	23-9-2010
18	SOC 1	US TM	Inactive	US	American Institute of Certified Public Accountants	85136837	23-9-2010
19	SOC 3	US TM	Inactive	US	American Institute of Certified Public Accountants	85136868	23-9-2010

tabel 17: geregistreerde trademarks op zoektermen “American Institute of Certified Public Accountants, SOC”

Zodoende heeft het AICPA haar richtlijn beschermd tegen (ongewenst en onwettig) gebruik. Leden van het AICPA mogen gebruik maken van SOC en de ondersteunende literatuurstukken, maar niet-leden mogen niet werken onder vermelding van SOC (1/2/3) of andere geregistreerde termen.

De NOREA heeft een handreiking gepubliceerd waarbij het trademark is gerespecteerd: Guidance to Richtlijn (ISAE) 3000 Service Organisation Control Reports for IT Organisations Based on the AICPA SOC 2 Report Model and the Trust Services Principles and Criteria (NOREA, 2016). Er mag verwezen worden naar service organisation control reports en er mag gesteld worden dat de handreiking is gebaseerd op het SOC 2-rapportmodel, maar niet dat er conform de SOC 2-richtlijn gewerkt is. Hiervoor is gekozen door de sterk afwijkende wet- en regelgeving. Doordat er gewerkt wordt met de NOREA Richtlijn 3000 is er geen sprake van een standaard SOC 2-rapport, maar van een afwijkend rapport dat de structuur van een SOC 2-rapport aanhoudt. Op deze wijze kan een Nederlandse IT-auditor werken met de SOC 2-richtlijn.

Afrondend kan worden gesteld dat het trademark van het AICPA geen obstakel is in het ten uitvoer brengen van een SOC 2-opdracht, mits er wordt gewerkt op basis van de NOREA Guidance to Richtlijn (ISAE) 3000 Service Organisation Control Reports for IT Organisations Based on the AICPA SOC 2 Report Model and the Trust Services Principles and Criteria.

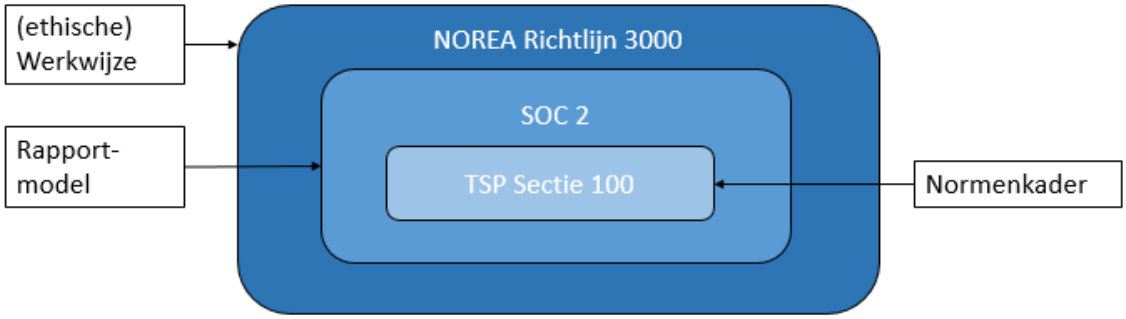
Plaatsing in de NOREA Richtlijn 3000
Zoals eerder vermeld is, is er een NOREA-handreiking in ontwikkeling voor SOC 2. Deze handreiking zal een vertaling zijn, zowel taal- als toepassingstechnisch. Dit betekent dat in plaats van de AT 101 aan te houden zoals SOC 2 in Amerika doet, de NOREA Richtlijn 3000 zal worden gebruikt als basis voor een SOC 2-opdracht.

De NOREA Richtlijn 3000 heeft geen vastgesteld normenkader en stelt ook geen vast kader voor de rapportage. De NOREA Richtlijn 3000 is als het ware een leeg kader dat gedragsregels opstelt voor het handelen voor, tijdens en na een opdracht alsmede hoe vanuit een ethisch perspectief gehandeld dient te worden (NBA, 2016). Dit betekent in de praktijk dat de NOREA Richtlijn 3000 een flexibel product is dat kan worden gebruikt om de gewenste richtlijnen te toetsen. Door het rapportmodel van SOC 2 toe te passen in de NOREA Richtlijn 3000 krijgt deze verklaring invulling. Dit betekent dat het NOREA Richtlijn 3000-rapport de hoofdstukindeling van SOC 2 alsmede de invulling van deze hoofdstukken aanhoudt. Zodoende krijgt de NOREA Richtlijn 3000 de volgende invulling:

- Sectie I: Vermelding van het management;
- Sectie II: Assurancerapport van de onafhankelijke auditor;
- Sectie III: Beschrijving van het systeem door de serviceorganisatie;
- 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.

Vervolgens is er een geïntegreerd normenkader toegevoegd, doordat SOC 2 werkt met de TSP Sectie 100. Zodoende wordt er invulling gegeven aan een NOREA Richtlijn 3000-rapport met een SOC 2-rapportmodel en toetsing volgens de TSP Sectie 100.

Dit is weergegeven in figuur zestien.



figuur 16: vormgeving SOC 2-rapport conform de NOREA Guidance to Richtlijn (ISAE) 3000 Service Organisation Control Reports for IT Organisations Based on the AICPA SOC 2 Report Model and the Trust Services Principles and Criteria

De NOREA heeft zich in eerste instantie gebaseerd op Nederlandse wet- en regelgeving en Nederlandse beroepsreglementen. Een SOC 2-rapport mag enkel ondertekend worden door een Amerikaanse accountant, namelijk een Certified Public Accountant (CPA) en SOC-logo's mogen alleen door het AICPA worden uitgegeven. Wanneer er een Nederlandse NOREA Richtlijn 3000 wordt aangehouden met het SOC 2-rapportmodel, kan dit enkel door een RE-auditor ondertekend worden, maar kunnen er geen logo's aangevraagd worden door verschillen in de beroepsreglementen.

Wanneer een ISAE 3000, de internationale variant van de NOREA Richtlijn 3000 gebruikt wordt, kan dit wel maar dit brengt de verwachting mee dat er conform alle Amerikaanse vereisten en wet- en regelgeving is gehandeld. Voor nu kan de NOREA nog niet garanderen dat overal aan voldaan is, waardoor SOC 2 momenteel wordt aangeraden op basis van de NOREA Richtlijn 3000. De voertaal van het rapport zal ook Engels zijn wat internationale betrekkingen vergemakkelijkt. Er kan wel een volledig SOC 2-rapport worden gepubliceerd, maar dit dient te voldoen aan alle Amerikaanse vereisten, wet- en regelgeving en beroepsreglementen van het AICPA.

Het is mogelijk hier aan te voldoen, vooral voor grotere accountancykantoren, doordat zij al CPA's in huis hebben en internationaal opereren. Voor Nederlandse accountancykantoren en adviesbureaus wordt dit afgeraden omdat het uitgebreid onderzoek vereist om boven tafel te krijgen waaraan voldaan moet worden en wat voor kennis er nodig is.

Samenvattend kan worden gesteld dat in Nederland SOC 2-opdracht uitgevoerd zullen worden op basis van de NOREA Richtlijn 3000 waarin SOC 2 een model voor de indeling van het rapport verstrekt. Toetsing zal geschieden op basis van de TSP Sectie 100. Deze rapportages mogen enkel door RE's ondertekend worden.

Verlies van toetsing op het gebied van privacy
Doordat de SOC 2-richtlijn is ontwikkeld in Amerika, brengt dit enkele discussiepunten met zich mee. Het Nederlands en Engels verhouden zich niet hetzelfde ten opzichte van elkaar wanneer er een vertaling plaats vindt. Nuances komen niet over en woorden hebben tussen de landen een verschillende betekenis. Een voorbeeld hiervan is privacy: binnen de TSP Sectie 100 is privacy aangemerkt als één van de principles waarop getoetst kan worden. De Nederlandse definitie van privacy is echter anders dan de Amerikaanse definitie.

Ook de grondhouding ten opzichte van dataverzameling is structureel anders. Amerika is dat "het mag, mits", en in de EU "het mag niet, tenzij". Anders gezegd: het basale verschil tussen opt-out en opt-in. We zien ook een kloof in de definitie van persoonsgegevens. In de VS is die nauw, het moet in principe gaan om direct identificeerbare gegevens. En als dit zogenaamde 'public records' zijn, dan zijn ze ook 'public', compleet openbaar.

(Haes, 2015)

Hieronder volgt een vergelijking, gebaseerd op wat de beroepsverenigingen (AICPA en NOREA) als definitie aanhouden (tabel achttien):

Definitie Amerika:	**Definitie Nederland:**
Privacy encompasses the rights and obligations of individuals and organisations with respect to the collection, use, disclosure and retention of personal information. **(AICPA, 2013)**	Grondwet artikel 10: 1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer. 2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. 3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens. **(NOREA, 2015)**

tabel 18: definitieverschil privacy tussen Nederland en Amerika

De NOREA baseert zich op de grondwet voor het bepalen wat privacy is. Voor het bepalen van welke soort privacy relevant is, is er een scheiding gemaakt in de dimensies van privacy. Hier worden de volgende dimensies onderkend (NOREA, 2015):

1. Lichamelijke privacy — Grondwet artikel 11;
2. Ruimtelijke privacy — Grondwet artikel 12;
3. Relationele privacy — Grondwet artikel 13;
4. Informationele privacy — Grondwet artikel 10.

Voor de bovenstaande vergelijking heeft de NOREA de definitie van informationele privacy aangehouden. Dit betekent dat de nadruk ligt op bescherming en eerbiediging van de ruimte van het individu, waarbij de wet regels stelt met betrekking tot het gebruik van deze data en de verstrekking ervan, alsmede het informeren van betrokkenen over gebruik van persoonsgegevens. Dit behelst niet uitsluitend naam en BSN, maar ook IP-adressen, MAC-adressen, cookies etc.

"Het raamwerk in Europa is op basis van privacy als een mensenwaardigheidsrecht. In de VS wordt het gehandhaafd als een recht op consumentenbescherming", constateert Google-jurist Nicole Wong in The New York Times.

(Haes, 2015)

De Amerikaanse definitie is hierin tegenovergesteld: privacy behelst enkel de verantwoordelijkheden en rechten van individu en organisatie over opslag, gebruik, vrijgave en behoud van persoonsinformatie, maar stelt niet wie welke verantwoordelijkheid heeft. Daarnaast kijkt de definitie zeer nauw naar persoonsgegevens: dit zijn enkel direct identificeerbare gegevens (naam, BSN). Niet (direct) te identificeren gegevens vallen niet onder deze definitie en mogen anders behandeld worden. Afrondend is privacy in eerste aanzet niet een recht van menswaardigheid, maar van consumentenbescherming (claims etc.) volgens deze definitie (Dimov, 2013).

Dit betekent voor SOC 2 en specifiek de TSP Sectie 100 dat er niet naar behoren getoetst kan worden op basis van het principle “Privacy”. De definities verschillen tussen Nederland en Amerika dermate, dat er niet kan worden gesproken over privacy voor een Nederlander of een Europeaan in vergelijking met wat een Amerikaan bedoelt met privacy. Zodoende zou toetsing op het principle “Privacy” ook niet het doel behalen wat een Nederlander verwacht van het principle. Indien het principle wel getoetst wordt, loopt men het risico dat gebruikers een vertekend beeld krijgen van het gebruik van persoonsgegevens. Op nationaal gebied brengt dit onduidelijkheid met zich mee en is er geen zekerheid van dekking door wijzigingen in de wet (Meldplicht datalekken etc.). Op internationaal gebied daarentegen zou het toetsen op het principle “Privacy” compleet vertekende beelden scheppen tussen Nederlanders en Amerikanen en zou dit kunnen leiden tot valse verwachtingen of handelen tegen de wet.

De Amerikaanse definitie komt niet overeen met de Nederlandse grondwet noch de Wet Bescherming Persoonsgegevens (WBP). Daarnaast wordt momenteel de opvolger van de Europese Privacyrichtlijn ontwikkeld, de Europese Privacyverordening. Deze verordening zal nauwer kijken naar privacy binnen en buiten Europese grenzen.

> *Under EU law, personal data can be collected only under strict conditions and for a legitimate purpose. The main component of the EU data protection law is the Data Protection Directive 1995/46/EC.*
>
> *In the US, there is no all-encompassing law regulating the collection and processing of personal data. Instead, data protection is regulated by many state and federal laws.*
>
> **(Dimov, 2013)**

Waar in Amerika geen centrale wetgeving is met betrekking tot privacy, is deze wetgeving wel aanwezig in de EU. Mogelijke redenen hiervoor zijn de vele (vroegere) Europese dictators en het inlichtingenapparaat wat de Stasi had ingericht (Dimov, 2013). Regulering op deze wetgeving is ingericht en wordt strikt nageleefd. Privacy wordt gezien als een recht door Europeanen, waar Amerika anders tegen aankijkt (Dimov, 2013) (Haes, 2015). Met deze verschillen aan de grondslag kan worden gesteld dat de Amerikaanse definitie en werkwijze afwijkt van de Nederlandse definitie en werkwijze.

Op basis van definitieverschillen, verschillen in wet- en regelgeving en het risico op onduidelijkheid alsmede niet-behaalde verwachtingen wordt “Privacy” als (momenteel) onbetrouwbaar gezien. Daarnaast zijn de uitsluiting volgens de NOREA, de richtlijnen van de WBP en de aankomende Europese Privacyverordening andere redenen waarop besloten is het principle “Privacy” buiten scope te plaatsen voor het onderzoek (alsmede alle relevante beroepsproducten).

Geldigheid van een rapportage

Een audit kan worden gezien als een cyclisch proces. Het is van belang voor gebruikersorganisaties om periodiek een betrouwbare rapportage te ontvangen over de kwaliteit en veiligheid van hun uitbestede processen en diensten. Om het vertrouwen tussen organisaties op niveau te houden, is het van belang periodiek de kwaliteit van de dienstverlening te laten toetsen.

Op basis van dit beginsel is gesteld dat rapportages beperkt geldig zijn. Afhankelijk van wat een richtlijn stelt kan het zijn dat een rapportage één jaar geldig is (of langer), of geldig is mits geplande changes beschreven staan.

SOC 2 heeft als geldigheid het volgende gesteld:

> *For what time period is a SOC report valid?*
> *SOC reports do not technically expire. However, users may or may not choose to rely on the report, based on the amount of time that has passed since the period covered by the report. Management of service organisations may issue a "bridge letter" stating that no changes to the control environment have occurred since the date covered by the report.*
>
> **(AIPCA, 2015)**

Een SOC 2-rapportage is feitelijk onbeperkt geldig, mits alle relevante geplande changes benoemd zijn. Of een change relevant is, wordt bepaald door de gebruikersorganisatie en niet door de serviceorganisatie zelf. Mits een serviceorganisatie zijn planning op orde heeft kan zo voor enkele jaren de toekomst is een assurancerapport worden afgegeven.

Indien een organisatie zijn relevante changes niet benoemd heeft of niet kan benoemen, vervalt de rapportage zodra de eerste relevante change wordt doorgevoerd. Wanneer de rapportage vervolgens wordt opgevoerd als bewijs of assurancerapport door een organisatie, is dit niet geldig.

Wanneer een organisatie zijn changes wel kan benoemen, kan de serviceorganisatie een bridge letter afgeven. Een bridge letter is gericht aan een klant en geeft dezelfde mate van assurance af als een SOC 2-rapport. Zodoende kan een serviceorganisatie tot jaren na het afgeven van een SOC 2-rapport nog steeds assurance afgeven over zijn dienstverlening, mits gebruikersorganisaties hiermee akkoord gaan.

> *What is a bridge letter?*
> *Bridge letters are issued by the management of a service organisation. SOC reports often cover only a portion of the user organisation's calendar or fiscal year. The purpose of a bridge letter is to provide a representation from the service organisation regarding material changes that might have occurred in the organisation's controls covered in the SOC report, from the end of the SOC report period through a specified date.*
>
> **(AIPCA, 2015)**

Een gebruikersorganisatie kan echter aangeven geen vertrouwen meer te hebben in een SOC 2-rapport, bijvoorbeeld wanneer het niet meer aannemelijk is dat de afgegeven assurance relevant of dekkend is. Dit kan komen door de implementatie van een nieuw systeem, een platformmigratie of een uitgebreide wijziging in een datamodel gebruikt in het primaire proces.

Afrondend kan worden gesteld dat een SOC 2-rapportage feitelijk "onbeperkt" geldig is, mits relevante changes beschreven zijn. Indien deze beschreven zijn kan de organisatie een bridge letter afgeven aan gebruikersorganisaties. Wanneer gebruikersorganisaties van mening zijn dat er geen degelijke basis meer is voor assurance op basis van de rapportage dient er een nieuwe rapportage ontwikkeld te worden, om opnieuw assurance te scheppen voor gebruikersorganisaties.

SOC 3

Wanneer een SOC 2-opdracht volbracht is, kan een organisatie starten met een SOC 3-opdracht indien gewenst.
Een SOC 2-rapportage is slechts inzichtelijk voor een kleine, vooraf beperkte gebruikerskring. Wil een serviceorganisatie zijn prestaties wel kenbaar maken naar websitebezoekers of andere partijen, dan is een SOC 3-rapportage nodig. Dit is niet toegestaan met een SOC 2-rapportage, maar wel met een SOC 3-rapportage. Hiernaast is een volledige vergelijking weergegeven tussen SOC 2 en SOC 3 (figuur 17figuur zeventien).

figuur 17: uiteenzetting SOC 2 en SOC 3

Een SOC 3-rapport is een rapportage zonder details. Deze rapportage is ook vrij te distribueren, dus kan richting websitebezoekers en andere partijen verstrekt worden. Belangrijker is dat bij een succesvolle volbrenging een seal kan worden uitgevraagd bij het AICPA. Dit seal wordt geplaatst op de website van de serviceorganisatie.

Wanneer een bezoeker van de website hier op klikt, wordt hij doorgestuurd naar de (digitaal gearchiveerde) SOC 3-rapportage.

Van belang is dat een SOC 3-opdracht enkel als een type II-rapport kan worden opgeleverd, omdat er anders niet inzichtelijk is voor klanten hoe een dienst of proces beveiligd is. De NOREA heeft geen richtlijn of handreiking gepubliceerd voor SOC 3. Waarschijnlijk blijft een seal zoals hiernaast weergegeven in ieder geval op korte termijn niet mogelijk (trademarking, ondertekening door een CPA, verschillende beroepsreglementen etc.) maar kan een organisatie wel een SOC 3-opdracht doorlopen.

figuur 18: SOC 3-zegel

Momenteel kan het zegel in figuur achttien niet gebruikt worden gezien het een trademark betreft en door het AICPA uitgegeven moet worden, wat voor organisaties die op basis van de NOREA handreiking een SOC 2-opdracht uit laten voeren niet voldoen aan hun eisen. Dit komt door verschillen in Amerikaanse en Nederlandse wetgeving, alsmede verschillen in de werkwijzen van een IT-auditor.

Samenvattend is SOC 3 bestemd voor iedereen die de verklaring wenst te lezen. Zodoende kan assurance afgegeven worden op een wijze waarin vrije publicatie mogelijk is en een algemeen beeld kan worden geschept van de kwaliteit en veiligheid van de uitbestede processen en diensten, zonder dat dit ten koste gaat van de organisatie. Een SOC 2-rapportage is wel vereiste voordat dat SOC 3 als type II-rapportage gepubliceerd mag worden. Afrondend kan de organisatie na publicatie zijn rapportage publiceren, maar waarschijnlijk niet met een seal van het AICPA.

BIJLAGE 6 ONDERBOUWING DEELVRAAG 3

Inleiding
In deze bijlage is de onderbouwing van deelvraag drie “welke criteria zijn van belang voor organisaties om te starten met een SOC 2-opdracht?” beschreven. In paragraaf 6.3 is de samenvatting van de deelvraag opgenomen.

Beantwoording
Aantoonbare meerwaarde richting gebruikersorganisaties
Momenteel is er door een gebrek aan bekendheid nog niet genoeg duidelijk voor gebruikersorganisaties over de meerwaarde van SOC 2. Uit de interviews is gebleken dat organisaties veelal niet bekend zijn met SOC 2 en wat SOC 2 voor een gebruikersorganisatie kan betekenen (los van de internationale voordelen). Organisaties zijn momenteel nog voorzichtig in het starten van een SOC 2-opdracht doordat niet duidelijk is wat de voordelen zijn ten opzichte van een NOREA Richtlijn 3402-rapportage of een NOREA Richtlijn 3000-rapportage. De meerwaarde van de rapportage, vooral op het gebied van eenduidigheid en leesbaarheid, zijn nog niet bekend bij de opdrachtgevers. Indien de meerwaarde voor de gebruikersorganisaties onbekend blijft, zal er weinig gebruik worden gemaakt van een SOC 2-rapportage op basis van de NOREA Richtlijn 3000 in combinatie met de TSP Sectie 100 (voor meer informatie over de meerwaarde van SOC 2 wordt verwezen naar paragraaf 6.1 en 6.2).

De NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 is bekend bij gebruikers- en serviceorganisaties
Uit de interviews is gebleken dat zowel auditors, accountants als sleutelfiguren binnen gebruiker- en serviceorganisaties niet bekend zijn met de NOREA publicatie. Hetzelfde geldt voor de SOC 2-publicatie van het AICPA. Doordat de bekendheid laag is zal er niet snel met het rapport worden gewerkt, doordat accountants en management assurance via bekende rapporten wil ontvangen. Wanneer de NOREA publicatie bekendheid verwerft zal er in Nederland sneller worden gewerkt met het rapport. Voordat er sprake kan zijn adoptie in de markt moet er meer bekendheid komen voor de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100, waarna het voor organisaties wel zal lonen om een SOC 2-rapport te publiceren.

Momenteel zijn er weinig baten voor een organisatie om een SOC 2-rapport te publiceren doordat management en accountants van gebruikersorganisaties de rapportage niet kennen en niet zullen accepteren (los van wat er contactueel geëist is als assurancerapport).

Duidelijkheid in de toepassing van SOC 2 en de TSP Sectie 100
Uit interviews is gebleken dat organisaties enkele uitdagingen onderkennen in het toepassen van de TSP Sectie 100. De normen zijn op hoog niveau geformuleerd, zoals hieronder weergegeven (tabel negentien):

CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external system users to permit users to understand their role in the system and the results of system operation.

tabel 19: Common Criteria 2.1 TSP Sectie 100

De uitdaging voor organisaties is om de juiste mate van diepgang te verwerken in de controls. Anders gezegd, wanneer is het voldoende? Dit is subjectief doordat de norm op hoog niveau voorschrijft dat er beheersmaatregelen zijn die er zorg voor dragen dat medewerkers hun rol in het systeem begrijpen en resultaten kunnen interpreteren. Afhankelijk van hoe de serviceorganisatie de norm interpreteert en hoe de auditor de norm interpreteert kunnen er verschillen in de interpretatie ontstaan. De NOREA heeft voor dergelijke situaties vastgelegd dat er een beroep kan worden gedaan op het "professional judgement" van een auditor of voldaan wordt aan criteria en of het restrisico acceptabel is. Dit neemt subjectiviteit niet volledig weg. Van belang is dat auditors en organisaties vóór een audit afstemmen welke controls nodig zijn om een norm en de bijbehorende risico's af te dekken. Voordat SOC 2 op basis van de NOREA Richtlijn 3000 in combinatie met de TSP Sectie 100 een groei zal zien in zijn marktaandeel op het gebied van assurance is het noodzakelijk om hierin te communiceren dat afstemming noodzakelijk. Bij zowel serviceorganisaties als gebruikersorganisaties ontbreekt momenteel duidelijkheid over de juiste toepassing van SOC 2 en de TSP Sectie 100.

Duidelijkheid met betrekking tot de internationale geldigheid van een SOC 2-rapport
Voordat SOC 2 geadopteerd wordt, is het noodzakelijk voor organisaties om informatie in te winnen over de geldigheid van een SOC 2-rapport, afhankelijk van welke publicatie gekozen is (NOREA of AICPA). De NOREA is genoodzaakt om op basis van Nederlandse wet- en regelgeving alsmede beroepsreglementen enkele elementen te schrappen. Voor organisaties die een SOC 2-opdracht uit willen laten voeren is het van belang om te weten wat wel en niet mogelijk is met hun SOC 2-rapport. De auditor moet hierover kunnen adviseren, dit betekent dat er kennisoverdracht moet plaatsvinden vanuit de NOREA richting haar leden. Tevens dient er onderzoek gepleegd te worden naar de relevante Amerikaanse eisen zodat een organisatie een geïnformeerde keuze kan maken. Nadat onderzoek heeft plaatsgevonden kan er een oordeel worden gegeven hoe de organisatie een internationale SOC 2-rapportage kan laten ontwikkelen. Totdat er een oordeel geformuleerd kan worden is het raadzaam voor organisaties om zich te conformeren aan de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100, tenzij de organisatie zeker is dat er voldaan wordt aan de Amerikaanse eisen.

Vereenvoudiging in het assuranceproces
Uit de interviews is gebleken dat een vereenvoudiging in het assuranceproces een criterium is voor organisaties om te starten met een SOC 2-opdracht. Door een veelvuldigheid van (eigen ontwikkelde) normenkaders heeft een gestandaardiseerd assurancerapport de interesse van serviceorganisaties. Doordat de normen van de TSP Sectie 100 vastgesteld zijn en SOC 2 toetst op basis van de TSP Sectie 100 is hier geen afwijking van mogelijk. Daarnaast is gebleken dat een SOC 2-rapport helpt met het reduceren van het aantal klantaudits. Voor een serviceorganisatie betekent dit minder audits, minder voorbereidingstijd en meer eenduidigheid. Voor SOC 2 is dit een sterk punt, vooral richting organisaties met een diversiteit aan te toetsen normenkaders. Efficiëntie binnen het assuranceproces wordt zo gesteund wat de verdere ontwikkeling van de organisatie ten goede komt. De vraag om vereenvoudiging is een vraag vanuit de markt waar SOC 2 een antwoord op is. Vereenvoudiging wordt mogelijk gemaakt, wat bij kan dragen aan de marktadoptie van SOC 2.

Klantwens of eigen initiatief
Het is van belang om na te gaan of het starten van een assuranceopdracht een klantwens is of eigen initiatief vanuit de organisatie. Tijdens de interviews kon er geen correlatie ontdekt worden dat SOC 2 primair uit eigen initiatief wordt gestart of dat de klantwens bepalend is. Dit komt doordat SOC 2 in Nederland momenteel nauwelijks wordt gebruikt.

Het is nuttig om in te kunnen schatten vanuit welk perspectief meer vragen voor een SOC 2-rapportage voortkomen. Afhankelijk vanuit welk perspectief meer vraag komt, kan er gerichter in de markt gepositioneerd worden. Een klantvraag is een (veelal dwingend) verzoek voor een (vaak contractueel vastgestelde) assurancerapportage. Doordat hier vaak al contractueel bepaald is welke rapportage opgeleverd dient te worden is hier geen ruimte voor keuze of initiatief: er dient een rapportage opgeleverd te worden om te voldoen aan de eisen van een contract. Gezien SOC 2 momenteel niet of nauwelijks contractueel vastgelegd zal zijn voor serviceorganisaties zal een klantvraag niet snel resulteren in een SOC 2-rapportage. De marketing hiervoor betreft vooral bekendheid van de richtlijn zoals eerder benoemd.

Wanneer er sprake is van eigen initiatief kan er vanuit de organisatie gekeken worden naar andere, nieuwe of minder bekende richtlijnen. Deze richtlijnen worden vanuit dit perspectief gebruikt als extra zekerheid om te overleggen aan toekomstige klanten of om meer duidelijkheid te scheppen over de IT-infrastructuur. Er is sprake van ruimte voor ontwikkeling of een wens voor verbetering. SOC 2 zal vanuit dit perspectief meer kans hebben voor de nabije toekomst doordat contracten gewijzigd zouden moeten worden om over te stappen op een andere assurancerapportage. Hier ligt voor SOC 2 de kans op het gebied van marketing, als tool voor verbetering. Het stimuleren van verbetering binnen een organisatie (door een stringente audit, het inrichten van een degelijk audit trail etc.) en de aantoonbare borging hiervan kan voor toekomstige klanten een extra reden zijn om een overeenkomst aan te gaan met de serviceorganisatie.

Organische groei van SOC 2 en de TSP Sectie 100
Voor adoptie van SOC 2 in combinatie met de TSP Sectie 100 is het van belang dat het normenkader evolueert op basis van huidige en aankomende dreigingen. Het normenkader dient periodiek gereviseerd te worden om te zorgen dat de controls (nieuwe) risico's af blijven dekken. Een organische groei van het normenkader draagt bij aan de levensduur van SOC 2-rapporten in het algemeen. Een voorbeeld van deze groei is voor de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100 de toevoeging van het principle "Privacy" op basis van Nederlandse wet- en regelgeving. Indien deze groei uitblijft, is de kans reëel dat SOC 2 niet geadopteerd wordt doordat aan behoeften van gebruikersorganisaties niet voldaan kan worden.

BIJLAGE 7 ONDERBOUWING DEELVRAAG 4

Inleiding
In deze bijlage is de onderbouwing van deelvraag vier “wat ondersteunt de succesvolle uitvoering van een SOC 2-opdracht?” beschreven. In paragraaf 6.4 is de samenvatting van de deelvraag opgenomen.

Beantwoording
In eerste aanzet worden de SOC 2-generieke randvoorwaarden voor de uitvoering behandeld, vervolgens de randvoorwaarden voor een internationaal geaccepteerde SOC 2-rapportage.

SOC 2-generieke randvoorwaarden
Afstemming met de auditor
Voor een succesvolle uitvoering van een SOC 2-opdracht is het van belang dat er vanaf het begin van het proces afstemming wordt gezocht met de auditor. In samenspraak moet de juiste scope worden bepaald (welke principles), niet-toepasselijke controls worden vastgesteld en bovenal de juiste interpretatie worden gegeven aan de criteria van de TSP Sectie 100. Zonder afstemming met de auditor kan de organisatie haar voorbereiding ook plegen, maar blijft het de vraag of de auditor instemt met de interpretatie van de normen (en daaruit voortkomend de benoemde controls en hun werking).

Voor een organisatie levert deze afstemming meer zekerheid dat de interpretatie van de normen correct is. De auditor kan adviseren over de interpretatie van de normen zodat er tijdens de audit geen verrassingen ontstaan. Gezien er niet veel SOC 2-audits zijn uitgevoerd in Nederland is het voor de auditor ook raadzaam om zo vroeg mogelijk in het proces aan te haken om zo vanuit meerdere perspectieven bijsturing te kunnen verlenen en te leren de normen van de TSP Sectie 100 te benaderen. Om adoptie door de markt mogelijk te maken is het van belang dat de noodzaak tot afstemming bekend is bij klanten en auditors.

Kennis over SOC 2 bij zowel auditors als klanten
Voor een succesvolle uitvoering is naast de afstemming ook van belang dat alle partijen (in ieder geval op hoofdlijnen) bekend zijn met SOC 2. De auditor moet de materie kunnen uitleggen aan de service- en gebruikersorganisaties zodat zij de juiste keuzes kunnen maken met betrekking tot hun controls, scoping en interpretatie. Indien de kennis niet aanwezig is bij de klanten levert dit geen uitdagingen op, aangezien de auditor de organisatie kan adviseren. Klanten moeten wel bekend zijn met SOC 2 omdat organisaties anders niet kiezen voor een SOC 2-rapport. Klanten moeten meegroeien met de ontwikkelingen op het gebied van assurance om SOC 2 een kans op adoptie te geven.

Daarnaast dienen auditors bijgeschoold te worden in de toepassing van de TSP Sectie 100 om zo een juiste interpretatie te kunnen geven aan de normen. De NOREA dient hier een actieve rol in te nemen als beroepsgroep van IT-auditors. Zonder kennis bij klanten en auditors over de uitvoering van een SOC 2-opdracht is de kans op nieuwe SOC 2-opdrachten klein.

Het inrichten van een audit trail dat voldoet voor een SOC 2-audit
Audits maken voor hun bewijsvoering gebruik van een audit trail: een spoor van bewijs, zoals logbestanden, die bewijzen hoe een control functioneert. Uit interviews is gebleken dat het inrichten van een audit trail voor SOC 2 aandacht behoeft. Het ontsluiten van het juiste bewijs kan lastig zijn, maar is van vitaal belang voor de audit. Als de opzet, bestaan of werking van een control niet kan worden getoetst, kan de auditor geen goedkeuring verlenen over de control.

Bij het starten van een SOC 2-opdracht dient er aandacht besteed te worden aan het audit trail: zodra de normen geïnterpreteerd zijn en vertaald naar controls moet er gekeken worden hoe het juiste bewijs ontsloten kan worden. Dit voorkomt onnodig zoekwerk tijdens de audit en verbetert de toetsing van de controls. Indien het audit trail niet naar behoren kan worden ingericht, heeft dit (aanzienlijke) consequenties op het verloop van de audit.

Draagvlak met betrekking tot assurance
Het gedachtengoed van de organisatie met betrekking tot assurance moet ondersteuning bieden aan het proces. Van belang is dat het management van de organisatie assurance niet ziet als een kwestie van “vinkjes zetten” maar de achterliggende meerwaarde van assurance inziet. SOC 2 is een stringente audit en zal de eerste keer niet per definitie goed afgerond worden (verkeerde interpretatie, onvoldoende bewijsvoering etc.). Van belang is dat het management dit ziet als leermoment en doorgaat met de audits. Er moet draagvlak zijn dat het leervermogen van de organisatie stimuleert.

Gebruikersorganisaties dienen mee te groeien met ontwikkelingen op het gebied van assurance
Zoals eerder benoemd is het van belang dat gebruikersorganisaties meegroeien met ontwikkelingen. In een tijd waar een NOREA Richtlijn 3402 niet per sé de juiste assurance afgeeft over een proces is het van belang dat organisaties zich verdiepen in ontwikkelingen en niet stug blijven vragen om dezelfde rapportages. Zonder deze groei zal men niet de meerwaarde van SOC 2 inzien en op de huidige koers blijven.

Indien gebruikersorganisaties meegroeien ontstaat er een “slimmere” assurancemarkt waar gerichter en effectiever gehandeld kan worden. Dit geeft SOC 2 een kans op adoptie en draagt bij aan vernieuwing in het werkgebied assurance. Zonder deze groei heeft SOC 2 weinig kans. Voor serviceorganisaties is een randvoorwaarde dat gebruikersorganisaties op de hoogte zijn van SOC 2 en instemmen met het opleveren van een SOC 2-rapport, voordat de opdracht wordt gegund.

Ondersteuning vanuit de NOREA
Van cruciaal belang is dat er voldaan wordt aan de randvoorwaarde met betrekking tot ondersteuning vanuit de NOREA. De NOREA als beroepsgroep is verantwoordelijk voor het registreren van IT-auditors en het bijscholen van haar leden. De NOREA moet de kennis over de toepassing van de TSP Sectie 100 overdragen of verder laten onderzoeken in het geval dat deze kennis nog niet beschikbaar is. De kennis van de auditor is voor een deel afhankelijk van de NOREA die informatievoorziening over ontwikkelingen regelt.

Indien de NOREA deze verantwoordelijkheid niet op zich neemt, bestaat de kans dat eerdere punten met betrekking tot afstemming met de auditor en kennis over SOC 2 bij zowel auditors en klanten niet haalbaar zijn. De NOREA dient dit te faciliteren omdat zonder deze kennis auditors onvoldoende voorbereid kunnen zijn op de uitdagingen van een SOC 2-audit. Zonder deze continue ondersteuning van de NOREA is de kans op een succesvolle uitvoering van een SOC 2-opdracht laag.

Afnemen van een nulmeting
Doordat een SOC 2-audit op basis van de TSP Sectie 100 plaatsvindt is het voor zowel auditor als serviceorganisatie te adviseren een nulmeting uit te voeren voordat de daadwerkelijke audit plaatsvindt. Een nulmeting helpt de auditor en de auditee een gedeelde interpretatie te geven aan de normen, het audit trail te testen en biedt een mogelijkheid om voor de audit geconstateerde bevindingen te verhelpen. Zonder een nulmeting kan het voorkomen dat de organisatie de normen anders interpreteert dan de auditor of dat er geen bewijs kan worden ontsloten. Voor het succesvol uitvoeren van een SOC 2-opdracht is nulmeting aan te raden.

Duidelijkheid over mogelijke aanpassingen op de bedrijfsvoering
Afhankelijk van de interpretatie van een norm kan het zijn dat reeds geïmplementeerde controls voldoende zijn of dat extra controls wenselijk zijn. Extra controls kunnen leiden tot aanpassingen in de bedrijfsvoering. Voor organisaties is het van belang dit tijdig te weten zodat de juiste maatregelen kunnen worden getroffen. Hierbij ligt de verantwoordelijkheid bij de auditor om in te schatten wanneer extra controls noodzakelijk zijn. Hierover dient de auditor duidelijkheid te kunnen verschaffen, alsmede wat voor impact dit heeft op de huidige bedrijfsvoering.

Het leervermogen van de organisatie wordt gestimuleerd
Hier is enige mate van samenhang met het benodigde draagvlak voor assurance: een SOC 2-audit kan de eerste keer moeizaam verlopen. Dit is echter een kans om het leervermogen van de organisatie te stimuleren en personeel mee te laten denken over verbetering. SOC 2 steunt op dit leervermogen omdat organisaties niet elk jaar een audit uit gaan laten voeren waarop ze slecht zullen scoren, als dit niet verplicht is. Het leervermogen dient om de organisatie verbetering aan te laten brengen zodat bij de volgende audit betere resultaten worden behaald. Dit komt de levensloop van SOC 2 ook ten goede, omdat organisaties niet jaarlijks willen zakken voor een audit. Voor een SOC 2-opdracht is leervermogen vereist, omdat anders niet te bepalen valt of organisaties de audit aanhouden als deze niet verplicht is.

Internationaal geaccepteerde SOC 2-rapportage
Kennis van toepasselijke wet- en regelgeving
Voordat een rapportage als internationaal geaccepteerd kan worden aangemerkt, is het van belang dat een organisatie zekerheid heeft dat er voldaan is aan alle relevante wet- en regelgeving alsmede beroepsreglementen. Zonder deze zekerheid is de kans aanwezig dat de rapportage niet wordt geaccepteerd door Amerikaanse organisaties.

Een CPA ondertekent de rapportage
Waar in Nederland een RE-geregistreerde IT-auditor een SOC 2-rapportage dient te ondertekenen, dient volgens de Amerikaanse richtlijn een CPA (Certified Public Accountant) de rapportage te ondertekenen. In Nederland zijn ook CPA's aanwezig (vooral bij de grotere accountancykantoren) die deze rapportages kunnen ondertekenen.

BIJLAGE 8 ONDERBOUWING PROBLEEMSTELLING

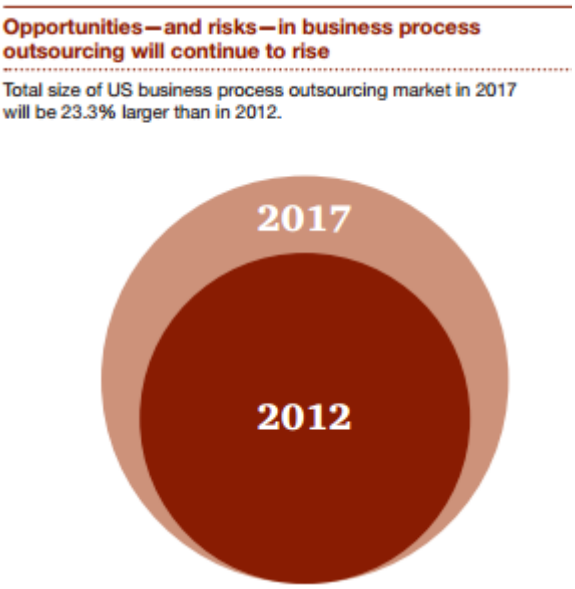
Inleiding
In deze bijlage is de onderbouwing opgenomen van de probleemstelling “welk type organisatie heeft baat bij een SOC 2-rapportage en hoe kan de SOC 2-richtlijn het meest effectief geïmplementeerd en/of getoetst worden, op basis van welke uitvoeringscriteria en leidt dit tot een algemeen toepasbare oplossing?”. In hoofdstuk zes is enkel de samenvatting van de deelvraag opgenomen.

Beantwoording
Welk type organisatie heeft baat bij een SOC 2-rapportage?
Het type organisatie dat baat heeft bij een SOC 2-rapportage valt niet onder één naam te groeperen. Er zijn meerdere kenmerken van het type organisatie dat baat heeft bij een SOC 2, maar hier valt geen overkoepelende term aan te geven. Op basis van de TSP Sectie 100 en de kenmerken van de geïnterviewde organisaties zal invulling worden gegeven aan dit onderdeel.

Vanuit de TSP Sectie 100 moet voldaan zijn aan de volgende punten voordat de TSP Sectie 100 gebruikt kan worden voor toetsing van een organisatie:

- Er is sprake van te auditen uitbestede processen;
- De te toetsen criteria hebben geen direct verband met de financiële verslaglegging;
- Er is sprake van een toetsbare IT-infrastructuur;
- De te auditen elementen zijn operational controls.

Los van het feit of de organisatie binnen het organisatietype valt dat baat heeft bij SOC 2 kan er niet getoetst worden op basis van de TSP Sectie 100 en kan er geen SOC 2-rapportage opgeleverd worden indien er niet is voldaan aan deze voorwaarden. Organisaties voldoen al snel aan deze kenmerken, gezien de huidige en verwachte mate van uitbesteding (figuur negentien).



figuur 19: huidige en verwachte mate van uitbesteding (Coopers, Pricewaterhouse, 2013)

Op basis van de interviews blijkt dat het type organisatie dat baat heeft bij een SOC 2-rapportage de volgende kenmerken heeft:

- Een complex assurancelandschap (door verschillende normenkaders en frameworks vanuit verschillende partijen) wat idealiter vereenvoudigd kan worden door een vastgesteld, marktontwikkeld, internationaal geaccepteerd normenkader;
- Een wens heeft om mee te groeien met ontwikkelingen op het gebied van assurance en (aankomende) IT-dreigingen;
- Het assuranceproces efficiënter en eenvoudiger maken door te streven naar een gestandaardiseerd assurancerapport, dat de wensen en eisen van meerdere gebruikersorganisaties af kan dekken;
- Een wens om Amerikaanse klanten te werven door een internationaal georiënteerde SOC 2-rapportage;

- Kennis op het gebied van SOC 2 (zowel gebruikers- als serviceorganisaties);
- De organisatie heeft leervermogen en kan dit gericht toepassen;
- Assurance wordt gezien als een proces met meerwaarde, niet als een kwestie van “vinkjes zetten”.

Gezien er te weinig informatie beschikbaar is over de mate waarin klantvragen en eigen initiatief van belang zijn voor het starten van een SOC 2-opdracht kan hier geen uitspraken over worden gedaan.

Het type organisatie dat baat heeft bij SOC 2 is te herkennen aan de bovenstaande kenmerken. Dit levert echter geen concreet profiel op. Op basis van het onderzoek wordt gesteld dat kleinere organisaties (bijvoorbeeld delen van het MKB) geen baat hebben bij SOC 2 doordat er sprake moet zijn van internationale klanten, of een complex assurancelandschap of een wens om vereenvoudiging door te voeren in het assuranceproces. De eerder genoemde kenmerken kunnen worden gebruikt om te bepalen of een organisatie baat heeft bij SOC 2, maar dienen niet gehanteerd te worden als een concreet profiel. Voor het ontwikkelen van een profiel is verder onderzoek nodig.

Hoe kan de SOC 2-richtlijn het meest effectief geïmplementeerd en/of getoetst worden?
Voor het succesvol ten uitvoer brengen van een SOC 2-opdracht zijn verschillende elementen van belang. Dit zijn:

- Afstemming tussen klant en auditor;
- Het uitvoeren van een nulmeting;
- Betrokken partijen zijn bekend met de SOC 2-richtlijn;
- Het inrichten van een audit trail voor SOC 2;
- Werkwijze conform de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100;
- Ondertekening door een CPA (indien een internationaal geldige SOC 2-rapportage is gewenst);
- Betrokken partijen zijn bekend met de juridische overwegingen van een SOC 2-rapportage.

Deze punten zijn geïdentificeerd op basis van de gevoerde interviews en het literatuuronderzoek. Elk element is individueel ingevuld om te komen tot een collectie van best practices.

<u>Afstemming tussen klant en auditor</u>
Zoals in deelvraag drie uitvoerig behandeld is, is het van belang om afstemming te zoeken. De abstractie van de normen van de TSP Sectie 100, de juiste scoping en het afnemen van een nulmeting zijn acties die voortkomen uit deze afstemming. Zonder deze afstemming kan het succesvol afronden van een SOC 2-opdracht bemoeilijkt worden door verschillende visies op normen of een verkeerde inschatting vanuit de klant.

Het afstemmen tussen de klant en auditor hoeft niet veel tijd te kosten, maar is cruciaal voor het verdere verloop van de opdracht. Zonder afstemming kunnen misverstanden ontstaan wat ten koste van het resultaat gaat.

<u>Het uitvoeren van een nulmeting</u>
Gezien organisaties niet bekend zijn met de TSP Sectie 100 is het aan te raden een nulmeting uit te voeren. Dit geeft de organisatie duidelijkheid omtrent de stand van zaken. Zo kan voor de daadwerkelijke audit herstelwerk worden uitgevoerd indien nodig en heeft de organisatie een hogere kans om de audit succesvol af te ronden.

Betrokken partijen zijn bekend met de SOC 2-richtlijn
Van belang voor de succesvolle uitvoering van een SOC 2-opdracht is de bekendheid van de richtlijn. Indien gebruikersorganisaties niet bekend zijn met het rapport, is de kans groot dat zij niet zullen instemmen met een SOC 2-rapportage. Daarnaast helpt het om de resultaten te interpreteren zodat misverstanden vermeden worden. Indien een SOC 2-rapportage gekozen wordt, is het aan te raden een kennissessie te organiseren over de werkwijze en toetsing van een SOC 2-audit. Zonder bekendheid is de kans klein dat een SOC 2-rapportage geaccepteerd wordt en zal men blijven werken met bijvoorbeeld de NOREA Richtlijn 3402.

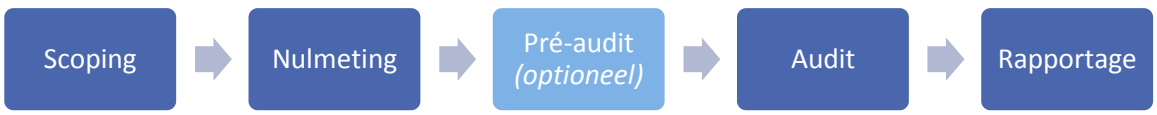
Het inrichten van een audit trail voor SOC 2
Voor een succesvol verloop van de SOC 2-audit is het van belang dat er stilgestaan wordt bij het audit trail. Abstracte normen dienen vertaald te worden in controls wanneer het nodig bewijs moeten kunnen ontsluiten. Het testen van dit proces dient tijdig te gebeuren om te zorgen dat het juiste bewijs op het juiste moment ontsloten wordt. Dit dient voor elke control ingebed te zijn en vanaf implementatie te functioneren. Zonder een degelijk audit trail is de kans aannemelijk dat de SOC 2-audit zonder succes doorlopen zal worden.

Werkwijze conform de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100
Voor organisaties die een SOC 2-rapport willen publiceren, is het aan te raden om indien mogelijk te werken volgens de NOREA Guidance to Richtlijn 3000 Service Organisation Control Reports for IT Service Organisations gebaseerd op het AIPCA SOC 2-rapportmodel en de TSP Sectie 100. Dit geeft organisaties de mogelijkheid om volgens een erkend product te werken en zodoende te leren hoe SOC 2 conform Nederlandse wet- en regelgeving geïmplementeerd dient te worden. Voor organisaties met internationale aspiraties is een mogelijkheid een Nederlandse SOC 2 uit te brengen, om zo ervaring op te doen met SOC 2 en de TSP Sectie 100 en tegelijkertijd onderzoek te doen naar de eisen voor een Amerikaanse SOC 2 om in een later stadium een Amerikaanse SOC 2-rapportage te publiceren.

Ondertekening door een CPA
Voor de Amerikaanse SOC 2-rapportage is het van belang dat een CPA de rapportage ondertekent. Voor organisaties die een Amerikaanse SOC 2-rapportage wensen is het noodzakelijk om hier van tevoren bij stil te staan. Er moet óf een CPA in dienst zijn van de organisatie óf in dienst van de auditor die de rapportage kan ondertekenen. Zonder deze ondertekening is de rapportage niet geldig op basis van Amerikaanse eisen.

Betrokken partijen zijn bekend met de juridische overwegingen van een SOC 2-rapportage
Voordat begonnen wordt met een SOC 2-opdracht is het van belang dat alle partijen bekend zijn met de overwegingen die bij een SOC 2-rapport horen. Of er voor een Nederlandse of een Amerikaanse rapportage gekozen wordt, beide rapportages brengen overwegingen met zich mee. Het is aan te raden deze overwegingen te bespreken met alle betrokken partijen voor de opdracht gegund wordt, aangezien dit van invloed is op de scope van de opdracht.

Bovenstaande punten uiten zich in de volgende implementatieaanpak (figuur twintig):



figuur 20: SOC 2-implementatieaanpak

Tijdens de scoping worden de te toetsen principles vastgesteld en wordt afstemming met de organisatie gezocht voor de interpretatie van de normen. Zodra de afstemming en scoping afgerond is wordt een nulmeting afgerond om inzicht te scheppen voor auditor en organisatie in de stand van zaken. Op basis van (mogelijke) bevindingen kan gekozen worden voor tijd voor het implementeren van herstelwerkzaamheden. Indien gewenst kan er een pré-audit plaatsvinden, bijvoorbeeld door een ander adviesbureau, om de objectiviteit of voorbereiding te optimaliseren. De volgende stap is het afnemen van de daadwerkelijke audit om vervolgens een concept rapportage op te leveren ter afstemming. Na afstemming wordt de rapportage definitief ondertekend en overlegd.

Welke uitvoeringscriteria zijn relevant?
De criteria zoals benoemd in deelvraag vier geven richting aan dit element van de probleemstelling. Gedurende het onderzoek zijn criteria aan het licht gekomen die bepalen of een SOC 2-opdracht succesvol kan worden uitgevoerd. Deze criteria zijn:

- Afstemming met de auditor;
- Kennis over SOC 2 bij zowel auditors als klanten;
- Het inrichten van een audit trail dat voldoet voor een SOC 2-audit;
- Draagvlak met betrekking tot assurance;
- Gebruikersorganisaties dienen mee te groeien met ontwikkelingen op het gebied van assurance;
- Ondersteuning vanuit de NOREA;
- Afnemen van een nulmeting;
- Duidelijkheid over mogelijke aanpassingen op de bedrijfsvoering;
- Het leervermogen van de organisatie wordt gestimuleerd.

Deelvraag vier gaat uitgebreid in op deze criteria. Onderbouwing per criterium is te vinden in paragraaf 6.4.

Leidt dit tot een algemeen toepasbare oplossing?
SOC 2 en de TPS Sectie 100 zijn redelijk flexibel in gebruik. Door de mogelijkheid om één of meer principles te toetsen kan een organisatie met een redelijke mate van vrijheid bepalen wat getoetst gaat worden. Hoe het getoetst gaat worden kan de organisatie echter niet bepalen: dit is vastgelegd in de normen van de TSP Sectie 100. Door de abstractie van deze normen is hier ook flexibiliteit te vinden. Andere normenkaders geven harde technische eisen waaraan voldaan dient te worden. Hierdoor neemt de algemene toepasbaarheid wel af, omdat er sprake is van een strikte set van maatregelen die zeer nauw zijn geformuleerd.

Voor wat betreft SOC 2 en de TSP Sectie 100 is er sprake van een algemeen toepasbare oplossing. Per organisatie zal de scope verschillen maar hoeft er verder (weinig tot) geen maatwerk te gebeuren. Zolang voldaan wordt aan de eisen zoals eerder benoemd kan elke organisatie die het wenst een SOC 2-opdracht laten uitvoeren.