



Atos Origin informs and enriches people's lives through the provision of personalised, secure and reliable technology- and people-based services.

# Service Quality Reporting

Management reporting ten behoeve van de ISAE 3402

**Ruud Brunenberg**

**8 Juni 2011**

**Eindhoven**

Versie: 1.0

08-06-11

Ruud Brunenberg

Titel: Service quality reporting  
 Ondertitel: Management reporting ten behoeve van de ISAE 3402

Auteur: Ruud Brunenberg  
 Onderwijsinstelling: Fontys Hogeschool Eindhoven  
 Studie: Bedrijfskundige Informatica  
 Studentnummer: 2108193  
 Afstudeerperiode : 7 februari 2011 – 17 juni 2011

Versie: 1.0  
 Status: Initieel / Concept / **Definitief**  
 Eigenaar: Ruud Brunenberg

Organisatie: Atos Origin B.V.  
 High Tech Campus 51/52  
 5656 AG Eindhoven

Organisatie begeleider: Hans Kappert  
 Director Internal Audit

## Document Historie

| Revisies |            |                      |                                                                                                                                                                                  |                 |
|----------|------------|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Versie   | Status     | Datum                | Wijzigingen                                                                                                                                                                      | Eindredacteur   |
| 0.1      | Concept    | 25-05-11             | Eerste concept versie volledige scriptie                                                                                                                                         | Ruud Brunenberg |
| 0.11     | Concept    | 26-05-11             | Review consistentie                                                                                                                                                              | Ruud Brunenberg |
| 0.2      | Concept    | 31-05-11             | Feedback Jos Papenhuijzen verwerkt                                                                                                                                               | Ruud Brunenberg |
| 0.3      | Concept    | 06-06-11<br>07-06-11 | Feedback verwerkt Hans Kappert, Ben de Backker, Cees Geerts en Myriam Krebbekx<br><br>Summary geschreven en stukje herschreven van het aanvullend advies. Bijlage E&F toegevoegd | Ruud Brunenberg |
| 1.0      | Definitief | 07-06-11             | Kosten en baten toegevoegd, Laatste review - final versie.                                                                                                                       | Ruud Brunenberg |

| Distributie |                  |                                                                                                   |                                                                                                                                                                    |
|-------------|------------------|---------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Versie      | Datum verzending | Naam                                                                                              | Functie                                                                                                                                                            |
| 0.1         | 25-05-11         | Hans Kappert<br>Jos Papenhuijzen<br>Cees Geerts<br>Ben de Backker<br>Myriam Krebbekx              | Bedrijfsbegeleider/Director internal audit<br>Sr. Customer compliance manager<br>Compliance & Security Officer<br>Quality & Security manager<br>Docentbegeleidster |
| 0.11        | 26-05-11         | Distributielijst idem aan v0.1                                                                    |                                                                                                                                                                    |
| 1.0         | 08-06-11         | Distributielijst idem aan v0.1. Verder:<br>Sheilindra Soebhag<br>Yvette Friebe<br>Dhr. E. Obdeijn | Lead IT Auditor<br>Docent Fontys Hogeschool<br>Extern gecommitteerde Fontys Hogeschool                                                                             |

| Reviews |              |                  |                                            |        |
|---------|--------------|------------------|--------------------------------------------|--------|
| Versie  | Datum review | Naam             | Functie                                    | Paraaf |
| 0.11    | 27-05-11     | Jos Papenhuijzen | Sr. Customer compliance manager            | JP     |
| 0.11    | 30-05-11     | Myriam Krebbekx  | Docentbegeleidster                         | MK     |
| 0.1     | 31-05-11     | Hans Kappert     | Bedrijfsbegeleider/Director internal audit | HK     |
| 0.11    | 31-05-11     | Ben de Backker   | Quality & Security manager                 | BB     |
| 0.11    | 31-05-11     | Cees Geerts      | Compliance & Security Officer              | CG     |

## Contactgegevens betrokkenen.

| Fontys Hogeschool:      | Ruud Brunenberg                                                                    |
|-------------------------|------------------------------------------------------------------------------------|
| Naam                    | Ruud Brunenberg                                                                    |
| Studentnummer           | 2108193                                                                            |
| Opleiding               | Bedrijfskundige Informatica                                                        |
| Profiel/Innovatiegebied | Business / IMS                                                                     |
| Adres                   | Liebetehofstraat 31                                                                |
| Postcode                | 6002 CM                                                                            |
| Plaats                  | Weert                                                                              |
| Telefoon                | 06 – 21 46 87 06                                                                   |
| E-mail adres            | <a href="mailto:R.Brunenberg@student.fontys.nl">R.Brunenberg@student.fontys.nl</a> |
| Afstudeerperiode        | van 7 februari 2011 t/m 17 juni 2011                                               |

| Fontys Hogeschool | Stagebureau Bedrijfskundige Informatica                    |
|-------------------|------------------------------------------------------------|
| Naam              | A.H.M (Antoniet) Barten- van der Rijt                      |
| Functie           | Administratief medewerker                                  |
| Adres             | Rachelsmolen 1 (Gebouw R1)                                 |
| Postcode          | 5600 AH                                                    |
| Plaats            | Eindhoven                                                  |
| Telefoon          | 0877 – 871 385                                             |
| E-mail adres      | <a href="mailto:a.barten@fontys.nl">a.barten@fontys.nl</a> |

| Fontys Hogeschool: | Docent Begeleider                                              |
|--------------------|----------------------------------------------------------------|
| Naam               | M.W.J. (Myriam) Krebbekx                                       |
| Functie            | Docent                                                         |
| Adres              | Rachelsmolen 1 (Gebouw R1)                                     |
| Postcode           | 5612 MA                                                        |
| Plaats             | Eindhoven                                                      |
| Telefoon           | 0877-870 553                                                   |
| E-mail adres       | <a href="mailto:m.krebbekx@fontys.nl">m.krebbekx@fontys.nl</a> |

| Atos Origin  | Opdrachtgever                                                              |
|--------------|----------------------------------------------------------------------------|
| Naam         | N.M. (Nico) Siepel                                                         |
| Functie      | Country Quality Manager Netherlands                                        |
| Adres        | High Tech Campus 51/52                                                     |
| Postcode     | 5656 AG                                                                    |
| Plaats       | Eindhoven                                                                  |
| Telefoon     | 06 – 53 36 24 90                                                           |
| E-mail adres | <a href="mailto:Nico.siepel@atosorigin.com">Nico.siepel@atosorigin.com</a> |

| Atos Origin  | Bedrijfsbegeleider                                                           |
|--------------|------------------------------------------------------------------------------|
| Naam         | J.J.W. (Hans) Kappert                                                        |
| Functie      | Director Internal Audit                                                      |
| Adres        | High Tech Campus 51/52                                                       |
| Postcode     | 5656 AG                                                                      |
| Plaats       | Eindhoven                                                                    |
| Telefoon     | 06 – 22 41 19 38                                                             |
| E-mail adres | <a href="mailto:Hans.kappert@atosorigin.com">Hans.kappert@atosorigin.com</a> |

## Voorwoord

3 december 2010, dat was de datum dat ik in contact kwam met Hans Kappert. In het kader van mijn studie bedrijfskundige informatica was ik op dat moment bezig met het afronden van het vak IT auditing. Hiervoor had ik met mijn projectgroep op die betreffende vrijdag een gesprek om te kijken of we een audit in de praktijk konden uitvoeren bij Atos Origin. Inmiddels zijn we een half jaar verder en voor u ligt mijn scriptie met als onderwerp service quality reporting.

Van het een is dus het ander gekomen; Mijn projectgroep en ik hebben indertijd toestemming gekregen om een audit uit te voeren bij Atos Origin. Gedurende die tijd was ik parallel op zoek naar een bedrijf om af te studeren. Atos Origin heeft mij tijdens de audit kunnen boeien als bedrijf en via Hans Kappert heb ik de mogelijkheid gekregen om mijn verblijf te verlengen. Ditmaal geen kleine praktijkopdracht, maar een uitdagende afstudeeropdracht om mijn studie bedrijfskundige informatica, ook wel ICT & Business, aan de Fontys Hogeschool ICT te Eindhoven af te ronden.

Atos Origin is een internationale IT-dienstverlener die wereldwijd actief is in 40 landen. Met een jaaromzet van 5,5 miljard euro en 50.000 medewerkers is Atos Origin een van de grote spelers wereldwijd. Begin juli zal Atos Origin nog een grotere speler worden omdat men dan fuseert met Siemens Integrated Systems. Daarmee komt het aantal medewerkers op meer dan 80.000, met een verwachte jaaromzet van 9 miljard euro.

Aangezien Hans Kappert fungeert als director internal audit zal het u niet verbazen dat mijn opdracht raakvlakken heeft met het vakgebied IT auditing. Mijn afstudeeropdracht is indertijd als volgt geformuleerd:

“Het completeren en implementeren van management rapportages ten behoeve van het aantoonbaar ‘in control’ zijn als onderdeel van de ISAE 3402 Assurance Standaard”

De ISAE 3402 is een third party reporting standaard die vanaf juni 2011 de oude SAS-70 standaard vervangt. Een ISAE 3402 rapport heeft als doel om de klant zekerheid te verschaffen dat de services die zij heeft uitbesteed aan de serviceorganisatie (in dit geval dus Atos Origin) goed beheerd worden (in control zijn). Dit is nodig voor de onderbouwing van de jaarrekening van de klant.

In het begin heb ik getwijfeld of ik met deze opdracht mijn competenties wel kon afdekken en of de opdracht niet te mager was om af te studeren. Naarmate ik de opdracht verder ging definiëren en uitschrijven werd de omvang me pas duidelijk. Tijdens het definiëren bleek dat de opdracht enorm divers was met voldoende mogelijkheden om mijn competenties te kunnen aantonen.

Omdat het een nieuwe standaard betreft kan ik mijns inziens terugkijken op een innovatieve opdracht. Voor zowel Atos Origin, de klant van Atos Origin en de service auditor was de standaard nieuw. Documentatie was dan ook niet of nauwelijks voor handen waardoor ik gedurende mijn afstudeerperiode constant meer theoretische kennis heb moeten vergaren.

Nu ik mijn afstuderen heb afgerond kan ik terugkijken op een geslaagde opdracht en samenwerking. Dit was niet mogelijk geweest als ik niet ondersteund zou zijn door een aantal medewerkers van Atos Origin. Daarom wil ik in het bijzonder de volgende mensen bedanken: Hans Kappert, als mijn bedrijfsbegeleider, Ben de Backker, Cees Geerts en Jos Papenhuijzen. Verder wil ik alle mensen die betrokken zijn geweest bij mijn afstuderen bedanken voor hun tijd en input. De medewerkers waren altijd bereid om te helpen of om nadere toelichting te geven. Tot slot wil ik voor de ondersteuning vanuit Fontys Hogeschool mijn docentbegeleidster Myriam Krebbekx bedanken.

Rest mij u veel leesplezier te wensen!

Eindhoven, juni 2011  
Ruud Brunenberg

## Inhoudsopgave

|                                                |    |
|------------------------------------------------|----|
| Samenvatting.....                              | 1  |
| Summary .....                                  | 3  |
| Verklarende woordenlijst .....                 | 5  |
| 1. Inleiding .....                             | 7  |
| 2. Beschrijving Atos Origin .....              | 9  |
| 3. De opdracht.....                            | 12 |
| 3.1 Achtergrond en Beginsituatie .....         | 12 |
| 3.2 Gewenste eindsituatie .....                | 12 |
| 3.3 Opdrachtoomschrijving.....                 | 12 |
| 3.4 Gewijzigde opdracht.....                   | 15 |
| 4. Achtergrond & Theoretische verdieping ..... | 17 |
| 4.1 Waarom een ISAE 3402?.....                 | 17 |
| 4.2 Een ISAE 3402 rapport.....                 | 18 |
| 4.3 De weg naar een ISAE 3402.....             | 19 |
| 4.4 SAS-70 vs. ISAE 3402 .....                 | 21 |
| 5. Onderzoek, analyse & advies.....            | 23 |
| 5.1 Onderzoek & Analyse.....                   | 23 |
| 5.2 Advies.....                                | 27 |
| 6. Implementatie.....                          | 28 |
| 7. Aanvullend advies & Best Practice .....     | 31 |
| 8. Kosten en Baten.....                        | 32 |
| 9. Conclusies & Aanbevelingen.....             | 33 |
| Evaluatie.....                                 | 35 |
| Literatuurlijst .....                          | 37 |
| Bijlagen.....                                  | 38 |

## Samenvatting

Mijn afstuderen heeft in de periode medio februari tot medio juni 2011 plaatsgevonden bij Atos Origin. Atos Origin is een internationale IT dienstverlener die wereldwijd actief is in 40 landen. Bedrijven besteden services uit aan Atos Origin op het gebied van technische infrastructuur, platformen, middleware / databases en applicatiebeheer. Ik ben werkzaam geweest binnen de divisie managed services waar ik werkte voor de afdeling quality & security management.

Aanleiding voor mijn opdracht was dat de SAS-70 auditstandaard opgevolgd zou worden door de ISAE 3402 assurance standaard. Dit zijn standaarden die dienen om een onafhankelijk oordeel over de beheersing van de uitbestede services af te geven aan de klant in een vastgelegd rapportageformaat. Nationale en internationale wet- en regelgeving vereisen namelijk dat bedrijven in control zijn over hun uitbestede diensten. Naast de operationele rapportages (Service Level Rapportages) zijn formele onafhankelijke auditrapporten noodzakelijk. De klant heeft deze nodig om aan zijn accountant aan te kunnen tonen dat ook de uitbestede services goed beheerst zijn. Zeker als deze services een (materieel) financieel belang hebben is een onafhankelijk auditrapport noodzakelijk voor de controle op de jaarrekening.

Voorheen werden deze rapporten opgesteld volgens de SAS-70 standaard. Deze standaard kende echter een aantal beperkingen waardoor een opvolger is ontwikkeld: De ISAE 3402. Ten opzicht van de SAS-70 kent de ISAE 3402 een aantal verschillen waarvan de belangrijkste 2 zijn: een risico analyse en een management assertion. Deze 2 punten zijn verplicht in de ISAE 3402 en laatstgenoemde is de concrete aanleiding geweest voor mijn afstudeeropdracht.

Voor de ISAE 3402 moet het management een management assertion letter ondertekenen die bij het rapport wordt toegevoegd. Met deze brief neemt het management van de serviceorganisatie (Atos Origin in dit geval) expliciet de verantwoordelijkheid voor de beheersing van de aan haar uitbestede services en de inhoud van het rapport. Om het management te ondersteunen bij het ondertekenen van deze brief zou er bottom-up gerapporteerd moeten worden waardoor men aantoonbaar kan maken dat de processen en daarmee de services goed beheerst zijn (in control). De vraag naar deze rapportages heeft geleid tot mijn afstudeeropdracht die als volgt is geformuleerd:

*"Het completeren en implementeren van management rapportages ten behoeve van het aantoonbaar 'in control' zijn als onderdeel van de ISAE 3402 Assurance Standaard"*

Om deze opdracht uit te voeren ben ik begonnen met het schrijven van een project initiation document volgens de PRINCE 2 methodiek. Omdat het een nieuwe standaard betrof en om me in te lezen in het auditing vakgebied heb ik eerst een theoretische verdieping gedaan. Vervolgens ben ik bij Atos Origin een onderzoek gestart om te inventariseren of er al rapportages waren die ik kon gebruiken of die ik kon uitbreiden en om te onderzoeken wat er precies gerapporteerd zou moeten worden. De resultaten uit dit onderzoek zouden bepalen welke activiteiten ik in een later stadium zou moeten uitvoeren om een rapportagecyclus te (ontwerpen en te) implementeren. De resultaten van het onderzoek heb ik vastgelegd in een onderzoeksrapport volgens de V2 methodiek. De belangrijkste bevindingen uit het onderzoek waren:

- Dat er monitoring controls waren. Dit zijn beheersmaatregelen (controls) die reflecteren op de functionering van processen en hun standaard beheersmaatregelen
- Dat er een tweetal rapportages waren over service quality, namelijk: compliance self assessments en service reviews. Deze 2 rapportages dekken de monitoring controls af.
- Dat de rapportages (compliance self assessments en service reviews) aan de onderkant van de organisatie nog niet goed en uniform waren ingeregeld.

Op basis van deze bevindingen heb ik het advies gegeven om eerst aan de onderkant de rapportagecyclus goed te implementeren alvorens te denken aan een rapportage voor de bovenkant van de organisatie. Als er aan de onderkant niets is valt er aan de bovenkant namelijk niets te consolideren. Dit advies heb ik vastgelegd in een adviesrapport en besproken met mijn stuurgroep. Hier is een opdrachtwijziging uit voortgevloeid.

De opdrachtwijziging hield in dat ik me in principe bezig ging houden met dezelfde activiteiten, alleen nu aan de onderkant van de organisatie. Concreet zou ik me bezig gaan houden met de implementatie van een online dashboard voor de compliance self assessments bij managed services. Verder zou ik nog een stuk aanvullend advies geven voor rapportage aan de bovenkant van de organisatie en ik zou een best practice rapport maken zodat de manier van werken bij Atos Origin NL wereldwijd verspreid kan worden. Atos Origin NL loopt op dit

gebied namelijk voor ten opzichte van de rest van de Atos Origin organisatie en het uiteindelijk doel is om wereldwijd uniform te gaan werken.

Voor de implementatie van de compliance self assessments heb ik het met gehele management van managed services gesprekken gevoerd en getracht draagvlak te creëren. De resultaten van de gesprekken heb ik vastgelegd in een requirements document waarin staat beschreven hoe de structuur, autorisaties en inrichting van de compliance self assessments zou moeten worden geïmplementeerd in het online dashboard. De informatie uit dit rapport is praktisch 1 op 1 overgenomen voor de inrichting van het online dashboard. Vervolgens heb ik een aantal tests uitgevoerd om te controleren of het ingericht dashboard overeenstemde met het requirements document. Tevens ben ik in deze periode aanspreekpunt geweest voor managers om uitleg te geven over en om ondersteuning te bieden bij de compliance self assessments. De resultaten van de eerste maand na de implementatie waren ruim naar verwachting. Er waren geen klachten over de inrichting en ruim 80% had de compliance self assessments ingevuld. Dit is een uitstekend resultaat voor een eerste maand.

Voor het aanvullend advies heb ik een klein onderzoek gedaan naar de requirements voor een rapportage aan de bovenkant van de organisatie. Mijn advies was om in de rapportage de volgende informatie op te nemen:

- Scores van de laatste operation manual audit. Dit is een audit waarbij de compliance van Atos Origins interne processen objectief is vastgesteld.
- Een professional judgment over de proces performance op geconsolideerd niveau middels stoplichtindicatoren
- Radargrafieken die de resultaten van de compliance self assessments weergeven op zowel geconsolideerd als primair niveau.
- Trend grafieken van de process performance en compliance
- Risico's

Naast deze rapportage zou er nog een formeel handtekeningen document moeten komen waarbij alle managers op unit of CDC niveau en hoger tekenen. Dit document zou een keer per jaar ingevuld moeten worden, ongeveer 2 maanden voordat de ISAE 3402 rapporten gedistribueerd worden naar de klanten. Met de rapportage en het handtekeningen document is het hoogste management voldoende ondersteund om de management assertion letter te ondertekenen.

In ontwikkeling is momenteel nog een best practice rapport wat gebruikt kan worden voor Atos Origin global. Hierin wordt de manier van werken met compliance self assessments en service reviews beschreven, evenals het advies wat hierboven is gegeven voor rapportage aan de bovenkant van de organisatie. Tevens wordt er een schatting gemaakt van de kosten en baten voor een volledige implementatie.

Mijn hele onderzoek bij elkaar genomen heb ik geconcludeerd dat Atos Origins constructie van compliance self assessments, service reviews en monitoring controls voldoende onderbouwing biedt om enerzijds aan te tonen dat Atos Origins processen en daarmee de services in control zijn en om anderzijds het management voldoende te ondersteunen bij het ondertekenen van de management assertion letter. Deze conclusie is tevens bevestigd door een externe auditor van Ernst & Young. Aan te bevelen valt wel om een rapportagecyclus te implementeren voor de bovenkant van de organisatie. Hiertoe zou ik aanbevelen om mijn advies voor de inhoud van deze rapportage over te nemen. Dit advies is doorgesproken met de manager van managed services die uitgesproken heeft dat de inhoud voor de rapportage voldoende en compleet is. Verder valt aan te bevelen om de werkwijze van Atos Origin NL te gaan gebruiken op global niveau. Tot slot zou ik nog willen aanbevelen om de volgende punten te verbeteren:

- **De compliance self assessments vragenlijst grondig reviewen**

De huidige vragenlijst heeft veel vragen die niet SMART geformuleerd zijn en de vragen zijn teveel gericht op de delivery vanuit de global factory NL. Aan te bevelen valt om de vragen SMARTer te formuleren en om een set vragen toe te voegen of aan te passen die specifiek bedoeld zijn voor de dirigerende rol voor de CDC's.

- **Beter controleren op de integriteit van de ingevulde percentages in de vragenlijst**

De Q&S'ers monitoren momenteel vooral de voortgang en niet zozeer de integriteit van de ingevulde percentages. Aan te bevelen valt om dit steekproefsgewijs vaker te doen.

- **Het online dashboard optimaliseren**

Momenteel worden er handmatig reminders uitgestuurd. Aan te bevelen valt om dit te automatiseren. Verder is het aan te bevelen om een functie in te bouwen in het online dashboard waarbij mensen zelf kunnen bepalen wanneer iets niet ingevuld kan worden. In het geval van bijvoorbeeld projectmanagement zijn er niet altijd projecten en een 0% of 100% score geeft een vertekend beeld in trendgrafieken.

## Summary

In order to graduate, I participated in an internship at Atos Origin from mid-February till mid-June 2011. Atos Origin is an international IT service provider which is active in 40 countries worldwide. Companies outsource services in the areas of technical infrastructure, platforming, middleware / databases and application management to Atos Origin. I worked in the division managed services where I worked for the department Quality & Security Management.

The fact that the SAS-70 audit standard would be succeeded by the ISAE 3402 assurance standard was the reason behind my graduation assignment. These standards serve to give clients an independent judgment in a fixed reporting format about the control of the outsourced services. National and international legislation and instructions demand that companies are in control for the services they outsourced. Besides the operational reporting (Service Level Reporting), formal and independent audit reports are necessary. The client needs such a report to prove to his accountant that the outsourced services are in control. An independent audit report is especially necessary for the control on the statements when these services are of (material) financial importance.

Before, these reports were composed according to the SAS-70 standard. However, this standard knew a number of restrictions causing a successor to be developed: the ISAE 3402. Compared to the SAS-70, ISAE 3402 has a number of differences. The most important two are: a risk analysis and a management assertion. These two are compulsory when the ISAE 3402 is used and the last one mentioned, the management assertion, was the concrete reason for my graduation assignment.

For the ISAE 3402, the management needs to sign a management assertion letter which is added to the report. With this letter, the management of the service organization (in this case that would be Atos Origin) takes explicit responsibility for the control of the services which have been outsourced to them and for the content of the report. In order to support the management with signing this letter, there should be bottom-up reported to prove that the processes and, with that, the services are in control. The request for these reports lead to my graduation assignment which has been formulated as follows:

*"Completing and implementing the management reporting for being demonstrably 'in control' as a part of the ISAE 3402 Assurance Standard".*

In order to execute this assignment, I started with writing a project initiation document, according to the PRINCE 2 methodology. Because the assignment regarded a new standard and to get more familiar with the auditing field, I started with deepening my theoretical knowledge. Subsequently, I started an investigation at Atos Origin to find out whether there already were reports which I could use or possibly extend, and to study what needed to be reported precisely. The results from this study would determine what activities I needed to execute in order to (develop and) implement a reporting cycle. The results of the study were registered according to the V2 methodology in a research report. The most important findings were that:

- There are so called monitoring controls which reflect on the functioning of processes and their standard controls
- There were two reports about service quality, namely: compliance self assessments and service reviews. Those two reports are covering the monitoring controls.
- The reports (compliance self assessments and service reviews) at the bottom of the organization were not good and uniformly implemented.

Based on the findings of my study, I advised to start with implementing a reporting cycle on the bottom level of the organization correctly before thinking about the reporting for the top level of the organization. After all, if there is nothing on the bottom level, there is also nothing that can be consolidated at the top level. I registered this recommendation in a recommendation report and discussed it with my steering committee. My assignment was altered, based on this recommendation.

The chance of the assignment implied that, in principal I would be dealing with the same activities, only now I would be dealing with the bottom level of the organization. Concrete, I would start implementing an online dashboard for the compliance self assessments for managed services. Furthermore, I would give an additional recommendation about management reporting for the top level of the organization and I would be writing a best practice report in order to spread the Dutch approach for working globally. Compared to other Atos Origin establishments, Atos Origin NL is ahead on this subject and the final goal is to start working uniformly worldwide regarding this subject.

For the implementation of the compliance self assessments I've had conversations with the complete management of managed services, trying to create support. The results of these conversations were registered in a requirements document which describes how the structure, authorizations, and organization of the compliance self assessments should be implemented in the online dashboard. The information from this report has been taken almost literally to establish the online dashboard. Next, I carried out some tests to check whether the set-up of the dashboard corresponded with the requirements document. Also, I was a focal point for the managers to explain the compliance self assessments and to provide support when necessary. The results of the first month after implementation were better than expected. There were no complaints about the set-up and more than 80 percent filled in the compliance self assessments. This is an excellent result for a first month.

For the additional recommendation, I did a small investigation into the requirements of a report to the top level of the organization. I recommended to insert the following information into the reports:

- Scores of the last operation manual audit. This is an audit where the compliance of Atos Origins internal processes is determined objectively
- A professional judgment about the process performance on consolidated level using traffic light indicators
- Radar graphs which show the results of the compliance self assessments on consolidated and primary level
- Trend graphs of the process performance and compliancy
- Risks

Besides these reports, there should be a formal signature document in which all managers on a unit or CDC level and above, sign. This document should be filled in once a year, approximately 2 months before the ISAE 3402 reports are distributed to the clients. With the reports and the signature document, the highest level of management is supported sufficiently to sign the management assertion letter.

A best practice report which can be used for Atos Original global is currently being developed. In this report, the way of working with compliance self assessments and service reviews is explained further, as is the recommendation which is given above for reporting on the top level of the organization. Furthermore, a rough estimate is given about the costs and benefits for a completely new implementation.

Taking my complete study into consideration, I concluded that Atos Origins construction of compliance self assessments, service reviews, and monitoring controls are sufficiently support to, on the one hand, prove that Atos Origins processes, and, with that the services, are in control, and, on the other hand, support the management sufficiently by signing the management assertion letter. This conclusion has also been confirmed by an external auditor of Ernst & Young. It is recommendable to implement a reporting cycle for the top level of the organization. To this end, I would recommend to take my recommendation about the content for this new report. This recommendation has been discussed with the manager of MS who has mentioned that the content of this report is adequate and complete. Furthermore, it is recommendable to start using the operating procedure of Atos Origin NL on a global level. Finally I would like to recommend to improve the following points:

- **To review the compliance self assessment questionnaire thoroughly**

The current questionnaire has a lot of questions which are not formulated SMART and a lot of questions are drawn up, based on the delivery from the global factory NL. I would recommend to formulate the questions in a more SMART way and to add or adjust a set of questions which are specially designed for the directing role of the CDC's.

- **To better check the integrity of the percentages**

The Q&S officers are currently mainly monitoring on the progress rather than the integrity of the percentages. I would recommend to at random check the integrity of the percentages more often.

- **To optimize the online dashboard**

Currently, reminders are sent out manually. I would recommend to automate this. Furthermore, I would recommend to build a function in the online dashboard which enables people to determine if questions can be answered or not. At the moment this is not possible but it would be desired. For example for project management: Projects are not always running so in that case a percentage cannot be filled in. 0% or 100% gives a distorted view in the trend graphs, so in that case people should be able to fill in nothing or something like 'none'.

## Verklarende woordenlijst

| Woord/Begrip                      | Verklaring/toelichting                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AICPA                             | American Institute of Certified Public Accountants. Deze instantie schrijft de ISAE 3402 richtlijnen voor.                                                                                                                                                                                                                                                                                                                                        |
| ASB                               | Auditing Standard Boards.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Audit                             | Het controleren van een organisatie.                                                                                                                                                                                                                                                                                                                                                                                                              |
| Auditperiode                      | De periode waarover de auditor de audit uitvoert en bewijslast verzameld                                                                                                                                                                                                                                                                                                                                                                          |
| Auditplan                         | In dit document wordt de scope, de beheersdoelstellingen en beheersmaatregelen, de uitvoerende auditors en de planning vastgelegd.                                                                                                                                                                                                                                                                                                                |
| (B)BSC                            | (Business) Balanced Scorecard. Dit is een methode om inzicht te verkrijgen in de prestaties van een organisatie                                                                                                                                                                                                                                                                                                                                   |
| Beheersdoelstelling               | Een verklaring van de verwachting dat er een of meerdere beheersmaatregelen bestaan die effectief werken om risico's in toereikende mate te mitigeren en/of een bewerking inzake de jaarrekening te bereiken.                                                                                                                                                                                                                                     |
| Beheersmaatregel                  | Maatregelen die in het desbetreffende proces zijn geplaatst om te kunnen bepalen of de beheersdoelstelling goed is uitgevoerd.                                                                                                                                                                                                                                                                                                                    |
| Bestaan                           | Het bestaan betreft de geïmplementeerde beheersmaatregelen in het onderzoeksobject op een bepaald moment.                                                                                                                                                                                                                                                                                                                                         |
| CDC                               | Customer Delivery Center. Een unit die klantspecifieke diensten levert.                                                                                                                                                                                                                                                                                                                                                                           |
| COBIT                             | Control Objectives for Information and Related Technology, een standaard raamwerk voor het gestructureerd inrichten van de IT organisaties.                                                                                                                                                                                                                                                                                                       |
| Compliance                        | (intern toezicht op) naleving van wet- en regelgeving door organisaties en/of het werken volgens de normen en regels die een organisatie zelf heeft opgesteld.                                                                                                                                                                                                                                                                                    |
| Control(s)                        | Zie beheersmaatregel                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Control measure                   | Zie beheersmaatregel                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Control objective                 | Zie beheersdoelstelling                                                                                                                                                                                                                                                                                                                                                                                                                           |
| COSO                              | COSO is een management model dat is ontwikkeld door The Committee of Sponsoring Organizations of the Treadway Commission (COSO). Dit comité heeft aanbevelingen gedaan en richtlijnen aangegeven ten aanzien van interne controle en interne beheersing.                                                                                                                                                                                          |
| Compliance Self Assessment (CSA)  | Een subjectieve management rapportage waarvoor een vragenlijst wordt ingevuld om de compliancy van de processen te meten.                                                                                                                                                                                                                                                                                                                         |
| DMAIC                             | Define Measure Analyse Improve Control. Een six sigma methodiek waaruit de V2 methode is ontstaan.                                                                                                                                                                                                                                                                                                                                                |
| Dossier                           | Een bundeling van bewijslast.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Evidence                          | Bewijslast voor het aantonen dat een bepaalde beheersmaatregel in place of operationeel is.                                                                                                                                                                                                                                                                                                                                                       |
| Gebruikersorganisatie             | Zie user organisation                                                                                                                                                                                                                                                                                                                                                                                                                             |
| global factory NL (GF NL)         | Dit is een organisatieonderdeel van managed services. Hier worden gestandaardiseerde services geleverd.                                                                                                                                                                                                                                                                                                                                           |
| HTTS                              | High Tech Transactional Services. Een organisatie onderdeel van Atos Origin.                                                                                                                                                                                                                                                                                                                                                                      |
| IFAC                              | International Federation of Accountants.                                                                                                                                                                                                                                                                                                                                                                                                          |
| In control                        | De organisatie is in control wanneer alle processen goed beheerst zijn.                                                                                                                                                                                                                                                                                                                                                                           |
| ISACA                             | Information Systems Services Audit and Control Association. Een internationale beroepsvereniging van beroepen in de vakgebieden IT governance, IT auditing, informatiebeveiliging en risicomanagement van automatisering.                                                                                                                                                                                                                         |
| ISAE 3402                         | International standard on Assurance Engagements (ISAE) No. 3402. De internationale opvolger van SAS-70. Deze standaard ziet toe op zogenaamde Third Party Assurance rapportages. Met zo een derden verklaring wordt aangegeven dat een serviceorganisatie, waar een gebruikersorganisatie activiteiten aan heeft uitbesteed, 'in control' is. Deze verklaring is bedoeld voor de accountant van de klant ten behoeve van de jaarrekeningcontrole. |
| Jaarrekeningcontrole              | Een controle op het jaarlijkse overzicht van de financiële situatie van een bedrijf                                                                                                                                                                                                                                                                                                                                                               |
| Letter of Representation (LOR)    | Dit is een onderdeel van de ISAE 3402 waarmee verklaard wordt dat de verstrekte data eerlijk en volledig is (representatief).                                                                                                                                                                                                                                                                                                                     |
| Management assertion letter (MAL) | Dit is een getekende verklaring van het management van de serviceorganisatie waarbij ze de verantwoordelijkheid voor de beheersing van de aan haar uitbesteede services en de inhoud van het rapport op zich nemen.                                                                                                                                                                                                                               |
| Materialiteit                     | De mate van materieel belang. Ter illustratie: een project van 1 miljoen kost uiteindelijk 2 miljoen. Op een jaaromzet van 5,5 miljard is dit niet van materiaal belang, op een jaaromzet van 50 miljoen wel.                                                                                                                                                                                                                                     |
| Mgt.                              | Afkorting voor management.                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Woord/Begrip                      | Verklaring/toelichting                                                                                                                                                                                                                                                                                      |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitoring controls               | Dit zijn beheersmaatregelen die reflecteren op de functionering van processen en hun standaard beheersmaatregelen                                                                                                                                                                                           |
| Managed Services (MS)             | Een divisie binnen Atos Origin die er voor zorgt dat de contractafspraken die met de klanten zijn gemaakt over het beheer van de infrastructuur conform de overeengekomen specificaties worden nagekomen.                                                                                                   |
| Operations manager                | Een manager die zich bezighoudt met de dagelijkse aansturing van de dienstverlening voor een specifieke klant of groep van klanten                                                                                                                                                                          |
| Operations manual                 | Dit is een intern Atos Origin document waarin de processen beschreven staan, inclusief hoe ze uitgevoerd zouden moeten worden.                                                                                                                                                                              |
| Oprol                             | Dit is een bottom up proces waar er vanuit de evidence een oordeel wordt gevormd over de beheersmaatregelen en vanuit de beheersmaatregelen over de beheersdoelstellingen. Dit wordt uitgevoerd door de service auditor.                                                                                    |
| Opzet                             | De opzet omvat de formele inrichting van het onderzoeksobject op een bepaald moment.                                                                                                                                                                                                                        |
| PID                               | Afkorting voor: Project Initiation Document. Dit is een projectplan geschreven volgens de PRINCE2 methodiek. Hierin is de aanpak van de opdracht beschreven.                                                                                                                                                |
| Q&S'er                            | Quality & Security officer, dit zijn medewerkers van Atos Origin die de taak hebben om de audits te begeleiden en te zorgen voor kwaliteit en informatiebeveiliging voor een bepaalde afdeling.                                                                                                             |
| RACI                              | Het RACI-model is een matrix die gehanteerd wordt om de rollen en verantwoordelijkheden van de personen die bij een project of lijnwerkzaamheden betrokken zijn weer te geven. Elke letter geeft een verantwoordelijkheid weer: Responsible, Accountable, Checked en Informed.                              |
| RFC                               | Request for change. Dit is een document wat gebruikt wordt bij de PRINCE2 methodiek om een opdrachtwijziging vast te leggen.                                                                                                                                                                                |
| SAS-70                            | Statement on auditing Standards 70. Dit is een auditstandaard wat een verklaring inhoudt van een externe (audit) partij over de uitbestede services van een klant (in dit geval Atos Origin), die bedoeld is voor de accountant van de klant t.b.v. de jaarrekeningcontrole.                                |
| Services                          | Diensten. Een service of dienst wordt uitgevoerd door een set van processen te doorlopen.                                                                                                                                                                                                                   |
| Serviceorganisatie                | Dit is de organisatie die de uitbestede services verzorgt.                                                                                                                                                                                                                                                  |
| Service auditor                   | De auditor van de serviceorganisatie                                                                                                                                                                                                                                                                        |
| Siemens IT Solutions and Services | Het bedrijf waarmee Atos Origin een langdurig partnership is aangegaan.                                                                                                                                                                                                                                     |
| SLA                               | Service Level Agreement, dit is een type overeenkomst waarin afspraken staan tussen aanbieder en afnemer van een dienst of product.                                                                                                                                                                         |
| SOC                               | Statement of Control. Het statement impliceert met een verklaring dat de hoogste leiding in control is.                                                                                                                                                                                                     |
| SOx                               | Afkorting voor Sarbanes-Oxley. Dit is een Amerikaanse wet op het vlak van het besturen van bedrijven en de financiële verslaglegging door bedrijven. Bedrijven zijn SOx plichtig indien ze genoteerd zijn op de Amerikaanse beurs of dat er een bepaald percentage in handen is van een Amerikaans bedrijf. |
| TOD                               | Een Test of Design dient ervoor om te beoordelen of de beheersmaatregelen goed geïmplementeerd zijn in opzet en bestaan.                                                                                                                                                                                    |
| TOE                               | Een Test of Operating Effectiveness dient ervoor om te beoordelen of de beheersmaatregelen goed geïmplementeerd zijn in opzet, bestaan en werking.                                                                                                                                                          |
| Type I                            | Bij dit statement wordt alleen de opzet en bestaan getoetst                                                                                                                                                                                                                                                 |
| Type II                           | Bij dit statement wordt de opzet, het bestaan en de werking getoetst.                                                                                                                                                                                                                                       |
| User auditor                      | De accountant van de klant                                                                                                                                                                                                                                                                                  |
| User organisatie                  | Ook wel user organization. De organisatie die de services uitbesteedt aan de serviceorganisatie (Atos Origin in dit geval).                                                                                                                                                                                 |
| Werking                           | De werking omvat het functioneren van de beheersmaatregelen met betrekking tot het onderzoeksobject over een bepaalde periode.                                                                                                                                                                              |

## 1. Inleiding

*Hoe tonen we aan dat de aan ons uitbestede services 'in control' zijn?*

Dit is de vraag die centraal heeft gestaan tijdens mijn afstuderen. De klant eist bij een uitbestedingdeal veelal dat het leveren van een assurance verklaring wordt opgenomen in het contract. Dit is nodig omdat de klant of haar accountant enerzijds inzicht wil hebben in de uitbestede services en dan voornamelijk de services die een groot (materieel) financieel belang kennen. Anderzijds is dit vaak vereist vanuit de wetgeving, zoals in het geval van de Amerikaanse Sarbanes-Oxley wetgeving (SOx). Deze wet geeft aan dat het management van een organisatie aantoonbaar in control moet zijn van haar onderneming en dat de user auditor van de klant een verklaring nodig heeft om de jaarverslagen goed te keuren.

Consequentie voor de serviceorganisatie (Atos Origin in dit geval) is dat er een betrouwbare rapportage naar de klant moet gaan over de uitbestede services. Om ervoor te zorgen dat dit rapport gebaseerd is op een onafhankelijk en onpartijdig onderzoek wordt er altijd een 3<sup>e</sup> partij betrokken: de externe auditororganisatie. Atos Origin voorziet hierin door voor een aantal standaard diensten een (klantonafhankelijke) generieke ISAE 3402 verklaring uit te geven. Dit komt de efficiency ten goede en verlaagt de audit druk binnen de organisatie in vergelijking met specifieke verklaringen per klant.

Voor de rapportage zijn er een aantal internationale standaarden waarvan SAS-70 veruit de bekendste is. 15 juni 2011 moet deze standaard verplicht opgevolgd worden door een nieuwe standaard, namelijk de ISAE 3402. De standaarden lijken erg op elkaar, maar er is een essentieel verschil wat een impact heeft op de serviceorganisatie. Voor de ISAE 3402 moet het management van de serviceorganisatie namelijk een management assertion letter tekenen en aan het rapport toevoegen. Daarmee neemt het management van de serviceorganisatie expliciet de verantwoordelijkheid voor de beheersing van de aan haar uitbestede services en de inhoud van het rapport.

Om het management te ondersteunen bij het ondertekenen van de management assertion letter zou er een stuk rapportage moeten komen over service quality. Dit is de aanleiding geweest van mijn afstuderen bij de internationale IT dienstverlener Atos Origin.

Mijn opdracht was om te onderzoeken hoe deze rapportage het beste ingericht kon worden. Daarvoor zou het nodig zijn om met alle lagen van het management te praten en om draagvlak en management commitment te creëren. Met de resultaten uit dit onderzoek zou ik een rapportagecyclus moeten ontwerpen en implementeren. Het uiteindelijke doel zou zijn: een geïmplementeerd en werkend proces dat leidt tot een periodieke management rapportage.

Voor de uitvoering van de opdracht heb ik een projectmatige aanpak gekozen volgens de PRINCE 2 methodiek. De uitgestippelde strategie was indertijd om eerst achtergrondkennis te vergaren middels een theoretische verdieping. Vervolgens een groot toegepast onderzoek te doen binnen de organisatie en met de resultaten van dit onderzoek een ontwerp maken voor een proces en een management rapportage. Vervolgens zou ik dit ontwerp gaan implementeren.

Gedurende mijn toegepast onderzoek kwam ik er echter achter dat er geen draagvlak was om eerst een rapportage aan de bovenkant van de organisatie in te regelen omdat er aan de onderkant van de organisatie nog niet generiek gerapporteerd werd. Dit maakt consolidatie aan de bovenkant van de organisatie moeilijk realiseerbaar. Daartoe is mijn opdracht enigszins gewijzigd. In essentie heb ik dezelfde activiteiten ondernomen als mijn oorspronkelijke opdracht, alleen op een lager niveau in de organisatie. Met de wijziging van mijn opdracht zijn er een tweetal deliverables bijgekomen: een aanvullend advies voor de inrichting van rapportage op het niveau waar mijn opdracht in eerste instantie voor bedoeld was en een best practice rapport. Laatstgenoemd rapport wordt meegenomen naar Atos Origin Global. Atos Origin Nederland is op het gebied van audit rapportages namelijk het verste ten opzichte van alle andere Atos Origin organisaties. Uiteindelijk zou de manier van werken, zoals die in Nederland onder andere door mij geïmplementeerd is, zich als een olievlek moeten verspreiden over de andere Atos Origin vestigingen wereldwijd.

Deze scriptie beschrijft de resultaten van mijn afstuderen. Deze resultaten zijn verweven met een stuk proces en uitleg van gemaakte keuzes. Hoofdstuk 2 geeft een beschrijving van Atos Origin en mijn rol binnen de organisatie. Hoofdstuk 3 geeft alle details over de opdracht en de wijziging van mijn opdracht. Hoofdstuk 4 geeft een stuk globale achtergrondinformatie omdat ISAE 3402 en alles wat er bij hoort nogal complex is. Tevens worden de resultaten van mijn theoretische verdieping in dit hoofdstuk beschreven. Hoofdstuk 5 gaat in op de

resultaten van mijn toegepast onderzoek en het stukje advies wat daarbij hoorde. Dit advies heeft uiteindelijk geleidt tot de wijziging van mijn opdracht. Hoofdstuk 6 staat volledig in het teken van de implementatie: de inventarisatie, de implementatie, ondersteuning en testing. Hoofdstuk 7 beschrijft mijn aanvullend advies en de eerste resultaten van het best practice rapport. Vervolgens wordt er in hoofdstuk 8 kort ingegaan op de kosten en baten die met die project gemoeid zijn geweest en in hoofdstuk 9 wordt er afgesloten met de belangrijkste conclusies en aanbevelingen.

## 2. Beschrijving Atos Origin

Atos Origin is een internationale aanbieder van IT-diensten. Het bedrijf zet de visie van klanten om in resultaten door middel van hi-tech transactiediensten (HTTS), advies (Consulting), systeemintegratie (SI) en beheer (managed services). Het bedrijf heeft een jaaromzet van 5,5 miljard euro en heeft 50.000 werknemers in 40 landen, waarvan +/- 7000 in de Benelux. In de Benelux is Atos Origin marktleider. Verder is Atos Origin de wereldwijde IT-partner voor de Olympische Spelen en heeft een klantenkring bestaande uit internationale, gerenommeerde bedrijven uit alle sectoren. Atos Origin staat genoteerd aan de Paris Eurolist Market en opereert onder de namen Atos Origin, Atos Worldline (transactiediensten) en Atos Consulting.<sup>1</sup> De naam Atos Origin komt voort uit een fusie die in 2000 heeft plaatsgevonden tussen het Franse bedrijf Atos en het Nederlandse bedrijf Origin, een dochteronderneming van Philips.

In december 2010 is er besloten om een strategisch partnership aan te gaan met Siemens IT Solutions and Services. Deze is in maart 2011 goedgekeurd door de Europese commissie<sup>2</sup> en men is momenteel bezig met de integratie. Met het partnership wordt Siemens gedurende 5 jaar een aandeelhouder met een aandeel van 15% in Atos Origin. Het aantal medewerkers zal groeien naar +/- 80.000 en de jaaromzet zal naar verwachting stijgen naar 8,7 miljard euro. Door het partnership zal Atos Origin marktleider worden in Europa op het gebied van managed services. Doelen van het partnership zijn onder andere om business te genereren in snel opkomende gebieden en om sterker te worden op het gebied van innovatie.

Atos Origin is een van de weinige bedrijven die een totale ICT-oplossing kan aanbieden. Dit komt tot uiting in het consult-build-operate concept van Atos Origin. Dit concept staat garant voor continue zekerheid en kwaliteit. Het houdt in dat Atos Origin een ICT-oplossing niet alleen ontwikkelt, maar ook implementeert en in beheer neemt.

Het concept bestaat uit diensten voor verschillende stadia in de levenscyclus van een ICT-oplossing, zoals:

- business consultancy
- program- en projectmanagement
- ontwerp en ontwikkeling
- integratie met bestaande applicaties en infrastructuur
- training
- onderhoud en beheer
- outsourcing

Er is veel tijd en kennis nodig om een ICT-oplossing operationeel te houden. Dankzij het full life cycle-concept kan een klant die zorg overdragen aan Atos Origin. Zo kan de onderneming van de klant zich volledig concentreren op de eigen strategie en kernactiviteiten.

Atos Origin werkt bovendien in alle landen waarin ze actief is met een marktgerichte focus. Atos Origin probeert te anticiperen op specifieke marktontwikkelingen door lokale kennis aan te wenden en tegelijkertijd de brede expertise die binnen de Atos Origin Group voorhanden is, optimaal te ontsluiten. Zo kan Atos Origin eenvoudiger oplossingen, die in andere landen reeds zijn geïmplementeerd, uitwisselen en kennis en resources delen. Voor de klant betekent dit dat men vrijwel altijd de beste oplossing krijgt met een relatief korte time-to-market.

In Nederland heeft Atos Origin meerdere vestigingen die verspreid liggen over een zestal steden:



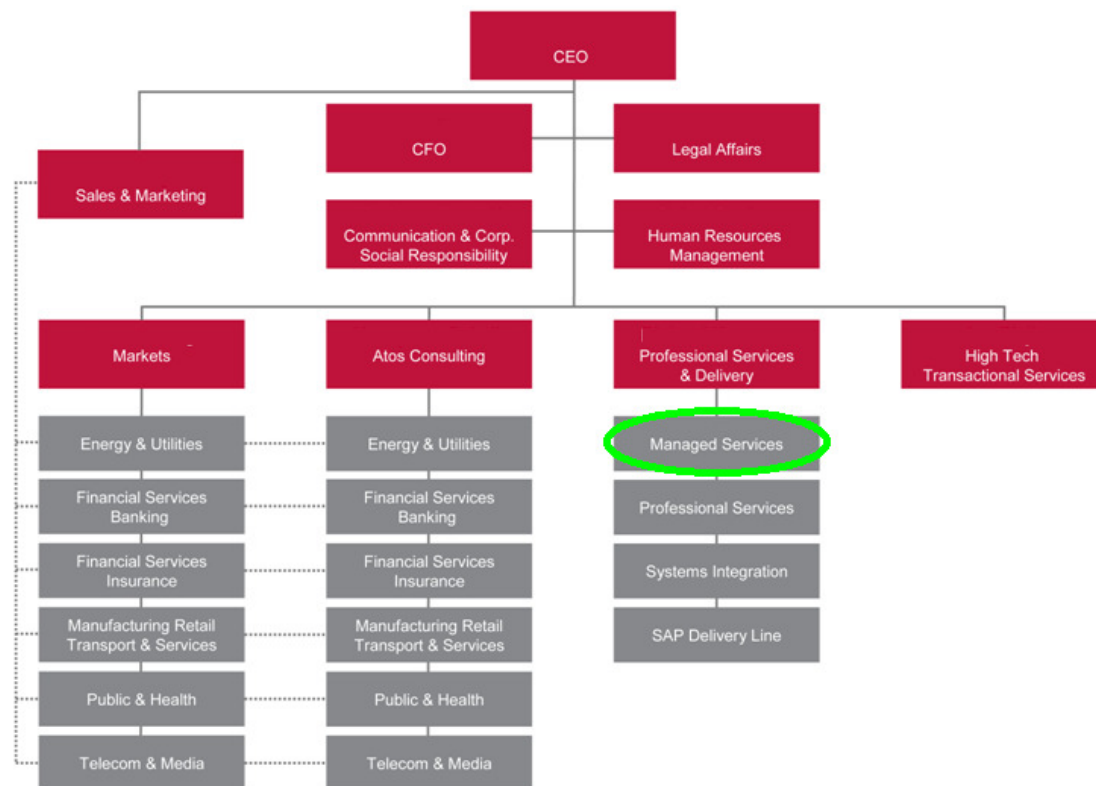
Figuur 1: Vestigingen Atos Origin NL

<sup>1</sup> Literatuurlijst bron 8

<sup>2</sup> Literatuurlijst bron 10

Gedurende mijn afstuderen is de vestiging High Tech Campus in Eindhoven mijn vaste standplaats geweest. In verband met werkzaamheden heb ik echter gemiddeld twee dagen in de week gewerkt op het hoofdkantoor in Utrecht. Incidenteel heb ik op andere locaties gewerkt in verband met interviews e.d.

Ik ben werkzaam geweest bij de divisie Managed Services. Onderstaand organigram maakt duidelijk waar deze divisie zich bevindt in de organisatie.



Figuur 2: Organigram Atos Origin NL

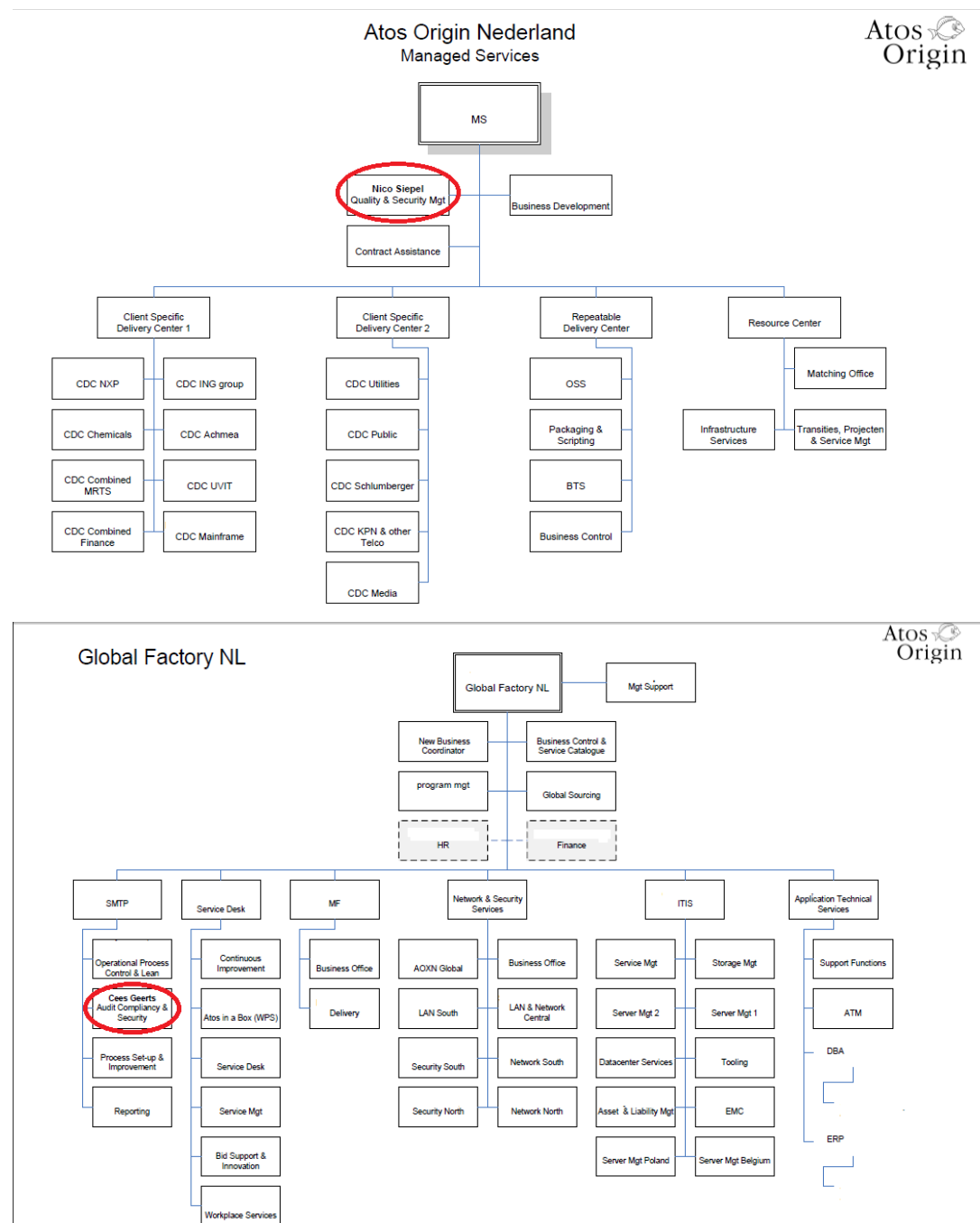
Managed services maakt onderdeel uit van Professional Services & Delivery, dat er voor zorgt dat de contractafspraken over het beheer van de infrastructuur die met klanten zijn gemaakt conform de overeengekomen specificaties worden nagekomen. Hier worden nieuwe concepten ontwikkeld, getoetst en ingezet voor het eigen expertisegebied. Managed services vervult een spilfunctie in het realiseren van de gewenste output in nauw overleg met de markten, de partners en de toeleveranciers.

Binnen managed services is het streven naar optimale efficiency een van de belangrijkste drivers. De andere is kwaliteit. In totaal zijn binnen managed services bijna tweeduizend mensen werkzaam.

Managed services is verder opgesplitst in twee organisatieonderdelen, namelijk de global factory NL die gestandaardiseerde services levert en managed services die klantspecifieke services levert. De relatie tussen de 2 organisatieonderdelen is als volgt: De Customer Delivery Centers (hierna: CDC's) vanuit het organisatieonderdeel managed services leveren klantspecifieke diensten. Naast de klantspecifieke diensten moeten er ook veel diensten geleverd worden die standaard zijn. Deze worden geleverd door de global factory NL.

Primaire taak van de CDC's is integratie van de te leveren diensten, waarbij zoveel mogelijk standaard diensten van de global factory NL worden ingekocht. Waar de klant specifieke diensten heeft gekocht, vindt levering vanuit de CDC plaats. In de praktijk betekent dit dat het organisatieonderdeel global factory NL bijna uitsluitend levert aan organisatieonderdeel managed services. De CDC's zijn echter altijd eindverantwoordelijk voor het contract met de klanten en daarmee de diensten die geleverd moeten worden. Daarom hebben zij een management / dirigerende / integrerende rol waarin ze zich houden op de (kwaliteit van) diensten die geleverd worden vanuit de global factory NL.

Tijdens mijn afstuderen ben ik werkzaam geweest op de afdeling Quality & Security management. Deze afdeling valt onder het organisatieonderdeel managed services. Dit is af te lezen in onderstaande twee organogrammen. Omdat ik een afstudeeropdracht heb gekregen waar ik een onderzoek en implementatie moest doen voor heel de managed services organisatie heb ik echter met alle units in zowel de global factory NL als managed services te maken gehad. Hierbij heb ik vooral contact gehad met Cees Geerts vanuit de afdeling Service Management, Tooling & Processes (hierna: SMTP), op de afdeling Audit Compliancy & Security in de global factory NL. Cees is verantwoordelijk voor het uitgeven van de generieke ISAE 3402 verklaringen van Atos Origin NL voor zowel managed services als de global factory NL. Hij valt daarbij onder de verantwoordelijkheid van de afdeling Quality & Security management. Hierdoor is hij zeer nauw betrokken geweest bij mijn onderzoek en implementatie.



Figuur 3: Organigram Atos Origin NL - Global Factory NL & Managed Services

### 3. De opdracht

ISAE 3402 is een complexe standaard waarbij nogal wat komt kijken. Onderstaande tekst geeft in essentie de achtergrond en beginsituatie aan. Uitgebreidere achtergrondinformatie wordt behandeld in hoofdstuk 4.

#### 3.1 Achtergrond en Beginsituatie

Bedrijven die services uitbesteden blijven hier uiteindelijk zelf eindverantwoordelijk voor. Daartoe zullen bedrijven vooral bij services die een groot (materieel) financieel belang kennen een of andere vorm van toezicht willen hebben op de partij aan wie is uitbesteed. De userorganisatie (de klant van Atos Origin in dit geval) zal van de serviceorganisatie (Atos Origin in dit geval) zekerheid moeten verkrijgen over de mate van beheersing over de services die daar uitgevoerd worden. De uitbestedende organisatie heeft dus behoefte aan een onafhankelijk en onpartijdig onderzoek en oordeel. Het uitoefenen van toezicht is niet alleen een wens van de uitbestedende partij of haar accountant, maar vaak ook vereist vanuit de wetgeving, zoals in het geval van de Amerikaanse Sarbanes-Oxley wetgeving, die aangeeft dat het management van een organisatie aantoonbaar in control moet zijn van haar onderneming.

Atos Origin is een serviceorganisatie die samenwerkt met partners als Ernst & Young, KPMG en Deloitte. De partners voeren de audit uit bij Atos Origin en gaan op zoek naar bewijslast die de beheersmaatregelen afdekken. Nadat de bewijslast verkregen is zal de service auditor beoordelen of deze voldoende is om de beheersmaatregel af te dekken. Zodra alle beheersmaatregelen beoordeeld zijn zal er een oprol gedaan worden naar het niveau van beheersdoelstellingen. Daarbij wordt gekeken of de beheersdoelstellingen voldoende zijn afgedekt door de beheersmaatregelen. Na deze beoordeling wordt er een conclusie getrokken die als opinie wordt verwerkt in een rapport. Door een externe auditpartij te gebruiken wordt de onpartijdigheid en onafhankelijkheid die gewenst is gewaarborgd. Een SAS-70-verklaring is een rapportagevorm die in de praktijk veel wordt gebruikt om over de effectiviteit van de beheersmaatregelen bij de serviceorganisatie te rapporteren. Iedere methode heeft zijn voor- en nadelen, maar in de praktijk is de SAS-70-verklaring een alom geaccepteerde standaard.

Serviceorganisaties die momenteel gebruik maken van SAS-70 verklaringen krijgen 15 juni 2011 te maken met de verplichte overgang naar een nieuwe standaard voor rapportage over interne beheersing ten behoeve van derden. Deze nieuwe standaard (ISAE 3402) zal in de praktijk de huidige SAS-70 standaard vervangen waardoor de ISAE 3402 een internationale basis krijgt, gedragen door het IFAC (International Federation of Accountants en de ASB (Auditing Standards Boards, US).

Groot verschil in de ISAE 3402 standaard ten opzichte van de SAS-70 standaard is dat het management een zogenaamde management assertion letter moet tekenen. Met het ondertekenen van deze management assertion letter doet het management een bewering over de opzet, het bestaan en de werking van het beschreven beheersraamwerk. Hiermee neemt het management van de serviceorganisatie expliciet de verantwoordelijkheid voor de beheersing van de aan haar uitbestede services en de inhoud van het rapport.

Om het management te ondersteunen bij het tekenen van deze management assertion letter zal er een periodieke rapportagecyclus moeten komen waardoor het management op basis van geconsolideerde rapportages een handtekening kan zetten.

#### 3.2 Gewenste eindsituatie

Atos Origin wenst dat er een proces geïmplementeerd is waarmee men op een periodieke basis een management rapportage kan genereren. Het proces dient getest te zijn op haar werking en gebruikers dienen geïnstrueerd te zijn. De uitgerolde management rapportage moet voldoende informatie en bewijslast bevatten zodat het management voldoende onderbouwing heeft om de management assertion letter te kunnen ondertekenen. Het management moet tevens in staat zijn om vanuit een geconsolideerde rapportage te 'down drillen'.

#### 3.3 Opdrachtomschrijving

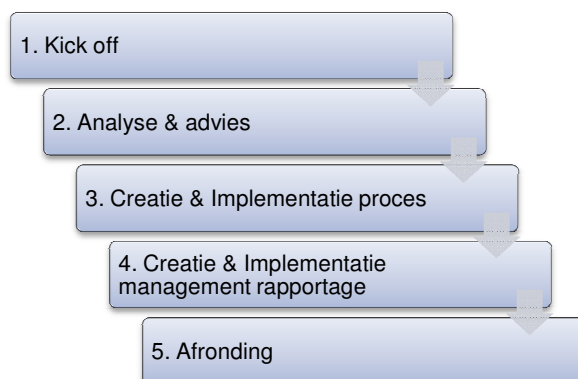
Concreet was mijn opdracht om een management rapportage te ontwerpen die het management ondersteunt om de management assertion letter te ondertekenen. Daartoe diende er een periodieke rapportagecyclus geïmplementeerd te worden.

Bovenstaande opdrachtomschrijving was voor mijzelf in eerste instantie ook nog redelijk vaag. Daarom heb ik indertijd gekozen voor een projectmatige aanpak volgens de PRINCE 2 methodiek. Daartoe heb ik gedurende de

eerste 2 weken van mijn afstuderen een project initiation document (hierna: PID) geschreven om de opdracht te definiëren en te concretiseren (zie bijlage A). Om het PID te schrijven was eerst een stuk oriëntatie nodig. In het voorwoord heb ik reeds uitgelegd dat ik voor mijn afstuderen al een audit had uitgevoerd bij Atos Origin. Daardoor had ik al een goed beeld van de werkzaamheden die gedaan moesten om te komen tot een audit/assurance rapport en verder had ik al een beeld van de opbouw van de organisatie. Doordat ik deze voorkennis reeds had, heb ik ter verdere oriëntatie alleen een aantal gesprekken gevoerd met mensen uit de stuurgroep en mensen vanuit de afdeling SMTP (zie figuur 3).

Omdat de ISAE 3402 een compleet nieuw onderwerp was voor alle betrokkenen is er in het begin van mijn afstuderen nogal eens onduidelijkheid geweest. De mensen uit mijn stuurgroep zitten allen hoog in de organisatie waardoor het risico bestond dat de geformuleerde opdracht niet als zodanig uitgevoerd kon worden. Het risico bestond dat de mensen hoog in de organisatie mogelijk niet tot in detail weten wat er 'op de vloer' precies aanwezig was. Dit is een logisch risico binnen een grote en complexe organisatie, zeker omdat er pas een reorganisatie achter de rug was. Uit mijn toegepast onderzoek zou moeten blijken of dit risico werkelijkheid zou worden. Omdat dit een risico was, met een waarschijnlijk hoge impact, is er indertijd met mijn bedrijfsbegeleider afgesproken om van week tot week te kijken of de opdracht als zodanig geformuleerd nog kon worden uitgevoerd en of het realistisch was binnen de gestelde tijd. Dit zou kunnen resulteren in een latere wijziging van de opdracht en/of van de deliverables.

Uiteindelijk heeft er ook een wijziging in mijn opdracht plaats gevonden maar daarover meer in de volgende paragraaf. Hieronder is weergegeven hoe de opdracht gedefinieerd was aan het begin van mijn afstuderen. In mijn PID had ik mijn project gedefinieerd in een vijftal fases. Deze fases staan hieronder beschreven, inclusief de bijbehorende deliverables.



Figuur 4: Fases opdracht

#### Fase 1: Kick off

Gedurende deze fase diende er een project plan geschreven te worden volgens de PRINCE2 methodiek. Verder zou er een theoretische verdieping uitgevoerd moeten worden waarbij achtergrondkennis vergaard moest worden op het gebied van SAS-70 en ISAE 3402. De verdieping zou geen wetenschappelijk onderzoek zijn, maar meer de vorm hebben van een toegepast onderzoek.

*Deliverables:* Project Initiation Document, Onderzoeksrapport theoretische verdieping.

#### Fase 2: Analyse en advies

Gedurende deze fase zou er onderzocht worden wat er momenteel beschikbaar was aan management rapportages en of hier eventueel op kon worden ingehaakt. Tevens was het zaak om in deze fase de informatie die gewenst was voor de uiteindelijke rapportage boven water te krijgen. Dit zou samengevat moeten worden in een onderzoeksrapport waarbij de V2 methode van Ko Vleugel gehanteerd zou worden. Vervolgens zou er een advies geschreven worden waaruit blijkt hoe de gewenste situatie het beste bereikt kon worden.

*Deliverables:* Research report, Recommendation report

#### Fase 3: Creatie en implementatie proces

In de vorige fase zou bekend moeten zijn geworden wat er gewenst is en hoe deze informatie uit de organisatie gehaald zou kunnen worden. Gedurende deze fase zou er op basis van de voorgaande rapporten een proces

ontwikkeld worden. Bij de ontwikkeling van dat proces zouden tevens procedures en werkinstructies ontwikkeld worden. Zodra deze klaar waren zou er een proces geïmplementeerd moeten worden waarbij getest zou worden of het proces functioneert zoals het beoogd. Mocht het niet werken zoals gewenst dan zouden er aanpassingen gemaakt worden waarop een nieuw stukje implementatie zou volgen. Hierop zou een tweede testrun volgen. Alle uitgevoerde tests zouden worden vastgelegd in een testboek.

*Deliverables:* Process description (incl. RACI), Procedures and work instructions, Testbook.

#### Fase 4: Creatie en implementatie management rapportage

Deze fase zou waarschijnlijk parallel lopen aan de vorige fase. Indien het proces geïmplementeerd was zou de benodigde informatie bottom-up geconsolideerd kunnen worden. Gedurende deze fase zouden de processtappen ontwikkeld worden waarbij de geconsolideerde informatie in de uiteindelijke management rapportage zou worden gehangen, dan wel zou worden ingehaakt in een bestaande management rapportage. Hiertoe zou, indien nodig, een template worden ontwikkeld voor een nieuwe management rapportage. Deze processtappen zouden eveneens geïmplementeerd en getest worden. De uitgevoerde tests zouden worden toegevoegd in het reeds bestaand testboek. Indien nodig zouden er procedures en/of werkinstructies worden aangepast of geschreven.

*Deliverables:* Template management report, Procedures and work instructions, Testbook.

#### Fase 5: Afronding

Gedurende deze fase zou het projectresultaat aan de organisatie worden overgedragen. Middels een presentatie zouden de werkzaamheden toegelicht worden die zijn uitgevoerd, evenals de resultaten. Hierbij zou aangetoond moeten worden dat het proces functioneert zoals het beoogd en dat de mensen die er mee zouden moeten werken in de toekomst op de hoogte zouden zijn. Alle documentatie zou hier worden overgedragen en indien er nog punten openstonden zouden deze duidelijk gedocumenteerd worden zodat men intern verder kon werken met deze documentatie. Voor school zou er ook een afronding zijn, waarbij de afstudeerder zijn competenties zou verdedigen. Tevens zou hij een scriptie schrijven (dit doet hij parallel gedurende zijn afstudeerperiode) waarin hij zou toelichten wat hij gedurende zijn afstuderen heeft uitgevoerd.

*Deliverables:* Company presentation (handover), School presentation and Bachelor thesis

### **Scope**

In de scope was opgenomen:

- Een onderzoek naar de huidige en gewenste situatie, inclusief een onderzoek- en adviesrapport
- Creatie en implementatie van een proces om de vereiste informatie uit de organisatie te halen
- Procedures en werkinstructies voor dit proces
- Testen van het proces
- Creatie en implementatie van een management rapportage, inclusief het eventueel inhaken in hogere management rapportages
- Overdracht van alle documentatie en toelichting op de resultaten (presentatie)

Uitgesloten van de scope waren:

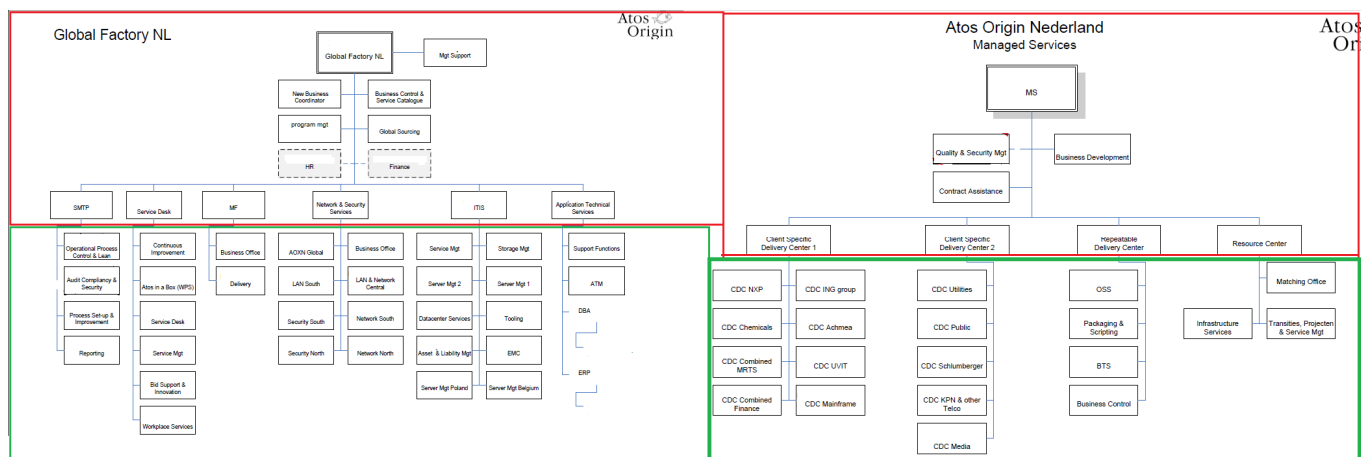
- Het creëren of updaten van procesbeschrijvingen en werkinstructies wanneer er tijdens het onderzoek blijkt dat deze ontbreken of outdated zijn.
- Het aanpassen van management rapportages die niet gerelateerd zijn aan de opdracht en/of SAS-70 ISAE 3402.
- Implementatie van het proces op andere locaties dan Atos Origin Nederland, Eindhoven (High Tech Campus)
- Aanpassingen in Atos Origins systemen
- Training
- Distributie van documenten in andere talen dan Engels
- Grondig nalopen van de documenten op Engelse spelfouten, grammatica en structuur.
- Nazorg na afronding

Relaties die verder niet betrokken worden in het project zijn:

- Klanten van Atos Origin
- Leveranciers van Atos Origin

### 3.4 Gewijzigde opdracht

Zoals eerder aangegeven is mijn opdracht gewijzigd. De reden hiervoor was dat ik gedurende mijn toegepast onderzoek erachter kwam dat er aan de onderkant van de organisatie nog niet goed en/of generiek gerapporteerd werd over een tweetal service quality rapportages. Mijn oorspronkelijke opdracht ging uit van het ontwerpen en implementeren van een rapportage op het niveau van de rode kaders in onderstaand plaatje.

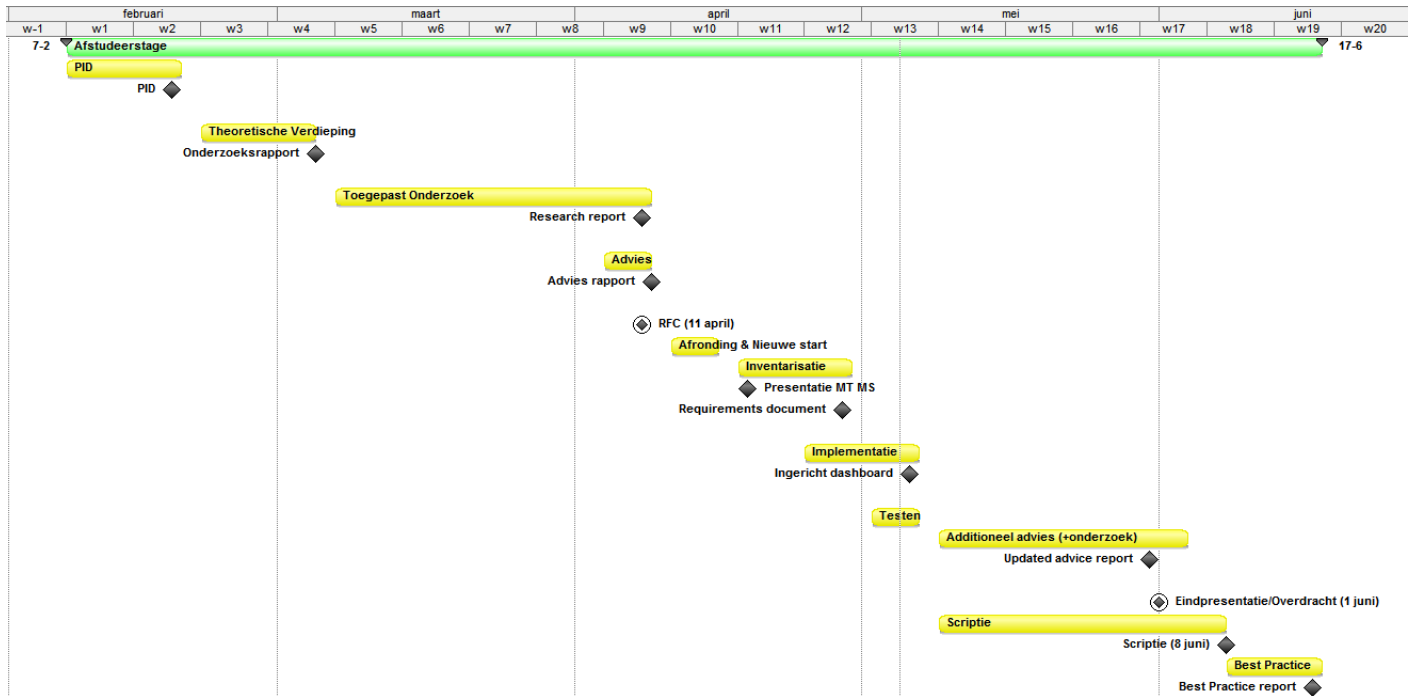


Figuur 5: Organogrammen Atos Origin Managed Services: Global Factory NL & managed services - Niveau voor rapportage

Om op dat niveau een management rapportage te maken zou er echter eerst moeten worden gekeken of er op het niveau van de groene kaders iets aangepast moest worden in de huidige rapportages. Vervolgens zou er een consolidatie moeten plaatsvinden uit de rapportages op het niveau van de groene kaders, naar het niveau van de rode kaders. Omdat de rapportages over service quality echter nog niet goed en/of generiek ingeregeld waren, voor met name het organisatiedeel managed services, viel er weinig te consolideren op het niveau van de rode kaders. Daarom was de oorspronkelijk geformuleerde opdracht niet meer als zodanig uitvoerbaar. Hiervoor zou geen draagvlak zijn omdat er een rapportage uit zou komen die maar half gevuld zou zijn.

Er is daarom besloten om de focus van mijn opdracht te verschuiven naar de groene kaders. Daar was het makkelijker om draagvlak te verkrijgen omdat het logischer is om bottom-up de rapportagestructuur in orde te maken. Bovendien was dit een populair onderwerp aangezien SAS-70 vanaf 15 juni verplicht wordt vervangen door de ISAE 3402. De awareness betreffende dit onderwerp is gedurende de eerste maanden van 2011 ook steeds meer bij het management doorgedrongen.

De opdrachtwijziging is vorm gegeven in een request for change (hierna: RFC). Dit is een formeel document wat gebruikt wordt bij de PRINCE 2 methodiek, indien een opdrachtwijziging nodig is. Dit document is formeel besproken en goedgekeurd door de stuurgroep van Atos Origin en de begeleiders vanuit school. De huidige opdracht en daarmee de deliverables zijn daardoor enigszins gewijzigd. Onderstaande timeline met toelichting geeft dit duidelijk weer.



Figuur 6: Timeline

Als je de timeline vergelijkt met de fases en deliverables zoals die in eerste instantie geformuleerd waren dan komen de veranderingen en overeenkomsten neer op de volgende punten:

#### Overeenkomsten:

- Fase 1 & 2, inclusief hun deliverables zijn onveranderd. Het onderzoeksrapport en adviesrapport zijn na de RFC alsnog afgerond en formeel goedgekeurd.
- De afrondende fase, inclusief de deliverables zijn onveranderd gebleven.

#### Veranderingen:

- Fase 3 & 4, die mogelijk parallel aan elkaar zouden worden uitgevoerd zijn gewijzigd tot één fase (fase 3 -implementatie). Binnen deze fase zijn een drietal activiteiten uitgevoerd: Inventarisatie, implementatie en testen. De deliverables zijn ook gewijzigd. Bij de eerste opdrachtomschrijving moest het volgende opgeleverd worden: Een procesbeschrijving (incl. RACI matrix), werkinstructies en procedures, een template mgt. rapportage en een testbook. Na de RFC werd dit: Een requirements document (RACI), een ingericht dashboard (als het ware een elektronische mgt. rapportage) en optioneel werkinstructies en een testbook.
- Een 4<sup>e</sup> fase met 2 aanvullende deliverables, namelijk een stuk advies (geüpdate advies rapport) om te adviseren hoe de rapportages het beste geconsolideerd kunnen worden voor het niveau van de rode cirkels en een best practice rapport zodat de manier van werken bij Atos Origin NL overgenomen kan worden door andere Atos Origin vestigingen wereldwijd.

Al met al zijn de deliverables dus niet zozeer veranderd. Groot verschil ten opzichte van de oorspronkelijke opdrachtomschrijving is dat de activiteiten op een lager niveau in de organisatie plaats hebben gevonden en dat ik niet zelf een proces heb bedacht. In plaats daarvan ben ik een reeds bestaande rapportagecyclus, zoals die bij de global factory NL gehanteerd wordt, gaan implementeren voor managed services. Punt 2 uit de scope is dus komen te vervallen. Daartegenover staat dat er in scope bij zijn gekomen: een best practice rapport en de inrichting/implementatie van een dashboard voor managed services.

## 4. Achtergrond & Theoretische verdieping

ISAE 3402, SAS-70, monitoring controls, management assertion letter, service auditor, serviceorganisatie, allemaal begrippen die al een keer voorbij zijn gekomen maar ik kan me voorstellen dat het lastig is om deze goed op het netvlies te krijgen. Bij de start van mijn afstuderen was dit ook voor mij een probleem. Vandaar dat ik me eerst in de theorie heb verdiept om te onderzoeken wat er nu allemaal komt kijken bij een ISAE 3402 rapportage en om te onderzoeken wat de verschillen zijn met de voorganger SAS-70.

Omdat het een compleet nieuwe standaard betreft was het niet vreemd dat er nauwelijks literatuur voor handen was. Daarom heb ik mijn informatie vooral gehaald uit het handboek van de ISAE 3402, artikelen van gerenommeerde bedrijven als Ernst & Young en KPMG en gesprekken met auditors van Atos Origin. De verkregen informatie uit deze literatuurstudie heb ik met elkaar vergeleken en vervolgens heb ik mijn deelvragen concreet beantwoord. De resultaten van deze verdieping heb ik beschreven in een onderzoeksrapport waarbij ik een standaard opbouw heb gehanteerd<sup>3</sup>. Voor de concrete resultaten van dit rapport wil ik echter verwijzen naar bijlage D. De reden dat ik de resultaten hier niet expliciet behandel is dat ik sinds de theoretische verdieping steeds meer te weten ben gekomen over achtergronden en relaties tussen onderwerpen op het gebied van auditing. Deze informatie kwam naar boven uit gesprekken met auditors van Atos Origin, externe auditors en door het bijwonen van een round table van ISACA over de ISAE 3402. Hierdoor kan ik op dit moment naar mijn mening helderder en gestructureerder beschrijven wat er allemaal bij een ISAE 3402 komt kijken. De antwoorden van mijn deelvragen zijn desalniettemin enigszins verweven of deels opgenomen in de beschreven achtergrondinformatie hieronder. Met deze achtergrondinformatie zouden de volgende hoofdstukken, die ingaan op de producten, makkelijker te lezen moeten zijn.

### 4.1 Waarom een ISAE 3402?

Uitbesteding van diensten of productie is een van de instrumenten van ondernemingen en overheden om zich te focussen op de voor hen belangrijkste taak: het realiseren van de doelstellingen van de onderneming. Door uitbesteding kunnen deze organisaties meer middelen overhouden voor zaken als innovatie, een snellere time-to-market en een meer flexibele organisatie.

Het inregelen en beheersen van de uitbesteding brengt echter aandachtspunten met zich mee voor de beheersing van de verschillende services. Uitbesteding van services is namelijk geen uitbesteding van alle verantwoordelijkheid, ook al zijn alle afspraken en het monitoren daarvan nog zo goed vastgelegd in SLA's. Vanuit de principes van goed ondernemingsbestuur blijft de organisatie die de services uitbesteedt eindverantwoordelijk voor de beheersing van deze services. Vooral bij services die een groot (materieel) financieel belang kennen, zal de uitbestedende organisatie (de userorganisatie) een of andere vorm van toezicht op de partij aan wie wordt uitbesteed (de serviceorganisatie) moeten uitoefenen. Het uitoefenen van toezicht is niet alleen een wens van de uitbestedende partij, maar vaak ook vereist vanuit de wetgeving, zoals in het geval van de Amerikaanse Sarbanes-Oxley wetgeving, die aangeeft dat het management van een organisatie aantoonbaar in control moet zijn van haar onderneming. Het in control zijn geldt dus niet alleen voor de processen die binnen de eigen onderneming worden uitgevoerd, maar ook voor de processen die extern worden uitgevoerd en direct of indirect verband houden met de interne beheersing van de onderneming. De uitbestedende organisatie zal dus zekerheid moeten verkrijgen over de mate van beheersing, van de processen die door de serviceorganisatie uitgevoerd worden.<sup>4</sup>

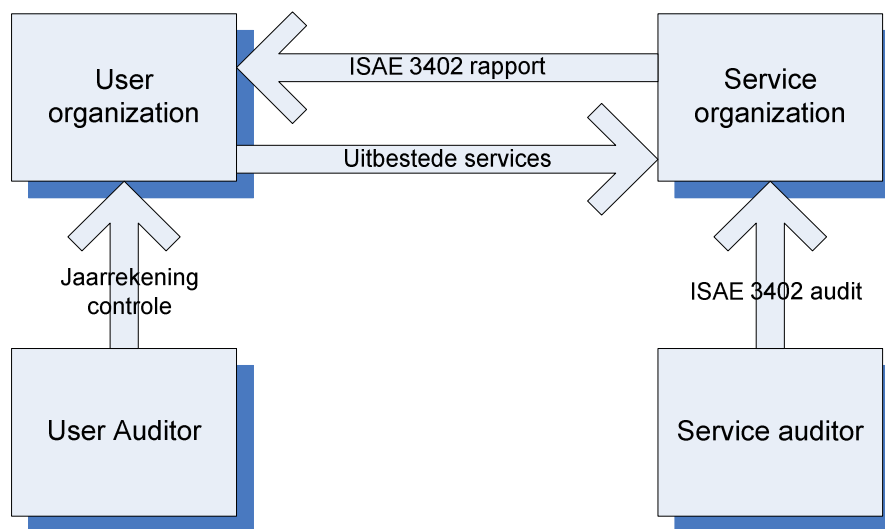
Om deze zekerheid te verkrijgen is een interne verantwoordingsrapportage (bijvoorbeeld in de vorm van een SLA-rapportage) vaak onvoldoende. De gewenste onafhankelijkheid en onpartijdigheid ontbreekt als de verantwoordingsrapportage wordt opgesteld door de partij die ook de dienstverlening levert. Onafhankelijk onderzoek is voor gebruikersorganisaties dan ook noodzakelijk. De serviceorganisatie levert deze onafhankelijkheid door samen met een externe audit partij een rapportage op te stellen volgens een erkende standaard. Er zijn verschillende standaarden, maar in de praktijk is de SAS-70 standaard een alom geaccepteerde en erkende standaard die veruit het meeste gebruikt wordt om te rapporteren over beheersmaatregelen bij serviceorganisaties. De SAS-70 wordt op 15 juni echter opgevolgd door een nieuwe standaard, namelijk de ISAE 3402. Deze standaard zal SAS-70 in de praktijk vervangen waardoor de ISAE 3402 een internationale basis krijgt, gedragen door het IFAC en de ASB.<sup>5</sup>

<sup>3</sup> Literatuurlijst bron 12

<sup>4</sup> Literatuurlijst bron 4

<sup>5</sup> Literatuurlijst bron 2

Onderstaande afbeelding vat de relatie tussen alle betrokken partijen samen.



Figuur 7: Relaties betrokken partijen

Ieder jaar wordt een jaarrekeningcontrole uitgevoerd door de user auditor (accountant van de klant). Onder de jaarcontrole vallen niet alleen services van de user organisatie, maar ook de uitbestede services. De user auditor heeft voor deze uitbestede services een verklaring nodig dat de uitbestede services 'in control' zijn. Hiervoor geeft de service auditor van de service organisatie (Atos Origin in dit geval) een ISAE 3402 rapport af (voorheen een SAS-70). Op basis van dit rapport kan de user auditor controleren of de jaarrekening van de user organisatie niet in gevaar komt door de uitbestede services.

## 4.2 Een ISAE 3402 rapport

Er zijn 2 soorten ISAE 3402 rapporten, namelijk een type 1 en een type 2 rapport. Een type 1 rapport toetst de beheersdoelstellingen in opzet en bestaan (test of design; TOD). De opzet omvat de formele inrichting van het onderzoeksobject op een bepaald moment. Het bestaan betreft de geïmplementeerde beheersmaatregelen in het onderzoeksobject op een bepaald moment. Een type 2 rapport toetst naast opzet en bestaan ook op de werking (test of operating effectiveness; TOE). De werking omvat het functioneren van de beheersmaatregelen met betrekking tot het onderzoeksobject over een bepaalde periode<sup>6</sup>. Onderstaande afbeelding<sup>7</sup> geeft de opbouw van een ISAE 3402 rapport duidelijk weer.

| Report Contents                                                                                                                                                             | Type I Report | Type II Report |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|----------------|
| 1. Independent service auditor's report (i.e. opinion)                                                                                                                      | Included      | Included       |
| 2. Service organization's description of controls.                                                                                                                          | Included      | Included       |
| 3. Information provided by the independent service auditor; includes a description of the service auditor's tests of operating effectiveness and the results of those tests | Optional      | Included       |
| 4. Other information provided by the service organization (e.g. glossary of terms).                                                                                         | Optional      | Included       |

Figuur 8: Opbouw ISAE 3402 rapport

<sup>6</sup> Literatuurlijst bron 13

<sup>7</sup> Literatuurlijst bron 11

Verder kan er een onderverdeling gemaakt worden in specifieke en generieke ISAE 3402 rapporten. Dit onderscheid is gemaakt om te voorkomen dat er tientallen klantspecifieke rapporten gepubliceerd moeten worden wat een enorme tijdsinspanning en veel geld kost. Serviceorganisaties werken vaak voor meerdere opdrachtgevers die elk hun eigen behoeften hebben en eigen eisen stellen aan beheersing. Voor vrijwel al deze klanten zal de serviceorganisatie het verzoek krijgen om aan te tonen dat de uitbestede services goed beheerst (in control) zijn. Als er dan een rapportage gemaakt wordt over interne beheersing volgens een algemeen geaccepteerde en erkende standaard (SAS-70 / ISAE 3402) dan kan er een generieke (klantonafhankelijke) rapportage gepubliceerd worden over de dienstverlening. Daarmee wordt deze rapportage voor diverse gebruikers zinvol. De scope van de audit wordt dan bepaald aan de hand van het service portfolio.

### 4.3 De weg naar een ISAE 3402

Om tot een ISAE 3402 te komen zijn er nogal wat stappen die gezet moeten worden. Onderstaande afbeelding geeft dit weer:



Figuur 9: Stappen om tot een ISAE 3402 te komen

Omdat bovenstaand plaatje in principe bedrijfsafhankelijk is, is er bij iedere beschrijving cursief gedrukt hoe Atos Origin de inrichting vorm heeft gegeven.

#### Risicoanalyse

In tegenstelling tot voorganger SAS-70 is een risico analyse verplicht voor de ISAE 3402. Er dient een risico analyse uitgevoerd te worden op de processen van de serviceorganisatie. Vervolgens kan er aan de hand van de uitkomsten van de risico analyse een selectie gemaakt worden van de meest relevante processen en beheersmaatregelen waarover men wenst te rapporteren.

*Voor Atos Origin geldt dat deze risico analyse is uitgevoerd op global MS niveau.*

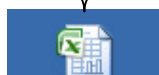
#### Framework

Vanuit de risico analyse is een selectie gemaakt van processen waarover men wilt rapporteren. Voor deze processen moet er een framework ontwikkeld worden. Een framework bestaat uit beheersdoelstellingen (control objectives) en beheersmaatregelen (control measures). Deze worden door de serviceorganisatie opgesteld en de service auditor zal deze beoordelen. De doelstellingen en maatregelen moeten voldoen aan de eisen van de AICPA en worden vaak gebaseerd op bekende standaarden zoals COBIT (een standaard framework voor het inrichten van een IT-organisatie) of ROB (Richtlijnen voor banken).

*Atos Origin NL loopt op het gebied van auditing voor op de andere Atos Origin vestigingen wereldwijd. Atos Origin NL had al een framework: het NL IT control framework. Dit framework kent haar eigen control objectives en measures en is niet aligned met het global framework: het key control framework. Het NL IT control framework is meer uitgebreid dan het key control framework. Dit is ook logisch aangezien het key control framework voor meerdere landen bruikbaar moet zijn en aangezien deze landen nog niet zo ver zijn op dit gebied moeten de controls minder gedetailleerd zijn. Omdat er een verschil is tussen het NL IT control framework en het key control framework is de volgende constructie gekozen:*

| Key control framework (Global) |                                    | NL IT Control framework (NL) |                         |
|--------------------------------|------------------------------------|------------------------------|-------------------------|
| Control objective 1            | <del>CO1 – Control measure 1</del> | Control objective A          | COA – Control measure 1 |
|                                | <del>CO1 – CM2</del>               |                              | COA – CM2               |
|                                | <del>CO1 – CM3</del>               |                              | COA – CM3               |
| Control objective 2            | <del>CO2 – CM1</del>               | Control objective B          | COB – CM1               |
|                                | <del>CO2 – CM2</del>               |                              | COB – CM2               |
|                                | <del>CO2 – CM3</del>               |                              | COB – CM3               |
| Etc.                           | <del>CO2 – CM4</del>               | Etc.                         | COB – CM4               |

Figuur 10: Relatie key control framework en het NL IT control framework



*De control objectives uit het key control framework zijn gemapt tegen de control measures van het NL IT control framework. Dit is samengevat in een mapping document waar de relaties zijn beschreven. Mocht er op global niveau iets wijzigen aan het framework dan hoeft enkel het mapping document aangepast te worden. Op deze manier kan er ook voor andere audits (denk aan bijvoorbeeld ISO) een mapping gemaakt worden waardoor er niet iedere keer een nieuw framework opgesteld moet worden. Het is daarbij wel belangrijk om de control measures zo goed en compleet mogelijk te definiëren.*

*De control objectives en measures van zowel het key control framework als het NL IT control framework zijn gebaseerd op COBIT en COSO.*

#### Audit

Zodra een framework is vastgesteld kan de audit verder worden voorbereid. Eerste stap in dit proces is om de scope te bepalen. Omdat de scope van een ISAE 3402-rapport wordt bepaald door de serviceorganisatie, moet de auditor van de gebruikersorganisatie altijd vaststellen of het rapport toereikend is om te voldoen aan de assurance eisen die de gebruikersorganisatie heeft. Het vaststellen van de scope van de audit is dan ook een essentieel onderdeel. In het geval van een generieke audit wordt de scope echter uitsluitend vastgesteld door de serviceorganisatie. Hierbij speelt ervaring en contact met contractmanagers en quality & security managers een belangrijke rol.

Zodra de scope rond is kan er een auditplan gemaakt worden. Hierin wordt onder andere opgenomen wat de onderzoeksobjecten zijn(scope), welke beheersmaatregelen er getoetst gaan worden en hoelang de auditperiode is. Het auditplan wordt in samenspraak met de service auditor opgesteld.

Zodra het auditplan gereed is kan er gestart worden met de audit. De service auditor zal de beheersmaatregelen binnen de scope gaan testen gedurende een bepaalde periode. Hij zal hiervoor bewijslast proberen te verzamelen en uiteindelijk bottom-up een oprol doen. Afhankelijk van de aangeleverde bewijslast zal er per beheersmaatregel (control measure) gekeken worden of deze voldoende bewezen is. Indien dit niet het geval is zal er gezocht worden naar aanvullende bewijslast (compensating controls) die de beheersmaatregel alsnog voldoende kan afdekken. Vervolgens zal er gekeken worden of er voldoende beheersmaatregelen 'groen' zijn om de beheersdoelstelling (control objective) ook op groen te zetten. Hierbij kan het zijn dat er ondanks een meerderheid aan 'rode' beheersmaatregel toch wordt besloten om de beheersdoelstelling op groen te zetten. Dit heeft er mee te maken dat bepaalde beheersmaatregelen als key kunnen worden beschouwd. Het kan zo zijn dat 2 beheersmaatregelen zo essentieel zijn (key controls) dat de beheersdoelstelling ondanks het falen van meerdere beheersmaatregelen alsnog op groen wordt gezet.

In de ISAE 3402 standaard is tevens beschreven dat de service auditor gebruik mag maken van de inspanningen van interne audits. Dit kan voor de serviceorganisatie een enorme kostenbesparing opleveren. Waar normaal gesproken de service auditor binnenkomt en start met het testen op de vloer, wordt dit nu gedaan door de interne afdeling. De interne afdeling bouwt een dossier op met bewijslast en geeft een mening over de beheersmaatregelen. Vervolgens toetst de service auditor een bepaalde sample (hier zijn verplichte richtlijnen voor beschreven in de ISAE 3402) van het dossier van de interne afdeling. Hier zouden in principe dezelfde conclusies uit voort moeten komen. Zo niet dan wordt er een grotere sample getoetst omdat de service auditor dan geen gegrond oordeel kan geven. Indien dezelfde conclusies worden getrokken dan gaat de service auditor een oprol doen van het niveau van beheersmaatregelen naar het niveau van beheersdoelstellingen. Op basis van de beheersdoelstellingen komt de auditors opinie tot stand.

*Atos Origin gebruikt voor 2011 de eerst beschreven methode waarbij de service auditor de audit uitvoert.*

#### ISAE 3402

Nadat het auditwerk gedaan is kunnen de resultaten verwerkt gaan worden tot een ISAE 3402 rapport. De opbouw van dit rapport is vorige paragraaf reeds besproken (figuur 8). De service auditor zal sectie 1 en 3 van het ISAE 3402 rapport invullen. De serviceorganisatie zal sectie 2 en optioneel sectie 4 invullen.

Onderdeel van een ISAE 3402 rapport zijn echter nog een tweetal brieven, namelijk: de letter of representation en de management assertion letter. Laatstgenoemde is in tegenstelling tot eerstgenoemde een verplicht onderdeel ten opzichte van de SAS-70.

Met de letter of representation zegt het management als het ware dat alle verstrekte data representatief is. Met andere woorden, alle verstrekte data is volledig geweest en eerlijk aangeboden aan de service auditor.

Met de management assertion letter doet het management, overeenkomstig een Sox 404-rapport, een bewering over de opzet, het bestaan en de werking van het beschreven beheersraamwerk (framework). Hiermee neemt het management van de serviceorganisatie expliciet de verantwoordelijkheid voor de beheersing van de aan haar uitbestede services en de inhoud van het rapport.

Zodra deze brieven ondertekend zijn door het management kan de ISAE 3402 aangeboden worden aan de klant. In het geval van een klantspecifiek rapport zullen de belangrijkste resultaten uit het rapport nog besproken worden met de gebruikers organisatie en de user auditor.

#### 4.4 SAS-70 vs. ISAE 3402

Omdat de impact te kunnen bepalen voor de serviceorganisatie en omdat het mijn inziens belangrijk was om achtergrondkennis te verkrijgen over de vorige standaard heb ik onderzocht wat de beperkingen, verschillen en overeenkomsten zijn tussen de SAS-70 en de ISAE 3402. De *belangrijkste* zijn hieronder weergegeven.

##### Beperkingen SAS-70:

- Een beperkte scope van de verklaring. Een SAS-70 verklaring bevat uitsluitend interne beheersdoelstellingen en beheersmaatregelen die relevant zijn voor de betrouwbaarheid van financiële informatie. Er zijn geen doelstellingen en maatregelen op het gebied van continuïteit en/of compliance. Dit is voor een gebruikersorganisatie vaak een essentieel aandachtspunt
- Ontbreken van materialiteit (of risico-inschatting) ten aanzien van de informatie waarover wordt gerapporteerd.

In de afgelopen jaren is de scope van SAS-70-rapportages breder ingestoken dan alleen gericht op de financiële doelstelling<sup>8</sup>. Dit heeft geleid tot de vraag om een nieuwe aanpak en standaard.

##### Overeenkomsten:

- Beide standaarden verplichten het management tot het afgeven van een zogenoemde letter of representation aan de service auditor. Deze brief wordt niet ter beschikking gesteld aan de gebruikersorganisaties of de auditors daarvan.
- Beide standaarden maken het mogelijk gebruik te maken van een interne audit dienst bij het uitvoeren van de diverse procedures. Net als bij SAS-70, is het volgens ISAE 3402 niet toegestaan dat de auditor in het oordeel verwijst naar procedures die zijn uitgevoerd door interne auditors. Het is wel toegestaan om op werkzaamheden van interne auditors te steunen. In het rapport moet er expliciet zichtbaar gemaakt worden welke werkzaamheden zijn uitgevoerd door de interne audit afdeling.
- Beide standaarden verplichten de service auditor om zijn kennis over de beheersmaatregelen te actualiseren tot aan de datum van het uitbrengen van het rapport. Dit om vast te stellen of er gebeurtenissen zijn opgetreden die mogelijk het oordeel beïnvloeden of die om andere redenen zouden moeten worden gecommuniceerd met de gebruikers van het rapport.

##### Verschillen:

- Het meest ingrijpende verschil is dat het management een 'statement of control' (SOC) moet afgeven door de management assertion letter te ondertekenen.
- Bij een SAS-70-onderzoek beoordeelt de service auditor opzet, bestaan en eventueel werking van de beheersmaatregelen van de serviceorganisatie. Bij ISAE 3402 moet de service auditor ook de toepasselijkheid van de beheersmaatregelen voor de organisatie en daarmee uiteindelijk voor de gebruiker van het rapport, de klant of accountant van de klant, beoordelen. Voor het beoordelen van de toepasselijkheid van beheersmaatregelen zal eerst inzicht moeten bestaan in de risico's. Het begrip risico en materialiteit en daarmee risicoanalyse neemt bij ISAE 3402 een centrale en veel belangrijkere rol in dan bij SAS-70 het geval is.
- De serviceorganisatie moet niet alleen een beschrijving opstellen van haar beheersmaatregelen (zoals bij SAS-70), maar de beschrijving (sectie 2) dient ook het gehele systeem van interne beheersing te omvatten. Uiteraard dient daarbij de relatie te worden gelegd tussen de risico's, het systeem van beheersing en de uiteindelijke beheersmaatregelen. De risico's c.q. de risicoanalyse zelf maakt geen onderdeel uit van de rapportage.
- ISAE 3402 staat het niet toe om een beperkte mate van zekerheid te geven. SAS-70 doet dit wel.

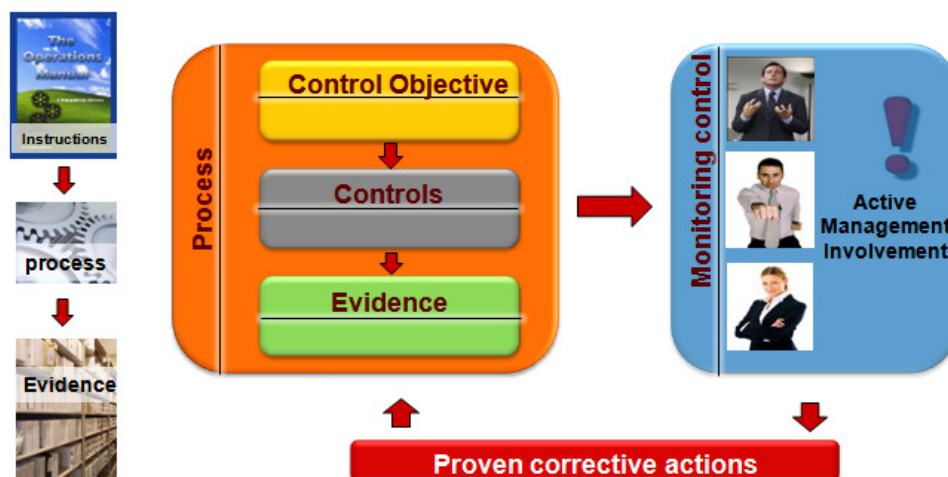
<sup>8</sup> Literatuurlijst bron 9

- SAS-70 is een auditing standaard, ISAE 3402 is een assurance standaard. Bij een SAS-70 wordt voorgeschreven hoe de audit uitgevoerd moet worden en het rapport gaat van service *auditor* naar user *auditor*. Bij een ISAE 3402 gaat het rapport van de service *organisatie* naar de gebruikers *organisatie*. Via de management assertion wordt er echter een mate van zekerheid afgegeven over de diensten die geleverd worden. Dit wordt in het ISAE 3402 rapport in de opinie meegenomen.

### Impact op de serviceorganisatie

De grootste impact op de organisatie wordt veroorzaakt door de management assertion letter. Het management moet de noodzaak van deze verklaring in gaan zien en er zal een manier gezocht moeten worden om het management te ondersteunen bij het tekenen. Hoe kan het management *aantonen* dat ze in control is op alle niveaus binnen de organisatie? Verder is er de risicoanalyse die een veel belangrijkere rol speelt dan bij SAS-70. De organisatie kan bij de ISAE 3402 eigenlijk niet meer om deze risicoanalyse heen.

*Om het management te ondersteunen bij het tekenen van de management assertion letter heeft Atos Origin besloten om het framework uit te breiden met zogenaamde monitoring controls. Dit zijn beheersmaatregelen die reflecteren op de functionering van processen en hun standaard beheersmaatregelen. Zodra de monitoring controls dus in place zijn betekent dit dat de processen in control zijn. Met behulp van een rapportage over de monitoring controls kan het hoogste management vanuit een helicopterview zien welke processen in control zijn. Voor de processen die niet in control zijn kan er dan een downdrill gedaan worden om hierop te sturen. Met andere woorden: het management is actief betrokken. Onderstaande afbeelding visualiseert dit.*



Figuur 11: Overzicht relatie monitoring controls t.o.v. framework, processen etc.

*Aan de linkerkant van de afbeelding: De generieke werkinstructies vertalen zich naar bedrijfsprocessen en vanuit deze bedrijfsprocessen moet er uiteindelijk evidence (bewijslast) komen om aan te tonen dat de processen in control zijn. Het blauwe blok in het plaatje geeft aan dat de monitoring controls iets zeggen over het gehele oranje blok. Het management is actief betrokken en stuurt indien processen niet in control zijn. Dit leidt tot actiepunten waardoor het proces wordt verbeterd en waardoor evidence aangeleverd kan worden. Met de evidence kunnen vervolgens de controls en het control objective worden afgedekt. Dit is een proces van continue monitoring waarbij het management actief betrokken is bij de beheersing van de processen.*

*De risicoanalyse is reeds in de vorige paragraaf behandeld. Hier werd verteld dat deze op global niveau wordt uitgevoerd.*

## 5. Onderzoek, analyse & advies

*'Het zou best kunnen dat er al iets is hoor, maar ik weet het niet!'*

Dit is een uitspraak die ik gedurende mijn afstuderen geregeld gehoord heb. Deze uitspraak is ook logisch te verklaren. De organisatie is enorm groot en complex met veel verschillende management lagen. Daarnaast zijn er de afgelopen jaren een aantal reorganisaties geweest waardoor vaak niet voor iedereen duidelijk is wat voor informatie er al voorhanden is in de organisatie.

Voor mij was het dan ook een logische stap in mijn afstuderen om te beginnen met een onderzoek naar de informatie die al beschikbaar was in de organisatie. In mijn geval was dit een onderzoek naar de management rapportages.

Om dit onderzoek structureel aan te pakken heb ik gekozen om volgens de V2 methodiek (afgeleid van Define Measure Analyse Improve Control (Hierna: DMAIC) van Ko Vleugel te werk te gaan. Dit betekende dat ik eerst zou onderzoeken hoe de huidige en gewenste situatie binnen Atos Origin was, om vervolgens te kijken waar de gaps zaten. Hierop zou ik een gapanalyse doen en aan de hand van deze analyse zou ik een advies geven aan Atos Origin. Het advies zou de juiste aanpak beschrijven om deze gaps op te lossen. De resultaten van mijn onderzoek zijn vast gelegd in een onderzoeksrapport (bijlage E).

Het uiteindelijke doel was om middels dit onderzoek een goede basis te leggen om mijn vervolgstappen te kunnen plannen en om, indien nodig, het management met feiten te adviseren en te overtuigen om een bepaalde weg in te slaan.

### 5.1 Onderzoek & Analyse

De eerste stap in mijn onderzoek was om te kijken wat voor management rapportages er al waren. Hiervoor heb ik een aantal gesprekken gevoerd met mensen die verantwoordelijk waren voor de aanlevering van deze rapportages. Mijn doel was om te kijken wat ik kon gebruiken uit deze rapportages en/of waar ik kon inhaken op deze rapportages. Met andere woorden: welke data zou ik eventueel kunnen consolideren en welke ondersteunende informatie mist er in de huidige rapportages, die het management wenst ter ondersteuning bij het ondertekenen van de management assertion letter.

Uit de gevoerde gesprekken kwam al vrij snel naar voren dat ik me moest focussen op een tweetal rapportages die zich focuste op compliance en service quality. Deze 2 rapportages waren:

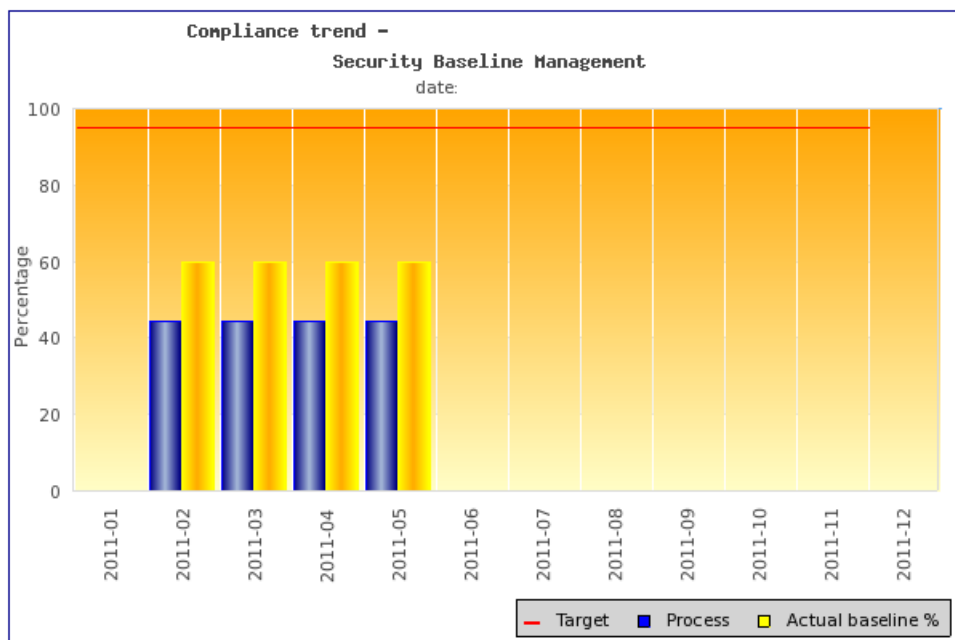
- **Compliance self assessments**

Dit is een subjectieve rapportage die maandelijks wordt aangeleverd per service of klant. Er wordt een vragenlijst ingevuld waarin de managers in een percentage aangeven hoe goed hun dienstverlening is. Ze geven hier aan hoe ze scoren per proces, met andere woorden: zijn onze processen in place? en zijn we dus in control?

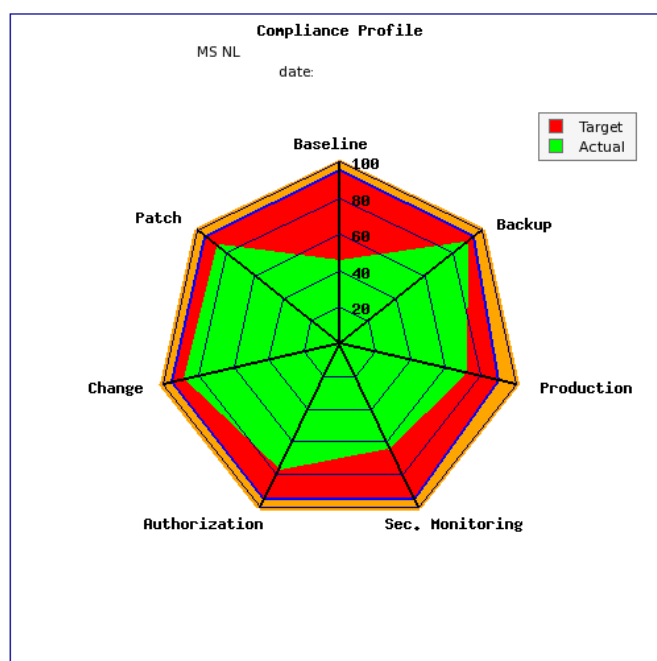
- **Service reviews**

Dit is een maandelijks review die wordt gehouden over de geleverde dienstverlening. Bij deze meetings zijn aanwezig: mensen van de global factory NL vanuit de units operational processes & control en lean audit compliancy & security en Quality & Security officers (hierna: Q&S' ers). Op deze manier wordt de dienstverlening beoordeeld met een objectieve blik van buitenaf. Verder zijn uiteraard de verantwoordelijke operations managers en de unit of CDC manager aanwezig.

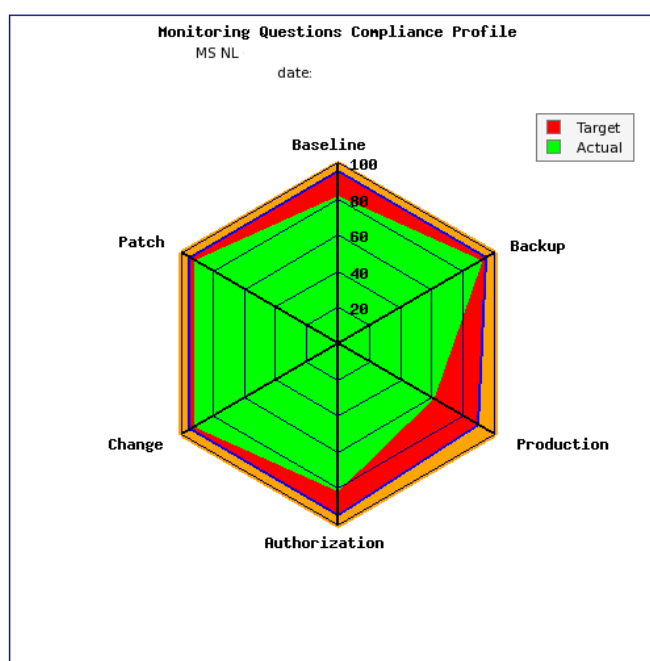
In de review wordt met name behandeld: De service performance (harde cijfers vanuit een datawarehouse), de compliance resultaten uit de compliance self assessments en de follow up van actiepunten. Voor de compliance resultaten wordt als input de compliance self assessment gebruikt. Met behulp van het online dashboard kunnen de resultaten grafisch worden weergegeven in trend- en radargrafieken. Onderstaande afbeeldingen illustreren dat:



Figuur 12 - Voorbeeld Trendgrafiek. Gegeneerd vanuit het compliance self assessments online dashboard



Figuur 13 - Voorbeeld Radargrafiek..  
Gebaseerd op de ingevulde vragenlijst.



Figuur 14 - Voorbeeld Radargrafiek –  
Gebaseerd op de vragen uit de vragenlijst die  
de monitoring controls afdekken

Verdere rapportages die ik bij mijn inventarisatie ben tegengekomen maar waar ik gedurende de rest van mijn afstuderen nauwelijks meer mee in aanraking ben gekomen waren:

- Business Balance Scorecards (BBSC)
- Operational performance indicator (OPI) rapportage
- SLA rapportages
- Breached SLA rapportage (top 20 accounts)
- Extended Dutch management (EDMT) review
- Business reviews
- Key performance indicator reporting op global niveau
- Priorities en severities rapportages per unit of CDC

Deze rapportages worden vooral gebruikt op een hoger niveau in de organisatie (figuur 5). Aangezien hier nauwelijks tot niets staat over service quality heb ik mij gedurende mijn onderzoek gefocust op de eerder genoemde 2 rapportages die wél over service quality rapporteren.

De volgende stap in mijn onderzoek was om te kijken hoe bovenstaande 2 rapportages gebruikt werden binnen managed services en de global factory NL. Met andere woorden; hoe ziet de rapportagestructuur eruit? Verder diende er onderzocht te worden of met deze 2 rapportages de monitoring controls afgedekt konden worden om te bewijzen dat de processen en daarmee de services in control zijn. Indien de monitoring controls niet afgedekt zouden kunnen worden, zou dit aanleiding zijn om aanvullende informatie te verwerken in de management rapportages, of om een compleet nieuwe rapportage te maken. Dit zou dan het startpunt zijn voor mijn vervolgtraject. Omdat deze informatie aan de start van mijn afstuderen niet bekend was, was het in het begin van het project ook lastig om een goed gedefinieerde planning te maken. Zoals eerder besproken in hoofdstuk 3, was dit ook de aanleiding om van week tot week te kijken wat haalbaar en realistisch was en indien nodig de opdracht te wijzigen.

Het eerste wat ik vervolgens ben gaan onderzoeken is hoe de rapportagestructuur van de compliance self assessments en de service reviews eruitzag voor de global factory NL en managed services en waar er afwijkingen waren.

### Rapportagestructuur Global Factory NL:

Voor de global factory NL heb ik geconstateerd dat er gebruik wordt gemaakt van een online dashboard voor de compliance self assessments. De vragenlijst kan elektronisch worden ingevuld en afgetekend. De bedoeling is dat de verantwoordelijke managers voor een service de vragenlijst invullen, of in laten vullen en vervolgens aftekenen. Vervolgens worden de resultaten van verschillende services binnen een unit geconsolideerd naar unit niveau waar de verantwoordelijke unit manager aftekent. Ter illustratie:

|                                    | Unit / Service Name              | Type        | Role(s)                                           | Signature | Input complete |
|------------------------------------|----------------------------------|-------------|---------------------------------------------------|-----------|----------------|
| Signature View scores              | MSGF NL ITIS Server Management I | consolidate | Sign-off                                          |           |                |
| Signature View scores Input scores | MSGF NL ITIS CIS COD ESX         | primary     | Sign-off update<br>Mark update<br>Peter update    |           |                |
| Signature View scores Input scores | MSGF NL ITIS CIS COD Linux       | primary     | Sign-off update<br>Mark update<br>et Peter update |           |                |
| Signature View scores Input scores | MSGF NL ITIS CIS COD Wintel      | primary     | Sign-off update<br>Mark update<br>et Peter update |           |                |

Figuur 15: Voorbeeld overzicht rapportagestructuur

De afbeelding laat zien dat er een drietal services zijn waarvoor de compliance self assessment wordt ingevuld. De bovenste regel geeft aan dat deze 3 services geconsolideerd worden op unit niveau. De units worden verder geconsolideerd op afdeling niveau en uiteindelijk wordt er getekend door de manager van de global factory NL. Over het algemeen werd dit indertijd zeer goed nageleefd en voor bijna alle services werd de vragenlijst ingevuld.

Toen ik echter de lijst van services vergeleek met het organigram viel mij op dat dit alles behalve een 1 op 1 vertaling was. Een aantal services waar over gerapporteerd werd waren niet terug te vinden in het organigram en andersom waren er units in het organigram die niet terugkwamen in het online dashboard.

Omdat ik dacht dat voor de scope van de generieke ISAE 3402 het hele serviceportfolio moest worden meegenomen ben ik verder gaan onderzoeken wat de oorzaak was dat er niet gerapporteerd werd door bepaalde units. Dit heeft aardig wat doorlooptijd gekost omdat ik met het volledige management (+/- 25 personen) van de global factory NL contact moest leggen. Het heeft echter wel inzicht geboden aan de unit audit compliancy & security (zie ook figuur 3), die verantwoordelijk is voor de compliance self assessments voor de global factory NL, waarom bepaalde units niet rapporteerden, of nog niet rapporteerden. Met de resultaten van deze inventarisatie heeft deze unit weer een up-to-date beeld gekregen van de huidige situatie betreffende rapportages binnen de global factory NL.

Naast de compliance self assessment werden er binnen de global factory NL ook nog service reviews gehouden. Op het moment van mijn onderzoek werd dit gedaan voor bijna alle services. Afhankelijk van de services kon er echter worden besloten om de service review op consolidated of op afdeling niveau uit te voeren in plaats van op primary niveau.

### Rapportagestructuur Managed Services NL:

Voor managed services constateerde ik dat het met de compliance self assessment niet zo goed gesteld was als bij de global factory NL. Alles ging nog handmatig: de vragenlijst werd in Excel ingevuld en de resultaten werden vervolgens handmatig geconsolideerd. Verder constateerde ik dat de naleving na de laatste reorganisatie ook een stuk minder was geworden. Er was echter wel een pilot gestart om de werkwijze van de global factory NL over te nemen (online dashboard).

Verder heb ik geconstateerd dat de service reviews nog alles behalve geïmplementeerd waren bij managed services. Op het moment van mijn onderzoek stond dit nog in de kinderschoenen en waren ze hiermee halverwege voor de CDC's. Reden hiervoor was dat dit nooit verplicht gesteld was. Gedurende mijn onderzoek heb ik ook met de manager van managed services gesproken over dit onderwerp en ik heb hem kunnen overtuigen van het nut van deze service reviews. Op basis van o.a. dat gesprek heeft hij ervoor gezorgd dat de service reviews als verplicht onderwerp terug zouden komen in de maandelijkse MT meetings. Het doel hier van is dat men straks *aantoonbaar* kan maken dat men in control is.

Tenslotte was een van mijn bevindingen dat geen units van het repeatable delivery center (Hierna: RDC) rapporteerden middels compliance self assessments of service reviews. Hierop ben ik gesprekken aangegaan met de managers van deze units om boven water te krijgen waarom dit niet gebeurde. Alle units hadden hiervoor op het moment van toetsing een geldige reden voor. Op termijn zou hier echter meer aandacht aan besteed moeten worden.

### Afdekking monitoring controls:

Mijn onderzoek wees uit dat de compliance self assessments en de service reviews de monitoring controls voor zowel de global factory NL als voor managed services afdekte. Reden hiervoor was dat de vragenlijst van de compliance self assessment uniform was voor de global factory NL en managed services. De vragen dekten de monitoring controls aan de ene kant af, de service review aan de andere kant. Ter illustratie:

| Monitoring control                                                                                    | Evidence                                                                                                                    | Afgedekt door                                                                 |
|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Management reviews approvals of changes and initiates corrective actions in case of missing approvals | Evidence showing that all Change Approvals were obtained and that necessary corrective actions were defined and followed up | Service review chapter 3 (3.2). Self assessment questionnaire question CHM060 |

Figuur 16: Voorbeeld afdekking monitoring control

Het eerste gedeelte van de monitoring control (management reviews approvals of changes) wordt afgedekt door een vraag in de service reviews. Het tweede gedeelte (and initiates corrective actions in the case of missing approvals) wordt afgedekt door de service review. Daar worden immers de compliance resultaten besproken en daar worden er acties uitgezet en wordt er gemonitord op de naleving van deze acties.

Met de huidige situatie op het netvlies en met de theoretische kennis over de ISAE 3402 in het achterhoofd was het niet lastig om de gewenste situatie te formuleren. In een notendop kwam het erop neer dat het management bottom-up een rapportagestructuur zou willen waarbij de monitoring controls afgedekt zouden zijn. De resultaten zouden geconsolideerd moeten worden en middels een bottom-up handtekeningenstructuur zou het hoogste management kennis moeten nemen van het niveau waarop Atos Origin in control was. Daarmee zouden ze voldoende ondersteund zijn om de management assertion letter te ondertekenen.

### Analyse

De huidige en de gewenste situatie analyserend constateerde ik dat er eigenlijk maar 1 grote gap was die zo snel mogelijk opgelost moest worden, namelijk het uniformeren van de werkwijze betreffende self assessments en service reviews tussen de global factory NL en managed services. Als het aan de onderkant namelijk niet goed is ingeregeld, dan is een consolidatie op een hoger niveau ook niet mogelijk. Verder waren er wat kleinere gaps, zoals het RDC dat niet rapporteerde volgens compliance self assessment en service reviews en voor de global factory NL waren er ook enkele units die nog niet op deze wijze rapporteerden. Bij alle gaps was men echter al bezig met een oplossing omdat dit reeds bekend was. Zo was men voor de eerstgenoemde gap al bezig met een pilot voor de implementatie bij managed services.

Mijn hele onderzoek bij elkaar genomen heb ik geconcludeerd dat Atos Origins constructie van compliance self assessments, service reviews en monitoring controls voldoende onderbouwing biedt om enerzijds aan te tonen dat Atos Origins processen en daarmee de services in control zijn en om anderzijds het management voldoende te ondersteunen bij het ondertekenen van de management assertion letter

De compliance self assessments en service reviews moeten dan wel uniform voor alle units of CDC's worden uitgevoerd. Daarom zou de eerstgenoemde gap zo snel mogelijk opgelost moeten worden. Daarna zou er moeten worden onderzocht of er op een hoger niveau nog iets geconsolideerd of gerapporteerd moet worden.

## 5.2 Advies

De conclusie en aanbevelingen heb ik verder uitgewerkt tot een alternatief in een adviesrapport (Bijlage F). Ik heb hierbij gezocht naar andere alternatieven, maar omdat er al van alles in gang was gezet om deze gaps op te lossen was het niet realistisch dat er opeens een heel andere weg ingeslagen zou gaan worden. Ook gezien het feit dat de ISAE 3402 verplicht is voor perioden van onderzoek waarin de datum 15 juni is inbegrepen.

Het advies dat ik vervolgens aan Atos Origin heb gegeven was logischerwijs dan ook mijn enige alternatief. Het alternatief omvatte:

- Dat uit het onderzoek was gebleken dat er binnen de organisatie al allerlei activiteiten in gang gezet waren (pilot voor implementatie online dashboard compliance self assessment bij managed services en voor onderdelen waar nog niet gerapporteerd was, was veelal een plan om dit in bijvoorbeeld het 3<sup>e</sup> kwartaal te gaan doen omdat de unit bijvoorbeeld pas net was opgezet) en dat deze dingen ook goed waren om uiteindelijk bottom-up te kunnen bewijzen dat de processen en daarmee de services in control zijn. Mijn advies was dan ook om hier vooral mee door te gaan en om dit eerst goed te regelen alvorens na te gaan denken over een rapportage boven het niveau van de compliance self assessments en service reviews. Immers, als er primair aan de onderkant nog niet goed gerapporteerd wordt, dan valt er aan de bovenkant ook weinig te consolideren.
- Om de implementatie van het online dashboard voor de compliance self assessment meer prioriteit te geven. Momenteel was dit namelijk een aandachtspunt waar maar mondjesmaat tijd vrij voor kon worden gemaakt.

Na dit advies is in overleg met de stuurgroep mijn opdracht formeel gewijzigd middels een RFC. Er was besloten dat ik me zou gaan focussen op de implementatie van het online dashboard tool zoals punt 2 uit het advies beschrijft. Ik ben daarvoor betiteld als projectleider. Tijdens de implementatie zou ik optioneel ook een stukje testing doen (voornamelijk controles) en verder zou ik nog een stuk onderzoek doen om een advies te kunnen geven voor de rapportage die boven het niveau van de compliance self assessments en service reviews zou moeten worden gemaakt (mijn eigenlijke opdracht). Tot slot zou ik de manier van werken vastleggen in een best practice rapport.

## 6. Implementatie

Door de opdrachtwijziging zou ik een rapportagecyclus gaan implementeren aan de onderkant van de organisatie in plaats van aan de bovenkant. Hierdoor kreeg ik een stuk meer te maken met andere medewerkers van Atos Origin die reeds gestart waren met de implementatie van het online dashboard voor de compliance self assessments. Enerzijds was dit Cees Geerts die het online dashboard had ontworpen en geïmplementeerd voor de global factory NL. Anderzijds was dit Jos Papenhuijzen die verantwoordelijk was voor de compliance self assessments voor managed services. Hij consolideerde de ingevulde Excel vragenlijsten.

Met deze 2 personen heb ik de doelstellingen en de aanpak afgestemd. Het doel was om binnen 3 weken draagvlak te creëren en het online dashboard te implementeren bij managed services. De gekozen aanpak was om eerst draagvlak te creëren en om parallel of gelijk erna gesprekken te houden om te gaan inventariseren. Er diende geïnventariseerd te worden hoe de structuur per CDC eruit zou moeten gaan zien en wie er geautoriseerd zou moeten worden. Verder diende er uitgezocht te worden of CDC's de vragen op de vragenlijst allemaal konden beantwoorden.

Voor deze implementatie ben ik toen benoemd tot projectleider. Dit hield in dat ik gesprekken zou gaan plannen en houden met alle CDC managers en indien nodig ook met operations managers en/of Q&S'ers. Ik zou aanspreekpunt zijn voor alle CDC's bij managed services, dus als mensen vragen hadden of hulp nodig hadden dan zou ik hen daarmee helpen. Verder zou ik geregeld met Cees en Jos afstemmen hoe de implementatie verliep zodat we het zo soepel mogelijk konden laten verlopen met een zeer korte doorlooptijd. Indien nodig kon ik hen ook inschakelen om mij te ondersteunen.

De eerste stap was dus om draagvlak te creëren. Ik werd hierbij getipt dat er maandelijks een MT meeting was voor managed services waar alle CDC managers bij waren. Hiertoe heb actie ondernomen door contact op te nemen met de manager van managed services. Ik heb hem kunnen overtuigen dat deze presentatie toegevoegde waarde had en daarop heb ik 3 kwartier tijd gekregen om deze presentatie te houden bij het MT. Cees Geerts heeft toen aangeboden om deze presentatie te houden aangezien hij een stuk dieper in de materie zat omdat hij dit hele traject al een keer had geïmplementeerd voor de global factory NL. De presentatie is vervolgens gehouden met het nodige succes. De meeste CDC managers zagen het nut er wel van in en gedurende de meeting heeft de manager van managed services zijn commitment uitgesproken waardoor duidelijk werd dat de compliance self assessments en de service reviews een verplichte aangelegenheid zouden worden voor alle CDC managers. Dit heeft er toe geleid dat er draagvlak kwam waardoor de implementatie snel en soepel kon verlopen.

Al voor de presentatie had ik contact proberen te leggen om afspraken te plannen maar dit ging vaak moeizaam. Na de presentatie liep dit een soepeler en mede daardoor is het mij gelukt om binnen 2 weken met alle CDC managers (12 personen) individuele gesprekken te voeren. Tijdens deze gesprekken zijn structureel dezelfde onderwerpen behandeld die neer kwamen op het volgende:

- Hoe zou de structuur voor CDC x eruit moeten komen te zien? Met andere woorden: hoeveel compliance self assessments gaan we invullen? Gaan we dit per klant doen, per groepje (kleinere klanten, of per contract of proces?
- Hoe moeten de autorisaties voor het online dashboard ingeregeld worden? Wie moeten er kunnen lezen, updaten en aftekenen?
- Welke vragen uit de vragenlijst zijn niet van toepassing voor een specifiek compliance self assessment (per klant bijvoorbeeld)?

Om deze gesprekken te kunnen voeren heb ik eerst onderzoek gedaan naar de mogelijkheden en beperkingen van het online dashboard zodat ik tijdens de gesprekken gelijk kon bedenken of bepaalde structuren ook technisch mogelijk waren. De resultaten uit deze gesprekken heb ik gebundeld in een overzichtelijk requirements document wat als het ware precies beschrijft wat er in het online dashboard moet worden ingesteld. Onderstaande afbeelding illustreert hoe ik dit heb vastgelegd.

| CDC X - Consolidated                                                                                                                                                                                         | CDC X – Klant 1                                                     | CDC X – Klant 2                                                                                                         | CDC X – Klant 3                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|--|-------------|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|--------|---------------|------------------------|-------------|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|--------|---------------|--------|-------------|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|--------|---------------|----------------|-------------|--|
|                                                                                                                                                                                                              | <b>Applicable:</b> All questions<br><br><b>Not applicable:</b> none | <b>Applicable:</b> All questions except SBL mgt, VUL mgt and SM&L.<br><b>Not applicable:</b> SBL mgt, VUL mgt and SM&L. | <b>Applicable:</b> All questions<br><br><b>Not applicable:</b> none |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
| <b>Authorization Matrix:</b><br><br><table><tr><td><b>Sign off</b></td></tr><tr><td>Naam 0</td></tr><tr><td><b>Update</b></td></tr><tr><td></td></tr><tr><td><b>Read</b></td></tr><tr><td></td></tr></table> | <b>Sign off</b>                                                     | Naam 0                                                                                                                  | <b>Update</b>                                                       |  | <b>Read</b> |  | <b>Authorization Matrix:</b><br><br><table><tr><td><b>Sign off</b></td></tr><tr><td>Naam 1</td></tr><tr><td><b>Update</b></td></tr><tr><td>Naam 1, Naam 2, Naam 3</td></tr><tr><td><b>Read</b></td></tr><tr><td></td></tr></table> | <b>Sign off</b> | Naam 1 | <b>Update</b> | Naam 1, Naam 2, Naam 3 | <b>Read</b> |  | <b>Authorization Matrix:</b><br><br><table><tr><td><b>Sign off</b></td></tr><tr><td>Naam 2</td></tr><tr><td><b>Update</b></td></tr><tr><td>Naam 1</td></tr><tr><td><b>Read</b></td></tr><tr><td></td></tr></table> | <b>Sign off</b> | Naam 2 | <b>Update</b> | Naam 1 | <b>Read</b> |  | <b>Authorization Matrix:</b><br><br><table><tr><td><b>Sign off</b></td></tr><tr><td>Naam 3</td></tr><tr><td><b>Update</b></td></tr><tr><td>Naam 1, Naam 3</td></tr><tr><td><b>Read</b></td></tr><tr><td></td></tr></table> | <b>Sign off</b> | Naam 3 | <b>Update</b> | Naam 1, Naam 3 | <b>Read</b> |  |
| <b>Sign off</b>                                                                                                                                                                                              |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
| Naam 0                                                                                                                                                                                                       |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
| <b>Update</b>                                                                                                                                                                                                |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
|                                                                                                                                                                                                              |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
| <b>Read</b>                                                                                                                                                                                                  |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
|                                                                                                                                                                                                              |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
| <b>Sign off</b>                                                                                                                                                                                              |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
| Naam 1                                                                                                                                                                                                       |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
| <b>Update</b>                                                                                                                                                                                                |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
| Naam 1, Naam 2, Naam 3                                                                                                                                                                                       |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
| <b>Read</b>                                                                                                                                                                                                  |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
|                                                                                                                                                                                                              |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
| <b>Sign off</b>                                                                                                                                                                                              |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
| Naam 2                                                                                                                                                                                                       |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
| <b>Update</b>                                                                                                                                                                                                |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
| Naam 1                                                                                                                                                                                                       |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
| <b>Read</b>                                                                                                                                                                                                  |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
|                                                                                                                                                                                                              |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
| <b>Sign off</b>                                                                                                                                                                                              |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
| Naam 3                                                                                                                                                                                                       |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
| <b>Update</b>                                                                                                                                                                                                |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
| Naam 1, Naam 3                                                                                                                                                                                               |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
| <b>Read</b>                                                                                                                                                                                                  |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |
|                                                                                                                                                                                                              |                                                                     |                                                                                                                         |                                                                     |  |             |  |                                                                                                                                                                                                                                    |                 |        |               |                        |             |  |                                                                                                                                                                                                                    |                 |        |               |        |             |  |                                                                                                                                                                                                                            |                 |        |               |                |             |  |

Figuur 17: Voorbeeld vastlegging resultaten uit inventarisatie

Het daadwerkelijke administratieve werk om de informatie uit mijn requirements document over te nemen in het online dashboard heb ik echter overgelaten aan Cees Geerts. Dit is gebeurd om 2 redenen: ten eerste om een dubbele controle te hebben zodat de kwaliteit zeker goed zou zijn en ten tweede is Cees de persoon die het online dashboard in beheer heeft en er eindverantwoordelijk voor is. Verder kent Cees de organisatie al een stuk langer en zodra hij structuren zou tegenkomen die er voor hem raar uit zouden zijn zou hij dit terugkoppelen naar mij, waarop ik eventueel verdere uitleg zou vragen aan de CDC managers. Zelfde gold voor de vragenlijst. De vragenlijst heb ik niet opgesteld en ik had te weinig kennis van alle processen om de discussie tot in detail aan te kunnen gaan of vragen op NA (not applicable) gezet moesten worden. De CDC- of operations managers die hier dagelijks mee te maken hebben zouden mij dan te allen tijde vast kunnen praten. Er was afgesproken dat Cees mijn resultaten zou bekijken en dat hij, indien hij dingen tegen zou komen waar hij het niet mee eens was, mij zou vragen om verdere toelichting te vragen bij de CDC of operations managers. Indien deze toelichting voor Cees nog steeds niet voldoende zou zijn, dan zou hij de discussie zelf verder voeren met de CDC managers om tot een gezamenlijke oplossing te komen.

Om de voortgang zo min mogelijk te hinderen en om managers zo snel mogelijk de kans te geven om de compliance self assessments zelf in te vullen hebben we gedurende de inventarisatie parallel het online dashboard ingericht. Hierdoor hebben we het voor elkaar gekregen om voor het einde van de maand voor alle CDC's het dashboard klaar te zetten. De volgende stap was om er voor te zorgen dat alle compliance self assessments ook ingevuld zouden gaan worden (communicatie) en om te testen of de implementatie conform het requirements document was. Dit was als het ware weer een extra controle waarbij ik het administratief werk van Cees zou controleren.

Voor de communicatie heb ik samen met Jos Papenhuijzen een e-mail uitgestuurd naar alle CDC managers en mensen met update autorisaties. Dit is via Jos gebeurd was om te voorkomen dat mensen van een onbekende te horen krijgen dat ze iets moeten doen. Jos heeft de aansturing voor de CDC's altijd verzorgd en heeft mij toen naar voren geschoven als aanspreekpunt. Aangezien Jos echter eindverantwoordelijk is voor dit traject bij managed services heeft hij de taak op zich genomen om mensen erop aan te spreken indien er niets ingevuld werd. Zaak was om vooral duidelijk te maken waarom dit moest en dat het in principe geen extra inspanning was omdat de invulling nu elektronisch zou gaan gebeuren in plaats van handmatig. Instructies voor het online dashboard heb ik niet meer hoeven te maken omdat deze reeds voorhanden waren. Deze waren voor het online dashboard voor de global factory NL al een keer geschreven en aangezien de werkwijze voor zowel de global factory NL als voor managed services hetzelfde is konden de werkinstructies uniform gebruikt worden.

Het testen is vooral in overleg en ad hoc gebeurd. Dit zijn allemaal kleine testjes geweest waarbij ik vooral heb gekeken of het online dashboard ingericht was zoals die zou moeten zijn ingericht. Hiertoe heb ik onder andere alle informatie uit mijn requirements document vergeleken met de informatie die in het online dashboard was geïmplementeerd. Differentiaties heb ik vastgelegd in de mail waarop actiepunten zijn vastgelegd. Deze actiepunten zijn inmiddels al uitgevoerd en daarmee is de implementatie ook afgerond. In overleg is besloten om dit niet vast te leggen in een testboek, omdat dit statische informatie is.

Kijkende naar het resultaat heb ik geconstateerd dat het gebruik van het online dashboard nog niet nabij de 100% ligt. Om aan te kunnen tonen dat Atos Origin in control is, is dit wel iets waar naar gestreefd moet worden.

Aangezien dit de eerste maand was mag er naar mijn mening toch tevreden terug worden gekeken. De resultaten waren namelijk als volgt:

- Op primary niveau (dus 1 vragenlijst voor bijvoorbeeld klant x) waren van de 44 compliance self assessments er:
  - 28 volledig ingevuld
  - 8 gedeeltelijk ingevuld
  - 8 niet ingevuld
  - 33 van de (gedeeltelijk) ingevulde vragenlijsten waren afgetekend
- Op consolidated niveau waren 5 van de 12 CDC's afgetekend.

Al met al is dus ruim 80% ingevuld waarvan ruim 90% ook is afgetekend. Voor een eerste maand is dit een prima resultaat. Voor de aankomende maanden is het doel om dit percentage verder omhoog te krijgen en om mensen die nu niet hebben ingevuld aan te sporen om dit wel te doen.

## 7. Aanvullend advies & Best Practice

Nu de rapportagecyclus aan de onderkant van de organisatie geïmplementeerd was kon er gebrainstormd gaan worden over een rapportagecyclus voor de bovenkant van de organisatie. Deze rapportagecyclus was mijn eigenlijke opdracht en na de opdrachtwijziging werd er van mij verlangd om een advies te geven voor deze rapportage.

Ik heb hiertoe een aantal gesprekken gevoerd om de requirements voor deze rapportage boven water te krijgen en ik heb tevens getoetst bij de externe auditor of deze informatie in theorie voldoende was om aan te tonen dat de processen en daarmee de services in control waren.

De resultaten van dit onderzoekje heb ik verwerkt tot een aanvullend advies wat ik heb opgenomen in het eerder geschreven adviesrapport. Het geadviseerde alternatief uit dat rapport kon ik nu namelijk concreet maken en uitbreiden. Het advies wat ik aan Atos Origin heb gegeven was het volgende:

Het ontwikkelen van een nieuwe management rapportage waarin de volgende inhoud moet worden opgenomen. (bij voorkeur allen op 1 (A3) slide).

- Score van de laatste operations manual audit. Dit is een objectieve weergave van compliancy aan processen. De scores zijn nuttig om te vergelijken met de meer subjectievere scores van de compliance self assessments en service reviews.
- Een professioneel judgment over de proces performance middels stoplichtindicatoren op consolidated niveau voor zowel de global factory NL als managed services. Op langere termijn zou dit wellicht grafisch meer gedetailleerd weergegeven kunnen worden middels bijvoorbeeld een radargrafiek.
- Radargrafieken over de compliancy op consolidated en primary niveau voor zowel managed services en de global factory NL. Deze zijn makkelijk te exporteren uit het online dashboard.
- Trendgrafieken over de process performance en compliancy (bovengenoemde 2 punten) per CDC/Unit.
- Risico's. Om interpretatieverschillen te voorkomen zouden hiervoor een aantal standaard risico klassen moeten worden gemaakt.

Verder is het zaak dat er een handtekeningendocument komt voor zowel de global factory NL als managed services waarin bottom-up alle managers vanaf het niveau unit/CDC een handtekening zetten. Dit zou gedaan moeten worden +/- 2 maanden voordat de ISAE 3402 rapporten gepubliceerd worden. Dit geeft het management voldoende tijd om te tekenen en om nog navraag te doen indien nodig.

Het best practice rapport schrijf ik pas in de laatste weken van mijn stage, na de verplichte inleverdatum van mijn scriptie. Het rapport zal beschrijven hoe men bij Atos Origin NL omgaat met het ondersteunen van de management assertion letter. Hierin komen de onderwerpen terug die ook in deze scriptie zijn beschreven. Concreet zullen de behandelde onderwerpen worden: Essentie (Waarom is dit nodig?), Werkwijze Atos Origin NL: Monitoring controls, compliance self assessments, service reviews en rapportage op een hoger niveau. Voor laatstgenoemde punt zal ik het aanvullend advies opnemen wat hierboven kort is beschreven. Tot slot zal ik ook een stuk kosten/baten opnemen in dit rapport om een indicatie te geven van de kosten (in uren) voor de implementatie. Daarbij ga ik er vanuit dat er nog geen basis is en dat alles nog moet worden opgestart.

Op het moment van schrijven heb ik reeds de eerste gesprekken gehad met Atos Origin Engeland, India, Global Internal Control en Global MS om alvast te laten zien hoe de werkwijze in Nederland is. Het best practice rapport zal na mijn afstuderen gebruikt worden om dit toe te lichten voor de andere landen. De behoefte om dit uniform te regelen is zeker aanwezig en er is volop interesse naar de werkwijze van Atos Origin NL!

## 8. Kosten en Baten

Kosten en baten is een onderwerp wat tijdens mijn afstuderen geen concrete rol heeft gespeeld. Om die reden zal de informatie uit dit hoofdstuk ook niet terugkomen in de conclusie en samenvatting. In mijn PID heb ik aan het begin van het project aangegeven dat er geen concreet budget was voor mijn project en dat kosten niet direct inzichtelijk zijn. Ter indicatie is in dit hoofdstuk toch een korte uiteenzetting gegeven van de totale kosten van mijn afstudeerproject. Opgemerkt moet worden dat de weergegeven cijfers een schatting zijn. De kosten zijn weergegeven in uren omdat er geen directe aanschafkosten zijn geweest.

| Directe Kosten                                                |                  |                |           |
|---------------------------------------------------------------|------------------|----------------|-----------|
| Stagevergoeding                                               |                  |                | 19 weken  |
| Indirecte kosten                                              |                  |                |           |
| Gesprekken met het management                                 |                  |                | 30 uur    |
| Gesprekken met bedrijfsbegeleider                             |                  |                | 80 uur    |
| Gesprekken met collega's (in directe relatie met de opdracht) |                  |                | 100 uur   |
| E-mail verkeer met betrokkenen                                |                  |                | 20 uur    |
|                                                               |                  | <b>Totaal:</b> | 230 uur   |
| Overhead                                                      |                  |                |           |
| Gebruik van faciliteiten:                                     |                  |                |           |
|                                                               | Laptop           |                | Bruikleen |
|                                                               | Vergaderruimtes  |                | 40 uur    |
|                                                               | Printers         |                |           |
|                                                               | Werkplek         |                | 19 weken  |
|                                                               | Conference Calls |                |           |

De belangrijkste baten van het project zijn:

- Een geïmplementeerde rapportagecyclus aan de onderkant van de organisatie waarmee aangetoond kan worden dat Atos Origin haar services goed beheerst heeft. Tevens is deze rapportage een middel om beter te kunnen managen. Doordat de rapportages nu worden gemaakt met behulp van een online dashboard worden er uren uitgespaard ten opzichte van de vorige, handmatige rapportagecyclus.
- Een gegrond advies wat als basis kan dienen om een rapportagecyclus aan de bovenkant van de organisatie te implementeren.
- Een best practice wat gebruikt kan worden om een uniforme werkwijze te introduceren op global niveau. Een uniforme werkwijze op global niveau kan het maturity level van de organisatie betreffende dit onderwerp laten stijgen.

Voor het best practice rapport zal er nog een kostenbaten analyse gemaakt worden. Hierbij wordt gekeken naar de verwachte kosten voor een implementatie bij een Atos Origin in het buitenland. Deze zal tijdens de afstudeerzitting verder worden toegelicht.

## 9. Conclusies & Aanbevelingen

Om aan te tonen dat de aan Atos Origin uitbestede services in control zijn geeft Atos Origin ISAE 3402 rapportages aan haar klanten. Dit zijn assurance rapportages waarbij het management middels de management assertion letter expliciet de verantwoordelijkheid neemt voor de beheersing van de aan haar uitbestede services en de inhoud van het rapport.

Om het management te ondersteunen in het aantonen dat de processen en daarmee de services ook daadwerkelijk goed beheerst zijn heeft Atos Origin monitoring controls geïntroduceerd. Dit zijn controls die reflecteren op de functionering van processen en hun standaard beheersmaatregelen. Indien de monitoring controls in place zijn betekent dit dus dat Atos Origin in control is voor dat proces. De monitoring controls moeten echter wel afgedekt worden door bewijslast. Deze bewijslast wordt geleverd door een tweetal management rapportages. Enerzijds de compliance self assessment en anderzijds de service reviews.

Compliance self assessments zijn subjectieve rapportages die maandelijks worden aangeleverd per service of klant. Er wordt een vragenlijst ingevuld waarin de managers in een percentage aangeven hoe goed ze scoren op onderdelen van een proces. De percentages worden geconsolideerd tot een gemiddelde score voor een proces waarna deze vergeleken worden met de target score. Indien deze target gehaald wordt is het proces goed beheerst.

Service reviews zijn rapportages over de dienstverlening die maandelijks worden besproken met enerzijds de operations- en unit- of CDC managers. Anderzijds met mensen die met een objectieve blik de dienstverlening beoordelen. In de service review wordt voornamelijk ingegaan op de service performance en op de compliancy. Voor laatstgenoemd onderdeel worden automatisch gegenereerde grafieken van de compliance self assessments gebruikt. In de service reviews wordt er voor gezorgd dat er verbeteracties worden uitgezet en wordt er gemonitord of deze ook worden opgevolgd.

Aangezien de resultaten van de compliance self assessment worden opgenomen in de service reviews kan geconcludeerd worden dat de monitoring controls afgedekt worden door de service review.

De besproken 2 rapportages reiken echter niet tot het hoogste management die uiteindelijk de management assertion letter moeten gaan ondertekenen. Daarom beveel ik aan om een management rapportage te maken en te implementeren met daarin geconsolideerde informatie van de service reviews (overzichten process performance en compliancy, inclusief trendgrafieken). Verder opgenomen zou moeten worden: De risico's (materialiteit) en scores van de laatste operations manual audit. Het management zou tevens ondersteund moeten worden middels een handtekeningendocument waar alle managers vanaf het niveau unit/CDC hun handtekening zetten. Dit document zou +/- 2 maanden voor publicatie van de ISAE 3402 gemaakt moeten worden.

Verder zou ik willen aanbevelen om de werkwijze van Atos Origin NL mee te nemen naar global niveau. Atos Origin NL loopt op dit gebied voor op de andere Atos Origin organisaties dus het is goed om een uniforme werkwijze te introduceren. Het best practice rapport dat momenteel nog in ontwikkeling is zou hiervoor als basis kunnen dienen.

Tot slot heb ik nog een aantal verbeterpunten die ik gedurende mijn afstuderen ben tegengekomen. Ik zou willen aanbevelen om:

- **De compliance self assessments vragenlijst grondig te reviewen**

De vragenlijst die gebruikt wordt heeft veel vragen die niet SMART geformuleerd zijn. Dit is een risico aangezien er percentages ingevuld kunnen worden die bijvoorbeeld niet meetbaar (en dus aantoonbaar) zijn. Verder is de vragenlijst vanuit de global factory NL opgesteld en er zijn vragen die teveel gebaseerd zijn op de delivery en te weinig op de dirigerende rol van de CDC's. Deze vragen zouden anders geformuleerd moeten worden door bijvoorbeeld een extra set vragen te maken speciaal voor de dirigerende rol van de CDC's. Op korte termijn zou een interpretatiedocument een oplossing kunnen zijn waarin wordt uitgelegd hoe de vraag vanuit de delivery (global factory NL) en vanuit de CDC (dirigerende rol) zou moeten worden ingevuld. Indien men global gaat werken met de compliance self assessments moet er nogmaals een review komen om tot een uniforme vragenlijst te komen die wereldwijd inzetbaar is.

- **Te controleren op de integriteit van de ingevulde percentages**

Ik heb gemerkt dat de Q&S'ers vooral de voortgang monitoren en niet zozeer de integriteit van de ingevulde percentages in de compliance self assessments vragenlijst. Het zou goed zijn om dit steekproefsgewijs te doen. Dit zou een taak kunnen zijn voor de Q&S'ers, alsmede voor de interne afdeling die geheel objectief een oordeel kan vormen.

- **Het online dashboard te optimaliseren**

Momenteel worden mensen die de vragenlijst moeten invullen per e-mail op de hoogte gebracht dat de vragenlijst ingevuld moet worden. Dit zou geautomatiseerd kunnen worden waarbij de mensen met update en afteken rechten een automatische reminder krijgen wanneer ze de vragenlijsten moeten invullen en/of aftekenen.

Verder zou het in bepaalde gevallen mogelijk moeten zijn om de mensen zelf te laten bepalen of ze een percentage invullen of de vraag als not applicable willen behandelen. In het geval van project management zijn er namelijk niet altijd projecten die lopen. Het invullen van 0% of 100% geeft dan een vertekend beeld omdat dit de eigenlijke percentages in de trendgrafieken omhoog of omlaag trekt. Een oplossing zou kunnen zijn om voor een specifiek onderdeel mensen de mogelijkheid te geven om bijvoorbeeld 'geen' in te vullen. Deze mogelijkheid is er momenteel niet.

## Evaluatie

De afstudeerstage bij Atos Origin was mijn eerste stage bij een grote organisatie. Met de theoretische kennis en het vele projectmatige werken wat ik op school had geleerd zag ik de opdracht vol vertrouwen tegemoet. De eerste weken van mijn afstuderen ben ik hier echter aan gaan twijfelen. Door omstandigheden was mij de opdracht nog steeds niet duidelijk. Hierdoor wist ik eigenlijk niet goed wat er precies van mij verwacht zou worden. Na de eerste weken is de opdracht echter steeds helderder geworden en ondanks dat het niet helemaal was wat ik verwacht had vond ik het een uitdagende opdracht waar ik veel van zou kunnen leren.

De medewerkers van Atos Origin stonden vanaf dag 1 klaar om mij te helpen en te begeleiden. Ik werd vanaf de eerste dag al meegenomen naar vergaderingen en besprekingen om enerzijds achtergrondinformatie te verkrijgen, maar anderzijds ook om te ervaren hoe vergaderen er in de praktijk aan toe gaat. Ik heb verder altijd de ruimte gekregen om me te verdiepen, ook in andere vakgebieden dan waar ik werkzaam was. Indien ik uitleg nodig had was er altijd wel iemand in de interne organisatie die de tijd nam om mij deze te bieden en ook heb ik de mogelijkheid gehad om met externe partijen te spreken. Kortom, ik kan zeggen dat ik de cultuur en de werksfeer als zeer prettig heb ervaren.

Gedurende mijn opdracht zijn alle competenties die ik de afgelopen 3 jaar heb geleerd in mijn BI opleiding teruggekomen. In het bijzonder de competenties analyseren, adviseren en realiseren. Het enige aspect wat ik in de opleiding heb gemist maar waar ik wel veel te maken mee heb gehad is de Engelse taal. Deze taalkennis is in de opleiding zeer summier behandeld. Ik kwam echter terecht in een grote internationale IT dienstverlener waardoor al mijn documentatie in het Engels aangeleverd moest worden. Tevens diende ik af en toe gesprekken te voeren met internationale medewerkers waar de voertaal ook Engels was. Gelukkig had ik nog een redelijke basiskennis waardoor dit uiteindelijk geen hoge drempel is gebleken. Het is wel een leermoment geweest en ik heb mijn Engels weer enigszins opgekrikt.

Andere leermomenten die ik gedurende mijn afstuderen heb gekend waren:

- *Plannen*  
Dit is een aspect dat ik op school al geregeld ben tegengekomen en ik was ook van mening dat ik dit redelijk kon. In de praktijk heb je echter te maken met drukke agenda's, tijdsschattingen van taken en het wegvallen of bijkomen van taken. Dit kan een gigantische impact hebben op de planning. Zaak is dan ook om wekelijks de planning bij te houden en proactief te plannen. Dit betekent afspraken ruim van tevoren plannen indien je verwacht dat je informatie nodig hebt van iemand. Afzeggen gaat immers makkelijker dan 2 weken moeten wachten tot de desbetreffende persoon een gaatje vrij heeft in zijn agenda. Verder zijn buffers essentieel om een planning realistisch te kunnen houden. Een uitspraak van mijn bedrijfsbegeleider die ik niet snel zal vergeten was: '*Jij bent projectleider, jij moet in control zijn*'. Uitloop kan grotendeels voorkomen worden door goed te plannen en door te escaleren wanneer mensen niet bereid zijn om mee te werken of niet reageren. Al met al is dit voor mij enorm nuttig geweest om te leren aangezien ik overweeg om later iets te gaan doen met project management.
- *Parallel werken*  
Een van mijn zwakkere punten waar ik gedurende mijn stage veelvuldig mee te maken heb gehad was parallel werken. Ik doe het liefste iets in één keer goed en start dan aan het volgende. Parallel werken is echter iets waar je niet omheen kunt in de praktijk. Dit heb ik beter leren doen door voor mezelf weekplanningen te maken waar ik onder andere gebruik maakte van timeboxen.
- *Timeboxen*  
Indien er een deadline is en er is beperkte tijd over dan kan je timeboxen. Dit principe heb ik op het gegeven moment gehanteerd bij mijn toegepast onderzoek. De essentie van het principe is dat je, ondanks dat je iets misschien nog niet helemaal af hebt, doorgaat naar het volgende wat je gepland hebt zodat je op het einde toch iets kunt opleveren. Het zij met veel aannames erin.
- *Communicatie naar het management*  
Het management heeft vaak drukke agenda's en lange mailings waar stap voor stap iets uitgelegd wordt, worden vaak niet gelezen. Insteek van het management is vaker: Als het echt belangrijk is dan hoor ik het nog wel. Geleerd heb ik dus om de mails zo kort en concreet mogelijk te houden en de opbouw als volgt te doen: Eerst zeggen wat je wilt, daarna pas het waarom of de achtergrondinformatie. Als het management namelijk geïnteresseerd is lezen ze vanzelf wel verder. Verder heb ik geleerd om bij geen reacties te escaleren of gewoon meeting request in hun agenda te zetten. Op het gegeven moment kunnen ze niet meer om je heen en zullen ze wel moeten. Dit is ook weer in het kader van plannen en project management belangrijk. Jij bent er namelijk voor verantwoordelijk dat er iets

- ingeleverd wordt en als je daarvoor informatie van het management nodig hebt dan moet jij koste wat kost deze maar zien te verkrijgen. Ook als mensen minder bereid zijn om mee te werken.
- *Voorbereiding interviews*  
Een aspect waar ik dacht redelijk goed van op de hoogte te zijn. Echter is tijdens mijn afstuderen gebleken dat voorbereiding echt essentieel is. Je zit tegen mensen die veel kennis hebben op een bepaald vakgebied en het is naast de standaard voorbereiding (wat wil je precies weten en hoe ga je dat vragen) essentieel om je proberen te verplaatsen in de geïnterviewde. Welke vragen kun je verwachten en hoe ga je daar op antwoorden? Eventueel kun je al navraag doen van tevoren voor vragen die je verwacht maar niet zelf kunt beantwoorden. Dit geeft je een stuk meer 'munitie' tijdens zo een interview om mensen te kunnen overtuigen, dan wel om draagvlak te creëren.
  - *ISAE 3402, SAS-70 en het audit vakgebied*  
Mijn afstuderen heeft me inzicht gegeven in het audit vakgebied en alle aspecten die erbij komen kijken.

Dit zijn de belangrijkste leermomenten voor mij geweest tijdens mijn afstuderen. Al met al kan ik stellen dat ik in een tijdsbestek van ruim 4 maanden veel heb geleerd. Ik heb de opdracht als interessant en breed ervaren en ben uiteindelijk tot het gewenste resultaat gekomen. Terugkijkend zou ik qua aanpak weinig dingen anders hebben gedaan. Wat ik wel anders zou hebben gedaan en dit vloeit rechtstreeks voort uit mijn leermomenten, is de benadering van het management en het proactief plannen.

## Literatuurlijst

In deze literatuurlijst staan de bronnen gesorteerd weergegeven op nummer, waarnaar ook verwezen wordt in de scriptie (onderaan in de voetnoten). Niet naar alle bronnen is specifiek gerefereerd in de scriptie. Redenen hiervoor kunnen zijn: De bronnen hebben als vergelijkmateriaal gediend om de integriteit van andere bronnen te bevestigen of bronnen zijn puur als referentie gebruikt.

### Standaarden:

1. IAASB (2009). *ISAE 3402, Assurance Reports on Controls at a Service Organization*. Geraadpleegd op 17 februari 2011.

### Artikelen

2. Beek, J. van., & Francken, M. (2010). *SAS-70 herzien, focus ISAE 3402 blijft op beheersingsmaatregelen financiële verantwoording*. Compact, nr. 1, 38-42. Geraadpleegd op 18 februari 2011.
3. Ewals, R. (2010). *Een nieuw hoofdstuk voor de IT-Auditor*. De IT-auditor, nr. 3. Geraadpleegd op 16 februari 2011.
4. Houtekamer, D., & Graaf, R de (2009). *ISAE 3402: einde van SAS-70 in zicht?* de EDP auditor, nr. 1. Geraadpleegd op 15 februari 2011.
5. Russel, M. (2010). *New gold standard to change third party assurance*. Internal Auditing & Business Risk magazine Geraadpleegd op 16 februari 2011.
6. Verweij, S. (2009). *SAS-70 maakt plaats voor ISAE 3402*. Spotlight, nr. 3, 52-56. Geraadpleegd op 15 februari 2011.

### Scripties

7. Bruijn, S de. (2008). *Eindrapport: Doe mij maar een SAS-70*. Utrecht Geraadpleegd op 4 mei 2011.

### Internet

8. Atos Origin (2011). *Bedrijfsprofiel*. Geraadpleegd op 9 maart 2011 via [http://www.nl.atosorigin.com/nl-over\\_atos\\_origin/bedrijfsprofiel/default.htm](http://www.nl.atosorigin.com/nl-over_atos_origin/bedrijfsprofiel/default.htm)
9. BDO (n.b.). *ISAE 3402: Afscheid van SAS-70 en TPM?*. Geraadpleegd op 18 mei 2011 via: <http://www.bdo.nl/ras/Pages/ISAE3402.aspx>
10. Europa Press Releases (2011). *Mergers: Commission approves acquisition of Siemens IT Services by Atos Origin*. Geraadpleegd op 11 mei 2011 via <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/366>
11. ISAE3402.com (2011). *ISAE 3402 reports*. Geraadpleegd op 18 mei 2011 via [http://isae3402.com/ISAE3402\\_reports.html](http://isae3402.com/ISAE3402_reports.html)
12. Lissa (n.b.). *Het schrijven van een onderzoeksrapport*. Geraadpleegd op 1 februari 2011 via <http://artikelen.foobie.nl/verslagen-scripties/het-schrijven-van-een-onderzoeksrapport/>
13. Norea (n.b.). *Goedkeurend (redelijke mate van zekerheid)*. Geraadpleegd op 18 mei 2011 via <http://www.norea.nl/Norea/Thema's/Richtlijnen/Goedkeurend+RMVZ.aspx>
14. Sikkema, T. (2009). *ISAE 3402 samenvatting: Enkele belangrijke kenmerken en verschillen in vergelijking met SAS-70*. Geraadpleegd op 19 februari 2011 via <http://www.hutaudit.nl/website/hutaudit.nsf/cms/Nederlands-Nieuws-ISAE%203402%20presentatie#topcontent>

Verder heb ik nog veel interne documentatie gebruikt maar deze wordt vanwege het vertrouwelijke karakter niet vermeld. De interne informatie bestond veelal uit rapportages en templates voor rapportages, raamwerken, service beschrijvingen en interviewverslagen.

## Bijlagen

Hieronder is een overzicht gegeven van de bijlagen:

### **Bijlage A: Project Initiation document**

*(Aangehechte Bijlage)*

### **Bijlage B: Request for change**

*(Aangehechte Bijlage)*

### **Bijlage C: Logboek**

*(Aangehechte Bijlage)*

### **Bijlage D: Theoretische verdieping**

*(Aangehechte Bijlage)*

### **Bijlage E: Research report**

*(Vertrouwelijke Bijlage, niet opgenomen in gepubliceerde openbare versie)*

### **Bijlage F: Recommendation report**

*(Vertrouwelijke Bijlage, niet opgenomen in gepubliceerde openbare versie)*

## Bijlage A: Project initiation document

### Project Initiation Document graduation Ruud Brunenberg

|                 |   |               |           |
|-----------------|---|---------------|-----------|
| AUTHORS         | : | R. Brunenberg |           |
| PRINCIPAL       | : | N. Siepel     |           |
| DOCUMENT NUMBER | : | NLD-AUD-0187  |           |
| VERSION         | : | 1.0           |           |
| SOURCE          | : | Atos Origin   |           |
| STATUS          | : | Final         |           |
| DOCUMENT DATE   | : | 28-2-2011     |           |
| NUMBER OF PAGES | : | 3192          |           |
| OWNER           | : | R. Brunenberg | INITIALS: |

## Content

|                                                    |    |
|----------------------------------------------------|----|
| 1. Introduction and background of the project..... | 4  |
| 2. Project definition .....                        | 7  |
| 3. Initial Business Case.....                      | 11 |
| 4. Project organization structure .....            | 13 |
| 5. Role descriptions .....                         | 14 |
| 6. Initial Project planning.....                   | 16 |
| 7. Controls .....                                  | 22 |
| Risk Log .....                                     | 24 |
| Quality Plan .....                                 | 25 |
| Project File.....                                  | 26 |
| Product Descriptions .....                         | 27 |
| Communication/reporting plan.....                  | 29 |

## Document History

*Revisions:*

| VERSION | DATE       | DESCRIPTION                                                                                         | AUTHOR        |
|---------|------------|-----------------------------------------------------------------------------------------------------|---------------|
| 0.1     | 07-02-2011 | Changes in template / English / Paragraph 1.1                                                       | R. Brunenberg |
| 0.2     | 08-02-2011 | Added: 1.2.2-1.2.4 / 2.1-2.2 / 2.4-2.6 / 4 / 5                                                      | R. Brunenberg |
| 0.3     | 09-02-2011 | Added: 3 / Quality plan / 7<br>Edited: 1.2.2 / 2.2 / 5                                              | R. Brunenberg |
| 0.4     | 10-02-2011 | Added: 7 / Communication plan<br><br>Edited: 2.2 / 2.4<br><br>Deleted: 1.2.4                        | R. Brunenberg |
| 0.5     | 11-02-2011 | Edited: 2.2 / 2.4 / lay-out and grammar / consistency                                               | R. Brunenberg |
| 0.6     | 14-02-2011 | Added: Project file / Product descriptions / Project plan                                           | R. Brunenberg |
| 0.7     | 15-02-2011 | Edited: 1.2.1 / 7.1-7.2 / Quality plan<br>Added: planning (project plan) / 2.3                      | R. Brunenberg |
| 0.8     | 16-02-2011 | Edited: 2.1 / Risk Log<br>Processed feedback after meeting with Country Quality Manager Netherlands | R. Brunenberg |
| 0.9     | 16-02-2011 | Processed feedback after meeting with Director Internal Audit                                       | R. Brunenberg |
| 1.0     | 22-02-2011 | Processed feedback from Mart van Hulten                                                             | R. Brunenberg |

*Distribution**This document is sent to:*

| VERSION | DATE       | NAME            | FUNCTION                            |
|---------|------------|-----------------|-------------------------------------|
| 0.6     | 14-02-2011 | Ben de Backker  | Country Quality Manager Netherlands |
| 0.7     | 15-02-2011 | Ben de Backker  | Country Quality Manager Netherlands |
| 0.9     | 16-02-2011 | Hans Kappert    | Director Internal Audit             |
| 1.0     | 22-02-2011 | Mart van Hulten | Teacher Fontys Hogeschool           |
|         |            | Hans Kappert    | Director Internal Audit             |
|         |            | Mart van Hulten | Teacher Fontys Hogeschool           |

*Approvals*

This document is approved by:

| VERSION | DATE       | NAME                                               | FUNCTION                  | INITIALS |
|---------|------------|----------------------------------------------------|---------------------------|----------|
| 0.9     | 16-02-2011 | Hans Kappert (on behalf of the steering committee) | Director Internal Audit   |          |
| 1.0     | 25-02-2011 | Hans Kappert (on behalf of the steering committee) | Director Internal Audit   |          |
| 1.0     | 22-02-2011 | Mart van Hulten                                    | Teacher Fontys Hogeschool |          |

# 1. Introduction and background of the project

## 1.1 Introduction

### 1.1.1 Goals of the document

This document is formulated to appoint all relevant basis information and the point of departure from the project, so that it can be managed on the correct way. It is purposed to define the project, to serve as a basis for the management of the project and to make it possible to judge the success of the project.

This project initiation document (PID) discusses the next fundamental aspects of the project:

- What do you want to achieve with this project?
- Why is it important to achieve those targets?
- Who are involved with managing the project, and what are their roles and responsibilities?
- How and when measures as discussed in this PID will be realized.
- How the document will be used:
  - To be sure that the project has a healthy basis before the principal is asked to commit himself to the project.
  - To serve as basis document so that the principal can check and watch over the progress and changes, and so that questions can be judged concerning the validity of the project during the execution of it.

### 1.1.2 Structure of the document

To indicate which parts will be updated, and therefore will receive new versions, during the progress of the project, this PID is divided into two sections: a static part and a dynamic part.

The static part consist the next chapters and appendixes:

- Introduction and background project (Chapter 1)
- Project definition (Chapter 2)
- Project organization structure (Chapter 4)
- Role descriptions (Chapter 5)
- Controls (Chapter 7)
- Quality plan
- Product descriptions
- Communication / reporting plan

The dynamic part consists the next chapters and appendixes:

- Initial Business Case (Chapter 3)
- Initial Project Planning (Chapter 6)
- Risk log
- Project file

## 1.2 Background

### 1.2.1 Context of the project

Atos Origin is a leading international IT services provider. Atos Origin provides integrated designs, builds and operate solutions to large multi-national clients in carefully targeted industry sectors. Their business approach is based on establishing long-term partnerships that encourage success through mutual benefit. The company's annual revenues are EUR 5.1 billion and it employs 49,000 people in 40 countries. Atos Origin is the Worldwide Information Technology Partner for the Olympic Games and has a client base of international blue-chip companies across all sectors.

Atos Origin is one of the few companies that can provide all the 'design, build, and operate' elements of a business solution. More than two third of the revenue base is recurring, deriving from multi-year outsourcing and application maintenance contracts, and Atos Origin delivers this within a global framework of three major Service Lines:

- Atos Consulting
- System Integrations
- Managed Operations

For more information about those three service lines, see: [http://www.atosorigin.com/en-us/about\\_us/Company\\_Profile/default.htm](http://www.atosorigin.com/en-us/about_us/Company_Profile/default.htm)

The project will be carried out by the service line Managed Operations (MO). Managed operations is spread over multiple establishments in the Netherlands. The project focus shall mainly lie on the establishments located in Eindhoven and Utrecht. When it is needed to speak with people from other establishments, this will be done with either office communicator, or with a conference call. The subject of the project is the transition from SAS-70 to ISAE 3402. See next paragraph for more details.

### 1.2.2 Concrete occasion of the project

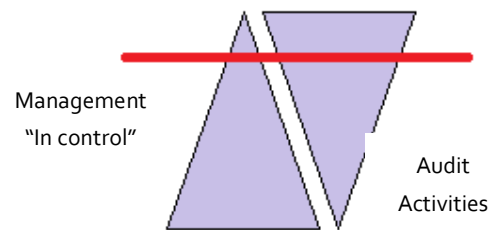
Atos Origin Netherlands starts in 2011 with a new standard for reporting about internal control for third parties. Formerly they used the standard SAS-70, now they must use ISAE 3402. This standard will replace the SAS-70 standard worldwide and will be used on an international basis. The standard is supported by the IFAC (International Federation of Accountants) and the ASB (Auditing Standards Board, US). For this standard Atos Origin needs to preventively check if processes are in control, so that they don't get to hear afterwards that certain processes are not. The preventive checks will occur due to monthly management reports which can be judged by the management so that the management is timely informed about the processes which are in control. This makes it possible to govern processes, so that management can proof that all processes are in control when an external auditor performs an audit. The need for the external auditor to deeply check can be minimized due to the management reports that can be handed to him. Therefore, his audit activities might change, and might be less than in the case of SAS-70.

The management reports needs to be realized and implemented. As soon as it is implemented and optimized in the Netherlands, it can be used on a global level.

The definition of the problem can be named as followed:

*"Complement and implement management reports for provable "be in control" as part of the ISAE 3402 Assurance standard and the Business Balanced Score Card."*

Underlying goal is to spare costs through lower costs for audit activities. The picture below shows this:



When the management will be more in control (red line is going down), then the audit activities will decrease. This means that the costs will drop, not only the direct audit costs, but also indirect costs, because less people need to get interviewed and instructed etcetera.

### 1.2.3 Reasons for a project approach

A project approach is chosen because in this way the project can be divided into pieces with milestones, so that it can be easily managed. This way the project progress can be easily controlled. The reasons for a project approach are in this case as follows:

- It is needed to cooperate with people from different disciplines.
- There is a limited term available for the project, therefore it is needed to use the available time effectively and efficient.

## 2. Project definition

Name of the project : Graduation Ruud Brunenberg  
Project code : NLD-AUD-0187  
Department : Managed Services Quality and Security  
Budget holder : N. Siepel

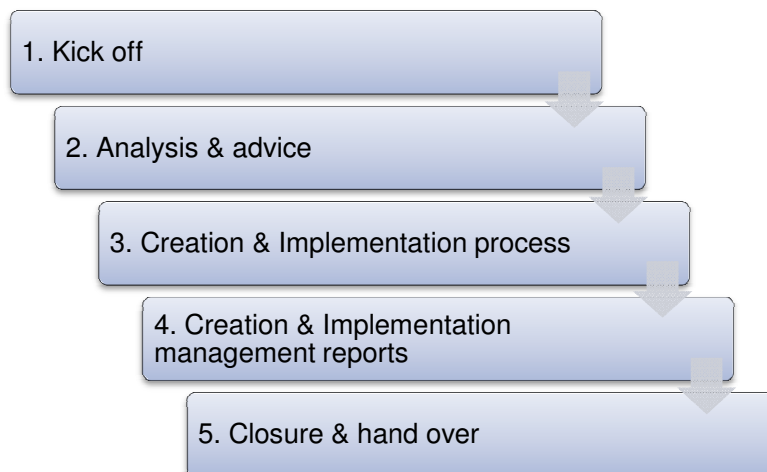
### 2.1 Project objectives

Support Atos Origin with the transition process from SAS-70 to ISAE 3402 by creating management reports. With those management reports, the management can easily see if processes are in control, so they should be able to govern their processes more easily. Due to that it's very likely that more processes will be in control. This way it is easier for Atos Origin management to sign off the management association letters in assurance reports. Eventually this way of working makes it possible to decrease the audit effort, which will result in less costs for audit activities. Goals of the project are to:

- Define data out of processes which is wished/needed for management reports
- Create a process to extract the wished data out of the processes and to hook it into a management report.
- Create management reports which are reliable, verifiable and integer.

### 2.2 Approach and Phasing

The picture below represents the different phases. Parallel on these phases is writing an essay.



#### Phase 1: Kick off

Activities which will take place in this phase are:

- Creating a project initiation document (PID), discuss this with the principal and receive a go/no go.
- Preliminary investigation. The project manager will search relevant background information in primary, secondary and tertiary sources. The focus of this investigation lies on research for the subject ISAE 3402.

Questions that need to be answered are:

- Is it possible to receive a clean ISAE 3402 assurance report, by using management reports?
- Optionally: How do management controls as defined in the theory match with the regular management of Atos Origin?

### Phase 2: Analysis & recommendation

Activities which will take place in this phase are:

- Regularly update/specify the planning when it's clearer which activities have to be done.
- Investigate which management reports there are available
- Investigate which data is wished for the new management reports (or missing in the current ones)
- Determine how the current management reports can be used/modified in combination with the new information
- Define the required information, control objectives and monitoring controls for those reports
- Create an recommendation report where an recommendation is given about how to get the required data out of the organization

### Phase 3: Creation & Implementation process

Activities which will take place in this phase are:

- Create a process description for the new process
- Create procedures / work instructions
- Implementation process including responsibilities, accountabilities, consult, inform (RACI)
- Test implemented process (2 runs if feasible)

### Phase 4: Creation & Implementation management reports

Activities which will take place in this phase are:

- Realize a template for the management reports
- Fill template with data from phase 3 to proof that reporting can be done
- Test implemented template/reporting (2 runs if feasible)
- Hook report into the management reporting

### Phase 5: Closure & hand over

Activities which will take place in this phase are:

- Acceptation test with steering committee
- Hand over project / project output to responsible
- Complete the essay
- Preparation of- and present the presentation

## **2.3 Scope**

In scope is:

- An investigation with a research report about the IST and SOLL situation.
- Creation and implementation of a process to receive the wished/requested data out of the organization
- Procedures and work instructions for this process
- Creation and/or completion of management reports, including hooking those reports into higher management reports
- Testing of the process
- Filled management reports
- Hand over with verbal explanation (presentation)

**Excluded from the scope is:**

- Create or update process descriptions, procedures and work instructions which are not related with ISAE 3402 / SAS-70
- Edit management reports which are not related with ISAE 3402 / SAS-70
- Implementation elsewhere then Atos Origin Netherlands, Eindhoven (High Tech Campus)
- Modifications in Atos Origin systems
- Purchasing hard- or software for the project
- Training
- Distribution from documents in another language than English.
- Aftercare after completion of the project
- Check/Revise documents on English grammar and structure

Relations who will not be involved in the project are:

- Customers from Atos Origin
- Suppliers from Atos Origin

## 2.4 Results / deliverables

The results are described by phase in the table below. All deliverables will be reported in English, the essay excepted. The English which will be used in documents is very basic because the author of the documents isn't experienced with writing in other languages then Dutch. Extended descriptions of the results can be find in the appendix "Product descriptions".

|               |                                                 |                                                                                                                                                                  |
|---------------|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Writing Essay | 1. Kick off                                     | <ul style="list-style-type: none"> <li>• Project Initiation document</li> <li>• Research report (theoretical deepening)</li> </ul>                               |
|               | 2. Analysis & Advice                            | <ul style="list-style-type: none"> <li>• Research report (analysis)</li> <li>• Advice report</li> </ul>                                                          |
|               | 3. Creation & implemenation process             | <ul style="list-style-type: none"> <li>• Process description</li> <li>• Procedure- / workinstructions</li> <li>• Testbook part 1</li> </ul>                      |
|               | 4. Creation & implementation management reports | <ul style="list-style-type: none"> <li>• Management report template(s)</li> <li>• Filled templates (=management report(s))</li> <li>• Testbook part 2</li> </ul> |
|               | 5. Closure & Hand over                          | <ul style="list-style-type: none"> <li>• Essay</li> <li>• Presentation (hand over)</li> <li>• Presentation (school)</li> </ul>                                   |

It is possible that some deliverables can't be hand over, or are partly hand over at the end of the project. This is because the time term is pretty short, and the planning pretty tight. Therefore there is a weekly meeting where the planning and deliverables are reviewed. When it's necessary the deliverables will be changed in consultation with the steering committee. This depends on different occasions, named in the paragraphs below.

## 2.5 Pre requisites and assumptions

### Pre requisites

To get the right result within the given time, there are some pre requisites. The pre requisites concern activities which should be taken or situations that need to fulfill certain requirements. The current pre requisites concern:

- Documentation which is requested contains a correct representation of the reality. Considerations, actions and decisions will be partly made on basis of this documentation. It is important that the documents don't contain invalid information, because this can have consequences for the result of the project.
- Atos Origin is responsible for purchasing, installing and maintenance of needed hard-/software which is required for the project.
- The project initiation document has to be approved by the steering committee before the project may start.

### Assumptions

The following assumptions are made:

- Sufficient time to test (minimum of 2 test, estimated time 3 days/test)
- Management reports already exist
- Data is accessible in Atos Origin systems
- Cooperation from Atos Origins employees
- Atos Origin will provide sufficient support to assist when the project needs input.
- Project manager will not be absent during the project

## 2.6 Constraints

The project knows the following constraints:

- Availability of the steering committee and Atos Origin employees
- Accessibility of the steering committee and Atos Origin employees
- Turnaround of 85 days
- Deadline 17 June 2011
- Level of knowledge from the project manager and the involved people

## 2.7 Dependencies

- The project depends on the available time
- Information given by the management and other staff
- Support when necessary
- Availability and assistance of management and staff
- Approachability and accessibility of needed data in systems
- Work circumstances

## 2.8 Relations with other projects and activities

### 3. Initial Business Case

This document contains the considerations to start the current project. It forms the justification of the project and will be judged by the steering committee. The foundation of the project will be evaluated on a regular basis of this Business Case.

#### Reasons:

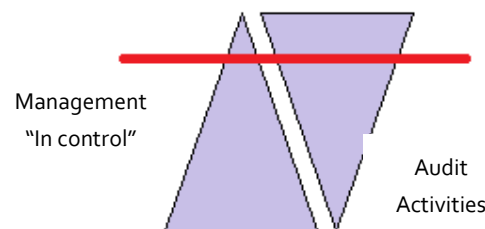
Atos Origin Nederland starts in 2011 with a new standard for reporting about internal control for third parties. Formerly they used the standard SAS-70, now they must use ISAE 3402. This standard will replace the SAS-70 standard worldwide and will be used on an international basis. The standard is supported by the IFAC (International Federation of Accountants) and the ASB (Auditing Standards Board, US). For this standard Atos Origin needs to preventively check if processes are in control, so that they don't get to hear afterwards that certain processes are not. The preventive checks will occur due to monthly management reports which can be judged by the management so that the management is timely informed about the processes which are in control. This makes it possible to govern processes, so that management can proof that all processes are in control when an external auditor performs an audit. The need for the external auditor to deeply check can be minimized due to the management reports that can be handed to him. Therefore, his audit activities might change, and might be less than in the case of SAS-70.

The management reports needs to be realized and implemented. As soon as it is implemented and optimized in the Netherlands, it can be used on a global level.

The definition of the problem can be named as followed:

*"Complement and implement management reports for provable "be in control" as part of the ISAE 3402 Assurance standard and the Business Balanced Score Card."*

Underlying goal is to spare costs through lower costs for audit activities. The picture below shows this:



When the management is will be more in control (red line is going down), then the audit activities will decrease. This means that the costs will drop, not only the direct audit costs, but also indirect costs, because less people need to get interviewed and instructed etcetera.

#### Expected benefits:

- Cost savings, direct and indirect costs due to decreasing audit activities
- Better possibilities to govern processes
- Better quality of processes and therefore services (PDCA circle)

- With the result of this project it's more easily for the management to sign off the management association letter in assurance reports

#### **Finances:**

Because this project is a graduation assignment, costs are not directly insightful. There is no budget agreed with the principal. Below there are some costs which will be made for the project. This document will not describe estimated costs or costs in detail.

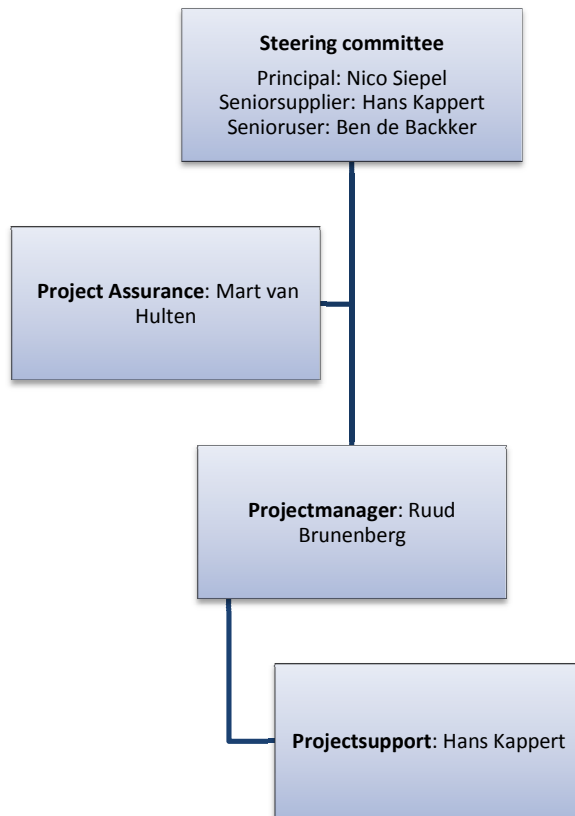
#### Direct costs:

- Remuneration

#### Indirect costs:

- Use of resources provided by Atos Origin (mostly employee time)
- Overhead costs

## 4. Project organization structure



## 5. Role descriptions

### 5.1 Principal

#### Role description:

The principal, in this case Nico Siepel, is the one who gave the assignment for the project. The principal is the requested party, which has to communicate clearly about his wishes and demands.

#### Project related tasks:

- Clear communication of wishes and demands to the project manager
- Clarify indistinctness

#### Specific responsibilities:

The principal is responsible for the delivery of needed information and documentation with regard to the scope of the project if requested by the project manager.

Furthermore, the principal is also responsible for the approval of the project at the end of the route.

### 5.2 Senior user

#### Role description:

The senior user, in this case Ben de Backker, is a representative of the eventual end-users of the project, and is the person where the project will be hand over too.

#### Project related tasks:

- Clear communication of wishes from the end-users
- Approve proposal documents

#### Specific responsibilities:

The senior user is responsible for the corrective representation of all end users, and he has to make sure that the outcome is also optimized for them.

### 5.3 Senior Supplier

#### Role description:

The senior supplier, in this case Hans Kappert, is the one who delivers information and other requisites to the project manager. This means that when there is more information required about Atos Origin, which the project manager needs, then it is the senior suppliers task to deliver this information.

#### Project related tasks:

- Deliver information and devices in regard with the project

#### Specific responsibilities:

The senior supplier is mainly responsible for delivering information and devices during the project.

## 5.4 Project assurance

### Role description:

Project assurance means that the earlier determined quality and time planning of the project are achieved. Without this external control, there can be made mistakes by people who work a lot with the project. By focusing on small details, other important details can be forgotten, completed to late or completed with a bad quality.

### Project related tasks:

- Controlling the quality of the end products (results) of the project
- Controlling the time planning and intervene when this goes wrong
- Controlling the total status of the project and controlling if details don't get missed.

### Specific responsibilities:

Project assurance is mainly responsible for the control of end products (results) from the project and to keep grip on the time planning of the project.

## 5.5 Project manager

### Role description:

The project manager is the person who makes sure that the project is governed and executed; in this case that is Ruud Brunenberg.

### Project related tasks:

- Watch over the time planning and the quality of the project
- Make sure all activities are performed in time
- If necessary, consult with the steering committee about request for changes on the project in progress.
- Make sure distribution is done correctly
- Perform the project activities according planning

### Specific responsibilities:

Mainly responsible for executing the project activities according planning and for controlling the time planning and to guarantee the quality of end products (results) as earlier agreed.

## 5.6 Project support

### Role description:

Project support is, as the name already says, support to the project manager when necessary. When the project manager has a problem which he can't solve, when he has an opinion about a subject, or when he self don't has enough expertise, he will call in project support. In this case project support is given by Hans Kappert.

### Project related tasks:

- Support the project manager when he has problems which he can't resolve
- Giving a second opinion

### Specific responsibilities:

Support the project manager when he asks too.

## 6. Initial Project planning

### Project plan description:

This plan concerns the creation of management reports within the framework of the transition from SAS-70 to ISAE 3402. The plan describes how the project is approached.

### Pre requisites

To get the right result within the given time, there are some pre requisites. The pre requisites concern activities which should be taken or situations that need to fulfill certain requirements. The current pre requisites concern:

- Documentation which is requested contains a correct representation of the reality. Considerations, actions and decisions will be partly made on basis of this documentation. It is important that the documents don't contain invalid information, because this can have consequences for the result of the project.
- Atos Origin is responsible for purchasing, installing and maintenance of needed hard-/software which is required for the project.
- The project initiation document has to be approved by the steering committee before the project may start.

### Assumptions

The following assumptions are made:

- Sufficient time to test (minimum of 2 test, estimated time 3 days/test)
- Management reports already exist
- Data is accessible in Atos Origin systems
- Cooperation from Atos Origins employees
- Atos Origin will provide sufficient support to assist when the project needs input.
- Project manager will not be absent during the project

### Constraints

The project knows the following constraints:

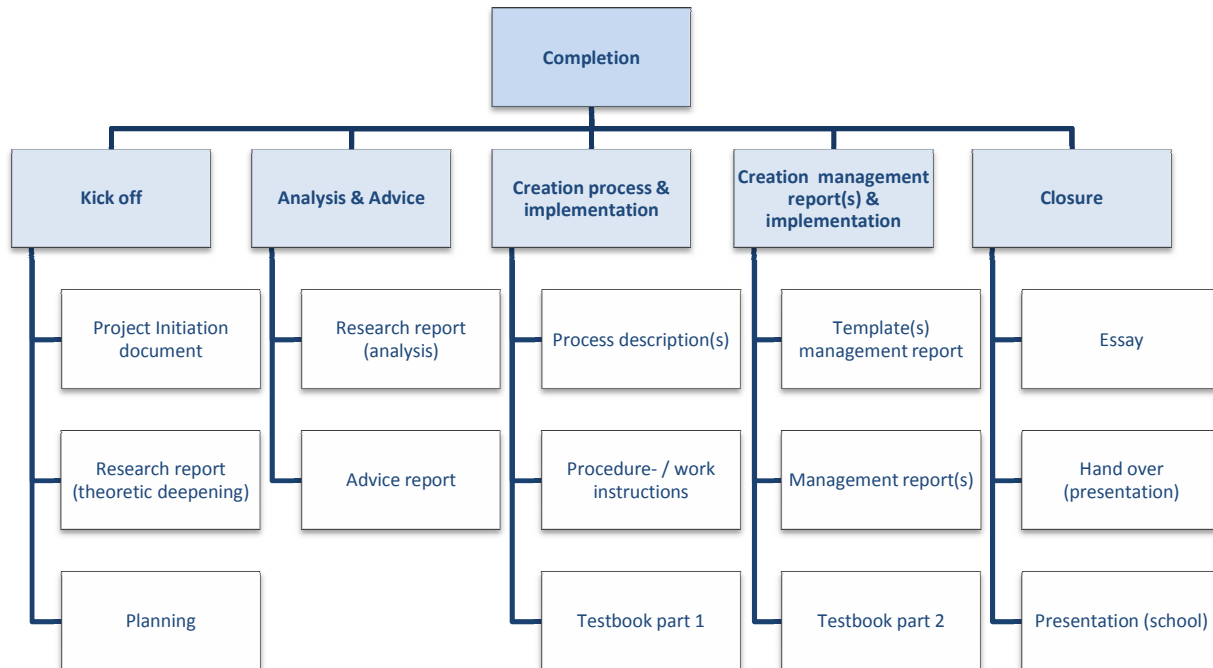
- Availability of the steering committee and Atos Origin employees
- Accessibility of the steering committee and Atos Origin employees
- Turnaround of 85 days
- Deadline 17 June 2011
- Level of knowledge from the project manager and the involved people

### Dependencies

- The project depends on the available time
- Information given by the management and other staff
- Support when necessary
- Availability and assistance of management and staff
- Approachability and accessibility of needed data in systems
- Work circumstances

## 6.1 Project planning

Product decomposition structure:



**Product flowchart:**

| Product                               | Completion By   | Completion To      | Phase                                          |
|---------------------------------------|-----------------|--------------------|------------------------------------------------|
| Project initiation document           | Project manager | Steering committee | Kick off                                       |
| Research report (theoretic deepening) | Project manager | Project assurance  | Kick off                                       |
| Planning                              | Project manager | -                  | Kick off                                       |
| Research report (analysis)            | Project manager | Steering committee | Analysis & Recommendation                      |
| Recommendation report                 | Project manager | Steering committee | Analysis & Recommendation                      |
| Process description(s)                | Project manager | Steering committee | Creation process & implementation              |
| Procedure- / work instructions        | Project manager | Steering committee | Creation process & implementation              |
| Testbook (part 1)                     | Project manager | -                  | Creation process & implementation              |
| Template management report(s)         | Project manager | Steering committee | Creation management report(s) & implementation |
| Management report(s)                  | Project manager | Steering committee | Creation management report(s) & implementation |
| Testbook (part 2)                     | Project manager | Steering committee | Creation management report(s) & implementation |
| Essay                                 | Project manager | Project assurance  | Closure                                        |
| Hand over (presentation)              | Project manager | Steering committee | Closure                                        |
| Presentation (school                  | Project manager | Project assurance  | Closure                                        |

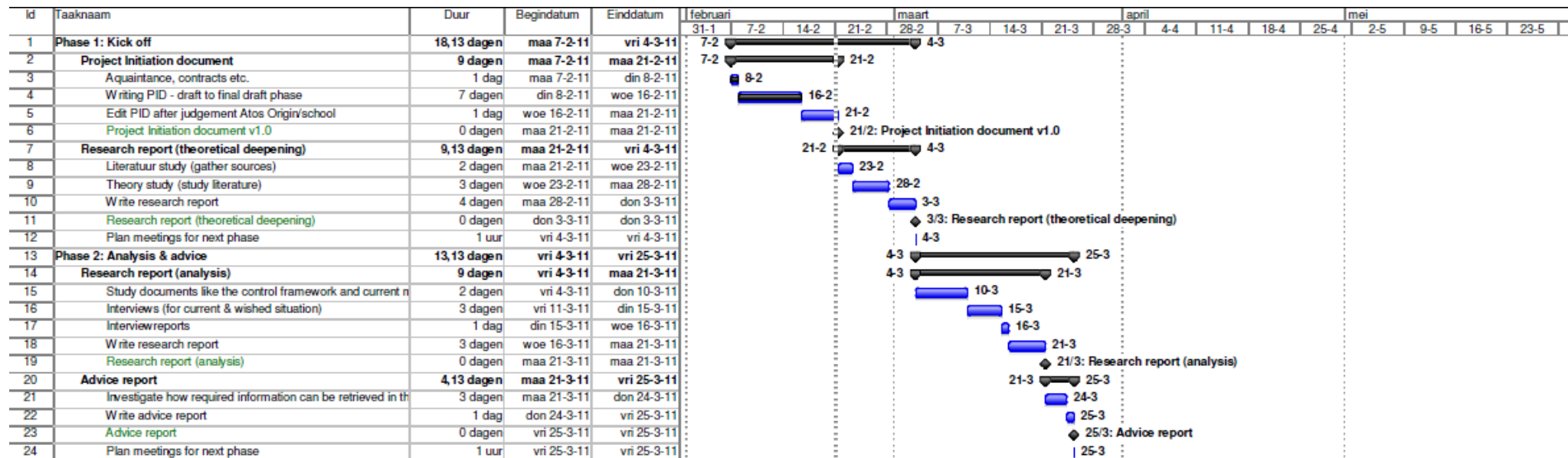
**Product descriptions:**

For the product descriptions, see appendix: product descriptions

## Activity network:

The planning as mentioned below is part of the dynamic part of this document and is liable to adjustments and changes when the project process requires this.

- The project planning knows approximately 4 days for progress meetings and reporting to school. Those activities are not calculated in the different phases so the milestones and turnaround are in reality almost a few hours/days later.
- This is a worst case planning, there are no margins. Because of that the planning (and possible the deliverables) will be adjusted week by week, in dialogue with project support or the steering committee
- Three free days are not took along in the planning. Those days, including the 4 days for project management will set the end date of the project on 17 June 2011



Pagina 1

**Project budget:**

Because this project is a graduation assignment, costs are not directly insightful. There is no budget agreed with the principal. Below there are some costs which will be made for the project. This document will not describe estimated costs or costs in detail.

Direct costs:

- Remuneration

Indirect costs:

- Use of resources provided by Atos Origin (mostly employee time)
- Overhead costs

**Needed resources:**

- Workspace
- Laptop
- Badge
- Access to the internal Atos Origin network
- Software:
  - Microsoft office suite (including MS Office Communicator, MS Project & MS Visio)
  - Mindjet Manager
- Power supply
- Internet connection
- Translate tooling
- Printer
- Meeting room
- Presentation room
- Employees from Atos Origin
  - Reporting Group
  - Quality & Security officers
  - Process managers

## 7. Controls

### 7.1 Reporting

For extended product descriptions, see appendix: product descriptions

|                                                                                               | Steering committee      | Project Assurance       | Project Support                   | Project Manager      |
|-----------------------------------------------------------------------------------------------|-------------------------|-------------------------|-----------------------------------|----------------------|
| Project Initiation document                                                                   | Approve                 | Advise<br>Check         | Advise<br>Check                   | Create<br>Distribute |
| Research report (theoretical deepening)                                                       | Receive for information | Check Approve           | Receive for information           | Create<br>Distribute |
| Research report (analysis)                                                                    | Approve                 | -                       | Advise<br>Check                   | Create<br>Distribute |
| Recommendation report                                                                         | Approve                 | -                       | Advise<br>Check                   | Create<br>Distribute |
| Process description                                                                           | Approve                 | -                       | Advise<br>Check                   | Create<br>Distribute |
| Procedure- / work instructions                                                                | Approve                 | -                       | Advise<br>Check                   | Create<br>Distribute |
| Testbook part 1 (for testing the process)                                                     | Approve                 | -                       | Advise<br>Check                   | Create<br>Distribute |
| Template management report(s)                                                                 | Approve                 | -                       | Advise<br>Check                   | Create<br>Distribute |
| Filled template (=management report(s))                                                       | Approve                 | -                       | Advise<br>Check                   | Create<br>Distribute |
| Testbook part 2 (for testing the implemented process with as a result the management reports) | Approve                 | -                       | Advise<br>Check                   | Create<br>Distribute |
| Presentation (hand over)                                                                      | Approve                 | Receive for information | Advise<br>Check                   | Create<br>Distribute |
| Essay                                                                                         | Receive for information | Check<br>Approve        | Advise Receive<br>for information | Create<br>Distribute |
| Presentation (for school)                                                                     | Receive for information | Check<br>Approve        | Advise Receive<br>for information | Create<br>Distribute |
| Logbook                                                                                       | -                       | Check<br>Approve        | Receive for information           | Create<br>Distribute |
| Planning                                                                                      | Approve                 | Receive for information | Advise<br>Check Approve           | Create<br>Distribute |

## 7.2 Progress monitoring

| Meeting                         | Presents                                                           | Frequency                             | Time             | Objective                      | Subjects                                                             |
|---------------------------------|--------------------------------------------------------------------|---------------------------------------|------------------|--------------------------------|----------------------------------------------------------------------|
| Progress                        | Project manager<br>Project support<br>Optional: Steering committee | Min. 1x / week<br>Probably more often | Friday morning   | Discuss project                | Achievements previous week, goals next week.<br>Feedback on products |
| Reporting to steering committee | Project manager<br>Steering committee                              | After each phase                      | -                | Consultation about the project | How did the phase elapsed                                            |
| Reporting to project assurance  | Nobody physical                                                    | 1x / week through mail                | Friday afternoon | Provide understanding          | Progress, achievements last week                                     |

## 7.3 Tolerances

During the project there are some tolerances when it appears that the planning for a phase is too tight. When the deadline can't be achieved in time, there is a 5% tolerance without asking the steering committee for permission. When the deadline appears to be higher as 5%, then it's needed to ask permission from the steering committee, before the project continues.

## 7.4 Risk management

In the next chapter a risk log is assimilated. In this log, risks are described which can be reckoned foregoing of the project. After closure of each phase there will be looked at the risk log. If there occurred risks during a phase, then the actions will be taken, as foregoing described in the risk log. Furthermore there will be looked if there are new risks after each phase. If there are new risks, those will be assimilated again in the risk log. It is also possible that there are unexpected risks during the course of a phase. In that case the risks will be discussed with the steering committee so that those can be handled as good as possible.

## 7.5 Issue management

During the project it is always possible that there are incidents which couldn't be reckoned in advance. When this happens there will be planned and held a meeting with the steering committee. In this meeting the incident will be discussed, and the consequences will be discussed.

## 7.6 Abnormality and escalation procedure

When it is necessary to deviate from the original project plan, it is needed that the steering committee approves this. First instance this means that a request for change (RFC) needs to be created. In this RFC needs to be described what the abnormality's are, what the causes of the abnormality's are and what will be changed in the renewed project plan. This has to be approved by the steering committee before the project continues. Worst case, the steering committee could decide that the project has to be stopped because the abnormalities are too big.

## Risk Log

| Project code:   |           | NLD-AUD-0187                                                                                                       |          | Name project:    |        | Graduation Ruud Brunenberg |          |                                                                                                                                          |       |        |
|-----------------|-----------|--------------------------------------------------------------------------------------------------------------------|----------|------------------|--------|----------------------------|----------|------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|
| Product name:   |           | RISK LOG                                                                                                           |          | Project manager: |        | Ruud Brunenberg            |          |                                                                                                                                          |       |        |
| Product number: |           | A.31                                                                                                               |          |                  |        |                            |          |                                                                                                                                          |       |        |
| Id.             | Requester | Description                                                                                                        | Category | Chance           | Impact | Time                       | Priority | Countermeasure                                                                                                                           | Owner | Status |
|                 |           |                                                                                                                    |          |                  |        |                            |          |                                                                                                                                          |       |        |
| 1               |           | Inaccessible steering committee                                                                                    | O        | 5                | 2      |                            | 10       | Search other employees who have enough knowledge or possibilities to keep the project going when the steering committee isn't accessible |       |        |
| 2               |           | Inaccessible employees                                                                                             | O        | 3                | 1      |                            | 3        | Search other employees who can hand out the same needed information                                                                      |       |        |
| 3               |           | Unexpected technical issues (HDD crash by example)                                                                 | T        | 1                | 3      |                            | 3        | Back up on a weekly basis                                                                                                                |       |        |
| 4               |           | Closure of the project by Atos Origin (by example coursed through abolishing ISAE 3402 and continuing with SAS-70) | C        | 1                | 3      |                            | 3        | Closure of project, discuss with companion how to reach targets for the graduation stage.                                                |       |        |
| 5               |           | Absence of project support                                                                                         | O        | 5                | 2      |                            | 10       | Search for other project support                                                                                                         |       |        |
| 6               |           | Limited level of knowhow (by the project manager and/or Atos Origin employees)                                     | O        | 1                | 2      |                            | 2        | Search other ways to get the right knowhow.                                                                                              |       |        |
| 7               |           | Insufficient time to test                                                                                          | O        | 5                | 2      |                            | 10       | Discuss next steps with steering committee, look for space in the planning (extra time). Ask support or exclude steps.                   |       |        |
| 8               |           | No management reports exist                                                                                        | O        | 0                | 2      |                            | 0        | Adjust planning, discuss steps with project support                                                                                      |       |        |
| 9               |           | Data is not accessible in Atos Origin systems                                                                      | O        | 4                | 1      |                            | 4        | Retrieve the data from other people or arrange access to the systems Adjust planning if necessary .                                      |       |        |
| 10              |           | Insufficient support of Atos Origin                                                                                | O        | 1                | 3      |                            | 3        | Discuss with steering committee, Increase understanding by employees and perform pressure to the responsible managers.                   |       |        |
| 11              |           | Absence of project manager                                                                                         | O        | 2                | 3      |                            | 6        | Discuss further actions with steering committee                                                                                          |       |        |

# Quality Plan

This Quality plan is part of the project initiation document. The target is to define the quality techniques and standards which will be applied in the project, and the responsibilities to reach the demanded quality levels.

## Quality Expectations from principal:

### Information

The quality of information. The principal expects that the quality of the information which eventually will be taken up in the management reports fulfills the next quality aspects:

- Reliability
- Integrity
- Verifiability

The management report also has to be in accordance with the ISAE 3402.

### Way of reporting

If possible Atos Origin templates need to be used. All documents need to have a clear document history with clear version administration. Furthermore all deliverables have to be documented in English (except the essay) and fulfill the quality aspects as mentioned above. With the steering committee is agreed that the level of English writing skills are enough to report in English. Mistakes with words and grammar can't be assigned to the project manager because his skills aren't advanced enough.

When Atos Origin templates are not available, new ones have to be created in the style of Atos Origin's templates.

For interviews during the project, interview reports will be created.

The project manager is responsible for correct distribution of the documents/reports.

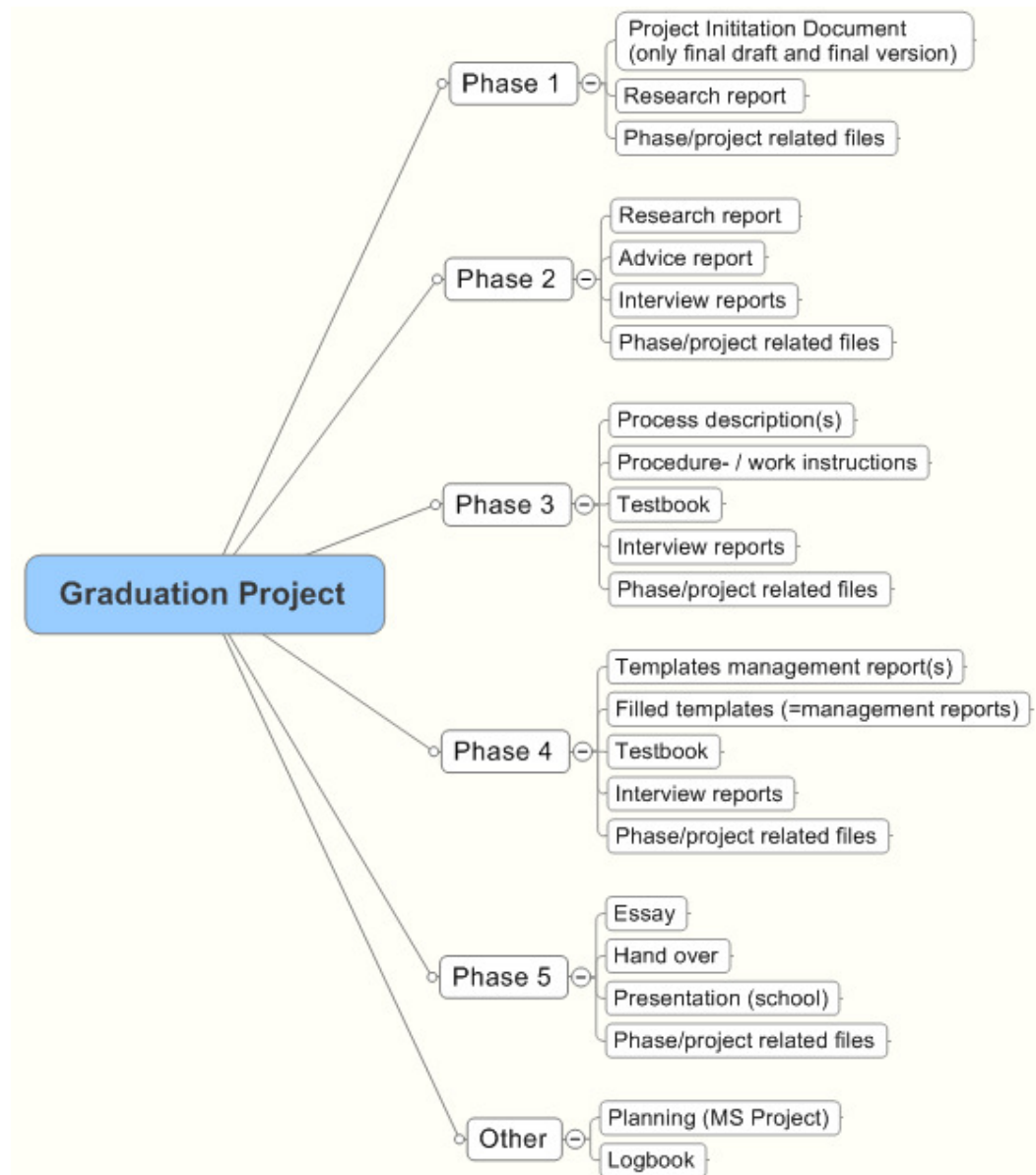
A decisions list and an action list will be made for meetings with the steering committee. The available Atos Origin template will therefore be used.

## Acceptation criteria:

1. The information given in reports/deliverables needs to specify the quality aspects as mentioned above.
2. There has to be proof that the process delivers the required information for the management report(s) and that this information is correctly assimilated in the management report template(s) and/or hooked in existing management report(s).
3. There has to be proof that the process can deliver the requested information over and over.
4. The information in management report(s) needs to be verifiable.
5. All documentation needs to be clearly by hand over. There has to be documented what is done so that it's clear to the organization how they can work further with the process and management report(s).

## Project File

All versions of the reports/deliverables will be published on Livelink. The structure of the maps might change during the project. But as basis the map structure as sketched below will be used.



# Product Descriptions

## Project Initiation Document

This document forms the basis to start the project. It describes the project, the approach, the expectations, and deliverables, using the method PRINCE2.

## Research report (theoretical deepening)

To do the project some theoretic knowledge is required. Therefore an investigation will take place for the subject ISAE 3402. In this rapport there will be documented which sources are used for the investigation, and the most relevant information is documented. There will be a management summary.

## Research report (analysis)

This report describes the results of the preliminary investigation. The report makes clear what the IST and SOLL situations are. The rapport describes:

- How much management reports there are currently available
- Which data is wished for the new management reports (or missing in the current ones)
- How the available management reports can be used /modified
- Concrete description/definition of the requested/wished information, control objectives and monitoring controls with further explanation.

## Recommendation report

An recommendation report based on the research report (analysis). The recommendation reports gives recommendation about how to get the data as if defined in the research report (analysis) out of the organization.

## Process description

This product is mainly based on the recommendation report. In the recommendation report is described which activities have to be taken and by who, to get the required data out of the organization. This has to be translated to a process description with responsibilities. This description will be made in a flowchart. When the process description is finished, is it very likely that it has to be edited continuously during this phase, due to test results.

## Procedure- / work instructions

To implement the process it's necessary to instruct employees. Therefore procedures and work instructions have to be written. In those instructions is described what the activities are which a certain function is responsible for, and how he is able to execute those activities.

## Testbook part 1 (for testing the process)

The process needs to be tested. This testbook describes the steps from the start of the process until the activities when the required/wished information is delivered as output. Therefore it's needed to report the tests which are going to, and which are executed. In the testbook is also described if actions are needed, and if so, how they should be taken.

## Template(s) management report

The process which is just implemented should have the wished/requested information as output. To structure this data a template is necessary. The template can be an already existing, or an edited template. But it is also possible completely new templates have to be developed.

#### Filled templates (=management report(s))

The templates as described above need to get filled. Therefore the output of the process has to be filled into the management report templates. How and by who this has to be done should be described in the process description and procedures/ work instructions.

#### Testbook part 2 (for testing the implemented process)

The process needs to be tested. This testbook is the same as the previous mentioned but now it is filled up with descriptions of the steps which have to be taken to use the output data from the process so that the templates can be filled in. Therefore it's needed to report the tests which are going to be, and which are already executed. In the testbook is also described if actions are needed, and if so, how they should be taken.

#### Essay

This document describes what I have done and especially why I did that during my graduation. I try to justify my actions during the graduation project and I ground decisions which I took. I demonstrate that I'm capable to oversee the whole route and to reflect on it. The report is kind of a process report.

#### Presentation (hand over)

There will be a presentation for the steering committee and other involved and interested people. During the presentation the results of the project are discussed. If there are things which are not finished, then there will be a document which describes this in detail so that other people can continue with it. Questions can be asked and if necessary there will be changes on the latest documents before final hand over.

#### Presentation (school)

There will be an adjusted presentation for school which focuses more on competences and the process then on the results. I will try to justify my actions and decisions which I made/took during the graduation.

#### Logbook

The logbook describes from day to day which activities are done and how much hour are spent on it. It has a higher overview page where from week to week concrete is described what is done and how much days/hours were spent on it.

#### Planning

A Gantt Chart planning is made using MS Project. This planning will be constantly changed if necessary during the project. Changes will be made in dialogue with project support, and if necessary with the steering committee.

## Communication/reporting plan

### Communication Channels:

| From               | To                                      | Information                                    | Medium                                   | Frequency          |
|--------------------|-----------------------------------------|------------------------------------------------|------------------------------------------|--------------------|
| Project manager    | Project Assurance                       | Progress                                       | E-mail                                   | 1x/week            |
| Project Assurance  | Project manager                         | Feedback                                       | E-mail                                   | When necessary     |
| Project manager    | Steering committee                      | Concept and Final versions documents and plans | E-mail, hardcopy's, presentations        | According planning |
| Steering committee | Project manager                         | Feedback                                       | E-mail, verbally                         | When necessary     |
| Project manager    | Project support                         | Progress                                       | Verbally, conference call, communicator  | 1x/week            |
| Project manager    | Steering committee<br>Project Assurance | Appointment completion and final presentation  | E-mail, telephone, verbally              | Onetime            |
| Atos Origin staff  | Project manager                         | Project relevant information and requirements  | Verbally (interviews), E-mail, telephone | When necessary     |

### Incidental:

| From                            | To                           | Information                                         | Medium                      | Situation                                                |
|---------------------------------|------------------------------|-----------------------------------------------------|-----------------------------|----------------------------------------------------------|
| Project member                  | Steering committee           | Reason and expected time                            | E-mail, telephone           | Absence                                                  |
| Project manager                 | Steering committee           | Request for change (RFC)                            | Verbally, e-mail, telephone | Not planned/agreed abnormality's                         |
| Project support                 | Project manager              | Proposal (optionally with a RFC)                    | Verbally, e-mail, telephone | New insights / problems with current approach            |
| Steering committee (vice versa) | Project manager (vice versa) | Request rush meeting                                | Verbally, e-mail, telephone | Unforeseen situations which requires immediate attention |
| Project manager                 | All involved people          | Description of the situation, possible consequences | Verbally, e-mail, telephone | Unforeseen circumstances (accident, decease etc.)        |

## Bijlage B: Request for change

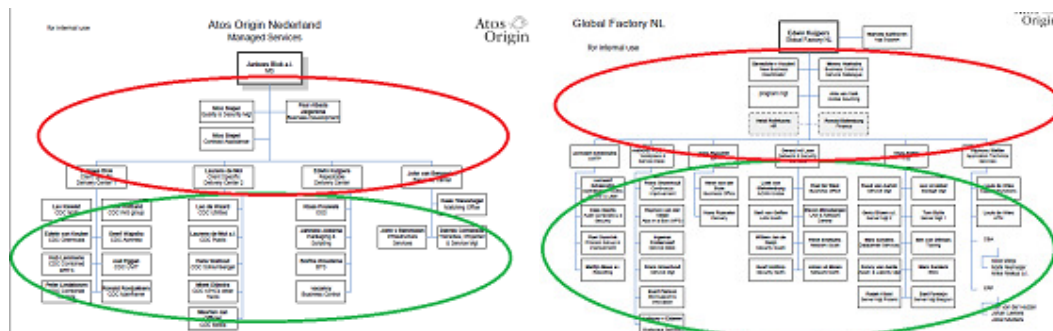
| REQUEST FOR CHANGE            |                            |                               |             |
|-------------------------------|----------------------------|-------------------------------|-------------|
| <b>Product:</b>               | Graduation Ruud Brunenberg | <b>Product Id.:</b>           | NA          |
| <b>Date identified.:</b>      | 06-04-2011                 | <b>Issue Log Id.:</b>         | NA          |
| <b>Date update:</b>           | 07-04-11                   | <b>Impact<sup>9</sup>:</b>    | S / T       |
| <b>Submitted by:</b>          | Ruud Brunenberg            | <b>Name decider:</b>          | Nico Siepel |
| <b>Decision<sup>10</sup>:</b> |                            | <b>Priority<sup>11</sup>:</b> | H           |
| <b>Date decision:</b>         |                            | <b>Initials decider:</b>      |             |

### 1. Issue(s)

During the investigation for my research report I found out that the current graduation assignment is probably not possible to execute within the time. The reasons here fore are described below.

When we started to define the assignment for my graduation we started from a perspective that reporting bottom up was already implemented, or that the implementation would be finished very soon.

My original assignment should focus on a report on a higher level. This report should consist data which is a consolidation of reports which are already there. This is shown in the org. charts below.



Originally I should pass a few phases, which are:

- 1. Kick off
- 2. Research, Analysis & recommendation
- 3. Creation & Implementation process
- 4. Creation & Implementation management report
- 5. Closure

During phase 2 I started with research to find out which reports there already where, and to investigate the opportunities to hook into those reports. I needed to find out what the requirements where from the management and if it was necessary to create a completely new report and to implement this. However, during this investigation I found out that the basis (green circle) which we originally went from wasn't available yet. For the global factory the reporting bottom up was properly calibrated. However, for the CDC's ( managed services) this was almost the

<sup>9</sup> T=Time, M=Money, Q=Quality, S=Scope, R=Risks

<sup>10</sup> A=Assigned, R=Rejected, P=Postponed

<sup>11</sup> H=High, M=Medium, L=Low

opposite.

The relevant reporting which I should use to consolidate in a higher level report is based on two reports: self assessments and service reviews. Those reports cover the so called monitoring controls. For my original assignment I should base my work activities on those reports. However, during my research I found out that this is only recently implemented in the global factory, and that for managed services this is still in transition. This transition can still take a while, and when finished my graduation time is almost finished. Furthermore the 2 organization parts aren't aligned yet. Different templates and input for service reviews are used. To get a good reporting structure/basis everything should be standardize and aligned. Then it's also relatively easy to consolidate data bottom up and to hook this in existing management reports on a higher level, or to create a new management report (my original assignment). When I continue with my current assignment I will probably run into a few bottlenecks:

- It's hard to consolidate data which can't be retrieved bottom up.

- The reporting I should implement is possibly only 50% filled because data cannot yet be retrieved bottom up, because the reporting will be empty, because implementation is not finished yet. Therefore the use of my product for the organization is low, and the cooperation will also be less, because this has a lower priority then commissioning the lower layer/basis.

Therefore I think it's better to help with the implementation of self assessments and service reviews in the CDC's. I know how the reporting structure is at this point, and how it should be. It would be good to make sure that the implementation is going to be structured and that the communication is good and uniform. Therefore I think I can support to get this as soon as possible up and running. At the moment this goes pretty slow because not much time is reserved for this subject, due to other day to day problems and work activities. However, this should be arranged as soon as possible, because the ISAE 3402 is already there in mid June.

Cees Geerts indicated that he was pretty sure he could convince Ernst and Young that only the basis layer (green layer) in combination with the current management reports is enough to prove that Atos Origin is in control.

In discussion with Ben de Backker, Cees Geerts, and Jos Papenhuijzen, is decided that this way is probably the best to continue. Therefore I will get a different role, almost a role like project manager, trying to structure the implementation which is already going on, but is progressing slowly. All persons as mentioned above identified the importance of the basis layer. Without this layer, the layer above can't be created very well, and it's possible this should cause a lot of extra/double work. The commitment for the basis layer is also a lot higher, because the priority is higher

## **2. Description Proposed Change**

- Finish my current research report. This report describes the current situation and the reporting structure, and consists info about the services/clients where over reporting is done. This report is almost finished, however, some information is still missing, and I like to finish this so that it's also useful for Atos Origin. Besides that it's something which covers a competence which I have to achieve for my graduation.
- Finish my recommendation report. This report is currently based on the research report. However, if some things come up during the closure of my research report, I have to take this with me into my recommendation. Besides that I would like to change my recommendation a little bit. I would like to add an recommendation for the implementation of a management report, or the hooking in existing management reports. By doing this I still fulfill a part of my original assignment. Only difference is that I don't implement it, but only give an recommendation, including a possible design to implement. This designing aspect is also required for me, because this covers a competence which I should achieve during my graduation.
- Structure the implementation of the self assessments and service reviews within managed services. I will support and execute by all activities which have to be done. This consists activities like: implementing, communicating, testing, standardize. Those activities will be further defined in a conversation which I will have on 08-04-11.
- Create a best practice report, which can be used to implement the same reporting structure for other Atos Origin establishments in other countries.
- The closure of my current project planning will be the same, this consists hand over and writing of my thesis.

A new planning will be created as soon as this RFC is approved by my principal and school.

### **3. Impact proposed Change** (Time, Money, Quality, Scope, Risks)

The impact of the proposed change is high. The scope of the assignment will change drastically. The assignment will be executed on a whole different level, and the eventually desired management report will not be a deliverable anymore. Only an recommendation will be given where a proposal is done about the best way to implement a higher level report.

The time range will be the same because my graduation has an end date which is not extendible. As earlier discussed in the PID, the impact on money is hard to define. However, in my opinion, the impact will be the same. The hours I need to speak and work with people shall not difference much from my original assignment.

The quality aspect will also not change very much. The quality criteria will be the same, however the acceptance criteria will change because other deliverables will come up. The impact will be defined later because it's not yet completely clear which activities and deliverables will come in place. For the risks the same applies.

## Bijlage C: Logboek



|                     |                    |                     |           |
|---------------------|--------------------|---------------------|-----------|
| Student:            | Ruud Brunenberg    | Aantal dagen        | 70        |
| Docentbegeleider:   | Dhr. M. van Hulten | Begindatum periode: | 7-1-2011  |
| Bedrijfsbegeleider: | Dhr. H. Kappert    | Einddatum periode:  | 17-6-2011 |

| Week | Opmerkingen/Blog                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | T/A/V/Z dagen* | Soort T/A/V/Z | Werkdagen | Aantal uren |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|---------------|-----------|-------------|
| 1    | Kennismaking, eerste gesprekken gehad, contracten e.d. in orde gemaakt, begin gemaakt aan PID en eerste versies doorgesproken.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | -              | -             | 5         | 37:45:00    |
| 2    | PID afgerond, 2 dagen verlof gehad.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2              | V             | 3         | 26:00:00    |
| 3    | Pid geaccordeerd. Gestart met literatuurstudie, bronnen bestudeerd en eerste versies onderzoeksrapport gemaakt.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 1              | Z             | 4         | 31:30:00    |
| 4    | Deze week met name vanuit thuis de theoretische verdieping afgemaakt. Tevens afspraken vooruitgepland voor de volgende fase. Alles loopt nog mooi volgens planning                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | -              | -             | 5         | 39:00:00    |
| 5    | 2 dagen verlof gehad ivm carnaval. Met 3 mensen gesproken t.b.v. mijn onderzoek. Laptop ontvangen, geconfigureerd en intern netwerk verkend. Qua planning loopt alles nog ok. Ik verwacht meer tijd kwijt te zijn met onderzoek dan gepland, maar ik ben er achter gekomen dat er meer geïmplementeerd is dan ik dacht waardoor dit naar alle waarschijnlijkheid elkaar compenseert.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2              | V             | 3         | 23:30:00    |
| 6    | <b>Werkzaamheden:</b> Beetje vastgelopen deze week. Afspraken gepland, input die ik gekregen heb bestudeerd en daarop weer nieuwe afspraken gepland voor verdere toelichting, enkele meetings bijgewoond met EY, bedrijfsbezoek gehad. <b>Planning:</b> Ik loop hier iets uit op de planning aangezien ik niet de input heb (middels gesprekken/interviews) die ik nodig heb om mijn research rapport te schrijven. Ik verwacht echter wel in te lopen bij de implementatie omdat er in de factory al een hele hoop is geïmplementeerd. Tevens heb ik al een gedeelte van mijn scriptie af dus voor alsnog kan dit worden opgevangen. <b>Leermomenten:</b> Vergaderen in de praktijk,                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2              | V             | 3         | 22:05:00    |
| 7    | <b>Werkzaamheden:</b> Input verzameld voor mijn onderzoeksrapport middels interviews, mailings en calls. <b>Planning:</b> Ik heb helaas niet kunnen inlopen op de planning. Sterker nog, ik ben een dag verder uitgelopen. Oorzaak hiervan is de aardige hoeveelheid werk die ik moet doen voor mijn onderzoeksrapport (had 3 dagen hiervoor staan, dat haal ik net niet) en ik moest veel meer interviews houden/input verzamelen dan ik verwachtte. <b>Leermomenten:</b> Het gebruik van timeboxen en kernkwadranten. Verder een gesprek gehad met een consultant waarbij ik aan mijn toekomst heb gedacht. In principe ben ik nu uit dat ik wil gaan starten binnen het afgebakend gebied van BPM/BPI/BPR consultancy, en dat ik waarschijnlijk iets met LEAN wil gaan doen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | -              | -             | 6         | 43:45:00    |
| 8    | <b>Werkzaamheden:</b> Deze week verder gegaan met het vergaren van informatie voor mijn onderzoeksrapport, daartoe een aantal interviews/gesprekken gehad. Ik wacht echter nog op een hoop info die ik niet aangeleverd krijg doordat mensen geen tijd hebben om op korte termijn te spreken of mail te beantwoorden. Hier gaat snel 2-3 weken overheen. Heb daartoe mijn onderzoeksrapport en adviesrapport afgemaakt met een hoop aannames erin zodat ik deze wel kan aftikken op de planning. De informatie die ik later krijg zal ik later nog verwerken. <b>Planning:</b> Al met al aardig op planning, heb mijn rapporten af, al staan daar nog veel aannames in en zijn ze nog niet geschikt om als final te publiceren. Ik maak me meer zorgen om de rest van de planning. In mijn planning zou ik halverwege deze week al klaar zijn met mijn onderzoeksfase en doorgaan met de ontwerp en implementatiefase. Er is echter gebleken dat er nog een stuk meer geverifieerd en onderzocht moet worden. Dit is allemaal met mensen met drukke agenda's dus ik verwacht dat dit nog minimaal 2 weken gaat duren. Ook om het e.a. af te stemmen. Zonder deze basis kan ik als het ware ook niet verder naar de volgende fases. Het is dan simpelweg niet duidelijk wat ik moet doen. Enigste voordeel is dat er al een hoop geïmplementeerd is van de werkzaamheden die ik in eerste instantie | -              | -             | 5         | 40:25:00    |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |   |   |   |          |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|----------|
|    | <p>verwachte te doen. Daar verwacht ik dus een beetje tijd terug te winnen, maar ik vrees dat ik al met al ga uitlopen. Ik weet ook niet hoe het zit met de ondersteuning die ik eventueel kan krijgen. Ik verwacht dat dat uiteindelijk wel gaat lukken, zekr ook omdat de standaard dit vanaf half juni verplicht stelt. Dan moet het dus eigenlijk geïmplementeerd zijn en af. Ik zit daarvoor geregeld met de betrokkenen om tafel. Het is dus ontzettend moeilijk om te plannen hoe de werkzaamheden er uit gaan zien op langere termijn. Daarom kijken we nu van week tot week wat we kunnen doen en hoever we kunnen komen. Daarbij zal ik uiteraard wel mijn competenties in het oog houden.</p> <p><b>Leermomenten:</b> De noodzaak van buffers in een planning, ik had deze in eerste instantie wel erin, maar deze heb ik eruit moeten halen omdat ik anders de opdracht niet binnen de gestelde tijd kon plannen. Hierbij zijn indertijd wel duidelijke afspraken gemaakt dat we van week tot week kijken hoe we zorgen dat ik wel de werkzaamheden kan doen voor mijn competenties, maar dat ik voor andere dingen bijvoorbeeld ondersteund ga worden. Verder was het een leermoment dat je af en toe gewoon echt niets kunt doen omdat je geen input hebt, en dat je het de dag erna echt superdruk hebt omdat je opeens een overload aan info krijgt waardoor je opeens heel veel aangrijppunten hebt om dingen te doen/onderzoeken.</p> |   |   |   |          |
| 9  | <p><b>Werkzaamheden:</b> Deze week wederom een hoop interviews en gesprekken gehad t.b.v. van mijn onderzoek. Tevens is uit een brainstormsessie gebleken dat mijn huidige opdracht waarschijnlijk aangepast moet worden. Hiertoe is een RFC ingediend. Verder een round table bijgewoond van de ISACA, met als onderwerp de ISAE 3402. <b>Planning:</b> Ik loop steeds verder uit op planning omdat het onderzoek veel omvatter is als ik van tevoren had voorzien, en omdat managers vaak niet of moeilijk te pakken te krijgen zijn. Mijn stagebegeleider heeft, toen hij mij de opdracht gaf, ook niet voorzien dat er op een lager niveau nog niet alles geïmplementeerd is. Doordat dit er niet is kan ik geen informatie consolideren op een hoge niveau. Uit een brainstormsessie is dan ook gebleken dat mijn implementatie activiteiten zich misschien op een lager niveau moeten gaan afspelen. Daartoe is een RFC ingediend.</p> <p><b>Leermomenten:</b> Ik krijg opeens informatie die ik naar mijn mening al eerder had kunnen krijgen, wat het voor mij makkelijker zou hebben gemaakt. Echter kom ik er nu achter dat mensen niet altijd even bereid zijn om mee te werken. Nu ik als het ware werk voor hun doe, merk ik dat ik opeens een stuk meer info krijg wat mij enorm helpt.</p>                                                                                                                                               |   |   | 5 | 41:15:00 |
| 10 | <p><b>Werkzaamheden:</b> Nieuwe route ingeslagen met een geaccepteerd RFC. Daarvoor gelijk gestart met het scedulen van meetings om de inventarisatie t.b.v. de implementatie rond te krijgen. Verder mijn onderzoeksrapport vanuit de vorige fase afgerond. Dit is echter een document wat niet af lijkt omdat er constant dingen schuiven en verbeterd worden waardoor ik aan het aanpassen kan blijven. Daarom heb ik ook besloten om er nu een punt achter te zetten. Op deze datum is/was het zo geregeld. Mijn focus zal nu liggen op het coördineren van de implementatie. Daarvoor ben ik momenteel druk bezig met een inventarisatie. <b>Planning:</b> De planning is aangepast. Momenteel lig ik op planning volgens de nieuwe planning. <b>Leermomenten:</b> Hoe ik het beste het mgt kan benaderen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 1 | T | 5 | 43:00:00 |
| 11 | <p><b>Werkzaamheden:</b> Deze week heb ik een hoop gesprekken gehad met CDC managers. Na een MT presentatie afgelopen maandag waar het hoge mgt ook management commitment uitsprak is het e.a. in een stroomversnelling gekomen waardoor ik opeens een hoop stappen heb kunnen zetten. Voor 7 van de 12 CDC's heb ik momenteel de rapportagestructuur duidelijk, en deels is deze al geïmplementeerd in de tooling. Ik heb alles gedocumenteerd in een requirements document. Dit is nu nog een kwestie van de juiste vinkjes zetten en namen opvoeren. <b>Planning:</b> Ik loop iets voor op de laatste planning. Naar verwachting zal a.s. week alles worden geïmplementeerd, anders wordt de eerste week van mei gebruikt om alles te finetunen en af te ronden. Vervolgens zal ik me op mijn scriptie gaan storten en op een best practice report. <b>Leermomenten:</b> Hoe cruciaal het is om tijdens de voorbereiding van gesprekken te anticiperen op vragen vanuit het oogpunt van de geïnterviewde.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                        |   |   | 5 | 40:20:00 |
| 12 | <p><b>Werkzaamheden:</b> Deze week wederom een hoop gesprekken gehad met CDC managers en Operation managers. De implementatie loopt vlot vanwege een hoge bereikbaarheid van medewerking. Waarschijnlijk door het commitment van het MT tijdens de presentatie die wij eerder hebben gegeven. Voor alle CDC's is de rapportagestructuur inmiddels duidelijk en voor 9 van de 12 is deze reeds geïmplementeerd. <b>Planning:</b> Ik loop nog steeds voor op de planning. Komende week zal ik als projectleider zijnde aanspreekpunt zijn als er problemen zijn met de tooling of het invullen. Daarnaast zal ik beginnen aan mijn scriptie en mijn best practice rapport. <b>Leermomenten:</b> Gesprekken op mgt niveau gaan eigenlijk steeds beter. Verder, in een vragenlijst die ik nu gebruikt wordt er veel and gebruikt. Ik heb geleerd om dit niet te doen omdat je dan bijvoorbeeld 50% moet invullen als de vraag/statement voor and wel goed is, en die erna niet goed of niet helemaal goed. Dan kan je ze beter opsplitsen.</p>                                                                                                                                                                                                                                                                                                                                                                                                              | 1 | A | 4 | 31:30:00 |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |    |     |    |           |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|-----|----|-----------|
| 13 | <b>Werkzaamheden:</b> Aanspreekpunt voor problemen nu dat de implementatie is voltooid. Daarvoor heb ik verschillende keren dingen moeten aanpassen. Verder een aantal tests uitgevoerd om de integriteit en de compleetheid in de tooling te testen met de requirements. Daarna verder gegaan met brainstormen voor de scriptie, gesprekken gehad t.b.v. een eventuele baan voor na mijn stage, en een gesprek gehad met de externe auditor om mijn advies aan te vullen. <b>Planning:</b> Ik loop nog steeds volgens planning. Komende 3 weken ga ik 80% van mijn tijd in de scriptie steken. Parallel zal ik werken aan het advies en ondersteunende en testwerkzaamheden verrichten. |    |     | 5  | 39:15:00  |
| 14 | <b>Werkzaamheden:</b> Scriptie - nagedacht over opbouw en inhoud, eerste onderdelen geschreven. Service review bijgewoond (half dagdeel). Oriënterende gesprekken gehad voor advies m.b.t. traject na het afstuderen. <b>Planning:</b> Alles loopt nog volgens planning. Niet echt kunnen opschieten deze week met scriptie waardoor ik een uitdaging heb in de komende weken om mijn tijd efficiënt te benutten. Hiervoor een tijdsschema gemaakt (timeboxen).                                                                                                                                                                                                                          | 1  | V   | 5  | 32:20:00  |
| 15 | <b>Werkzaamheden:</b> Scriptie - Verder gewerkt aan concept versie. Verder een aantal gesprekken gehad voor mijn aanvullend advies en voor de implementatie op global niveau. CV e.d. in orde gemaakt en contacten gelegd voor sollicitaties. <b>Planning:</b> Alles verloopt nog volgens planning.                                                                                                                                                                                                                                                                                                                                                                                      |    |     | 7  | 54:30:00  |
| 16 | <b>Werkzaamheden:</b> Scriptie afgemaakt en presentatie en linkedin gemaakt. <b>Planning:</b> Alles loopt volgens planning.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |    |     | 7  | 48:15:00  |
| 17 | <b>Werkzaamheden:</b> Presentatie afgemaakt en voorbereid. Eerste feedback verwerkt voor scriptie. Presentatie gehouden. <b>Planning:</b> Alles loopt nog volgens planning al wordt het door een weekendje praag wel krap om binnen een goede dag alle feedback te verwerken.                                                                                                                                                                                                                                                                                                                                                                                                            | 2  | A/V | 3  | 24:30:00  |
| 18 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |    |     |    |           |
| 19 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |    |     |    |           |
|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 12 |     | 80 | 618:55:00 |

\*

T = Terugkomdag

A = Verplichte ATV dag

V = Verlofdag

Z = Ziekte dag

# Onderzoeksrapport

---

Theoretische verdieping SAS-70 naar ISAE 3402



**Auteur** : R. Brunenberg  
**Versie** : 1.0  
**Status** : Definitief  
**Datum** : 25-05-2011  
**Pagina's** : 4

**Eigenaar** : R. Brunenberg

**Paraaf:**

## Document Historie

| Revisies |            |          |                                                                                                     |                 |
|----------|------------|----------|-----------------------------------------------------------------------------------------------------|-----------------|
| Versie   | Status     | Datum    | Wijzigingen                                                                                         | Eindredacteur   |
| 0.1      | Initieel   | 22-02-11 | Eerste opzet template, inleiding gemaakt                                                            | Ruud Brunenberg |
| 0.2      | Concept    | 23-02-11 | Inleiding afgerond, achtergrond gemaakt                                                             | Ruud Brunenberg |
| 0.3      | Concept    | 28-02-11 | Achtergrond aangepast, Vraagstelling en methode gemaakt                                             | Ruud Brunenberg |
| 0.4      | Concept    | 01-03-11 | Eerste opzet resultaten, ruwe informatie verwerkt                                                   | Ruud Brunenberg |
| 0.5      | Concept    | 02-03-11 | Verfijnen resultaten sectie                                                                         | Ruud Brunenberg |
| 0.6      | Concept    | 03-03-11 | Conclusie, discussie, aanbevelingen toegevoegd<br>Besloten om discussie, aanbevelingen weg te laten | Ruud Brunenberg |
| 0.7      | Concept    | 04-03-11 | Deelvraag 3 antwoord toegevoegd bij resultaten                                                      | Ruud Brunenberg |
| 1.0      | Definitief | 25-05-11 | Status 1.0 – PDF                                                                                    | Ruud Brunenberg |
|          |            |          |                                                                                                     |                 |

| Distributie |                  |      |         |
|-------------|------------------|------|---------|
| Versie      | Datum verzending | Naam | Functie |
|             |                  |      |         |
|             |                  |      |         |
|             |                  |      |         |

| Goedkeuringen |                   |      |         |        |
|---------------|-------------------|------|---------|--------|
| Versie        | Datum goedkeuring | Naam | Functie | Paraaf |
|               |                   |      |         |        |
|               |                   |      |         |        |
|               |                   |      |         |        |

## Inhoudsopgave

|    |                              |    |
|----|------------------------------|----|
| 1. | Inleiding .....              | 4  |
| 2. | Achtergrond .....            | 5  |
| 3. | Vraagstelling & Methode..... | 8  |
| 4. | Resultaten.....              | 9  |
| 5. | Conclusie .....              | 13 |

## 1. Inleiding

Ten behoeve van mijn afstudeerstage bij Atos Origin is enige theoretische achtergrondkennis gewenst. Dit is tevens vanuit school een verplicht onderdeel voor het afstuderen. De aanleiding voor dit onderzoek is dus tweeledig; Enerzijds omdat achtergrondkennis voor het afstuderen gewenst, dan wel benodigd is, anderzijds omdat het verplicht is om af te kunnen studeren.

Voor mijn afstudeerstage is het de bedoeling dat ik een management rapportage ontwikkel. Atos Origin is momenteel bezig met een transitieproces van de SAS-70 standaard naar de ISAE 3402 standaard. Verdere toelichting hierover staat in het volgende hoofdstuk. Om in de assurance rapportages de zogenaamde sectie 2 te kunnen ondertekenen (de management assertion letter, met andere woorden: Het management tekent ervoor dat de services 'in control' zijn) dient er een management rapportage te komen waardoor het management met een gerust hart haar handtekening kan zetten onder sectie 2 van het assurance rapport. De gegevens in deze management rapportages moeten controleerbaar en verifieerbaar zijn. Daartoe dient er voor de organisatie een proces ontworpen te worden waarbij de operatie rapporteert aan het management. Deze rapportages kunnen eventueel weer worden gebruikt in management rapportages op hogere niveaus. Hiervoor kunnen onder andere zogenaamde monitoring controls (controle maatregelen die iets zeggen over een proces) gebruikt worden. Verder zal er uitgezocht moeten worden welke gegevens nog meer gewenst zijn. Zodra dat boven water is zal er een proces ontwikkeld, geïmplementeerd en getest moeten worden waarmee de gewenste data uit de organisatie kan worden verkregen. Er zal moeten worden onderzocht of deze data in bestaande management rapportages kan worden opgenomen, of dat er aparte rapportages ontwikkeld moeten worden.

Qua theoretische verdieping zou het dus handig zijn om achtergrondkennis te hebben over met name de ISAE 3402 standaard, maar ook wat achtergrondkennis over de oude SAS-70 standaard is gewenst.

## 2. Achtergrond

### Uitbesteding

Uitbesteding van diensten of productie is een van de instrumenten van ondernemingen en overheden om zich te focussen op de voor hen belangrijkste taak: het realiseren van de doelstellingen van de onderneming. Door het uitbesteden kunnen deze organisaties meer middelen overhouden voor zaken als innovatie, een snellere time-to-market en een meer flexibele organisatie. Het beheersen van deze dienstverlening en het beheer van de afspraken omtrent de dienstverlening, bijvoorbeeld via Service Level Agreements (SLA's), aan zowel de leveranciers- als kantzijde, is een activiteit die ook voor de IT-auditor uitdagingen biedt.

### Beheersing van uitbestede diensten

Het inregelen en beheersen van de uitbesteding kent niet alleen operationele uitdagingen, maar brengt ook voor de beheersing van de verschillende processen aandachtspunten met zich mee. Uitbesteding van processen is namelijk geen uitbesteding van alle verantwoordelijkheid, ook al zijn alle afspraken en monitoring daarvan nog zo goed vastgelegd in SLA's. Vanuit de principes van goed ondernemingsbestuur blijft de organisatie die de processen uitbesteedt eindverantwoordelijk voor de beheersing van deze processen. Vooral bij processen die een groot (materieel) financieel belang kennen, zal de uitbestedende organisatie (de gebruikersorganisatie) een of andere vorm van toezicht op de partij aan wie wordt uitbesteed (de serviceorganisatie) moeten uitoefenen. Het uitoefenen van toezicht is niet alleen een wens van de uitbestedende partij, maar vaak ook vereist vanuit de wetgeving, zoals in het geval van de Amerikaanse Sarbanes-Oxley wetgeving, die aangeeft dat het management van een organisatie aantoonbaar in control moet zijn van zijn onderneming. Het in control zijn geldt dus niet alleen voor de processen die binnen de eigen onderneming worden uitgevoerd, maar ook voor de processen die extern worden uitgevoerd en direct of indirect verband houden met de interne beheersing van de onderneming. De uitbestedende organisatie zal van de serviceorganisatie zekerheid moeten verkrijgen over de mate van beheersing over de processen die daar uitgevoerd worden.

### Rapportage omtrent beheersing

Voor de gebruikersorganisaties die behoefte hebben aan een onafhankelijk en onpartijdig onderzoek en oordeel, is een interne verantwoordingsrapportage (bijvoorbeeld in de vorm van een SLA-rapportage) vaak onvoldoende. De gewenste onafhankelijkheid en onpartijdigheid ontbreekt als de verantwoordingsrapportage wordt opgesteld door de partij die ook de dienstverlening levert. Onafhankelijk onderzoek is voor gebruikersorganisaties dan ook noodzakelijk. Aangezien serviceorganisaties vaak werken voor meerdere opdrachtgevers, die elk hun eigen behoeften en eisen stellen aan beheersing, zal een serviceorganisatie van meerdere opdrachtgevers de vraag krijgen aan te tonen dat zij 'in control' is. Wanneer een rapportage over de interne beheersing volgens een algemeen geaccepteerde standaard wordt opgesteld en beoordeeld, is deze rapportage voor diverse gebruikers zinvol. Een SAS-70-verklaring is een rapportagevorm die in de praktijk veel wordt gebruikt om over de effectiviteit van de beheersingsmaatregelen bij de serviceorganisatie te rapporteren. Iedere methode heeft zijn voor- en nadelen, maar in de praktijk is de SAS-70-verklaring een alom geaccepteerde standaard. Serviceorganisaties die momenteel gebruik maken van SAS-70 – verklaringen krijgen vanaf 15 juni 2011 te maken met de overgang naar een nieuwe standaard voor rapportage over interne beheersing ten behoeve van derden. Deze nieuwe standaard (ISAE 3402) zal in de praktijk de huidige SAS-70 standaard vervangen waardoor ISAE 3402 een internationale basis krijgt, gedragen door het IFAC (International Federation of Accountants en de ASB (Auditing Standards Boards, US). Hieronder staan deze 2 standaarden kort beschreven.

#### 1. SAS-70

In het begin van de jaren negentig van de vorige eeuw bracht de American Institute of Certified Public Accountants (AICPA) het Statement on Auditing Standards No. 70, Service Organizations (SAS-70) uit. De standaard was bedoeld om auditors van gebruikersorganisaties te ondersteunen bij de beoordeling van interne beheersingsmaatregelen. Hoewel ook andere, vergelijkbare standaarden of andere vormen van third party reporting kunnen worden gebruikt, is de SAS-70-standaard uitgegroeid tot een *de facto* standaard voor het rapporteren over beheersingsmaatregelen bij serviceorganisaties. Ook in Nederland is de SAS-70-standaard een veelgebruikte wijze om (auditors van) externe partijen (met name gebruikersorganisaties) zekerheid te verschaffen over de mate van interne beheersing. Het gebruik van een standaard als SAS-70 brengt een aantal voordelen met zich mee voor zowel de gebruikersorganisatie als de serviceorganisatie. De belangrijkste voordelen voor de gebruikersorganisatie zijn:

- het geeft de gebruikersorganisatie inzicht in en zekerheid over de wijze waarop de serviceorganisatie haar procesbeheersing heeft georganiseerd, waardoor de gebruikersorganisatie beter in staat is haar eindverantwoordelijkheid over de uitbestede processen te dragen; en
- de gebruikersorganisatie voldoet (indien van toepassing) aan de eisen die de diverse wet- en regelgeving haar stelt.

Omdat de scope van een SAS-70-rapport wordt bepaald door de serviceorganisatie, moet de auditor van de gebruikersorganisatie altijd vaststellen of het rapport toereikend is om te voldoen aan de assurance-eisen die de gebruikersorganisatie heeft. Het vaststellen van de scope van de audit is dan ook een essentieel onderdeel.

Een SAS-70-verklaring bevat uitsluitend interne controledoelstellingen en beheersingsmaatregelen die relevant zijn voor de betrouwbaarheid van financiële informatie. Het opnemen van interne controledoelstellingen en beheersingsmaatregelen op het gebied van continuïteit (voor zover dit toekomstgerichte doelstellingen betreft) en/of compliance (het voldoen aan wet- en regelgeving) is in principe niet toegestaan. Vaak wordt dit probleem ondervangen door in Sectie IV van een SAS-70-rapport de serviceorganisatie de maatregelen te laten beschrijven die op continuïteitsgebied genomen zijn. De auditor van de serviceorganisatie mag deze maatregelen echter niet toetsen.

Een SAS-70-rapport bestaat uit een aantal vaste onderdelen, afhankelijk van het type rapport dat wordt afgegeven. Het rapport zelf is opgebouwd uit het assurance rapport van de auditor, een algemene beschrijving van de organisatie en haar dienstverlening aangevuld met de wijze waarop zij de interne beheersing invult en een deel met doelstellingen van de interne beheersing met daaronder de gedetailleerde beschrijvingen van de beheersingsmaatregelen. Er zijn twee typen rapportages mogelijk:

- Type I-rapport: de auditor van de serviceorganisatie beperkt zich tot de opzet en het bestaan van de beheersingsmaatregelen;
- Type II-rapport: de auditor van de serviceorganisatie toetst ook de werking van de maatregelen en beschrijft de wijze van toetsing en uiteraard de resultaten van de toetsing.

## 2. ISAE 3402

De IAASB heeft in 2006 een onderzoek gedaan waarbij een nieuwe wereldwijde standaard voor onderzoeksrapporten van serviceorganisaties ontwikkeld moest worden. Deze standaard wordt aangeduid als de: *International Standard on Assurance Engagements (ISAE 3402) – Assurance Reports on controls at a Third Party Service Organization*.

De achterliggende doelstelling van de nieuwe standaard, die een volwaardig alternatief voor de SAS-70-standaard zal worden, is dat de onderzoeksrapporten bruikbaar zullen zijn voor een grotere groep belangstellenden en belanghebbenden. Bij de SAS-70-rapporten was de doelgroep beperkt tot het management en de auditor van de gebruikersorganisatie. Door het opnemen van meer typen interne beheersingsmaatregelen dan alleen de interne beheersingsmaatregelen gericht op financiële verslaglegging, zal een op ISAE 3402 gebaseerd rapport ook interessant zijn voor die serviceorganisaties waarvoor een SAS-70 tot op heden minder relevant was. Dit vanwege de nadruk op interne beheersingsmaatregelen gericht op financiële verslaglegging bij een SAS-70. Daarnaast is de ISAE 3402-standaard een internationale standaard die goed toepasbaar is binnen de al bestaande lokale controlestandaarden, zoals in Nederland de COS3000. Net zoals de SAS-70-standaard is de ISAE 3402-standaard assertion based waarbij gebruikgemaakt wordt van controledoelstellingen ten aanzien van het object van onderzoek. Het uitgangspunt bij het opzetten

van ISAE 3402 is het behouden van de sterke punten van SAS-70. Dit betekent dat een rapport conform de ISAE 3402-standaard niet sterk zal afwijken van bestaande SAS-70-rapporten, omdat de meeste principes uit SAS-70 zijn overgenomen in het concept van ISAE 3402. Gezien de beperkingen van de SAS-70-standaard zijn er in de ISAE 3402 een aantal aanvullingen op de SAS-70-standaard geformuleerd. De belangrijkste doelstellingen van de aanvullingen zijn ten eerste het doen toenemen van de bruikbaarheid van een rapport over de interne beheersingsmaatregelen van een serviceorganisatie en ten tweede het toevoegen van beheersingsmaatregelen die gerelateerd zijn aan de effectiviteit en efficiency van activiteiten/beheersingsmaatregelen – en door het toevoegen van beheersingsmaatregelen gerelateerd aan compliance met wet- en regelgeving. Door deze toevoegingen wordt de reikwijdte van het rapport vergroot.

De ISAE 3402-standaard kent twee typen rapporten die vergelijkbaar zijn met respectievelijk een SAS-70 Type I-rapport en een SAS-70 Type II rapport:

- Type A-rapport;
- Type B-rapport.

In een Type A-rapport wordt alleen een oordeel gegeven over de opzet en het bestaan, terwijl in een Type B rapport ook over de effectieve werking van de interne beheersingsmaatregelen gedurende een bepaalde periode een oordeel wordt gegeven.

### 3. Vraagstelling & Methode

**Onderzoeksvraag:** Wat houden de SAS-70 en ISAE 3402 standaard in?

**Deelvragen:**

1. Wat zijn de beperkingen in de huidige SAS-70 standaard?
2. Wat zijn de verschillen en overeenkomsten tussen ISAE 3402 en SAS-70 (Reikwijdte)?
3. Wat is de relatie tussen het COSO model en de standaarden?
4. Wat is de rol van risico's binnen de ISAE 3402 standaard?
5. Wat is de rol van de Management Assertion Letter?
6. Wat zijn monitoring controls en wat kun je ermee?
7. Welke gevolgen heeft de overgang naar de ISAE 3402 standaard voor serviceorganisaties?

**Onderzoeksdoelstelling:**

- Duidelijk krijgen wat de SAS-70 - en de ISAE 3402 standaard inhouden, en wat het transitieproces van SAS-70 naar ISAE 3402 met zich meebrengt.

#### **Methode**

De deelvragen heb ik beantwoord met behulp van een literatuurstudie. Ik heb navraag gedaan bij Atos Origin en Ernst & Young voor voorhanden literatuur. Hiervoor heb ik gesproken met Hans Kappert en Dennis Houtekamer. Hierbij is het mij duidelijk geworden dat er geen hardcopy boeken zijn over ISAE 3402, mede omdat dit een nieuwe standaard is. Daartoe heb ik via internet veel artikelen bij elkaar proberen te zoeken die geschreven waren door vakmensen, zowel in eigen persoon, als in opdracht van hun werkgever. Verder heb ik het handboek voor ISAE 3402, online gepubliceerd door de IFAC, geraadpleegd. Met de informatie uit de gevonden literatuur heb ik getracht de deelvragen te beantwoorden.

## 4. Resultaten

### 1. Wat zijn de beperkingen in de huidige SAS-70 standaard?

De beperkingen zijn hieronder puntsgewijs samengevat:

- De standaard gaat niet uit van een risicobenadering
- Reikwijdte is beperkt tot de betrouwbaarheid van financiële rapportages en shared service centers kunnen er geen gebruik van maken
- Een beperkte scope van de verklaring. Een SAS-70 verklaring bevat uitsluitend interne controledoelstellingen en beheersingsmaatregelen die relevant zijn voor de betrouwbaarheid van financiële informatie. Er zijn geen doelstellingen en maatregelen op het gebied van continuïteit en/of compliance. Dit is voor een gebruikersorganisatie vaak een essentieel aandachtspunt.
- In principe mogen alleen door de AICPA gecertificeerde accountants (met een CPA titel) een SAS-70 verklaring afgeven.
- De doelgroep is beperkt tot het management en de auditor van de gebruikersorganisatie
- Ontbreken van materialiteit (of risico-inschatting) ten aanzien van de informatie waarover wordt gerapporteerd.
- Bij een Type II rapport worden alleen de control activiteiten op hun werking getoetst. De andere COSO elementen zoals monitoring, information & communication etc niet.

### 2. Wat zijn de verschillen en overeenkomsten tussen ISAE 3402 en SAS-70 (Reikwijdte)?

Hieronder staat een duidelijk overzicht van de belangrijkste overeenkomsten en verschillen tussen de standaarden:

#### Verschillen:

- ISAE 3402 staat het niet toe om een beperkte mate van zekerheid te geven. SAS-70 doet dit wel.
- De basis onder het rapport is in het geval van ISAE 3402 een risicoanalyse waarbij een selectie gemaakt mag worden van de relevante processen en beheersmaatregelen waarover men wenst te rapporteren. Bij SAS-70 was dit niet verplicht.
- Het begrip materialiteit wordt bij ISAE 3402 expliciet gehanteerd. Hierbij gaat het om de materialiteit ten aanzien van de informatie waarover wordt gerapporteerd. Het moet duidelijk zijn voor de auditor van de serviceorganisatie dat het assurancerapport informatie bevat die voor gebruikersorganisaties van (groot) belang is voor de betrouwbaarheid van financiële informatie van de gebruikersorganisaties.
- Het ISAE 3402-rapport zal een verklaring van het management bevatten over het bestaan en effectief werken van de beheersingsmaatregelen. De verklaring wordt na het oordeel van de service auditor geplaatst. Momenteel bevatten SAS-70-rapporten alleen het oordeel van de service auditor en niet de verklaring van het management.
- SAS-70 is een auditing standaard, ISAE 3402 is een assurance standaard
- Bij ISAE 3402 geeft de auditor één oordeel over de beoordeling van drie aspecten uit de criteria<sup>12</sup>. Voor een Type II rapport zal het oordeel betrekking hebben op alle drie aspecten over de gehele periode. De IAASB is van mening dat het samenvoegen van de twee begrippen bestaan en werking uiteindelijk meer bijdraagt aan het beoordelen van de interne beheersingsmaatregelen van de serviceorganisatie.
- Voor een ISAE type 2 rapport dienen naast de control activiteiten ook andere COSO elementen getoetst te worden voor zover relevant.
- ISAE 3402 verplicht de service auditor om een beoordeling uit te voeren op de toereikendheid van de criteria die worden gebruikt door de serviceorganisatie voor het ontwikkelen van de omschrijving

<sup>12</sup> Suitable Criteria: Fairness of presentation, Suitability of Design, en Operating Effectiveness

van het controleraamwerk, de beheersingsdoelstellingen en de gerelateerde beheersingsmaatregelen. De IAASB heeft voor een ISAE 3402-rapport in tegenstelling tot een SAS-70-rapport een minimale set van criteria gespecificeerd, waaraan het controleraamwerk moet voldoen.

- De verspreiding van een SAS-70-rapport is momenteel beperkt tot het management van de serviceorganisatie, de gebruikersorganisaties en de accountants van de gebruikersorganisaties. Voor een ISAE 3402 rapport zijn verdere beperkingen aangebracht, zodat de gebruikers van het rapport alleen de bestaande klanten van de serviceorganisatie zijn. Daarnaast moet de accountant van de gebruikersorganisatie voldoende kennis hebben van de wijze waarop de inhoud van het rapport wordt gerelateerd aan de beheersingsmaatregelen van de gebruikersorganisatie. Ten slotte wordt in ISAE 3402 in de auditorparagraaf een directe verwijzing gemaakt over het beoogde gebruik.
- Bij gebruik van de inclusive-methode<sup>13</sup> diende er bij SAS-70 alleen de significante processen van de sub-serviceorganisatie opgenomen te worden in het rapport. Bij ISAE 3402 wordt er niet over significatie gesproken en dienen dus alle processen opgenomen te worden.

#### **Overeenkomsten:**

- Beide standaarden kennen twee typen rapporten, een type 1 of I rapport over de opzet en het bestaan (TOD) en een type 2 of II rapport over de opzet, het bestaan en de werking over een bepaalde periode (TOE).
- Beide standaarden maken het mogelijk gebruik te maken van een interne audit dienst bij het uitvoeren van de diverse procedures. Net als bij SAS-70, is het volgens ISAE 3402 niet toegestaan dat de auditor in het oordeel verwijst naar procedures die zijn uitgevoerd door interne auditors. Het is wel toegestaan om op werkzaamheden van interne auditors te steunen. In het rapport moet er expliciet zichtbaar gemaakt worden welke werkzaamheden zijn uitgevoerde door de interne audit afdeling.
- In de nieuwe standaard is, evenals onder SAS-70, niet omschreven in welke mate gebruik mag worden gemaakt van de werkzaamheden van een afdeling Interne Audit
- Noch SAS-70, noch ISAE 3402 verplichten de service auditor de steekproefomvang toe te voegen, tenzij een relevante afwijking is vastgesteld.
- De opmaak en presentatie van een ISAE 3402-rapport is vergelijkbaar met een SAS-70-rapport.
- Beide standaarden verplichten het management tot het afgeven van een zogenoemde letter of representation aan de service auditor. Deze brief wordt niet ter beschikking gesteld aan de gebruikersorganisaties of de auditors daarvan.
- Beide standaarden verplichten de service auditor om zijn kennis over de beheersingsmaatregelen te actualiseren tot aan de datum van het uitbrengen van het rapport. Dit om vast te stellen of er gebeurtenissen zijn opgetreden die mogelijk het oordeel beïnvloeden of die om andere redenen zouden moeten worden gecommuniceerd met de gebruikers van het rapport.

#### **Reikwijdte**

Ofschoon ISAE 3402 primair is bedoeld om verantwoording af te leggen over de interne beheersing die gericht is op de betrouwbaarheid van financiële rapportages, is de expliciete uitsluiting van andere controlemaatregelen niet langer van toepassing. Hierdoor is het mogelijk de reikwijdte van het rapport uit te breiden naar de twee andere COSO doelstellingen van interne beheersing, naleving van wet- en regelgeving en efficiëntie en effectiviteit van de bedrijfsvoering. Verder is de beperking die onder SAS-70 geldt voor controledoelstellingen gericht op de continuïteit van de bedrijfsvoering, niet langer van toepassing.

<sup>13</sup> Processen of diensten die de serviceorganisatie weer verder heeft uitbesteed worden wel meegenomen in de audit.

### 3. Wat is de relatie tussen het COSO model en de standaarden?

Het COSO model is een model om interne beheersing te regelen binnen een organisatie. In de praktijk worden de lagen uit het COSO model veel gebruikt als basis voor een normenkader. In het geval van de SAS-70 standaard was het uitsluitend toegestaan om de control activiteiten te toetsen op hun werking. Binnen de ISAA 3402 standaard is er meer ruimte en kunnen ook andere COSO elementen zoals monitoring en information & communication etcetera worden getoetst. Het gebruik van het COSO model is overigens niet verplicht voor de standaarden.

### 4. Wat is de rol van risico's binnen de ISAE 3402 standaard?

Nieuw in ISAE 3402 ten opzichte van SAS-70 is dat beheersdoelstellingen moeten voortkomen uit een set van beheersmaatregelen die tot doel hebben een risico te vermijden. De serviceorganisatie is verantwoordelijk voor het tijdig onderkennen van risico's en het nemen van de juiste en passende acties op de risico's. Hierbij kan de serviceorganisatie gebruikmaken van een formeel of informeel proces om relevante risico's te identificeren. Een formeel proces houdt mogelijk in dat de risico's worden ingeschat op basis van significantie, kans op voorkomen en het implementeren van maatregelen die de risico's afdekken. Voorts is specifiek opgemerkt in de ISAE standaard, dat een degelijk proces om beheersdoelstellingen te formuleren op zichzelf reeds een informeel proces betekent om risico's in te schatten. Vanuit de ISAE-standaard wordt een risicoanalyse zelf niet verplicht gesteld. Niettemin kan de IT-auditor de cliënt wel ondersteunen of adviseren indien de IT-auditor van mening is dat het uitvoeren van een (in)formele risicoanalyse belangrijk is. Uiteraard moet daarbij wel de blijvende onafhankelijkheid in acht worden genomen, indien de IT-auditor ook als externe auditor de ISAE 3402-mededeling gaat afgeven.

### 5. Wat is de rol van de Management Assertion Letter?

Onder ISAE 3402 geeft de externe accountant van de serviceorganisatie een assurance rapport af voor de opzet, het bestaan en de werking (laatste is optioneel) van een beheersingsraamwerk. Naast de verklaring van de externe accountant voegt ook het management van de serviceorganisatie een verklaring toe aan het rapport, een zogenoemde assertion. In deze verklaring doet het management, overeenkomstig een Sox 404-rapport, een bewering over de opzet, het bestaan en de werking van het beschreven beheersingsraamwerk. Hiermee neemt het management van de serviceorganisatie expliciet de verantwoordelijkheid voor de beheersing van de aan haar uitbestede processen en de inhoud van het rapport. Net zoals de getrouwheid van de jaarrekening primair de verantwoordelijkheid is van het management, geldt dit ook voor de getrouwheid van een verantwoording over de interne beheersing. Een assurance rapport is bedoeld om hier additionele zekerheid over te verstrekken, niet om een deel van de verantwoordelijkheid af te schuiven.

In deze management assertion letter worden onder meer de volgende zaken opgenomen:

- Voor wie het rapport bedoeld is (reikwijdte).
- De beschrijvingen in het rapport zijn *fair* en gelden voor de transacties in de periode van onderzoek (bij een type 2), waarbij specifiek is opgenomen welke services, transacties onderdeel zijn van het rapport. Voorts worden elementen opgenomen zoals de beheersomgeving, het risicobeheerproces, informatie en communicatie alsmede de *control activities*. Kortom, de relevante aspecten van het COSO model.
- Dat de beheersmaatregelen die de bijbehorende beheersdoelstellingen afdekken, adequaat zijn ontworpen en hebben gewerkt in de periode. Hierbij zijn de volgende criteria in ogenschouw genomen:
  - De risico's die een bedreiging vormen voor het behalen van de beheersdoelstellingen.
  - De beschreven beheersmaatregelen, indien die effectief hebben gewerkt, geven redelijke zekerheid dat de onderkende risico's het behalen van de beheersdoelstellingen niet verhinderen.
  - De beheersmaatregelen consequent zijn uitgevoerd door medewerkers met de vereiste vaardigheden en autoriteit.

Een mededeling van het management is overigens ook mogelijk bij een SAS-70-rapport, doch hiervan wordt in weinig gevallen gebruik gemaakt. Bij ISAE 3402 is er tevens een gestandaardiseerde mededeling opgenomen.

## 6. Wat zijn monitoring controls en wat kun je ermee?

Om de management assertion letter te tekenen, dient het management van de serviceorganisatie te beschikken over voldoende maatregelen om de werking van beheersingsmaatregelen effectief te bewaken. Waar het voorheen al aanbevelenswaardig was dergelijke beheersmaatregelen te implementeren, wordt dit nu een verplichting om voldoende onderbouwing te krijgen voor de vereiste managementbewering. Voor een aantal organisaties zal dit betekenen dat ze extra beheersmaatregelen moet beschrijven en wellicht ook implementeren. Deze extra beheersingsmaatregelen zijn de zogenoemde monitoring controls. Deze maatregelen zeggen iets over het verloop van de processen waardoor het management snel inzicht kan krijgen in de effectieve werking ervan.

## 7. Welke gevolgen heeft de overgang naar de ISAE 3402 standaard voor serviceorganisaties?

Indien besloten wordt over te gaan naar de nieuwe standaard zijn de belangrijkste activiteiten voor de serviceorganisatie:

- *Begrijpen van de veranderingen.* Dit betreft met name de noodzaak om een managementverklaring in het rapport op te nemen.
- *Overleg met de service auditor.* Het gaat daarbij met name om de verwachte impact op het rapport van de service auditor, zijn werkzaamheden en de impact op eventuele sub-serviceorganisaties. De nieuwe standaard 3402 stelt dat bij een inclusive rapportage niet alleen de controles van de sub-serviceorganisatie moeten worden beschreven en getest, maar ook de organisatiebrede beheersingsmaatregelen (hoofdstuk II). Daarmee zijn alle voordelen van een inclusive rapportage weg en is het handiger dat een sub-serviceorganisatie haar eigen rapport opstelt. Gericht op de gebruikers van de rapporten is het goed om tijdig de behoefte en consequenties van early adaption te bespreken.
- *Plannen van de transitie.* Dit omvat het opzetten van interne training, coördinatie met de eventuele juridische afdeling, het opstellen van een communicatieplan en het reviewen van de huidige rapporten en processen om vast te stellen hoe aan de nieuwe criteria voldaan gaat worden. In ieder geval dient aandacht te worden besteed aan de vraag of er een voldoende onderbouwing aanwezig is waarop de nieuwe management assertion gebaseerd gaat worden. Het is daarbij niet zoals bij SOx 404 dat het verplicht is dat alle management controls door het management eerst worden getest, voordat de auditor dit doet.

De invoering van ISAE 3402 is verplicht voor perioden van onderzoek, waarin de datum 15 juni 2011 is inbegrepen.

## 5. Conclusie

SAS-70 is een auditstandaard, waar ISAE 3402 een assurance standaard is. Beide standaarden hebben als doel om een rapport af te kunnen geven aan de gebruikersorganisatie waarbij de gebruikersorganisatie een redelijke mate van zekerheid ontvangt dat haar uitbestede processen goed beheerst worden door de serviceorganisatie.

Grote verschil tussen ISAE 3402 en SAS-70, is dat de reikwijdte van ISAE 3402 iets groter is. Tevens dient er in een ISAE 3402 rapport een management assertion letter ondertekend te zijn door het management. In deze verklaring doet het management, overeenkomstig een Sox 404-rapport, een bewering over de opzet, het bestaan en de werking van het beschreven beheersingsraamwerk. Hiermee neemt het management van de serviceorganisatie expliciet de verantwoordelijkheid voor de beheersing van de aan haar uitbestede processen en de inhoud van het rapport.

## Literatuurlijst

- Houtekamer, D., & Graaf, R de (2009). *ISAE 3402: einde van SAS-70 in zicht?* de EDP auditor, nr. 1.
- Russel, M (2010). *New gold standard to change third party assurance*. Internal Auditing & Business Risk magazine
- Ewals, R. (2010). *Een nieuw hoofdstuk voor de IT-Auditor*. De IT-auditor, nr. 3.
- Verweij, S (2009). *SAS-70 maakt plaats voor ISAE 3402*. Spotlight, nr. 3, 52-56.
- Beek, J. van., & Francken, M. (2010). *SAS-70 herzien, focus ISAE 3402 blijft op beheersingsmaatregelen financiële verantwoording*. Compact, nr. 1, 38-42.
- IAASB (2009). *ISAE 3402, Assurance Reports on Controls at a Service Organization*.