P.A. Schellen RE CISA

Peter-Willem Schellen is als Senior Associate werkzaam bij Ernst & Young Technology & Security Risk Services in Oslo, Noorwegen. Hij is gespecialiseerd in de beoordeling van algemene computerbeheersingsmaatregelen van grote SAP-omgevingen in de context van de statutaire jaarrekeningcontrole alsook naleving van overige wet- en regelgeving (met name Noorse en Amerikaanse wet- en regelgeving).

Flytoget

De wekker gaat vandaag al om 06.00 uur omdat ik vandaag van Oslo naar Stavanger zal reizen voor een belangrijke bijeenkomst. Gisteravond heb ik mijn Ernst & Young rugzak (met speciaal compartiment voor mijn notebook) en documenten al klaargezet. Vanuit mijn appartement is het vijf minuten lopen naar het Nationaltheatret station, waar ik de Flytoget naar het vliegveld zal nemen. Noorwegen is een digitale samenleving waar nagenoeg alles digitaal betaald kan worden, zo ook het kaartje van de Flytoget. Om 07.00 uur stap ik op de Flytoget. In de Flytoget neem ik de presentatie van de bevindingen van het EDP-onderzoek, dat de afgelopen drie maanden veel tijd in beslag heeft genomen, nog eens goed door. Gelukkig is de presentatie in het Engels opgesteld, mijn Noors is na vier maanden onderwijs nog niet op het niveau van een managementrapportage. Bij aankomst op het vliegveld bevestig ik mijn aankomst door het gebruik van mijn creditcard bij het poortje. Later op de dag zal ik per e-mail een bevestiging hiervan ontvangen, nog een voorbeeld van een papierloze transactie.

Landschappen

Het vliegveld van Oslo is niet het grootste van Europa en kent meer binnenlandse dan buitenlandse vluchten. Op zichzelf niet verwonderlijk, Noorwegen is ongeveer twaalf maal zo groot als Nederland en kent van zijn Noordelijke grens tot aan de hoofdstad eenzelfde afstand als van de hoofdstad tot Rome. Het is ook een land van buitengewone landschappen: bergen, gletsjers, fjorden, eilanden en bossen. Aangezien mijn klant zijn hoofdzetel in Stavanger heeft (de hoofdstad van de provincie Rogaland) neem ik de vlucht van 08.00 uur van Oslo naar Stavanger met SAS Braathens (de fusiemaatschappij van de nationale luchtvaartmaatschappij Braatens en de Scandinavische luchtvaartalliantie). Net als in de Flytoget bestaat er geen fysiek vliegbiljet voor de vlucht. Ook kent men bij binnenlandse vluchten geen verschillende klassen. Het enige verschil tussen een C en Y klasse is de mogelijkheid het biljet te wijzigen. Net voor het aan boord gaan valt me op dat een belangrijke contactpersoon bij de klant, een manager van de interne accoutantsdienst, dezelfde vlucht neemt. Hoewel deze persoon niet bij de presentatie van later vandaag aanwezig zal zijn, stel ik toch voor om naast hem plaats te nemen en hem enige informatie te verstrekken. Noorwegen kent namelijk een zeer eigen cultuur waarin persoonlijk vertrouwen erg belangrijk is. Tijdens de vlucht heb ik ook de mogelijkheid naar buiten te kijken en de landschappen maken wederom erg veel indruk.

Voorbereiding

De presentatie vandaag bij de klant, een grote oliemaatschappij die recent na privatisering door de overheid in Noorwegen en de Verenigde Staten aan de beurzen is genoteerd. Voor deze organisatie vervult Ernst & Young wereldwijd de rol van statutaire accountant. Het door ons uitgevoerde onderzoek heeft betrekking op de algemene computerbeheersingsmaatregelen in het licht van de Sarbanes-Oxley wet. In de periode september tot en met december 2005 zijn door ons team, bestaande uit een Senior Manager, twee Senior Associates en een Junior Associate, grofweg 240 beheersingsmaatregelen en de daarmee in verband staande documentatie en processen beoordeeld. Aangezien de presentatie voor de klant, met de interne accountantsdienst en voornaamste adviseur Pricewaterhouse-Coopers als vertegenwoordigers van de klant, pas om 12.00 uur zal beginnen, nemen we van 09.00 tot 11.00 uur alles nog eens goed door. De Noorse arbeidscultuur is erg individualistisch: tijdens het project heeft iedereen relatief zelfstandig aan zijn of haar onderdeel gewerkt. Ook kent de Noorse arbeidscultuur geen hiërarchie: Managers en Senior Managers hebben weliswaar een kwaliteitsverzekerende rol maar kennen ook een plicht om ongeveer 75 procent declarabel te zijn. Er zijn geen kritische zaken die onze aandacht opeisen. We besluiten wel om de voorlopige presentatie op een aantal punten te harmoniseren. Om 11.00 uur besluiten we onze voorbereiding en gaan naar de lunch. In Noorwegen zijn de werktijden in de herfst en de winter namelijk van 08.00 tot 16.00 uur en in de lente en de zomer van 08.00 tot 15.00 uur. Dit is met name ingegeven door het bijna arctische klimaat.

Presenteren

Om 11.30 uur rijden we van het Ernst & Young kantoor in Stavanger naar het hoofdkantoor van de klant, net buiten Stavanger op een industrieterrein. In Noorwegen kent men een tolsysteem voor wegen, hier kan men er ook voor kiezen een digitaal afrekensysteem te gebruiken. De maandelijkse afrekening hiervan kan ook als PDF-bestand via de e-mail wordt toegestuurd. Om 11.45 uur zijn we bij de klant gearriveerd, alwaar we naar een vergaderruimte worden gedirigeerd. Aangezien onze beoordeling van de algemene computerbeheersingsmaatregelen in het licht van de Sarbanes-Oxley wet, voor de klant een kritiek onderdeel vormt van een project waarin meerdere miljoenen Noorse kronen zijn geïnvesteerd, is er een groot publiek aanwezig: afvaardigingen van de opdrachtgever, PricewaterhouseCoopers en Ernst & Young. Aan onze zijde zijn niet alleen de EDP-auditors aanwezig maar is ook de Senior Manager aanwezig die de algemene coördinatie van alle Ernst & Young opdrachten naar de klant toe verzorgt. Uiteraard beginnen we met een voorstelronde, die voornamelijk in het Engels wordt gehouden, maar ook gedeeltelijk in het Noors. Eén interne accountant is namelijk een Engelsman en de SAP veiligheidsadviseur van PricewaterhouseCoopers is een Vlaamse. We beginnen de presentatie, conform Ernst & Young en algemene richtlijnen, met een inleidend verhaal over de doelstelling van het onderzoek, de begrenzingen en de indeling van de presentatie. Na het inleidend verhaal door mijn Senior Manager presenteren mijn twee andere Noorse collega's, een Senior Associate en een Junior Associate, hun bevindingen ten aanzien van de algemene computerbeheersingsmaatregelen. De bevindingen worden met enige vragen en commentaren goed ontvangen door de opdrachtgever. Bij de algemene computerbeheersingsmaatregelen is door mijn collega's met name getoetst op basis van ITIL en CobiT. Vervolgens nemen we een korte pauze, waarbij naar Noors gebruik enig fruit wordt genuttigd (Noorse werkgevers verzorgen dagelijks korven met vers fruit, met name om de gezondheid van de werknemers te versterken). Na de pauze nemen enkele deelnemers aan de presentatie afscheid. In mijn segment presenteer ik namelijk mijn bevindingen ten aanzien van de SAP computerbeheersingsmaatregelen. Deze zijn veelal erg technisch en specificiek, SAP is nu eenmaal een fascinerend maar tegelijkertijd buitengewoon complex pakket. Volgens de, voor Noorwegen aangepaste, Ernst & Young methodologie worden algemene computerbeheersingsmaatregelen ingedeeld in drie deelgebieden: Change Management, Access Management en Operations Management. De klant heeft echter een eigen indeling van de SAP computerbeheersingsmaatregelen. We behandelen eerst het deelgebied Change Management met de overeenkomstige 'Change Management' maatregelen van de klant met in hoofdzaak aspecten zoals transporten tussen SAP installaties en ABAP/4 standaarden. Vervolgens behandelen we het deelgebied Access Management met de overeenkomstige 'Role Administration', 'Access Administration', 'Privileged IDs', 'System Setup', 'Role Design' en 'Sensitive Data' maatregelen van de klant met in hoofdzaak aspecten zoals authorization objects, transaction codes, tables, authorization groups en hoe het systeem is geconfigureerd met betrekking tot zekerheidsinstellingen. We behandelen als laatste het deelgebied Operations Management met de overeenkomstige 'Auditing and Logging' en 'Job Scheduling' maatregelen van de klant met in hoofdzaak aspecten zoals het gebruik van logbestanden voor kritieke transacties en het monitoren van succesvolle 'batch runs'. De meer algemene aspecten binnen de deelgebieden, zoals het proces van het toekennen van gebruikersrechten, worden vanuit de generieke ITIL processen bestuurd. Ook hier worden, na enige vragen en commentaren van met name de SAP veiligheidsdeskundige van PricewaterhouseCoopers, mijn commentaren goed ontvangen door de opdrachtgever. Als afsluiting van de presentatie wordt met de opdrachtgever afgesproken in januari een dag af te spreken om een rondetafeldiscussie te houden met betrekking tot de formele commentaren alsook verbeteringsacties van de opdrachtgever. Wij vertrekken vervolgens om 15.45 uur terug naar het Ernst & Young kantoor.

Lotus Notes

Bij terugkomst op het Ernst & Young kantoor om 16.00 uur heb ik nog snel de mogelijkheid mijn Lotus Notes te repliceren, zodat ik in het vliegtuig mijn e-mail nog eens kan doornemen. Voor ik om 16.15 uur met een taxi naar het vliegveld vertrek, spreek ik met mijn Senior Manager af hem morgen te bellen voor de verdere afstemming van de werkzaamheden. Het inchecken gaat erg snel (het vliegveld van Stavanger is erg klein) en om 16.45 uur zit ik weer boven de wolken. In mijn e-mail tref ik, naast onder andere een vraag van Carlo Bavius van het IT Audit Portal (waar ik mede-redactielid ben), als PDF-bestand het december nummer van Data Z aan, het tijdschrift van de Noorse ISACA-afdeling (Noorwegen kent geen nationale organisatie zoals NOREA). Tot mijn verbazing lees ik dat ik van alle Noorse CISA-examen kandidaten in 2005 het beste resultaat heb behaald (een postdoctorale EDP-audit bij TIAS opleiding doet wonderen). Om 17.30 uur land ik na een interessante dag op het besneeuwde vliegveld van Oslo.