Beveiliging en service level agreements

Beveiliging moet een vaste plaats krijgen in uitbestedingsovereenkomsten

Mw. I.J.M. van Gogh, Bc en ing. P.M. Hoogendoorn

'The essence of knowledge is,
having it, to apply it;
not having it, to confess your ignorance'

Confucius

Uitbesteden van ICT-diensten en het daarbij waarborgen van het vereiste beveiligingsniveau van deze diensten is een onderbelicht en vaak vergeten onderwerp. Veelal wordt net voor het daadwerkelijk afsluiten van een contract nog snel even iets op papier gezet over de beveiliging. Dit leidt onontkoombaar tot teleurstellingen die met de steeds groter wordende afhankelijkheid van IT tot grote bedrijfsrisico's kunnen leiden. In dit artikel wordt antwoord gegeven op de vraag hoe een beveiligingsparagraaf in een uitbestedingscontract eruit zou kunnen zien. Ook de rol van de IT-auditor wordt daarbij nader belicht.
Dit artikel loopt vooruit op de publicatie van een tweetal studies van het Platform Informatiebeveiliging die uitgebreid ingaan op dit onderwerp. De eerste studie 'Beveiliging en SLA: Bedreigingen en normen in een klant-leverancierrelatie' zal in de loop van het jaar 2000 verschijnen. De tweede studie 'Beveiliging en SLA: Contractuele aspecten in een klant-leverancier-relatie' zal waarschijnlijk begin volgend jaar gepubliceerd worden.

Inleiding uitbesteding

Uitbesteden staat momenteel in het middelpunt van de belangstelling; overheden en bedrijfsleven zijn er druk mee bezig. Terug naar de kernactiviteiten, rationaliseren van bedrijfsdoelstellingen en decentralisatie zijn allemaal ontwikkelingen die hoog en laag in de organisatie spelen. De verantwoordelijken in die organisaties gaan nadenken over hun takenpakket en zullen keuzen maken over welke taken zij zelf nog willen uitvoeren en welke taken door andere, meer gespecialiseerde bedrijven uitgevoerd kunnen worden.
Ook minder elegante motieven kunnen een rol spelen. Zeker bij de uitbesteding van automatiseringstaken werd en wordt nog steeds als reden aangevoerd dat uitbesteden een oplossing biedt voor 'die slecht te managen IT-afdeling'[1].

Dat een dergelijke alles-of-niets-strategie niet werkt hebben enkele bedrijven aan den lijve ondervonden. Met hun automatiseringsafdeling verdween ook de kennis van bedrijfsspecifieke onderdelen, kennis die door de eigen automatiseerders werd aangewend om de IT-hulpmiddelen effectief in te zetten. Er verdween een stukje flexibiliteit. Immers, de eigen IT-afdeling vragen even iets tussendoor te doen is goed mogelijk; dezelfde vraag aan een IT-dienstverlener stellen is, afhankelijk van de vorm van uitbesteding, vaak een stuk moeilijker, zeker als dezelfde reactietijd wordt verlangd.

Kortom, uitbesteden is moeilijker dan aanvankelijk werd gedacht. Nu is de tijd aangebroken om te zoeken naar meer passende uitbestedingsmogelijkheden. Het uitbesteden van een goed afgebakend element van de totale IT-voorziening blijkt de oplossing. De gedachte hierachter is simpel: wat goed functioneert kan goed beschreven worden, de leverancier krijgt daarmee een duidelijk beeld van wat geleverd moet worden. Het voordeel van uitbesteden ligt in een dergelijk geval op het vlak van doelmatigheid. Het bewijs van deze doelmatigheid blijkt niet altijd even eenvoudig te leveren. De kosten die door de leverancier worden berekend, liggen goed vast; het vaststellen van de kosten die gemaakt worden door de eigen IT-afdeling, is minder gemakkelijk. Het falen van menig Total Cost of Ownership (TCO)-project moge hiervoor mede een indicatie zijn.

Samengevat zijn de ontwikkelingen op uitbestedingsgebied geëvolueerd van uitbesteden van de complete IT-afdeling, inclusief alle IT-kennis, naar het uitbesteden van enkele goed gedefinieerde IT-elementen. Voordeel daarvan is het behouden van de bedrijfseigen IT-kennis. Steeds meer bedrijven en instellingen streven naar het zijn en blijven van 'smart-buyer' om IT-diensten verstandig te kunnen inkopen.

Maken van afspraken

Zodra over uitbesteding wordt gedacht, moet ook worden nagedacht over de afspraken met de uitbesteder. Er dienen immers afspraken te worden gemaakt over bijvoorbeeld de beschikbaarheid van de diensten en de wijze waarop de diensten worden aangeboden. Ook de eventuele afbakening van diensten die door meerdere partijen worden geleverd, is een aandachtspunt, en zo zijn er nog vele andere punten van aandacht.

In dit verband wordt vaak gesproken over Service Level Agreements (SLA's), in het Nederlands veelal Dienst Niveau Overeenkomsten (DNO's) genoemd. In deze overeenkomsten worden de relevante afspraken betreffende de dienstverlening vastgelegd.

De structuur van de uitbestedingsrelatie bestaat doorgaans uit drie lagen, waarbij de globale uitgangspunten worden vastgelegd in een uitbestedingsraamcontract, de verdere concretisering daarvan plaatsvindt in SLA's en de operationele uitvoering ten slotte geregeld wordt in gebundelde werkafspraken (veelal Dossier Afspraken en Procedures genoemd). Daarbij wordt aangetekend dat de afspraken weergegeven in de uitbestedingsovereenkomst vaak breed toepasbaar maar weinig specifiek zijn, terwijl de gebundelde werkafspraken vaak wel zeer concreet maar daarmee ook sterk situationeel bepaald zijn. Het is met name de SLA die zowel voldoende concreet als breed toepasbaar is voor het vastleggen van afspraken. Het voorgaande is in figuur 1 weergegeven.

1) Bron: diverse artikelen in het IT beheer praktijkjournaal.

Proces van uitbesteding

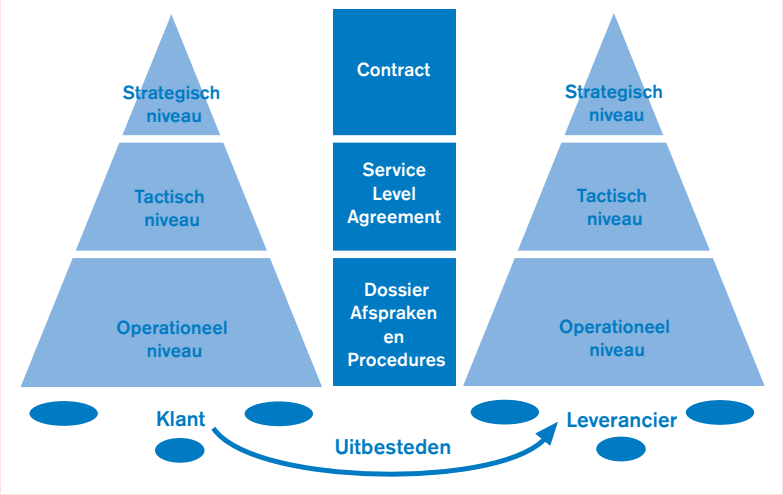
Het proces van uitbesteding kent een drietal fasen. In de eerste fase wordt bepaald wat het exacte object van uitbesteding is, in de tweede fase wordt door middel van een offertetraject een leverancier geselecteerd en een contract opgesteld. In de derde en laatste fase is er een operationele situatie. Deze fasen zijn een vereenvoudiging van het World Class IT Sourcing model (zie het artikel 'Uitbesteden vraagt om volwassen partijen' elders in deze Compact). In het WCITS-model is sprake van vijf fasen. In cursief is in figuur 2 aangegeven met welke fasen ons model overeenkomt. Op het beëindigen van een contract of het veranderen van leverancier wordt hier niet verder ingegaan.

Inzoomend op deze fasen (zie figuur 2) kunnen we de rol die de IT-auditor speelt in hoofdlijnen aangeven. Een uitwerking van de precieze werkzaamheden wordt gegeven in een aparte paragraaf aan het einde van dit artikel.

In de eerste fase wordt bekeken wat het object van uitbesteding is, wat het doel is dat met uitbesteding moet worden bereikt, wat de risico's zijn en welke requirements er aan leveranciers worden gesteld.
De IT-auditor kan in deze fase onderzoeken of het object van uitbesteding correct is gedefinieerd, en of er een gedegen risicoanalyse is uitgevoerd. Als adviseur kan de IT-auditor hier ook de complete risicoanalyse voor zijn rekening nemen en eventueel het object van uitbesteding definiëren.

In de tweede fase wordt een requirementsanalyse uitgevoerd en wordt het object van uitbesteding omgezet naar een offerteaanvraag. Indien er sprake is van een Europese aanbesteding zouden de deliverables een Request For Proposal en Request For Information zijn, en zoals de praktijk steeds weer leert is deze handelwijze ook verstandig indien er geen Europese aanbesteding moet worden uitgevoerd. Als uitgangspunt voor een goede overeenkomst dient een service level agreement te worden uitgebreid met een beveiligingsparagraaf.
In deze fase kan de IT-auditor de offerteaanvraag controleren op volledigheid, juistheid en correctheid. Tevens kan hij als adviseur optreden en het gehele traject begeleiden.
Nadat er een shortlist is samengesteld, kan de uitbesteder besluiten tot het laten verifiëren of de aanbieders op de short list kunnen waarmaken wat zij beloven. De IT-auditor kan in opdracht van de uitbesteder als externe auditor controles gaan uitvoeren. Het resultaat van een dergelijk onderzoek is dan een Third Party Mededeling. Als een leverancier is gekozen, wordt een contract opgesteld tussen de leverancier en de klant met daarin de juridische en serviceafspraken.

In de derde fase heeft de uitbesteding plaatsgevonden. In deze fase moet periodiek onderzocht worden of de geleverde kwaliteit voldoet aan de normen zoals die in de SLA zijn verwoord. De IT-auditor kan hier een aantal zaken controleren:
* via de rapportages van de leverancier en interne bevindingen aan klantzijde controleren of de kwaliteitsnormen gehaald worden;



Figuur 1. Klant-leveranciersrelatie.

* controleren of de maatregelen die de leverancier zou moeten nemen ook daadwerkelijk genomen zijn;
* controleren of het normenkader van de klant nog actueel is. Een te laag gestelde norm kan tot onaanvaardbare risico's leiden en een te hoog gestelde norm kan onevenredig veel kosten tot gevolg hebben.

Hoe ziet een goede SLA eruit?

De inzichten over wat de inhoud van een SLA zou moeten zijn, zijn in de loop der tijd geëvolueerd. In de begintijd van de uitbestedingen werden gedetailleerde afspraken over sterk technisch georiënteerde componenten gemaakt. Later zijn deze afspraken meer en meer servicegericht geworden, waarbij de technische details óf in de bijlage worden gemeld óf geheel aan de leverancier worden overgelaten.

De structuur van een SLA is meestal opgebouwd uit een juridisch contractueel deel en een servicebeschrijvend deel waarin de gevraagde dienstverlening in meer detail wordt gespecificeerd, meestal gestructureerd naar het (ITIL-)beheerproces. Het juridisch contractueel deel lijkt in eerste instantie wel duidelijk technisch gericht, immers de uitbestedende partij heeft besloten IT uit te besteden

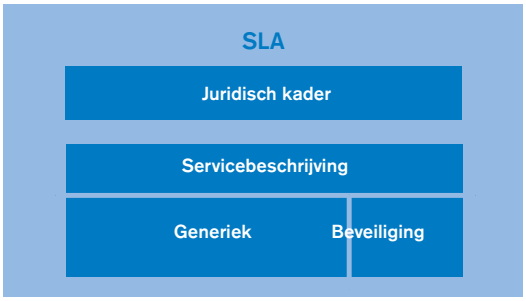
Figuur 2. Proces van uitbesteding.

Fase 1:	**Wat zijn de eisen/ wat willen we?**	**I *(1)*** ***Wie:*** eigenaar (IT of bedrijfsproces) ***Wat:*** eisen, wensen, niveau van beveiliging ***Waarvoor:*** opstellen van de eisen voor interne en externe SLA's
Fase 2:	**Hoe vormen we de eisen om naar contractuele normen?**	**II *(2 en 3)*** ***Wie:*** Service Level Manager/Jurist ***Wat:*** vertaling van eisen naar normen ***Waarvoor:*** SLA-clausules, opstellen SLA-normen op basis van eisen
Fase 3:	**Wordt de SLA nageleefd?**	**III *(5)*** ***Wie:*** uitbestedende partij ***Wat:*** audit ***Waarvoor:*** controle op naleving, bijstellen van de eisen, nemen van sancties

en zal vaak in technische zinsneden de gevraagde dienstverlening beschrijven.

Het servicebeschrijvend deel kan ook worden gesplitst in een servicedeel waarin meer in termen van beschikbaarheid afspraken worden gemaakt en een procedureel deel waarin procedures beschreven worden die aan de loketten van de dienstverlener geldig zijn. Hierbij moet gedacht worden aan wijzigingsprocedures zoals aanvragen voor nieuwe releases van software, een extra batchrun, verhuizingen, extra werkplekken, etc.

De vraag is nu waar de beveiliging wordt opgenomen in de SLA. Het is verstandig de beveiliging als apart deel op te nemen, aangezien het beveiligingsniveau veelal door een aparte Security Afdeling of Security Officer wordt vastgesteld en getoetst. In figuur 3 is weergegeven hoe een SLA er in de praktijk uit kan zien.



Figuur 3. Structuur van een service level agreement.

Het juridische kader vormt het eerste hoofdstuk en zoals reeds beschreven bestaat dit uit juridische en contractuele normen. Het tweede hoofdstuk bevat de servicebeschrijving en kan opgedeeld worden in twee delen: het generieke deel en het beveiligingsdeel. Het generieke deel bevat dan voornamelijk de normen wat betreft beschikbaarheid en het beveiligingsdeel bevat vooral de extra beveiligingsnormen omtrent exclusiviteit en integriteit (zie de volgende paragraaf). Als extra document kan het Dossier Afspraken en Procedures nog worden toegevoegd. Dit behoort niet direct tot de SLA aangezien hierin de normen in detail zijn uitgewerkt tot op procedureniveau. De structuur die hier is weergegeven, is niet verplicht, maar geeft een aardig beeld van de inhoud en een mogelijke structuur van een SLA.

Beveiligingsaspecten die als vanzelfsprekend zijn geregeld bij de klant, zijn niet vanzelfsprekend geregeld bij de outsourcingspartner.

Het allerbelangrijkste in een SLA is te kiezen voor 'meetbare', begrijpelijke elementen (prestatie-indicatoren). Bij voorkeur elementen die door de uitbestedende partij, zonder IT-kennis, begrepen kunnen worden. Voorbeelden hiervan zijn de openingstijden van de helpdesk of het aantal uren uitval achtereen per maand. Aan de normen met betrekking tot beveiliging dienen dus ook prestatie-indicatoren te worden toegekend, zoals het aantal (geslaagde/mislukte) hackingincidenten per periode.

Wat zijn de beveiligingsaspecten die een rol spelen bij uitbesteding?

Van meet af aan zijn beveiligingsaspecten in een SLA onderbelicht gebleven doordat er geen proces was dat de beveiligingsaspecten bewaakte, zoals het huidige ITIL-document Security Management dit nu wel doet. Toch verdienen deze aspecten aandacht, zeker wanneer er meerdere partijen bij de levering betrokken zijn. Te denken valt aan een leverancier die een consortium heeft gevormd, of aan een opzet waarbij delen van het uitbestedingsobject door verschillende leveranciers worden geleverd.

Er zijn vele aspecten die alle te maken hebben met beveiliging. In dit artikel wordt uitgegaan van de drie beveiligingsaspecten die gedefinieerd zijn in het VIR (Voorschrift Informatiebeveiliging Rijksdienst) van het Ministerie van Binnenlandse Zaken, te weten: beschikbaarheid, integriteit en exclusiviteit.
Let wel, dit zijn ook aspecten die normaal gesproken al in een SLA staan. Dit geldt in het algemeen voor het aspect beschikbaarheid.
Het verschil zit in het feit dat beschikbaarheid, bezien vanuit een beveiligingsoogpunt, slechts de vereiste beschikbaarheid geeft die volgens de opdrachtgever *minimaal* nodig is om geen schade of een toelaatbare hoeveelheid schade op te lopen.
De eisen uit beveiligingsoogpunt dienen dan ook beschouwd te worden als een minimale set eisen. Om andere redenen dan beveiliging kan gekozen worden voor een andere beschikbaarheidseis.

Andere aspecten, zoals integriteit en exclusiviteit, komen minder vanzelfsprekend voor in een SLA en dienen expliciet te worden opgenomen.
Veel gestelde vragen hierbij zijn:
1. Welke eisen zijn voor mij belangrijk?
2. Wat moet ik zelf doen en wat moet ik dan aan de leverancier opleggen?
3. Welke rapportage moet ik daarover afspreken?
4. Hoe weet ik dat de leverancier zich houdt aan de gemaakte afspraken?

De basis voor het antwoord op al deze vragen is na te gaan welke beveiligingseisen en -maatregelen in het eigen bedrijf impliciet gelden, specifiek de eisen en maatregelen die gelden voor de eigen beheerorganisatie en de aan haar toevertrouwde systemen. Deze impliciete eisen zullen naar de leverancier toe expliciet gemaakt moeten worden.

Voor elk van de eigen maatregelen dient nagegaan te worden of en zo ja, in hoeverre deze van belang zijn voor de leverancier. Bedenk hierbij dat de cultuur van het bedrijf belangrijk is. Beveiligingsaspecten die als vanzelfsprekend zijn geregeld binnen het eigen bedrijf zijn vaak niet of niet op dezelfde wijze geregeld bij een ander bedrijf en behoeven daarmee expliciete aandacht. Daarom wordt bij ieder hoofdstuk over een uitbestedingsobject, specifieke aandacht geschonken aan juist die, verborgen vanzelfsprekende, beveiligingsaspecten.

Het spreekt bijna voor zich dat rapportage zal moeten plaatsvinden over alle beveiligingsincidenten. Uit de rapportage dient tevens de effectiviteit te blijken van de afgesproken maatregelen. De aan de leverancier gevraagde maatregelen kunnen namelijk zowel te weinig effectief zijn, zodat aanscherping of vervanging van de maatregelen noodzakelijk is, als overbodig (te effectief) waardoor wellicht met goedkopere maatregelen volstaan kan worden. Als extra tip kan nog gegeven worden dat sterk gedetailleerde rapportages alleen noodzakelijk zijn als er sprake is van ernstige beveiligingsincidenten. De ervaring leert dat uitgebreide standaardrapportages niet gelezen worden en geen extra informatie geven.

Omdat het presenteren van een algemene lijst van beveiligingsdreigingen en -maatregelen eigenlijk zou neerkomen op het verwijzen naar de Code voor Informatiebeveiliging, is gekozen voor het presenteren van vier kenmerkende objecten van uitbesteding waarvan per object de specifieke beveiligingsaspecten worden behandeld.
Zo ontstaat een praktisch toepasbare lijst van dreigingen die kan worden geëvalueerd, waarna een selectie kan worden gemaakt uit de bij de dreigingen passende maatregelen.
Deze vier objecten van uitbesteding zijn:
* netwerkdienstverlening;
* systeemontwikkeling;
* werkplekautomatisering;
* rekencentrum.

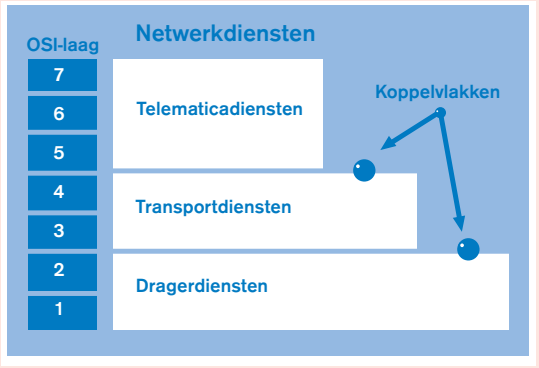
Deze objecten worden hierna toegelicht.

Netwerkdienstverlening

Netwerken zijn veel meer dan alleen de verbinding tussen verschillende automatiseringscomponenten. Netwerken vormen steeds meer een integraal geheel met een groot aantal samenwerkende systemen en omgevingen. Het vervagen van de grenzen van het netwerk heeft tot gevolg dat het steeds moeilijker wordt om de taken en verantwoordelijkheden rond het gebruik en beheer van het netwerk eenduidig vast te stellen.

Het diffuser wordende karakter van netwerken heeft tevens tot gevolg dat het nauwelijks meer mogelijk is tot een sluitende definitie te komen voor het ICT-object netwerkdienstverlening.
Om toch nog enige handvatten te bieden wordt uitgegaan van het in figuur 4 gegeven model van dienstverlening. De begrippen dragerdienst, transportdienst en telematicadienst worden hieronder verder uitgewerkt. Bij elk van de typen diensten worden de daarvoor specifieke beveiligingsdreigingen en -maatregelen verder uitgewerkt.

Dragerdiensten
Het verzorgen van voldoende transmissiebandbreedte tussen twee punten op het netwerk. Dragerdiensten omvatten de eerste en tweede laag van het OSI-model. Deze dienstverlening, die vooral een fysiek en infrastructureel karakter heeft, is met name van belang bij netwerken die een grote afstand moeten overbruggen of waarover een intensief netwerkverkeer plaatsvindt. Te denken valt aan huurlijnen, Frame Relay-koppelingen,



Figuur 4.
LAN/WAN-diensten.

ATM- en SDH-transmissiecapaciteit. In het algemeen wordt door de aanbieders van dragerdiensten naar keus een bepaalde bandbreedte aangeboden waarover het de afnemer vrij staat informatie, protocolonafhankelijk, te versturen.

Specifieke dreigingen en maatregelen
Bij dragerdiensten spelen er geen specifieke extra dreigingen, immers het transport van deze diensten wordt over bekabeling geleid die van een externe partij gehuurd wordt. Dit huren moet, ongeacht of men dit in eigen beheer doet of niet, toch bij een externe partij plaatsvinden. Doorgaans is men zich dan ook zeer wel bewust van de extra risico's die worden gelopen als informatie over externe verbindingen moet worden gestuurd. Het is daarmee zaak van de toeleverancier adequate maatregelen te verlangen. Het belangrijkste onderscheid moet worden gemaakt tussen verbindingen die men exclusief voor zichzelf heeft en verbindingen die men met anderen deelt, zoals Internet-verbindingen.

Voorbeelden van te treffen maatregelen zijn in tabel 1 weergegeven.

Transportdiensten
Het daadwerkelijk transporteren van informatie tussen twee of meer punten op het netwerk. De transportdiensten omvatten de derde en vierde laag van het OSI-model.
Deze dienstverlening is gericht op de softwarematige netwerkbesturing van de gegevensstromen op het netwerk. Te denken valt aan TCP/IP-koppelingen, LAN-koppelingen en X.25-koppelingen hoewel deze slechts aangrijpen op OSI-laag 3. Ook MPOA- of LANE-protocollen vallen hieronder omdat deze immers zorgen voor de mogelijkheid TCP/IP-protocollen te vervoeren over ATM. Ten slotte kan ook gedacht worden aan spraakdiensten, zoals telefonie.

Tabel 1.
Te treffen maatregelen bij dragerdiensten.

Classificatie van de informatie	Eigen netwerk	Openbaar netwerk (bijv. Internet)
Ongeclassificeerd	Geen	Toegangscontrole
Vertrouwelijk	Geen	Vercijfering op berichtniveau
Geheim	Vercijferd op lijnniveau	Vercijfering op berichtniveau
Zeer geheim	Vercijferd op lijnniveau	PKI

Specifieke dreigingen en maatregelen
Indien men het totale transport van informatie in eigen hand heeft, is men ook zelf in staat de routes van de informatie te bepalen en de instellingen van de apparatuur te kiezen. Wordt uitbesteed, dan ontstaan hier de volgende extra risico's:
* *Apparatuur kan ontregeld raken.* Behalve dat de apparatuur zodanig ingesteld kan worden dat er geen communicatie meer mogelijk is, is het ook mogelijk de apparatuur zo in te stellen dat informatie eenvoudig 'afgetapt' of zelfs gewijzigd kan worden. Dit risico kan vermeden worden door het risico expliciet te vermelden en van de leverancier te eisen dat de apparatuur zodanig wordt ingesteld dat deze niet door derden ontregeld kan worden.
* *Er kan incompatibiliteit tussen protocollen zijn.* De toeleverancier kan besluiten een bepaalde instelling of versie van protocollen te gebruiken. Dit hoeft niet altijd transparant te blijven voor de klant, en kan leiden tot het wijzigen van de intern gebruikte protocollen. Dit risico kan vermeden worden door de leverancier ook voor het koppelpunt de volledige verantwoordelijkheid te geven.

Telematicadiensten
Het aanbieden van toepassingen aan gebruikers waarbij het transport van gegevens over het netwerk noodzakelijk is. Telematicadiensten omvatten de bovenste drie lagen van het OSI-model. Deze dienstverlening zorgt voor de specifieke functionaliteit die binnen de netwerkomgeving aan de gebruikers beschikbaar gesteld kan worden. Te denken valt aan bestandsoverdracht, koppelen van asynchrone terminals aan X.25-diensten (paddienstverlening), e-mail, EDI, gatewaydienstverlening, videoconferencing, databasekoppelingen, Internet-sites, e-commercediensten, spraak (telefonie), PABX-koppelingen, etc.

Specifieke dreigingen en maatregelen
Deze diensten worden in hun geheel vormgegeven door externe partijen waarbij vaak nog weer subtoeleveranciers een rol spelen. Bij deze vorm van dienstverlening worden vaak specifieke diensten geleverd waarbij het om kritische bedrijfsgegevens gaat. Wees er hier in het algemeen op bedacht dat er cruciale bedrijfsinformatie wordt toevertrouwd aan de leverancier; denk daarbij aan e-commerce waarbij kennis over het productassortiment, prijzen en waarschijnlijk ook een deel van de logistieke afhandeling wordt verstrekt, informatie waar anderen dankbaar gebruik van kunnen maken (een prijslijst kan on line gewijzigd worden, ook ongeautoriseerd).
Bij e-mailservices worden alle berichten opgeslagen op servers van de leverancier, daar kunnen ze ook onbevoegd gelezen worden.
In het algemeen kan gesteld worden dat telematicadiensten dicht bij de corediensten van een bedrijf kunnen liggen. Dit vereist aandacht voor informatiebeveiliging.

Systeemontwikkeling

Definitie
Onder uitbesteden van systeemontwikkeling wordt verstaan het door een leverancier laten ontwikkelen van een specifiek voor die organisatie benodigd systeem. Systeemontwikkeling houdt zich bezig met het vertalen van functionele gebruikerseisen en -wensen naar software.

Beschrijving
Het ontwikkelen van een systeem is een vakgebied dat sterk in beweging is. Methoden en technieken volgen elkaar in snel tempo op. Dit blijkt uit het feit dat er in de universitaire wereld hard gewerkt wordt aan het wiskundig onderbouwen van systeemontwikkelmethodieken alsmede bewijsvoering betreffende correct werkende programmatuur. Dit laatste doel is nog niet bereikt en daardoor kan nog niet worden vertrouwd op de kwaliteit van de opgeleverde systemen.

De huidige methodieken kunnen worden onderscheiden in:
* *functionele aanpak*. De te bouwen functionaliteit wordt opgesplitst in deelfuncties net zo lang tot elementaire bouwstenen ontstaan die vervolgens geprogrammeerd kunnen worden.
De risico's hiervan zijn:
– uitlekken van vertrouwelijke informatie (de specificaties van de klant bevatten vaak vertrouwelijke elementen zoals gepatenteerde algoritmen en marketingstrategieën);
– verlagen van het kwaliteitsniveau. Nog steeds duren systeemontwikkeltrajecten lang waardoor vanwege tijdsdruk het risico wordt gelopen dat er concessies worden gedaan aan de kwaliteit.
* *objectgeoriënteerde aanpak*. Deze aanpak gaat veel meer uit van een gegevensmodel en bouwt containers (objecten) waarin met gegevens gemanipuleerd (gedrag van het object) wordt. Het ontwerpen van het gegevensmodel en de daarop aansluitende objecten is hier elementair.
Het grootste risico hierbij is het niet voldoende aandacht geven aan een correcte abstractie (gegevensmodel inclusief gedragsmodellering) waardoor een onjuiste objectklasse ontstaat. Hoewel de ontwerper het gevoel heeft een juist ontwerp te hebben gemaakt, kan dit feitelijk onjuist zijn. Omdat dit ontwerp op een hoog abstractieniveau wordt gemaakt, zijn de consequenties niet altijd meteen duidelijk. Pas in een laat stadium wordt ontdekt dat er gebreken zijn. Gebreken zowel ten aanzien van de gewenste functionaliteit als kwaliteitsaspecten zoals logische toegangsbeveiliging.
* *RAD en hiervan afgeleide methodieken.* In deze aanpak wordt gestart met het ontwerpen en coderen van de gebruikersinterface. Dit wordt ook wel prototyping genoemd of bottom-upbenadering. Het doel van de RAD-methodiek is om de gebruikers vanaf het begin te laten participeren in het project en te laten meebepalen welke functionaliteit er geboden moet worden en hoe deze functionaliteit naar de gebruikers toe ontsloten moet worden. In deze methode wordt gebruikgemaakt van zogenaamde timeboxes. Software wordt op een vastgestelde datum opgeleverd; hoewel men afspraken maakt over de op te leveren functionaliteit, is deze variabel in een timebox. Deze methode wordt ondersteund door diverse tools.

Het grootste risico van deze methode is de gebruikersfocus. Omdat het gehele ontwerp in zeer sterke mate wordt bepaald in samenwerking met de gebruikers van het systeem kunnen de andere kwaliteitsaspecten hieronder lijden. Immers, als er minder functionaliteit geleverd kan worden dan is afgesproken, zal men geneigd zijn die functionaliteit die opgemerkt wordt door de gebruikers voorrang te geven boven aspecten die door de gebruikers minder direct worden gezien. Met name de beveiligingsaspecten worden hier vaak de dupe van.

Met betrekking tot complexiteit is er een wezenlijk verschil tussen de functionele decompositiemethode en de objectgeoriënteerde aanpak. Daar waar functies nog kunnen worden gedecomponeerd op basis van intuïtie, en eventuele niet-optimale keuzen daarin nog vrij eenvoudig kunnen worden hersteld, zelfs op het allerlaatste moment, is het samenstellen van objecten en klassen van objecten een proces dat alleen op basis van kennis en ervaring met succes kan worden uitgevoerd. Een verkeerd gekozen objectklasse kan op het eind niet eenvoudig hersteld worden.

Algemene risico's bij systeemontwikkeling
Het gebruiken van de methoden en technieken alsmede de begeleidende tools is kenmerkend voor dit type werkzaamheden. Het kunnen vertalen van eisen en wensen van een opdrachtgever naar goed functionerende programmatuur is daarbij essentieel. Een ander aspect is het onder controle houden van een softwareontwikkelingsproject. De meeste recente cijfers wijzen uit dat wereldwijd circa 25 procent van alle systeemontwikkelingsprojecten is gestopt vanwege het niet tijdig en ver buiten afgesproken budgetten opleveren daarvan (bron: IDC).

Voor elke stap in het systeemontwikkelingstraject moeten met de leverancier afspraken worden gemaakt over de invulling. Naarmate het systeemontwerp concreter wordt, wordt ook voor de klant duidelijker wat de mogelijkheden van het systeem zijn. Het komt vaak voor dat de klant tijdens het ontwerp nog wijzigingen wil aanbrengen vanwege dit voortschrijdend inzicht. Het systeemontwikkelingstraject kan hierdoor vertraagd worden en vanwege het wijzigen op functioneel niveau kunnen andere eisen (bijvoorbeeld ten aanzien van toegangsbeveiliging) ontstaan. Het beheersen van alle relevante aspecten in een systeemontwikkelingstraject is een gedeelde verantwoordelijkheid van de klant en de leverancier.

Het uitbesteden van systeemontwikkeling kan op een aantal manieren worden vormgegeven:
* *geheel*. Mensen en middelen vormen geen onderdeel van de klantorganisatie. De verantwoordelijkheid ligt geheel bij de leverancier.
* *gedeeltelijk-1*. Mensen vormen geen onderdeel van de klantorganisatie. De gebruikte middelen vormen wel onderdeel van de klantorganisatie. Activiteiten vinden geheel plaats op locatie van de leverancier. De verantwoordelijkheid ligt gedeeltelijk bij de leverancier en gedeeltelijk bij de klant.
* *gedeeltelijk-2*. Het personeel wordt als geheel team onder de projectverantwoordelijkheid van de leverancier ondergebracht op locatie van de klant. De klant is geheel verantwoordelijk voor het naleven van de beveiligingsrichtlijnen.

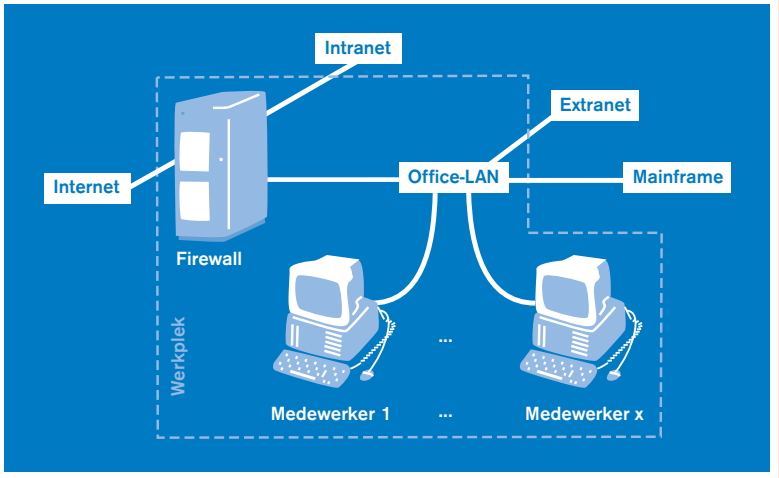
Beveiligingsaspecten
Bij het uitbesteden van systeemontwikkeling moeten ook afspraken worden gemaakt op het gebied van beveiliging. Voorbeelden van beveiligingsaspecten die bij uitbesteding van systeemontwikkeling van specifieke betekenis zijn:
* *ongeoorloofd gebruik van (output van) gegevens*. Denk hierbij aan het in opdracht laten programmeren van gepatenteerde ideeën.
* *opzettelijke inbreuk op systemen*. Denk hierbij aan het onjuist programmeren waardoor gegevens ten onrechte als juist worden geclassificeerd door de programmatuur terwijl zij dit niet zijn. Of aan websites waartoe toegang verkregen kan worden door slordig programmeren.
* *samengaan van de productie- en testomgeving*. De productie- en de testomgeving dienen te allen tijde van elkaar gescheiden te zijn om de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens en programmatuur te kunnen waarborgen.
* *stoppen en uitvallen van operationele processen*. Niet goed uitgeteste programmatuur kan, geoorloofde, condities tegenkomen waar de code niet op berekend is; het programma zal in de meeste gevallen stoppen.
* *onvoldoende autorisatie*. Als de geprogrammeerde controles door ongeautoriseerden kunnen worden uitgevoerd, ontstaan hierdoor ongewenste situaties waardoor frauduleus handelen mogelijk wordt.
* *onvoldoende aandacht voor beveiliging in systemen*. Tijdens het ontwikkelen van systemen dient extra aandacht te worden besteed aan beveiligingsfuncties in de systemen, zoals logische toegangsbeveiliging en encryptie.

Werkplekautomatisering

Definitie
Werkplekautomatisering bestaat uit PC-configuraties en bijbehorende (rand)apparatuur waarover de gebruiker direct kan beschikken. Deze omgeving wordt ook wel aangeduid met desktop-services of de clientomgeving.

Beschrijving
Onder werkplekautomatisering wordt veelal de kantoorautomatisering verstaan inclusief de apparatuur en programmatuur die nodig is om de gebruikers optimaal te kunnen ondersteunen bij de dagelijkse werkzaamheden. Voor werkplekautomatisering is voornamelijk het kwaliteitsaspect beschikbaarheid van belang; de gebruikers willen namelijk een zo veel mogelijk ongestoorde werking tijdens de werkdag.
Tevens is het van belang dat gebruikers tijdens kantooruren ergens terechtkunnen met hun vragen en problemen omtrent de werkplekautomatisering; hiervoor is veelal een helpdesk ingericht bij de leverancier.

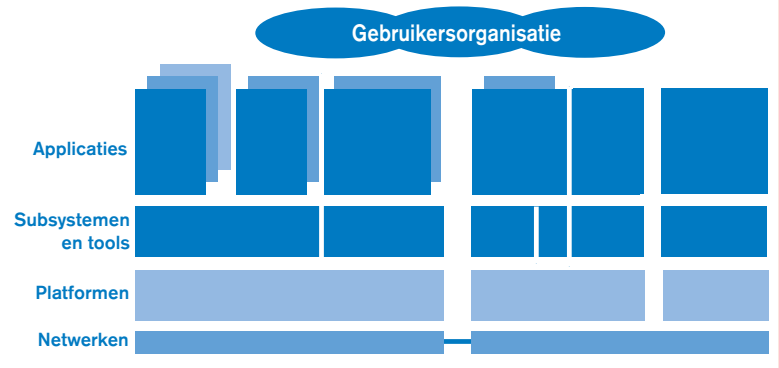
In figuur 5 is een situatie geschetst, zoals deze voor kan komen in een werkplekomgeving. Het omkaderde deel komt overeen met de werkplek in een willekeurige organisatie. Zoals in de figuur is weergegeven, bestaat de werkplek uit een Office-LAN met daaraan een aantal medewerkers en een externe koppeling voor de mobiele werkplek. De werkplek heeft diverse koppelingen met de binnen- en buitenwereld van een organisatie, zoals het intranet, Internet en het mainframe.



Figuur 5. Werkplekomgeving.

Bij het uitbesteden van werkplekautomatisering dienen afspraken te worden gemaakt over:
* het type werkplek dat benodigd is;
* vervanging van apparatuur en programmatuur;
* verwijdering van apparatuur.

Beveiligingsaspecten
Hierna wordt een aantal aandachtspunten gegeven die van belang zijn bij het maken van afspraken met de service provider over beveiliging bij uitbesteding van werkplekautomatisering. Bij elk aandachtspunt worden één of meer voorbeelden gegeven van voorkomende bedreigingen:
* *inbraak:*
– intern: een medewerker neemt zonder toestemming een laptop uit het magazijn mee naar huis;
– extern: een hacker breekt in het informatiesysteem in met alle mogelijke gevolgen van dien;
* *verlies van gegevens:*
– virusaanval;
– server crash;
– hacker die moedwillig gegevens verwijdert;
– onoordeelkundig opslaan van digitale informatie;
* *stoppen en uitvallen van operationele processen:*
– stroomstoring;
– server crash;
* *onvoldoende werkplekbeheer:*
– ondeskundige beheerders, waardoor uitval van werkplekken vaker voorkomt en het vaak lang duurt voordat de werkplek weer beschikbaar is;
* *onvoldoende configuratiebeheer:*
– geen geldige licenties en daardoor kans op hoge boetes;
– onvoldoende zicht op de aanwezige IT-componenten waardoor bijvoorbeeld ontvreemding van IT-componenten niet opvalt en geschikte beveiligingsmaatregelen niet genomen kunnen worden;
* *helpdesk:*
– ondeskundige helpdesk-medewerkers waardoor het lang duurt voordat een oplossing is gevonden voor IT-problemen van gebruikers die daardoor een bepaalde tijd niet kunnen werken (verlies van productieve uren).



Figuur 6. De basis-IT-infrastructuur.

Rekencentrum

Definitie
Onder een rekencentrum valt het geheel van activiteiten ten behoeve van het beheer en de exploitatie van geautomatiseerde gegevensverwerking.
Voor rekencentra zijn verschillende benamingen gangbaar, als datacentre en computercentrum.

Beschrijving
Het rekencentrum dient te worden gezien als het geheel van activiteiten gericht op de grootschalige exploitatie van de geautomatiseerde gegevensverwerking alsmede de beheeractiviteiten ten behoeve van de handhaving van de kwaliteit van de dienstverlening. Het rekencentrum bestaat uit een groot aantal componenten die onderverdeeld zijn naar een aantal niveaus:
* applicaties;
* subsystemen en tools;
* platformen;
* netwerken.

Figuur 6 geeft deze niveaus in hoofdlijnen weer.

Het rekencentrum neemt een grote rol in bij de verzorging van de geautomatiseerde informatievoorziening binnen veel organisaties. Dit is de reden dat voor rekencentra veelal hoge eisen worden gesteld aan de beveiliging van de componenten.
Binnen een rekencentrum is het kwaliteitsaspect beschikbaarheid de belangrijkste factor van succes, aangezien het rekencentrum zorgt voor bijna de gehele beschikbaarheid van de processen binnen de organisatie die de rekencentrumdiensten afneemt. Het is dan ook noodzakelijk dat in SLA's in eerste instantie de beschikbaarheidseisen voor de diensten van het rekencentrum worden aangegeven. In figuur 6 zijn de diverse IT-componenten weergegeven waaraan eisen gesteld kunnen worden.

Bij het stellen van eisen aan de rekencentrumdiensten zijn niet alleen de componenten van de IT-infrastructuur van belang, maar zeker ook de organisatorische aspecten. De organisatorische aspecten uiten zich in de twaalf IT-disciplines welke vereenvoudigd in figuur 7 zijn weergegeven in relatie tot SLA's.

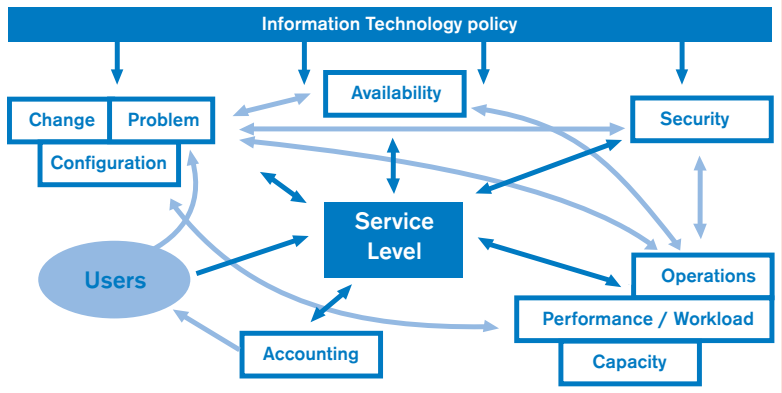
De twaalf IT-disciplines zijn een vereenvoudigde weergave van de Information Technology Infrastructure Library (ITIL). ITIL is een door de Engelse overheid samengestelde reeks van 'best practices' op het gebied

van beheer van informatievoorziening en geeft een procesgerichte benadering voor de opzet van het beheer.

Zoals in figuur 7 is af te lezen hebben alle IT-disciplines een relatie met het opstellen van SLA's. Deze relatie bestaat uit de eisen en afspraken die worden gemaakt om de verschillende IT-beheerprocessen te kunnen waarborgen. Voorbeelden van dergelijke eisen en afspraken zijn:
* Wijzigingen in programmatuur dienen te worden goedgekeurd door de uitbestedende organisatie (*Change management*).
* Alle IT-componenten binnen de IT-infrastructuur dienen te worden geregistreerd (*Configuration management*).
* Performance van het systeem is minimaal x mips (*Performance management*).

Hierboven zijn twee bronnen genoemd voor het stellen van eisen aan de dienstverlening met betrekking tot rekencentrumprocessen, te weten de IT-componenten en de beheerprocessen. Naast deze twee is nog een derde bron te noemen en wel de Third Party Mededeling (TPM). Een Third Party Mededeling wordt afgegeven door een onafhankelijke derde partij die een oordeel kan afgeven over het niveau van beveiliging binnen het rekencentrum van de service provider. Een dergelijk oordeel kan door de uitbestedende partij worden gebruikt bij de beslissing welke service provider wordt ingehuurd en bij het opstellen van eisen voor de dienstverlening. Als bijvoorbeeld blijkt dat het niveau van (informatie)beveiliging bij de service provider lager is dan het (gewenste) niveau binnen de eigen organisatie kan de uitbestedende partij ervoor kiezen een andere service provider in te huren of extra eisen te stellen aan beveiliging.

Beveiligingsaspecten
Hierna wordt een aantal aandachtspunten genoemd die van specifiek belang zijn bij het maken van afspraken over (informatie)beveiliging binnen een rekencentrum:
* *inbraak:*
– inbrekers doorbreken de fysieke toegangsbeveiliging van het rekencentrum;
– hackers doorbreken de logische toegangsbeveiliging van het netwerk/systeem;
* *uitval van systemen:*
– hardwarestoring;
– softwarestoring;
– menselijke fouten, zoals het morsen van vloeistoffen over de server;
* *ongeoorloofd gebruik van (output)gegevens:*
– privacygevoelige gegevens (bijvoorbeeld personeelsgegevens) bij een printer weghalen;
– beursgevoelige informatie aan dagbladen verkopen;
* *onvoldoende borging van beheerprocessen:*
– het doorvoeren van wijzigingen zonder voorafgaand onderzoek;
– het niet bijhouden van incidenten;
– het ontbreken van een calamiteitenplan;
* *onvoldoende autorisatiebeheer:*
– het niet verifiëren van aanvragen voor toegang tot systemen;
– het niet tijdig verwijderen van autorisaties van uitdiensttredende medewerkers.



Figuur 7. Relatie tussen IT-disciplines (vereenvoudigd model).

De rol van de IT-auditor

Welke kwaliteitskenmerken kunnen nu aan de beveiligingsparagraaf van een SLA worden toegekend en hoe kan een IT-auditor controleren of de beveiligingsparagraaf aan deze kwaliteitskenmerken voldoet?

We gaan ervan uit dat de klant een IT-auditor inschakelt om (meer) zekerheid te krijgen over de beveiligingsparagraaf in de SLA. Enerzijds kan dit de vorm aannemen van een onderzoek waarbij de IT-auditor gevraagd wordt een oordeel af te geven over de juistheid, volledigheid en toepasbaarheid van de beveiligingsparagraaf in de SLA.
Anderzijds kan dit de vorm aannemen van een controle van de leverancier waarbij de IT-auditor gevraagd wordt een oordeel af te geven over de wijze waarop de leverancier uitvoering geeft aan het gestelde in de beveiligingsparagraaf. Of in meer algemene zin hoe de leverancier zijn beheersingsmaatregelen heeft ingericht. Er wordt hier, zoals gezegd, gesproken van een TPM (Third Party Mededeling).

Van beide mogelijkheden bestaat ook een meer procesgerichte variant als gekeken wordt naar hoe de beveiligingsparagraaf tot stand is gekomen aan klantzijde en hoe de gevraagde beveiligingsmaatregelen worden geïmplementeerd en bewaakt aan leverancierszijde.

Uitgaande van een opdracht tot de beoordeling van de volledigheid en juistheid van de beveiligingsparagraaf kunnen onderstaande controles worden uitgevoerd:

Controle naar opzet
Tijdens de totstandkoming van de beveiligingsparagraaf is een aantal uitgangspunten gehanteerd. De auditor kan beschouwen of het proces van totstandkoming zorgvuldig en systematisch is uitgevoerd.
Waardevolle documenten hierbij zijn:

Het eigen beveiligingsplan
Veelal heeft het bedrijf een eigen informatiebeveiligingsplan. De auditor kan controleren of de beveiligingseisen en -maatregelen op een juiste wijze zijn vertaald naar eisen en maatregelen die van de leverancier worden verwacht. Het beveiligingsplan kan gezien worden als de baseline die geldt voor alle bedrijfsonderdelen en systemen.

Mw. I.J.M. van Gogh, Bc. is sinds 1998 als IRM-consultant werkzaam bij KPMG Information Risk Management binnen de unit Corporate Information Security. Zij houdt zich voornamelijk bezig met de Code voor Informatiebeveiliging en continuïteitsplanning. Zij neemt deel aan diverse werkgroepen van het Platform Informatiebeveiliging.

Ing. P.M. Hoogendoorn is sinds 1998 werkzaam bij KPMG Information Risk Management binnen de unit Information Security Management. Hij voert audits en adviesopdrachten uit gericht op beheersvraagstukken inzake informatietechnologie en informatiebeveiliging. Hij neemt deel aan diverse werkgroepen van het Platform Informatiebeveiliging.

De Code voor Informatiebeveiliging
De auditor kan controleren of de gevraagde maatregelen van de leverancier volledig zijn door de Code te raadplegen. Per specifiek systeem of bedrijfsonderdeel kunnen dan extra eisen en/of maatregelen worden opgesteld. De Code voor Informatiebeveiliging wordt dan toegesneden op de bedrijfsspecifieke eigenschappen.

De uitkomsten van een risicoanalyse, bijvoorbeeld een A&K-analyse
Uitkomsten uit een risicoanalyse kunnen beschouwd worden als een minimumset beveiligingseisen en -maatregelen. De auditor kan de resultaten van bijvoorbeeld een afhankelijkheids- en kwetsbaarheidsanalyse (A&K-analyse) gebruiken om te bepalen of deze maatregelen voorkomen in de beveiligingsparagraaf van de SLA (zie figuur 8).

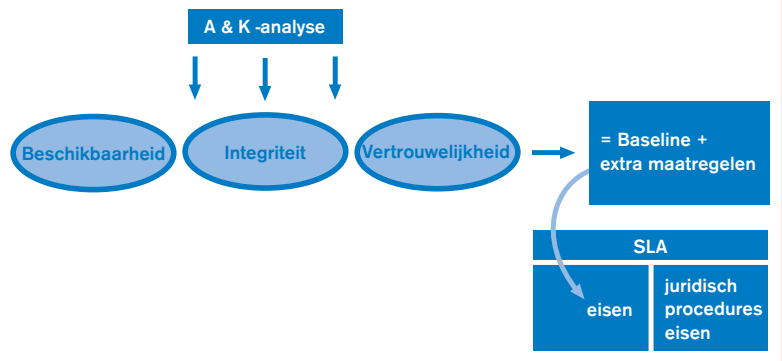
De producten- en dienstencatalogus van de leverancier
De auditor kan controleren of de beveiligingseisen en -maatregelen die de leverancier in zijn catalogus beschrijft aanvullend zijn, overeenkomen of zelfs strijdig zijn met wat de klant in zijn SLA heeft gezet.

Controle naar bestaan
Uiteraard dient de auditor te controleren of de beschreven beveiligingsmaatregelen ook daadwerkelijk zijn geëffectueerd. Of er registratie van beveiligingsincidenten plaatsvindt, of de verstrekte rapportages overeenkomen met de werkelijkheid, etc.

Uitgaande van een controle naar de implementatie bij de leverancier kunnen onderstaande controles worden uitgevoerd:

Controle naar opzet
De auditor kan beschouwen of het proces van implementatie van de gevraagde beveiligingsmaatregelen zorgvuldig en systematisch is uitgevoerd.
Waardevolle documenten hierbij zijn:
* de beveiligingsparagraaf van de SLA;
* het eigen beveiligingsplan; tevens kan worden gecontroleerd of het gehele proces van implementatie en bewaking zorgvuldig wordt uitgevoerd;
* de Code voor Informatiebeveiliging;
* de producten- en dienstencatalogus van de leverancier.

Figuur 8.
A&K-analyse.



Controle naar bestaan
Uiteraard dient de IT-auditor te controleren of de paragraaf in de SLA ook daadwerkelijk bestaat. Belangrijker is te controleren of er procedures bestaan en worden uitgevoerd die de kwaliteit van de beveiliging toetsen, de rapportages van de leverancier behandelen, het bestaan van een escalatieprocedure voor beveiligingsincidenten, etc.

Controle naar werking
Over een wat langere periode kan de IT-auditor beschouwen of de door de leverancier getroffen maatregelen effectief zijn, of de rapportages adequaat en toepasbaar zijn en of het gehele samenstel van maatregelen efficiënt is ingevoerd.

Het uitvoeren van deze controles is zeker geen sinecure en vereist een gedegen begrip van zowel het uitbestedingsobject als de informatiebeveiliging, en natuurlijk wat ons allen bindt, het vak IT-auditing.

Dankwoord

De auteurs danken het Platform Informatiebeveiliging voor de kennis die zij hebben opgedaan tijdens het verwezenlijken van de studie 'Beveiliging en SLA: Bedreigingen en normen in een klant-leverancierrelatie'.

Literatuur

[Baut98]
J.Bautz, M. ten Brink, G. Hulst, T. van Poeteren, R. Weijman en S. von Winckelmann, *Elektronische Werkplekbeveiliging: de bedreigingen versus de te nemen maatregelen*, NGI, ten Hagen & Stam, Den Haag 1998.

[BiZa94]
Ministerie van Binnenlandse Zaken (ACIB), *Voorschrift Informatiebeveiliging Rijksdienst*, 1994.

[KPMG99]
KPMG, *Visie op outsourcing van ICT: Een case studie naar de outsourcing van IT*, KPMG, Utrecht 1999.

[PlIn00]
Platform Informatiebeveiliging, *Beveiliging en SLA: Bedreigingen en normen in een klant-leverancierrelatie*, oktober 2000.

[Vank00]
G. Vankan, *Sourcing case: transportonderneming*, IT Beheer praktijkjournaal, jaargang 2 nr. 2, maart 2000.

[Zee97]
H.T.M. van der Zee et.al., *Succesvol outsourcen van IT in Nederland*, ten Hagen & Stam, Den Haag 1997.