

General IT-controls:

Complexiteit van organisaties zie je terug in IT

Mischa van der Vliet

Bijna geen enkele organisatie kan nog functioneren zonder vaak complexe IT. Dat betekent dat accountants bij audit-werkzaamheden, maar ook bij advisering, een helder beeld moeten hebben van de IT van hun klant. Audit around the computer kan niet meer.

SCHRIJVERS in *Accountancy* nieuws benadrukken regelmatig het belang van IT voor de accountant. IT speelt op twee gebieden een belangrijke rol voor de accountant. Enerzijds de wijze waarop IT kan worden ingezet voor de eigen bedrijfsvoering. Hierbij kan onder andere gedacht worden aan XBRL, SaaS en Web 2.0. Anderzijds is IT een factor om rekening mee te houden bij het uitvoeren van de financiële controles.

Raamwerk

Voor een uiteindelijke goedkeuring van de jaarrekening moet de accountant met een redelijke mate van zekerheid vaststellen dat de gebruikte gegevens betrouwbaar zijn. De meeste van deze gegevens ten behoeve van de controle van deze betrouwbaarheid van informatie verdwijnen echter in IT-systemen. Auditing around the computer – buiten de systemen om – is dan ook steeds minder een betrouwbare en juiste methode. Al met al is zonder beheersing van de IT menig proces tegenwoordig niet meer bestuurbaar. Reden genoeg voor een controlerende accountant om aan IT gerelateerde controles te onderzoeken. Dit artikel gaat in het op het raamwerk van de IT-controls, vervolgens zullen vanwege de complexiteit periodiek de general IT-controls specifiek worden beschreven.

Driedeling

Ruwweg kunnen de IT-gerelateerde controles in drieën worden gesplitst, namelijk in gebruikerscontro-

les, application controls en general IT-controls. Onder gebruikerscontroles vallen bijvoorbeeld zelfcontroles, collegiale controles en controles door een leidinggevende. Deze controles worden niet afgedwongen door de applicatie en zijn afhankelijk van de aanwezig procedures en de naleving daarvan. Dat zijn geen sterke instrumenten wanneer we het proces willen beheersen. Maar het is in ieder geval beter dan niets, want ook dat komt nog vaak voor. Kleinere organisaties hebben vaak moeite om de vereiste functiescheidingen door te voeren, waardoor controles ontbreken of niet worden nageleefd.

'Gebruikerscontroles zijn bijvoorbeeld zelfcontroles, collegiale controles en controles door een leidinggevende. Dit zijn geen sterke instrumenten.'

Application controls zijn controls die zijn verwerkt in de applicatie. Deze kunnen weer opgesplitst worden in invoer-, doorvoer- en uitvoercontroles. Voorbeelden zijn limieten en standaardwaarden, mutatieoverzichten, verbandscontroles tussen inkoop, voorraad en verkoop, etc. De mix van controles van application controls en de gebruikerscontroles dient te leiden

tot een goede beheersing van de betrouwbaarheid van de gegevens. Application controls zijn een stuk robuuster dan de gebruikerscontroles, maar deze zijn niet altijd in te voeren (denk hierbij bijvoorbeeld aan de beperking van een standaardpakket). De robuustheid kan echter teniet worden gedaan indien de general IT-controls niet goed zijn ingericht!

General IT-controls zijn voorwaarden-scheppend voor een goede beheersing van de IT-omgeving. Indien deze controles niet of niet toereikend zijn ingericht, kan de accountant niet steunen op de application controls en moeten aanvullende werkzaamheden worden uitgevoerd. En met de toenemende automatisering is het niet altijd mogelijk om controles buiten de applicatie uit te voeren, wat leidt tot een afnemende mate van zekerheid over de betrouwbaarheid van de gegevens. Een ongewenste situatie.

Inrichting general IT-controls

De accountant dient bij zijn controles dus altijd vast te stellen in hoeverre de general IT-controls zijn ingericht. Op hoofdlijnen is dat geen probleem. Voor verdieping zal inzet van een deskundige vaak noodzakelijk zijn. De literatuur, de richtlijnen van het NIVRA en de NOREA en de verschillende opleidingen voor de EDP-auditor zijn niet eenduidig over de schrijfwijze, de definitie en de onderdelen van de general IT-controls. Als best practice kan wel gesteld worden dat de volgende componenten in elk geval onderdeel zijn van de general IT-controls (zie kader). Service Level Management (SLM) of Dienstenniveaubeheer (DNB) is een nog niet veel toepaste general IT-control. Voor veel organisaties wordt dit steeds belangrijker om de IT in control te houden. De controlerende ac-

Onderdelen General IT-controls

1 Management en organisatie

De controle hiervan betreft de richting en inrichting van de organisatie op het gebied van de IT. Belangrijke onderwerpen zijn onder andere de verschillende inrichtingsmethodieken van de IT-organisatie en de daarbij behorende risico's. Tevens dient aandacht besteed te worden aan het IT-beleid, de risicoanalyse en het informatiebeveiligingsbeleid.

2 Wijzigingsbeheer

Wijzigingsbeheer is een cruciaal onderdeel om een uitspraak te doen over de beheersbaarheid van IT. Indien wijzigingsbeheer niet 'in control' is, kan de gehele IT-omgeving daardoor worden beïnvloed en is een verder onderzoek eigenlijk al overbodig. Dat kan er namelijk toe leiden dat een application control die vandaag goed functioneert morgen niet meer juist functioneert. Niet voor niets is wijzigingsbeheer om die reden een onderdeel van de general IT-controls.

3 Logisch toegangsbeheer

Logische toegang wordt ook wel aangeduid als autorisatiebeheer. Deze general IT-control wordt wel vaak door de accountant gecontroleerd. Door de toenemende complexiteit is een simpel

autorisatieoverzicht in Excel echter niet meer voldoende. Door de combinatie van functies, rollen en profielen is een autorisatie audit van een applicatie steeds meer een aangelegenheid voor specifieke tools. SAP heeft bijvoorbeeld meer dan 60.000 transactiecodes waarop een autorisatie kan worden verleend. Verder is het bij het logisch toegangsbeheer van belang om de specifieke risico's van een aantal gebruikers te onderkennen. Te denken valt hierbij aan de netwerkbeheerders, databasebeheerders en andere beheerders.

4 Fysiek toegangsbeheer

Opvallend is dat serverruimtes vaak niet zijn afgesloten of worden gebruikt als rook- of koffiekamer. Zeker in de zomer biedt de ruimte vaak enige verkoeling door de aanwezigheid van airconditioning. Gebruik op die manier leidt dan ook vaak tot problemen in de continuïteit, en kan ook gevaar opleveren. Terwijl geld en goederen vaak fysiek goed en veilig worden opgeslagen en veel in informatiebeveiliging wordt geïnvesteerd, blijken de gegevens fysiek makkelijk te benaderen. De fysieke beveiliging is op hoofdlijnen op een eenvoudige wijze door de accountant te controleren door de certificaten

op te vragen van het (eventueel) toegepaste systeem en door de procedures rondom de toegang te beoordelen.

5 Systeemontwikkeling

Elke organisatie heeft te maken met nieuwe applicaties c.q. software en de aanpassing daaraan. Het ontwikkelen van de software dient beheerst te verlopen. Hierover dienen afspraken te worden gemaakt met de ontwikkelorganisatie en door de organisatie moeten duidelijke kaders worden opgesteld. Alle business logic en control logic zal in elk geval moeten worden meegenomen in het ontwikkelproces.

6 Continuïteit

Onverstoorde IT is cruciaal voor de bedrijfsvoering van een organisatie. Het ene systeem en daarmee het bedrijfsproces kan echter langer verstoord worden dan het andere. Om de beschikbaarheid c.q. continuïteit in kaart te brengen moet een continuïteitsplan aanwezig zijn, met daarin een vast aantal onderdelen, zoals de risico's, maatregelen en uitwijkprocedures. Het continuïteitsplan moet bestaan uit een juiste mix van preventieve, detectieve, correctieve, repressieve en reactieve maatregelen.

countant dient vast te stellen welke afspraken met derden zijn gemaakt en in hoeverre die betrekking hebben op de financiële controle¹.

In een volgende bijdrage zal de general IT-control 'management en organisatie' verder worden uitgewerkt. Naast

een beschrijving van deze control zal een handzame controle lijst worden aangereikt zodat efficiënt kan worden gecontroleerd. **An**

¹ Ook deze general IT-control zal worden beschreven in een apart artikel.

Drs. Mischa van der Vliet RE is IT-auditor bij Auditconnect b.v. m.vandervliet@auditconnect.nl



Visser partners

Vennotabel AA - Maastricht - Ref. 06b03

- + Eén van de top 5 kantoren van Nederland, > 30 vestigingen. Heeft dominant marktaandeel in het MKB, maar ook (grote) familiebedrijven en beursgenoteerde ondernemingen zijn klant.
- + Geboden; interessante functie met concreet vennotabel perspectief - horizontale instroom bespreekbaar!, open collegiale en professionele werksfeer, uitstekend pakket arbeidsvoorwaarden.
- + Gevraagd; afgeronde AA-opleiding met certificerende bevoegdheid, > 5 jr. ervaring binnen accountantspraktijk, representatief, leidinggevende kwaliteiten.
- + Kijk voor deze en andere vacatures op onze website: www.visser-partners.nl

Raimtesonde 14
3824 MZ Amersfoort

T 033 453 53 50
F 033 453 53 51
E info@visser-partners.nl
I www.visser-partners.nl

werving & selectie + fusie & overname + training & coaching