Testen van applicatiecontroles

Drs. L.J. van der Perk RA en drs. P.N.M. Kromhout

Dit artikel opent met de trends en ontwikkelingen die leiden tot steeds meer geautomatiseerde controles. Deze trends en ontwikkelingen worden verder uitgediept in de daaropvolgende paragraaf, waarin controletransformatie, controlerationalisatie en de risicoanalyse worden bezien vanuit de accountant. Een groot deel van dit artikel is gewijd aan de verschillende soorten applicatiecontroles en het testen hiervan, aangevuld met implicaties voor de accountant en de eventueel noodzakelijke aanvullende tests voor het verkrijgen van additionele assurance.

Trends en ontwikkelingen

(SOx) compliance heeft de aandacht voor geautomatiseerde controles in de applicaties versterkt. Om compliance structureel te integreren in de organisatie en het risico op fouten in de financiële verslaglegging te voorkomen, is het efficiënter om geautomatiseerde controles (lees beheersingsmaatregelen) binnen de bedrijfsprocessen te verankeren zodat de controles meer en meer één geïntegreerd geheel worden met de systemen en dus de processen. Deze transitie van manuele detectieve controles naar geautomatiseerde preventieve controles, ook wel controletransformatie genoemd, maakt dat de controles effectiever, efficiënter, minder in aantal en dus goedkoper kunnen worden uitgevoerd. Bijkomend voordeel is dat bij een effectieve implementatie op basis van geautomatiseerde controles continue monitoring plaats kan vinden van de werking van de controles. Gevolg is dat governance en compliance steeds meer worden samengevoegd met de bedrijfprocessen. De genoemde ontwikkelingen leiden ertoe dat de auditor bij zijn werkzaamheden steeds vaker in aanraking komt met geautomatiseerde beheersingsmaatregelen (lees applicatiecontroles) waarop wordt gesteund. Hoe kunnen deze controles nu het meest efficiënt en effectief worden getest? Dit artikel biedt een handreiking voor de auditor bij het testen van de verschillende soorten applicatiecontroles.

Inleiding

Als onderdeel van de werkzaamheden in het kader van de jaarrekeningcontrole zien we dat ter ondersteuning van deze werkzaamheden bij veel klanten nog altijd de nadruk op de algemene IT-beheersingsmaatregelen (verder ITGC) ligt. Diverse (internationale) templates zijn voor ITGC opgezet, die zelfs verplicht in het controledossier dienen te worden opgenomen. Inzake het

Drs. L.J. van der Perk RA
is manager bij KPMG Financial Services in Amstelveen. Hij heeft bij verschillende soorten bedrijven een brede controle-ervaring opgedaan en is de afgelopen drie jaar betrokken geweest bij jaarrekeningcontroles in voornamelijk de financiële dienstverleningssector. Tevens is hij intensief betrokken geweest bij de implementatie en controle van stelsels van interne beheersingsmaatregelen (waaronder SOx) bij verschillende klanten.

vanderperk.laurens@kpmg.nl

Drs. P.N.M. Kromhout
is manager bij KPMG IT Advisory Financial Services en heeft zowel adviesopdrachten als IT-audits en procesaudits uitgevoerd bij financiële instellingen in het algemeen en bij lease- en bancaire instellingen in het bijzonder. Hij is momenteel betrokken bij de auditteams van grote bancaire instellingen en leasemaatschappijen, in het kader van het financial statement en het SOx-statement (integrated audit).

kromhout.paul@kpmg.nl

testen van applicatiecontroles is er echter minder guidance voorhanden. In een kleine enquête gehouden onder IT-auditors bleek dat slechts een beperkt aantal van hen daadwerkelijk meerdere soorten applicatieve controles test of heeft getest. Dit is opmerkelijk omdat het testen van applicatiecontroles door ontwikkelingen binnen het vakgebied, SOx en de toegenomen beheersing van ICT door ondernemingen een steeds belangrijker rol inneemt in de accountantscontrole. Wat is noodzakelijk om de documentatie en het testen van applicatiecontroles te verbeteren?

Bij de uitvoering en documentatie van het testwerk dient een goede beschrijving van de controle-informatie (beschrijving van de opzet van de controle, categorie van de controle, verantwoordelijk personeel voor het testen van de controle, doel van de controle) aanwezig te zijn. De vastlegging van het feitelijk testen van de applicatiecontroles in het kader van Test of Design / Walkthrough en Test of Effectiveness dient naast de uitgevoerde procedures tevens de resultaten, evaluatie en conclusie te bevatten. Vaak gebeurt het dat bij grote opdrachten meerdere teams werken, waarbij de applicatiecontroles worden getest op basis van de individuele kennis van de auditors en de vastlegging daarvan zeer divers is.

Standaardisatie van testmethode en documentatie is het middel om de kwaliteit van het testen en daaraan gekoppeld de vastlegging ervan te verbeteren en aldus de accountant te ondersteunen bij het vaststellen van het adequaat functioneren van de administratieve organisatie en interne beheersing.

Het artikel zal achtereenvolgens ingaan op de achterliggende gedachte en voordelen bij het meer en meer gebruikmaken van geautomatiseerde beheersingsmaatregelen, de verschillende soorten die we daarin onderkennen, het testen van de verschillende soorten en een korte handreiking betreffende de interpretatie van de resultaten.

Controletransformatie, controlerationalisatie en de risicoanalyse bezien vanuit de accountant

De overgang naar meer geautomatiseerde beheersingsmaatregelen is ingegeven vanuit diverse trends uit de business. In deze paragraaf zal kort op een aantal van deze trends, namelijk de controletransformatie, de controlerationalisatie en de risicoaanpak, worden ingegaan.

Controletransformatie, -rationalisatie en de Business Case

De controletransformatie van detectieve manuele controles naar preventieve applicatiecontroles is ingegeven door de wens om de hoge interne en externe inspanning bij en dus kosten die gepaard gaan met het testen van detectieve manuele beheersingsmaatregelen te verlagen. Preventieve maatregelen hebben een sterkere invloed op de beheersing (geen correctieve acties nodig) en preventieve applicatiecontroles hoeven slechts éénmaal getest te worden om het bestaan en de werking van de controles aan te tonen en daarmee te voldoen aan de richtlijn van de externe auditor, mits er sprake is van adequate algemene computercontroles. Zowel de wens om de efficiency van de bedrijfsprocessen te verbeteren als de behoefte van organisaties aan het reduceren van kosten en energie om te voldoen aan alle wet- en regelgeving, leidt ertoe dat er een verplaatsing ontstaat van manueel detectieve controles naar automatische preventieve controles ([Brou06]).

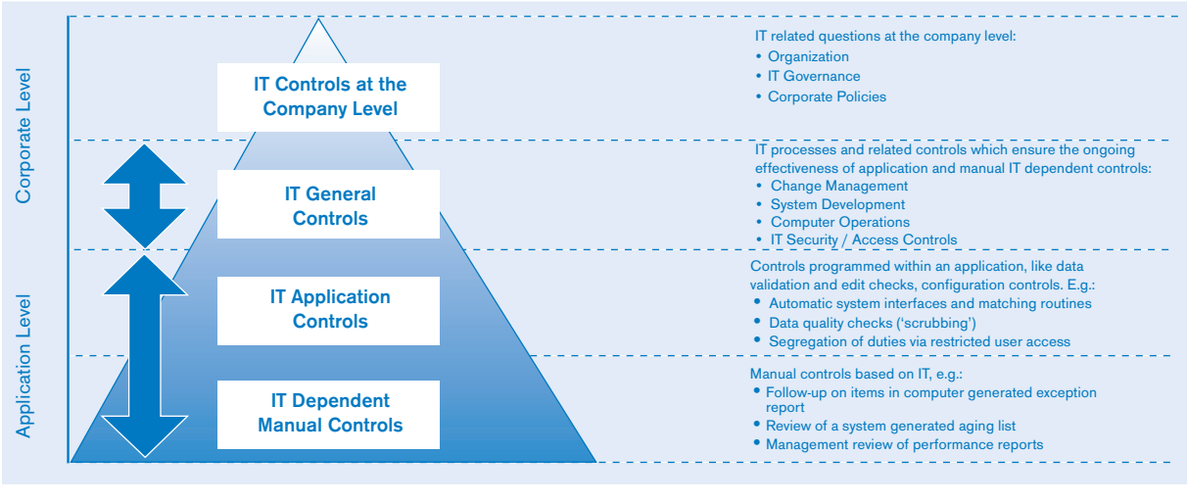
Naast de al genoemde controletransformatie zien we ook een sterke wens om niet alleen de aard van de controle te wijzigen, maar ook om het aantal controles te beperken. Deze trend wordt ook wel controlerationalisatie genoemd. De controlerationalisatie is ingestoken vanuit de bedrijven om nogmaals kritisch naar hun bedrijfsprocessen te kijken en niet alleen de kwaliteit (controletransformatie), maar ook de kwantiteit van de belangrijkste controles (controlerationalisatie) aan te pakken. Het rationaliseren van de controles wordt tevens ondersteund vanuit de transformatiegedachte waarbij meerdere manuele controles worden vervangen door bijvoorbeeld één applicatiecontrole. Een voorbeeld hiervan is een aantal klanten waar een project met de naam ‘Kill Excel’ is gestart om Excel te verbannen en alle calculaties, reconciliaties niet extracomptabel maar binnen de systemen te laten uitvoeren. Bijkomend voordeel is dat de beheersingsmaatregelen voor end user computing hierdoor vervallen, hetgeen dus tot minder beheersingsmaatregelen leidt.

Waartoe de controletransformatie en -rationalisatie uiteindelijk kan leiden, wordt kort uiteengezet in de ‘Business Case voor Application Controls’ ([ITGI06]). Als indicatief voorbeeld is een organisatie genomen die vijfhonderd controles voor SOx dient te implementeren waarbij een vergelijking tussen een manuele en applicatiecontroleaanpak is gemaakt.

Ondanks dat het documenteren van applicatiecontroles meer tijd in beslag kan nemen vanwege de complexiteit van de omgeving, bedraagt de besparing in het eerste

Tabel 1. Vergelijking van een applicatieve controleaanpak met een manuele controleaanpak ([ITGI06]).

	Manual Control Approach	Automated Control Approach
Total Controls	500	500
Effort to document per control	1 hour	3 hours
Total effort to document	500 hours	1.500 hours
Average sample size per control	10	1
Total sample items to test	5000	500
Effort to test per sample	30 minutes	30 minutes
Total effort to test	2.500 hours	250 hours
Total effort	3.000 hours	1.750 hours



Figuur 1. IT-controleraamwerk.

jaar toch al 1.250 uur (total effort manual – total effort automated). Indien we 'sustained compliance' beschouwen over een periode van vijf jaar bedraagt de besparing al 10.250 uur (4 × 2.250, het jaarlijkse verschil in total effort to test + 1.250 het verschil in total effort van het eerste jaar). De besparing over vijf jaar bezien bedraagt dan 13.000 (total effort manual) – 2.750 (total effort automated) is 10.250 oftewel 79% van 13.000. Gezien het feit dat applicatiecontroles over het algemeen gesproken betrouwbaarder kunnen zijn in hun werking, zijn de voordelen, zeker ook vanuit de risicogedachte nog groter, aangezien indien de betrouwbaarheid van de werking van de controle toeneemt, het risico op het niet werken van de controle afneemt.

Risicogedachte

De controletransformatie- en -rationalisatie-initiatieven van ondernemingen dienen beide vanuit een risicobenadering te worden geëvalueerd door de accountant. Belangrijkste doel van de accountant is het verlagen van het accountantscontrolerisico, aangezien het uiteindelijke doel het verstrekken van een (goedkeurende) verklaring bij de jaarrekening is (ook al zijn compliance en kostenreductie in de praktijk ook sterke drijfveren).

Met het toepassen van de risicoanalyse als controlebenadering komt de accountant tot een efficiënt en effectief ontworpen geheel van controlewerkzaamheden. De aard en omvang van deze controlewerkzaamheden is de resultante van de inschatting van de kans op fouten en omissies in de jaarrekening. De inschatting ten aanzien van fouten en omissies in de jaarrekening valt uiteen in een kans op onvolkomenheden voor en na de corrigerende werking van de interne beheersingsmaatregelen. Het eerste wordt aangeduid als inherent risico (IR)[1], het tweede als het internecontrolerisico (ICR)[2]. Uitgaande van het door de accountant aanvaarde accountantscontrolerisico[3], wordt op basis van het ingeschatte inherente risico en het internecontrolerisico het toegestane ontdekkingsrisico[4] bepaald en worden de uit te voeren gegevensgerichte controlewerkzaamheden geïdentificeerd.

De mate van automatisering heeft gevolgen voor de concrete invulling van de controlewerkzaamheden. Een geautomatiseerde controleomgeving heeft namelijk een belangrijke invloed op de inschatting van de hiervoor vermelde risico's. De accountant zal het uitvoeren van de controlewerkzaamheden aanpassen aan de mate waarin de controleomgeving is geautomatiseerd en rekening houden met de daarin opgenomen (geautomatiseerde) procedures en beheersingsmaatregelen.

Meer en meer gebruik van geautomatiseerde controles kan resulteren in een verlaging van het internecontrolerisico en het accountantscontrolerisico. Het woord 'kan' is hier gekozen aangezien de voorwaarde is dat de controle goed geprogrammeerd is en de ITGC ten aanzien van toegangscontrole en wijzigingsbeheer op orde zijn. De betrouwbaarheid en de effectiviteit van de controle moeten dan ook vastgesteld zijn. Een betrouwbare geprogrammeerde controle is veelal efficiënter en vereist minder interne en externe inspanning. Geautomatiseerde controles zijn er in verschillende soorten en de verschijningsvorm kan per applicatie heel verschillend zijn. Toch blijken in de kern de applicatiecontroles veel gelijkenis met elkaar te vertonen en zijn zij in een beperkt aantal basistypen in te delen waarbij ook voor het testen van dezelfde technieken gebruik kan worden gemaakt. Voor we het testen van de applicatiecontroles gaan behandelen zetten we eerst de verschillende soorten en hun kenmerken uiteen.

Soorten en testen van applicatiecontroles

Soorten applicatiecontroles

Kenmerk van een geautomatiseerde controle (applicatiecontrole) is dat de controle in de programmatuur is vastgelegd zodat ze consequent wordt uitgevoerd. In essentie betreft het vaak het berekenen en/of vergelij-

1) Definitie inherent risico: het risico dat materiële onjuistheden in de verantwoording optreden, afgezien van het effect van bestaande interne beheersingssystemen.

2) Definitie internecontrolerisico: het risico dat materiële onjuistheden niet of niet tijdig door de interne beheersingsmaatregelen worden voorkomen, dan wel niet of niet tijdig worden gesignaleerd en gecorrigeerd.

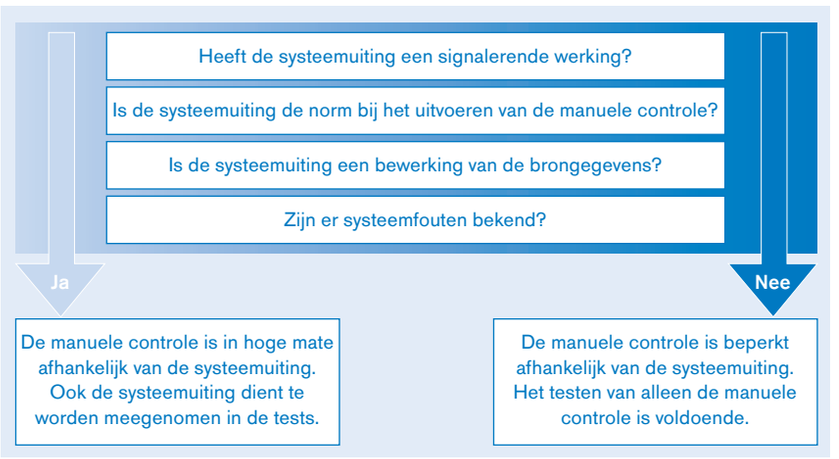
3) Definitie accountantscontrolerisico: het risico dat de accountant, ondanks zorgvuldige uitvoering van zijn controleprogramma, onbewust een onjuiste verklaring afgeeft bij een verantwoording die onvolkomenheden van materieel belang bevat.

4) Definitie ontdekkingsrisico: het risico dat materiële onjuistheden noch door de interne beheersing noch door de accountant worden gesignaleerd en gecorrigeerd.

ken van gegevens ([Fijn06]). Hoewel we vaak onderscheid maken tussen manuele controles en applicatiecontroles is er nog een 'tussen'categorie, de IT Dependent Manual Control, ofwel de IT-afhankelijke manuele controles, die karaktereigenschappen hebben van zowel de handmatige controle als de applicatiecontrole. Om de applicatiecontroles en IT-afhankelijke manuele controles in het IT-controleraamwerk te plaatsen verwijzen we naar figuur 1. Een IT-afhankelijke manuele controle is een manuele controle die enerzijds bestaat uit een puur handmatige handeling en anderzijds uit een geautomatiseerde handeling die leidt tot een systeemuiting, bijvoorbeeld uitvoer van één of meer applicatie(s) op een lijst of scherm. Of de IT-component getest moet worden, het is ten slotte primair een manuele controle, wordt bepaald door de afhankelijkheid van de manuele controle van de (geautomatiseerde) systeemuiting. Figuur 2 kan daarbij als hulpmiddel dienen om de mate van afhankelijkheid van IT te evalueren.

De afhankelijkheid wordt bepaald aan de hand van een viertal vragen:
- Heeft de systeemuiting een *signalerende* werking (verschillenlijsten, betalingen boven een bepaalde grens, bedragen boven een limiet, etc.) of is het rapport slechts een presentatie van gegevens uit een systeem?
- In hoeverre steunt de medewerker op de systeemuiting, is deze leidend bij het uitvoeren van de controle?
- Betreft het een een-op-een presentatie van gegevens of vinden er bewerkingen op de data plaats?
- Zijn er problemen bekend inzake de juistheid en volledigheid van de controle?

Het gaat om het totaalbeeld en de mate van afhankelijkheid wordt bepaald op basis van professional judgment. Bij weinig afhankelijkheid zal alleen het handmatige deel worden beoordeeld, bij veel afhankelijkheid zal ook de betrouwbaarheid van het geautomatiseerde deel moeten worden beoordeeld; je kunt ook zeggen dat bij grote afhankelijkheid de controle kan worden gesplitst in een manuele controle en een applicatiecontrole ([Gils06]). In dit artikel worden de volgende basistypen applicatiecontroles onderscheiden die in de subparagraaf 'Testen van applicatiecontroles' nader zullen worden toegelicht:
- *Toegangscontroles:* controles die waarborgen dat alleen die personen toegang krijgen die vanuit hun functie daartoe zijn geautoriseerd (exclusiviteit).
- *Applicatieconfiguratiecontroles:* controles die worden geëffectueerd door middel van het gebruik van instellingen, parameters en tabellen en daarmee de betrouwbaarheid van transacties waarborgen.
- *Fouten- en uitzonderingsrapportages:* rapportages die afwijkingen ten opzichte van een vooraf gedefinieerde norm signaleren en daarmee de juistheid van transacties waarborgen.
- *Geprogrammeerde controles:* controles, opgenomen in de programmatuur, die onder andere de invoer valideren op een vooraf gedefinieerde norm en de integriteit en controleerbaarheid van transacties waarborgen.
- *Aansluiting/verband-controles:* controles die de volledigheid van een transactie/verwerking waarborgen;
- *Interfaces:* controles die een juiste, tijdige en volledige overdracht van gegevens waarborgen.



Figuur 2. Bepalen van de afhankelijkheid van de manuele controle van de IT-controle.

Continue werking van applicatiecontroles

Naast het constateren van de feitelijke werking van de applicatiecontrole op het moment van testen wil de accountant ook een uitspraak over de continue werking van de applicatiecontrole, zodat de accountant daadwerkelijk kan steunen op de applicatiecontrole als interne beheersingsmaatregel. Bij de uitvoering van een integrated audit (SOx 404 en Financial Statement) is het verplicht om een systeemgerichte controleaanpak te hanteren. De algemene IT-beheersingsmaatregelen zijn derhalve onderwerp van onderzoek zodra de accountant steunt op beheersingsmaatregelen uitgevoerd door een applicatie en/of zodra de accountant gebruikmaakt van rapporten uit een IT-applicatie. Als blijkt dat de werking van een relevant deel van de ITGC ontoereikend is ('ineffective'), dan kan niet zomaar worden aangenomen dat de applicatiecontrole effectief werkt, ondanks dat deze tijdens een acceptatietest geaccordeerd is en getest. Bij ontoereikende ITGC kunnen de controles bewust of onbewust zonder te testen worden veranderd.

Redelijke zekerheid van de continue werking van applicatiecontroles dient te worden verkregen door de ITGC te testen. Ten aanzien van het effectief werken van geautomatiseerde controles ligt bij ITGC de focus op:
- *Change management:* kunnen zich wijzigingen in de applicatie voordoen die een impact hebben op de applicatiecontrole en is na de wijziging de applicatiecontrole getest op een juiste werking.
- *Autorisaties:* kunnen medewerkers de gewenste functiescheidingen omzeilen.
- *Datawijzigingen:* kunnen er directe datawijzigingen op de database worden uitgevoerd die niet volgens de

normale processen lopen en waarbij de beheersingsmaatregelen worden omzeild?

Hoe evalueren we de ITGC? Tekortkomingen in de ITGC (kunnen) leiden tot aandachtspunten in de management letter, maar leiden niet direct tot misstatements. Belangrijk hierbij is vooral de relatie tot de applicatiecontroles. Een ineffectieve applicatiecontrole kan direct leiden tot een misstatement. Kan de accountant nog wel steunen op de applicatiecontrole bij onvoldoende beheersing van ITGC? Het antwoord is in principe nee. In de praktijk zien we echter dat juist door overleg tussen de accountant en de IT Advisory-medewerker (of beoordelaar van ITGC) de daadwerkelijke risico's kunnen worden vastgesteld en gezamenlijk alternatieven worden bedacht om deze risico's te evalueren. Essentieel hierbij is om vast te stellen of een theoretische mogelijkheid van het zich voordoen van het risico op basis van het ontbreken van de continue werking van de beheersingsmaatregel zich ook daadwerkelijk heeft voorgedaan.

Testen van applicatiecontroles

Het testen van applicatiecontroles kan zeer verschillend zijn en is afhankelijk van de aard, timing en mate van testen. Tests kunnen worden uitgevoerd door het gebruik van de onderstaande testtechnieken:

- trial and error (falsificatie), bij voorkeur in de testomgeving (gelijk aan de productie) met testscripts;
- verificatie van systeeminstellingen, tabellen en parameters (configuraties);
- evaluatie van Gebruikers Acceptatie Test (GAT) indien deze in het jaar van de controle heeft plaatsgevonden of het zelf uitvoeren van een gebruikersacceptatietest (in de testomgeving);
- evaluatie van autorisatielijsten;
- re-performance van de beheersingsmaatregel, reconciliaties door het evalueren van data, bijvoorbeeld met behulp van auditsoftware zoals IDEA (specifiek voor pakket of generiek).

In de praktijk blijkt dat ten aanzien van de invulling van het testen van applicatiecontroles nog een verbetering dient te worden aangebracht ([Beug06]). Een handreiking daartoe zullen we in de nu volgende subparagrafen geven. Allereerst gaan we wat dieper in op de hierboven genoemde testtechnieken en vervolgens gebruiken we deze testtechnieken om de verschillende soorten applicatiecontroles te testen.

De testtechnieken nader bekeken

Falsificatie

Het testen door middel van trial and error (ook wel falsificatie genoemd) is vooral te gebruiken voor validatiecontroles, zoals geprogrammeerde controles, toegangscontroles en configuratie-instellingen, dus daar waar een norm wordt vergeleken met een invoerwaarde van de gebruiker. Een veelvoorkomende key control bij klanten is de functiescheiding tussen de invoer en goedkeuring van een transactie. De gebruiker die een transactie (betalingsverzoek) heeft ingevoerd mag niet tevens de betaling goedkeuren. Deze controle dient bij voorkeur in een aan de productieomgeving gelijk zijnde testomgeving te worden getest met betalingsvoorstellen. Let wel:

- Betreft het een controle op basis van een toegekende autorisatierol, controleer dan of er geen medewerkers zijn die beide rollen (invoer en acceptatie) hebben, of zichzelf deze rol kunnen toekennen.
- Betreft het een controle op user-id, dus onafhankelijk van het profiel, evalueer dan of er geen gebruikers zijn met meerdere user-ids.

Een ineffectieve applicatiecontrole kan direct leiden tot een misstatement

Een ander voorbeeld is het testen van een kredietlimiet, dus het testen van een goede werking van de geprogrammeerde limiet ('checkt het systeem daadwerkelijk altijd op kredietlimieten'). Hierbij kan men gezamenlijk met de gebruiker een limiet opvoeren die buiten diens rechten ligt en vervolgens testen of het systeem blokkeert en de gebruiker een melding geeft.

Verificatie van systeeminstellingen

Applicaties maken veelal gebruik van tabellen (ook wel stuurtabellen genoemd) en instellingen. Een voorbeeld dat we in de praktijk veelvuldig zien zijn productafhankelijke parameters. We zien deze bijvoorbeeld bij leasemaatschappijen, krediet/hypotheekverstrekkers maar ook bij groothandelsbedrijven. Het testen van deze controles is omvangrijk, aangezien er gewoonweg veel mogelijkheden zijn, en vooraf dient dan ook te worden bepaald (in samenspraak met de accountant) welke controles dienen te worden getest. Deze controles kunnen jaarlijks rouleren. Van belang is hierbij tevens wie de 'eigenaar' van de instellingen is en welke procedure wordt gehanteerd voor wijzigingen in de instellingen (ITGC). Let wel! Indien het beveiligingsinstellingen betreft dient de security officer te worden geconsulteerd. Onderstaand een aantal voorbeelden van verificatie van instellingen ter indicatie. Het betreft de evaluatie van:

- de limietbedragen in een tabel per functieniveau of per rol (dus: klopt de tabel met limieten per functieniveau of rol) of zelfs per product (dus: geldt de tabel voor alle producten);
- de renteberekening (gebruikt het systeem de juiste rente bij het juiste product);
- het kredietadvies door het systeem op basis van de gegevens van de kredietaanvrager (klopt het kredietadvies met de interne richtlijnen en de ingestelde parameters);

• de logging (logt het systeem de acties van een gebruiker, staat de logging 'aan' en is deze logging leesbaar);
• de matching van twee bestanden (koppelt het systeem bijvoorbeeld de juiste transacties aan elkaar en boekt het systeem beneden een ingestelde waarde het verschil automatisch naar de juiste rekening).

Evaluatie van autorisatielijsten

Autorisatielijsten in systemen kunnen variëren van makkelijk interpreteerbaar tot totaal onleesbaar. In het laatste geval is aanvullende documentatie van de opzet essentieel. Let erop dat de lijsten uit de productieomgeving komen, compleet zijn (dus inclusief de IT-organisatie) en recent. Naast de evaluatie van de autorisatielijst binnen één systeem dient er, indien er meerdere systemen zijn, ook een evaluatie over de systemen heen te zijn. Een bekend voorbeeld hierbij is de scheiding tussen frontoffice- en backofficesystemen. Binnen één applicatie kan de functiescheiding zijn gewaarborgd, echter indien de autorisaties van twee systemen worden gecombineerd niet. Mogelijke evaluaties van autorisatielijsten zijn:
• een goede koppeling van personen aan de rollen (dus: bevat de autorisatietabel de goede personen per functieniveau of rol);
• essentiële functiescheiding tussen vooraf met de accountant opgestelde kritieke rollen en functies, zoals aanmaken leverancier, invoeren facturen en autoriseren uitbetaling van facturen.

Bij wijzigingen in beveiligingsinstellingen dient de security officer te worden geconsulteerd

Voor een efficiënte en effectieve controle kan, zeker indien het grote bestanden en een combinatie van veel applicaties betreft, gebruik worden gemaakt van bestandsanalysetools zoals IDEA. Door middel van IDEA kunnen grote bestanden worden ingelezen en geanalyseerd. Tevens kan, door het bouwen van een script, de controle eenvoudig periodiek worden herhaald!

Gebruikersacceptatietest

Veel klanten incorporeren het testen van applicatiecontroles (bijvoorbeeld relevant in het kader van SOx 404) in gebruikersacceptatietests na het installeren van een nieuwe release en/of het in productie nemen van een wijziging. De auditor kan door een review uit te voeren op de hierbij vastgelegde documentatie zich een oordeel vormen van de controleomgeving en de werking van de controle. Let wel, in een aantal gevallen kan het noodzakelijk zijn dat de auditor zelf testwaarnemingen uitvoert dan wel bijwoont. In dat geval kan de auditor gezamenlijk met de klant de gebruikersacceptatietest uitvoeren.

Re-performance van de beheersingsmaatregel, reconciliatie

Indien grote hoeveelheden data nodig zijn voor het re-performen van een beheersingsmaatregel en/of het uitvoeren van een aansluiting kan de auditor gebruikmaken van hulpmiddelen. Computer Assisted Audit Techniques (verder CAAT's) zijn manieren waarop de auditor de computer gebruikt in een IT-omgeving om audit evidence te verzamelen en evalueren. Voorbeelden van CAAT's zijn Excel, een ingebouwde auditmodule, IDEA en ACL. Door het gebruik van de auditsoftware kan de auditor zeer gericht een beheersingsmaatregel controleren. Voorbeelden van het re-performen van controles zijn:
• het matchen van gegevens uit twee bronbestanden ter controle op een juiste en volledige matching;
• het zelf uitvoeren van een aansluiting op basis van bronbestanden ter controle op de reconciliatietools;
• het evalueren van een logbestand om vast te stellen of de invoerder van een transactie in alle gevallen afweek van de medewerker die de transactie autoriseerde;
• het evalueren van transacties boven een gestelde limiet in het systeem, waarbij indien het een gebruikerscontrole betreft de accountant gericht de transacties kan selecteren en kan controleren of de procedure hiervoor juist is gevolgd;
• het evalueren of de situatie die zich theoretisch kan hebben voorgedaan door het ontbreken dan wel niet werken van een controle, zich ook daadwerkelijk heeft voorgedaan. Bijvoorbeeld het evalueren van een logbestand om vast te stellen of functiescheiding daadwerkelijk is doorbroken.

Het testen van een applicatiecontrole beperkt zich niet tot het gebruik van één van de mogelijke testtechnieken. Voor het testen en om de effectieve werking van een applicatiecontrole vast te stellen dienen vaak meerdere aspecten te worden bekeken. Zoals uit bovenstaande voorbeelden ook blijkt kan bijvoorbeeld het testen van de effectieve werking van een kredietlimiet worden uitgevoerd met behulp van een combinatie van falsificatie, een evaluatie van autorisatielijsten en een evaluatie van de configuratie-instellingen.

Het testen van de verschillende soorten applicatiecontroles

In de hiernavolgende tabellen doen wij een handreiking voor het documenteren en testen van de diverse applicatiecontroles. In de tabel 'Testen applicatiecontroles' hebben we per basistype applicatiecontrole de stappen voor het uitvoeren van de test en enkele voorbeelden/activiteiten per stap opgenomen. Als eerste stap voor het testen van een controle stellen we de SOLL-situatie vast als meetlat waartegen we testen en

om vast te stellen of de controle in opzet aanwezig is. De tweede stap beschrijft het vaststellen van de IST-situatie om zodoende het bestaan van de controle aan te tonen. Idealiter willen we vervolgens SOLL en IST met elkaar vergelijken, echter in niet alle gevallen zal dit mogelijk zijn, en testen we de controle op werking door het gebruik van de eerdergenoemde testtechnieken. Indien de conclusie van de test is dat de controle effectief werkt en we kunnen steunen op de ITGC, zijn er geen verdere activiteiten nodig en wordt het risico door de beheersingsmaatregel afgedekt. Indien de controle niet aanwezig is of het risico niet volledig afdekt, heeft dit implicaties voor de accountant, aangezien er de mogelijkheid bestaat op een misstatement. De laatste actie is dan ook het in samenspraak met de accountant vaststellen van het daadwerkelijke risico (kans dat het ook plaatsvindt) en op basis van deze risicoanalyse het eventueel uitvoeren van additionele controlewerkzaamheden om zo alsnog het risico af te dekken. De voorbeelden zoals opgenomen in de tabellen zijn bedoeld ter indicatie en hebben niet de bedoeling om volledigheid na te streven.

Toegangscontrole

Logische toegangsbeveiliging is het meest gebruikte instrument om functiescheiding in applicaties af te dwingen. De kracht is afhankelijk van de kwaliteit van de programmatuur die de toegangsbeveiliging moet afdwingen, instellingen als wachtwoordlengte, etc. en natuurlijk de profielen die in de autorisatietabellen zijn opgenomen. De essentie van de autorisatiecontrole is dat het systeem per transactie vergelijkt of de gebruiker gerechtigd is om die transactie uit te voeren. Autorisatiecontroles zijn controles die zich richten op het waarborgen van de exclusiviteit van de transactie. Exclusiviteit refereert aan de beperking van de bevoegdheid en mogelijkheid tot het uitvoeren/wijzigen van transacties en/of uitvoeren van acties. In de tabel hebben we een splitsing gemaakt in Functiescheiding en Logische toegangsbeveiliging; alhoewel ze beide de toegangscontrole beslaan, worden ze apart getest en geëvalueerd.

Applicatieconfiguratiecontroles

Applicaties hebben veelal de mogelijkheid de werking van de procesgang te sturen met behulp van instellingen, parameters en tabellen. Samenvattend ook wel de configuratie (inrichting) van het systeem genoemd. Van belang is dat de parameters zodanige waarden bevatten dat de controledoelstellingen ten aanzien van de processen worden gehaald. Voorbeelden van interne richtlijnen en beleidsregels zijn:

Basistype	SOLL (Opzet)	IST (Bestaan)	Testen (Werking)	Implicatie voor de accountant	Aanvullende tests
Functie-scheiding	Stel vast dat belangrijke controletechnische functiescheiding (bijvoorbeeld aanmaken leverancier en inboeken aankoopfactuur) in opzet aanwezig is door middel van een evaluatie van de actuele en door het management geautoriseerde competentietabel. Indien SOLL niet aanwezig is, stel gezamenlijk met de klant en accountant de kritieke functiescheiding op (gewenste SOLL). Verzoek om systeemdocumentatie en krijg door middel van evaluatie en eventueel een interview inzicht in de mogelijkheden van autorisatie-inrichting van het betreffende systeem.	Beoordeel of de autorisatietabel daadwerkelijk uit het computersysteem komt, en actueel, volledig en leesbaar is.	Sluit zelf SOLL en IST met elkaar aan voor de functies waarvoor de functiescheiding belangrijk is (data-analyse door middel van IDEA kan hierbij zeer effectief en efficiënt werken). Evalueer de autorisatietabel op bijzonderheden zoals functionarissen van andere afdelingen (zoals automatiseerders en 'super-users'). Indien geen SOLL -situatie aanwezig is, evalueer of de kritieke functiescheiding zoals gezamenlijk opgesteld aanwezig is. Stel werking van de functiescheiding vast door transacties in te voeren met user accounts die daartoe eigenlijk niet in staat zouden moeten zijn (bij voorkeur in de gebruikerstest-omgeving die identiek is aan de productieomgeving).	Bij te ruime bevoegdheden is het risico aanwezig dat transacties door onbevoegden zijn doorgevoerd. Let wel, het risico is aanwezig, het is afhankelijk van de risicoanalyse welke conclusies te trekken zijn. Overwegingen daarbij zijn: - 'super-users' en IT-mensen hebben ruime bevoegdheden; - mate van impact van eventuele ongeautoriseerde transacties voor de betrouwbaarheid van de jaarrekeningcontrole. Indien de impact groot kan zijn, zonder dat het snel zou opvallen, is de ernst van de tekortkoming groot. Feitelijk kan niet gesteund worden op de applicatiecontrole en dient aanvullend getest te worden. De accountant zal tevens proberen 'overall' mitigating controls te identificeren en te testen.	Indien een autorisatietabel niet leesbaar/aanwezig is, kunnen gegevensgerichte werkzaamheden uitgevoerd worden (bijvoorbeeld door met behulp van een steekproef autorisatie achteraf te controleren in combinatie met een juiste verwerking van mutaties). Een mogelijkheid is tevens om transacties in te voeren met user accounts die daartoe eigenlijk niet in staat zouden moeten zijn. (Let wel: voorkomen dient te worden dat ongeautoriseerde transacties in het systeem terechtkomen.) Te ruime bevoegdheden van bepaalde medewerkers zijn niet terug te draaien; overweeg na te gaan of die user-id's überhaupt wel gebruikt zijn in de te onderzoeken periode. Een mogelijkheid is hierbij de inzet van IDEA (hetgeen wel een toegankelijke logging vereist) en het uitvoeren van een analyse op de user-ids. De accountant kan verder uitvoerig gegevensgerichte werkzaamheden uitvoeren en rekening houden met de organisatiestructuur. De accountant neemt het gehele plaatje van organisatie(-inrichting), processen en controles in ogenschouw.

Basistype	SOLL (Opzet)	IST (Bestaan)	Testen (Werking)	Implicatie voor de accountant	Aanvullende tests
Logische toegangs-beveiliging	Stel vast dat de beveiligingsinstellingen (o.a. de lengte van het wachtwoord, wijzigings-historie of syntaxis van het wachtwoord): - zijn opgesteld en geaccordeerd door het juiste manage-mentniveau; - zijn afgeleid van het IT-beveiligingsbeleid/ informatiebeveiligings-beleid; - voldoen aan eventueel beschikbare security baselines.	Beoordeel of de lijst met systeem-waarden daad-werkelijk uit het computersysteem komt. Stel vast dat de systeemwaarden actueel en volledig zijn en periodiek worden geëvalu-eerd.	Sluit de SOLL-lijst met de IST-lijst uit de applicatie aan (voor de waarden die betrekking hebben op de beveiliging). Beoordeel of een periodieke evaluatie heeft plaatsgevonden tussen SOLL en IST door de daartoe bevoegde personen. Indien geen SOLL aanwezig, evalueer IST met algemeen aanvaarde baselines. Stel door middel van falsificatie van een aselecte steekproef van instellingen vast dat de controle werkt (bijvoorbeeld dat het systeem aangeeft dat een wachtwoord niet aan bepaalde eisen voldoet na het invoeren van een bewust foutief wachtwoord). Stel vast of het mogelijk is door middel van een steekproef een aantal mogelijke instellingen inzake de beveiliging van de applicatie te evalueren door middel van waarnemingen ter plaatse op het scherm van bijvoorbeeld de applicatie-beheerder.	Voor de verwerking van de transactie levert dit geen specifiek risico op voor de controledoelstellingen van de accountant (zijnde juistheid, volledigheid, bestaan, waarde-ring, etc.). Wel zal de accountant een advies kunnen uitbrengen aan de klant gerelateerd aan het belang van continuïteit en integriteit van verwerking van transacties/mutaties.	Een aantal (legacy) systemen biedt (zeer) beperkte mogelijkhe-den voor het inrichten van de beveiliging van applicaties. Aanpassing van deze systemen kan (economisch) niet wenselijk worden geacht met inachtneming van het risico dat wordt gelopen. Beoordeel of het management op basis van een risicoanalyse de risico's gekoppeld aan de niet-gerealiseerde instellingen heeft aanvaard en beoordeel mogelijke aanvullende maatregelen die het management heeft genomen om een afdoende niveau van beveiliging toch te kunnen waarborgen.

- het boekingsschema;
- calculatieregels (interestcalculaties, voortijdige beëindiging vergoedingen);
- signaleringen van overschrijdingen (bijvoorbeeld op limieten of kortingen);
- instellingen die van toepassing zijn op de gehele applicatie (zoals geldigheidsduur van offertes, maxi-male limieten).

Configuratiecontroles, afhankelijk van de soorten instellingen, parameters en tabellen, zijn controles die zich richten op het waarborgen van de juistheid en vol-ledigheid (betrouwbaarheid) van de transacties. Veelal richten deze controles zich ook op bedrijfsrisico's naast de financial statement risico's.

Fouten- en uitzonderingsrapportages

Fouten- en uitzonderingsrapportages zijn controles die zich richten op het waarborgen van de juistheid van de transacties. Fouten- en uitzonderingsrapportages zijn nauw gerelateerd aan de configuratiecontroles. Het niet voldoen aan interne richtlijnen, beleidsregels en/ of geprogrammeerde controles dient te worden gesig-naleerd in de applicatie. Ter ondersteuning van deze signalering worden controlerapporten, uitzonderings-rapporten gedefinieerd. Ter illustratie enkele voorbeel-den van dergelijke rapportages:

- een afwijking van een interne richtlijn (een lijst met hypotheken met 0% rente);
- een batchcontrole (een lijst met facturen zonder fac-tuuradres);
- verschillenlijst (verschillen tussen de investerings-waarde en de inkoopfactuur);
- foutieve aanlogpogingen (lijst met medewerkers die meer dan drie keer een fout wachtwoord hebben inge-geven).

Ter identificatie van deze fouten en uitzonderingen zijn periodieke rapportages opgesteld of ingeregeld in een job scheduler die deze fouten en uitzonderingen aan een gebruiker kan rapporteren (IT dependent manual controls). Fouten- en uitzonderingsrapportages worden ook vaak gehanteerd als detectiecontrole, indien pre-ventieve (geprogrammeerde) controles niet mogelijk blijken.

Geprogrammeerde controles

Geprogrammeerde controles zijn applicatiecontroles die zich richten op de kwaliteitsaspecten integriteit (juistheid, volledigheid, tijdigheid) en controleerbaar-heid van de bewerkte gegevens in een bepaald proces. De controles zijn gericht op het vergelijken van een gegeven met een norm en worden bij afwijking gevolgd

Basistype	SOLL (Opzet)	IST (Bestaan)	Testen (Werking)	Implicatie voor de accountant	Aanvullende tests
Configuratie	Stel vast dat de organisatie interne richtlijnen en beleidsregels heeft opgesteld en dat deze geautoriseerd zijn door het juiste managementniveau. Stel vast dat de interne richtlijnen en beleidsregels zijn vertaald naar instellingen, parameters voor de applicatie (bijvoorbeeld de instelling van een kredietlimiet).	Beoordeel of de lijst met instellingen daadwerkelijk uit het computersysteem komt. Stel vast welke parameters relevant zijn en dat deze op het overzicht staan vermeld. Stel vast dat de instellingen periodiek worden geëvalueerd door de business owner.	Sluit de SOLL-lijst met de IST-lijst uit de applicatie aan (alleen voor die instellingen die van belang zijn bij het onderzoek). Beoordeel of een periodieke evaluatie heeft plaatsgevonden tussen SOLL en IST door de daartoe bevoegde personen. Stel vast of het mogelijk is door middel van een steekproef en falsificatie een aantal mogelijke instellingen (bijvoorbeeld de waarden gekoppeld aan de kredietlimieten) van de applicatie te evalueren met de SOLL-situatie. Maak gebruik van Computer Assisted Audit Techniques (CAAT's).	Indien de configuraties niet overeenkomen bepaal dan het risico ten aanzien van het halen van de controledoelstelling. Bijvoorbeeld het ontbreken van limieten voor het uitvoeren van risicovolle orders. De accountant zal handmatige beheersingsmaatregelen overwegen. Daarbij dient de accountant een afweging te maken of het een business risk betreft of een financial statement risk. De accountant zal namelijk dienen vast te stellen wat er misgaat en wat dientengevolge de impact is op de relevante controledoelstellingen. Tevens zal de accountant moeten vaststellen dat adequate corrigerende controlemaatregelen zijn genomen, geïmplementeerd en dat deze effectief werken.	De accountant zal de klant vragen aan te tonen wat voor mitigerende controlemaatregelen zijn genomen alsook wat voor corrigerende maatregelen zijn uitgevoerd. De accountant zal hierop gegevensgerichte werkzaamheden uitvoeren teneinde vast te stellen dat in overeenstemming met de aard van de transacties de transacties bestaan en juist en volledig zijn verwerkt in de financiële administratie. Tevens zal de accountant als onderdeel van de gegevensgerichte werkzaamheden een uitgebreide cijferanalyse uitvoeren alsook reconciliaties.

Basistype	SOLL (Opzet)	IST (Bestaan)	Testen (Werking)	Implicatie voor de accountant	Aanvullende tests
Fouten- en uitzonderingsrapportages	Stel vast of van een rapportage: - het doel is opgesteld; - de broninformatie is gedefinieerd; - een interpretatie van de gegevens aanwezig is. Stel vast dat de opzet door het juiste lijnmanagement is goedgekeurd. Beoordeel of is vastgesteld wat als onwaarschijnlijk respectievelijk als fout wordt aangemerkt en hoe dit wordt gesignaleerd. Hierbij dient te worden vastgesteld welke toleranties per gegevenselement aanvaardbaar zijn en welke afwijkingen daarvan als onwaarschijnlijk en welke als fout moeten worden aangemerkt.	Beoordeel of de rapportage uit het computersysteem komt. Stel vast dat de rapportage volledig en actueel is (default: na een batch of bij belangrijke processen dagelijks). Stel vast of de rapportage automatisch wordt gegenereerd (ingeregeld in een job scheduler) of manueel dient te worden opgestart. Stel vast of de gebruikers worden ondersteund in hun uitvoering door het gebruik van checklists. Stel vast of de rapportage voorafgaand aan in productie name door het juiste management is goedgekeurd.	Evalueer of de uitgangspunten, benodigde informatie, formules, doelstellingen overeenkomen met de definitie van de rapportage en beoordeel of de rapportage het beoogde doel afdekt. Stel vast dat de SOLL-rapportage overeenkomt met de IST-rapportage. Overweeg om met behulp van data-analyse (auditsoftware) de rapportage gebruikmakend van een volledige set data, opnieuw op te stellen en evalueer of deze overeenkomt met de verwachtingen op basis van de selectiecriteria (re-performance). Stel via een aselecte steekproef vast dat de signaleringen op de lijst juist zijn.	Als de uitgangspunten en opzet van de rapportage niet overeenkomen met de definitie van de rapportage, wordt de doelstelling van de rapportage niet bereikt en is de controle niet effectief. Als de rapportage ernstige tekortkomingen heeft op het gebied van juistheid en volledigheid, dan is het risico aanwezig dat transacties niet conform interne richtlijnen en beleid worden uitgevoerd of dat de integriteit van de data in gevaar komt. Feitelijk kan niet gesteund worden op de rapportage en dient een andere controlemaatregel te worden geselecteerd. Belangrijk is dat de accountant te weten komt hoe deze rapporten tot stand komen als deze rapporten integraal onderdeel uitmaken van de beschreven en geïmplementeerde control.	Als het rapport het beoogde doel niet afdekt, kan worden overwogen zelf een rapportage met auditsoftware te bouwen waarbij de definitie van de rapportage waarborgt dat het doel van de controlemaatregel wordt bereikt. Als het rapport niet juist en volledig blijkt, kan worden overwogen de rapportage met auditsoftware na te bouwen en de resultaten te evalueren. Evalueer of adequate actie is ondernomen op de met behulp van het lijstwerk geïdentificeerde afwijkingen van het normale patroon.

door een signalering aan de gebruiker. Voorbeelden van geprogrammeerde controles zijn:
- formules voor berekeningen (zoals kredietlimiet, berekenen annuïteit);
- functiescheiding (afdwingen van vierogenprincipe);
- workflow;
- minimaal noodzakelijke data-invoer;
- automatische boekingen;
- (totaal-)verbandcontrole;
- logging.

De geprogrammeerde controles zijn gedefinieerd in de programmacode en kunnen alleen door een wijziging in de programmatuur worden aangepast. Zonder wijziging blijft de geprogrammeerde controle werken. Dit is tevens het onderscheid met de configuratie-instellingen, waarbij de instellingen en dus de werking van de controle zonder wijziging van programmatuur kunnen worden gewijzigd door het 'eenvoudig' wijzigen van een instelling/parameter. Geprogrammeerde controles kunnen preventief, detectief of correctief van aard zijn. Bij afwijkingen van de norm dient de gebruiker een signalering te krijgen.

Aansluiting/verband-controles

Aansluiting/verband-controles zijn controles die zich richten op het kwaliteitsaspect volledigheid. Aansluitingen (reconciliaties) worden veelal uitgevoerd als controle op de goede (ver)werking van één applicatie of ter controle op de relatie met andere applicaties. Aansluitingen hebben tot doel (periodiek) verschillen te identificeren waarna gebruikers de eventuele verschillen/fouten adequaat dienen af te handelen. De aansluitingen zijn gericht op het aansluiten van de gegevens binnen een systeem of tussen twee of meer systemen. De aansluiting kan worden uitgevoerd aan de hand van een recordtelling (telling van het aantal records), een batchtotaal (telling dat een bepaalde waarde voorkomt), een hashtotaal (optelling van een opzichzelfstaande betekenisloze waarde) of een controletotaal (optelling van waarden). Aansluitingen kunnen zowel automatisch, gescheduled of op verzoek van de gebruiker worden uitgevoerd per gewenste periodiciteit (per uur, dag, week, maand, jaar).

Voorbeelden van aansluitingscontroles zijn:
- aansluiting tussen contractadministratie en grootboek;
- aantal assets in contractadministratie versus financiële administratie;
- waarde van de ingeboekte facturen versus de waarde van de inkooporders (saldo tussenrekeningen);
- leveranciersdetails in systeem X gelijk aan leveranciersdetails in systeem Y.

Basistype	SOLL (Opzet)	IST (Bestaan)	Testen (Werking)	Implicatie voor de accountant	Aanvullende tests
Geprogrammeerde controles	Stel vast dat de organisatie technische en/of functionele documentatie van de applicatie heeft waarin de geprogrammeerde controles in kaart zijn gebracht. Stel vast dat de documentatie en/of manuals up-to-date zijn.	Stel vast dat de geprogrammeerde controles werken door: - voor de belangrijkste geprogrammeerde controles van de norm af te wijken en vast te stellen dat signalering plaatsvindt; - vast te stellen of de controle detectief, preventief of correctief van aard is; - een code review.	Beoordeel of de in opzet aanwezige geprogrammeerde controles (SOLL) overeenkomen met de geïmplementeerde geprogrammeerde controles (IST) door middel van trial and error. Beoordeel of een periodieke evaluatie heeft plaatsgevonden tussen SOLL en IST (bijvoorbeeld in het kader van compliant zijn aan SOx of andere wet- en regelgeving). Beoordeel of de geprogrammeerde controle het beoogde doel afdekt. Beoordeel via trial and error of de controle conform de opzet blokkerend is of signalerend (bij signalerend kan de gebruiker de controle overrulen). Maak gebruik van Computer Assisted Audit Techniques (CAAT's).	Als de controle het beoogde doel niet (volledig) afdekt dient het management te overwegen om aanvullende beheersingsmaatregelen op te stellen en te implementeren. Als de controle signalerend in plaats van blokkerend is, dienen aanvullende beheersingsmaatregelen te zijn geïmplementeerd (zie ook fouten- en uitzonderingsrapportages). Het gaat hierbij om een duidelijke en gedocumenteerde logging en zichtbare follow-up van geïdentificeerde afwijkingen/bijzonderheden.	Het evalueren van in welke mate afwijkingen van de norm worden gesignaleerd door fouten- en uitzonderingsrapportages. Beoordeel of de controles die kunnen worden overruled door een gebruiker, worden gesignaleerd in een fouten- en uitzonderingsrapportage. Indien ja, is dit een compenserende maatregel. Indien nee, kan er niet op deze controle worden gesteund. Aanvullend kan worden gesteld dat dan manual controls toegepast moeten worden binnen de organisatie en daarop zal de accountant dan ook testwerkzaamheden verrichten. Met behulp van een basisadministratie kan dit inzichtelijk worden gemaakt en worden extra testwerkzaamheden uitgevoerd. Aanvullende gegevensgerichte controles zullen door de accountant worden uitgevoerd zoals daar zijn: cijferanalyse, reconciliaties en detailtestwerk. In feite gaat de accountant terug naar de primaire vastlegging.

De gerealiseerde aansluitingen binnen de applicatie of tussen de applicaties kunnen op verschillende wijze zichtbaar worden gemaakt. De realisatie van een aansluiting kan direct zichtbaar zijn in het systeem of aan de hand van rapportages. In het laatste geval kunnen de aansluitingsrapportages op de volgende wijze worden verkregen:

- direct uit het systeem (in het systeem geprogrammeerde rapportage);
- met behulp van een rapporteringstool;
- extracomptabel door het samenvoegen van verschillende databronnen in bijvoorbeeld een Excel-lijst.

Het gebruik van rapportages (en tools) komt veel voor, waarbij de aansluitingen veelal IT-afhankelijke gebruikerscontroles zijn. IT-afhankelijk duidt op het aspect dat de gebruiker weliswaar de controle uitvoert, echter hiervoor steunt op de juiste opzet,

Basistype	SOLL (Opzet)	IST (Bestaan)	Testen (Werking)	Implicatie voor de accountant	Aanvullende tests
Aansluiting/ verbands-controles	Stel vast dat de organisatie een considerans heeft van de in opzet aanwezige aansluiting(en) met hierin opgenomen de bronvermelding, het doel, de risico's binnen het proces, de periodiciteit en controles omtrent de aansluiting(en). Stel vast dat de documentatie en/of manuals up to date zijn voor het realiseren van de aansluitingen. Stel vast dat controleprogramma's aanwezig zijn ter ondersteuning van het uitvoeren van de aansluitingen.	Stel vast aan de hand van de aanwezigheid van aansluitingsrapportages dat de organisatie aansluitingen als controlemiddel gebruikt om de (ver)werking van de applicatie vast te stellen. Stel vast dat de aansluitingen onderdeel uitmaken van de (dagelijkse) controlewerkzaamheden door na te gaan of deze op de werk/checklists staan vermeld.	Beoordeel of de in opzet aanwezige aansluitingen (SOLL) overeenkomen met de aansluitingen zoals die worden uitgevoerd (IST). Beoordeel of een periodieke evaluatie heeft plaatsgevonden tussen SOLL en IST (bijvoorbeeld in het kader van compliant zijn aan SOx of andere wet- en regelgeving of als onderdeel van testmanagement na een wijziging). Beoordeel of de aansluiting(en) de beoogde doel(en) afdekt(ken). Maak gebruik van Computer Assisted Audit Techniques (CAAT's).	Als de controle het beoogde doel niet (meer) afdekt dient het management te overwegen om aanvullende controles op te stellen en te implementeren. Als de controles niet periodiek worden getest op werking is er geen zekerheid over juistheid en volledigheid.	Beoordeel of het ontbreken van de (periodieke) aansluiting wordt vervangen door een overkoepelende of andere aansluiting (een mitigerende controle). Voer met behulp van de bronbestanden en data-analyse een re-performance van de aansluiting/verbandscontroles uit. Identificeer en analyseer de verschillen.

Basistype	SOLL (Opzet)	IST (Bestaan)	Testen (Werking)	Implicatie voor de accountant	Aanvullende tests
Interfaces	Stel vast dat een beschrijving van de interface(s) aanwezig is waarin is opgenomen: - het bron- en het doelsysteem; - de soort interface (manueel, batch, real-time); - de gegevens die worden overgedragen; - de controles op juistheid, volledigheid en tijdigheid in de interface; - de foutencriteria; - de aanwezigheid van fouten- en uitzonderingsrapportages. Stel vast dat de documentatie en/of manuals up-to-date zijn.	Stel vast *welke* gegevens zijn overgedragen door de interface door te controleren of: - interfaceresultaatrapporten beschikbaar zijn (vaststellen wat de interface heeft overgedragen); - totalen van gegevenstransport (batch- of hashtotalen) beschikbaar zijn van de interface; - controles zijn uitgevoerd (interfacecontrolerapporten); - ontvangstbevestigingen aanwezig zijn.	Beoordeel of de in opzet aanwezige interfaces (SOLL) overeenkomen met de aanwezige interfaces (IST). Beoordeel of een periodieke evaluatie heeft plaatsgevonden tussen SOLL en IST (bijvoorbeeld in het kader van compliant zijn aan SOx of andere wet- en regelgeving of onderdeel van testmanagement na een wijziging). Beoordeel of de interface controles bevat om de juistheid, tijdigheid en volledigheid van de gegevensoverdracht te waarborgen. Beoordeel of de controlerapporten en/of resultaatlijsten daadwerkelijk uit het computersysteem komen en volledig zijn.	Als de interface geen controles bevat inzake volledigheid, tijdigheid en juistheid van de gegevensoverdracht dienen aanvullende controles te worden opgesteld om dit te waarborgen. De accountant zal gegevensgerichte werkzaamheden moeten uitvoeren inzake het waarborgen van de volledigheid en juistheid van transacties en de gegevensoverdracht aan de hand van lijstwerk en de analyse van geconstateerde verschillen.	De resultaten van de SOLL-situatie komen niet overeen met de IST-situatie. Ga na of met auditsoftware de interface kan worden nagebouwd en re-perform de interface. Evalueer de resultaten van de test met de gegevens in het bron- en het doelsysteem na de overdracht van de gegevens via de interface. De resultaten van de SOLL-situatie komen niet overeen met de IST-situatie. Stel vast dat de instellingen van de interface overeenkomstig de SOLL-situatie zijn. Door het toepassen van een aselecte steekproef op gegevens die worden overgebracht kan door het vergelijken van de gegevens in het bron- en het doelsysteem een beperkte mate van zekerheid worden verkregen.

bestaan en werking van de gedefinieerde aansluiting/rapportage.

Interfaces

Interfacecontroles zijn controles die zich richten op de kwaliteitsaspecten integriteit (juistheid, volledigheid, tijdigheid). Een interface is een (automatische) overdracht van gegevens tussen twee of meer applicaties of tussen modules binnen één applicatie. Dit kunnen onder andere financiële, operationele en betalingsgegevens zijn. Voor het overdragen van de gegevens bestaan ruwweg de volgende drie mogelijkheden:

- manuele overdracht: applicatie X produceert een lijst die manueel wordt ingevoerd in applicatie Y;
- volledig automatische overdracht (online, real-time): applicatie Y gebruikt direct data van systeem X en/of vice versa;
- overdracht via up-/download van gegevens: applicatie X genereert een file, die wordt ingelezen in applicatie Y.

Onafhankelijk van het soort interface gaat het in alle gevallen om een overdracht van gegevens tussen twee of meer applicaties of tussen modules binnen één applicatie. Voorbeelden van interfacecontroles zijn:

- hashtotalen; voor het verkrijgen van zekerheid omtrent de juistheid en volledigheid van de invoer en uitvoer door middel van controlevergelijkingen. Bij een hashtotaal kan de controletelling gebaseerd zijn op bijvoorbeeld het optellen van alle rekeningnummers;
- ontvangst- en bevestigingsberichten.

Samenvatting

De beschreven trends alsmede ontwikkelingen als ‘sustainable compliance’ en (IT) governance maken dat steeds meer applicatiecontroles worden opgenomen in de bedrijfsprocessen. Hierdoor zal zowel de financial auditor als de IT-auditor in toenemende mate met applicatie- en IT-afhankelijke manuele controles te maken krijgen. De aard en opzet van de controle is sterk afhankelijk van de applicatie en het soort applicatiecontrole. De zes basistypen applicatiecontroles die kunnen worden onderscheiden zijn in dit artikel beschreven. Hierbij hebben we getracht een handreiking te leveren voor zowel de IT- als de financial auditor voor wat betreft het testen van de applicatiecontroles, de implicaties voor de accountant en de eventueel noodzakelijke aanvullende tests.

Literatuur

[Beug06] Mw. B. Beugelaar RE RA en drs. C.J. Visch RA, *Integrated audit: een uitdaging voor de auditor?*, Compact 2006/2.

[Brou06] Drs. P.P.M.G.G. Brouwers RE RA, drs. M.A.P. op het Veld RE en drs. ing. A.T.J. Lissone, *Tool-based monitoring en auditing van ERP-systemen, van hebbeding naar noodzaak*, Compact 2006/2.

[Fijn06] R. Fijneman, E. Roos Lindgreen en K.H. Ho, *IT-auditing en de praktijk*, juli 2006.

[Gils06] H. van Gils, *IT controls KPC*, juli 2006.

[ITGI06] IT Governance Institute, *The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting 2nd Edition*, September 2006.

[Jenk01] B. Jenkins, P. Cooke en P. Quest, *An Audit Approach to Computers*, maart 1992.