Jaarrekening controle in het mkb: IT audit geïntegreerd in de controle-aanpak

Nederlandse Beroepsorganisatie van Accountants

NBA

#TUACC

TWEETUP HERVORMING ACCOUNTANCY

NOREA

DE BEROEPSORGANISATIE VAN IT-AUDITORS

Over de auteurs

Drs. Wilco Schellevis
Wilco is partner bij Visser & Visser Accountants-Belastingadviseurs en binnen deze organisatie verantwoordelijk voor Refine-IT. Wilco is primair actief op het snijvlak van IT en accountancy. Daarnaast is hij onder meer voorzitter van de SRA IT-Auditkring.

Drs. Vera van Dijk RA
Vera is werkzaam bij BDO Accountants & Adviseurs. Vera is enkele jaren werkzaam geweest in de controlepraktijk en is daarna een staffunctie gaan bekleden. Vanuit deze rol is zij voor vaktechniek betrokken geweest bij de ontwikkeling van IT-trainingen voor accountants.

Naast bovengenoemde auteurs hebben onderstaande projectgroepleden bijdragen geleverd:

- drs. Jeroen Biekart RE RA; werkzaam bij Noordbeek en voorzitter NOREA
- drs. Evert Brouwer RA RE; werkzaam bij Twine B.V.
- Jack van Crooij EMITA Msc, werkzaam bij FullFinance
- Gideon Folkers RA; werkzaam bij Refine-IT
- Robert Johan RE; werkzaam bij Soll-IT B.V.
- drs. Erik-Jan Kreuze RA RE; werkzaam bij Afier Audit + Assurance
- Pieter Mansvelder RA; werkzaam bij Kriton
- Ted O. Mos CISA RE RI; werkzaam bij TBM Groep
- Edwin Rosier RA; werkzaam bij BDO Accountants & Adviseurs

Voorwoord

De tijden van een papieren administratie zijn voorgoed voorbij, ook in het mkb. Niet langer kan de accountant zich veroorloven zijn controle 'om de automatisering heen' uit te voeren. In de dagelijkse accountantspraktijk groeit de behoefte om IT-aspecten concreet en gestructureerd te integreren in de accountantscontrole. Accountants worstelen regelmatig met deze integratie en het blijkt vaak niet eenvoudig te zijn om IT-deskundigheid goed in te zetten in het team.

Dit rapport is primair geschreven voor accountants die zich in hun dagelijkse werk bezig houden met jaarrekeningcontroles. Het is echter ook zeer geschikt voor IT-auditors die worden ingeschakeld om, samen met de accountant, de effectieve vraagstelling en scope van een jaarrekeningcontrole te bepalen.

Doel is het bij elkaar brengen van (traditionele) accountantscontrole en IT-Audit in een Integrated Audit Approach. Dat vraagt om passende kennis. In de praktijk zullen accountant en IT-auditor in veel gevallen dus nauw samenwerken. Deze innovatieve aanpak moet de kwaliteit van accountantscontrole helpen verhogen. De accountantscontrole kan zo efficiënter en effectiever en de accountant kan beter voldoen aan de verwachtingen die het maatschappelijk verkeer heeft.

Het rapport is tot stand gekomen door een gezamenlijk initiatief van NBA, NOREA en Tuacc. Met dit initiatief richten de auteurs zich op de ontwikkeling van een IT Integrated Audit Approach. Het rapport is geschreven door een projectgroep waarin professionals - accountants en IT-auditors - op vrijwillige basis zitting hebben.

Bewust hebben we in dit rapport trends in IT en specifieke onderwerpen als cloud en cybercrime achterwege gelaten. De doelstelling van deze publicatie is het schetsen van een raamwerk voor controles in een geautomatiseerde omgeving; een methodiek die tijdsbestendiger is dan actuele trends in IT.

Dit rapport is bedoeld voor discussie. Inhoudelijke reacties en commentaren zijn welkom via het secretariaat van NOREA: norea@norea.nl.

Amsterdam, 15 april 2014

Drs. V. (Vera) van Dijk RA
Drs. W. (Wilco) Schellevis

Inhoud

	Bladzijde
Voorwoord	3
Inleiding	7
Opbouw	8
1 Voorbereiding	11
1.1 Inleiding	11
1.2 IT-omgeving op hoofdlijnen	11
1.3 Specifieke IT-aspecten bij de voorbereiding van de opdracht	12
1.4 Documentatie	15
1.5 Communicatie	15
2 Risicoanalyse en planning	17
2.1 Inleiding	17
2.2 Inzicht in de entiteiten haar omgeving, inclusief de IT-omgeving	18
2.2.1 Vervolg op de voorbereidingsfase	18
2.2.2 Inzicht in de entiteit volgens de NV COS	19
2.2.3 Het P6-model	19
2.3 Beheersingsmaatregelen	23
2.3.1 Application controls	24
2.3.2 General IT Controls	26
2.3.3 Relatie Application controls – General IT Controls	29
2.4 Risicoanalyse	30
2.4.1 Het R6-model	30
2.4.2 Uitbesteding van IT-processen, applicaties en hardware	32
2.5 Controleaanpak en planning	34
2.5.1 Controleaanpak	34
2.5.2 Controleprogramma	35
2.6 Documentatie	35
2.7 Communicatie	36
3 Interimcontrole	39
3.1 Inleiding	39
3.2 Voorbereiding van de interimcontrole	39
3.3 Uitvoeren systeemgerichte werkzaamheden gericht op key-controls	40
3.3.1 Testen van application controls	41
3.3.2 Testen van de werking van General IT Controls	43
3.4 Uitbesteding van IT processen, applicaties en hardware	47
3.4.1 Standaard 402 en de interim controle	47
3.4.2 Standaard 3402 en de interim controle	48
3.5 Documentatie	49
3.6 Communicatie	51

4 Eindejaarscontrole 53
4.1 Inleiding 53
4.2 Voorbereiding van de eindejaarscontrole 53
4.3 Uitvoeren gegevensgerichte werkzaamheden 56
4.3.1 Controlewerkzaamheden 56
4.3.2 Data-analyse 57
4.4 Documentatie 59
4.5 Communicatie 60

5 Afronding 63
5.1 Inleiding 63
5.2 Afronding 63
5.2.1 Beoordelen gebeurtenissen na de einddatum van de verslagperiode 63
5.2.2 Beoordelen continuïteit 63
5.2.3 Opvragen schriftelijke bevestigingen 64
5.2.4 Verstrekken controleverklaring 64
5.2.5 Administratieve afhandeling dossier 64
5.3 Documentatie 64
5.4 Communicatie 64

Definities & afkortingen 65

Literatuurverwijzingen 73

Bijlage 1 IT-omgeving 75

Bijlage 2 Identificatie specifieke IT aspecten o.b.v. NV COS t.a.v. de voorbereidingsfase 77

Bijlage 3 Identificatie specifieke IT aspecten o.b.v. NV COS t.a.v. de risicoanalyse en planning 80

Bijlage 4 Identificatie specifieke IT aspecten o.b.v. NV COS t.a.v. interim-controle 83

Bijlage 5 Identificatie specifieke IT aspecten o.b.v. NV COS t.a.v. eindejaarscontrole 89

Bijlage 6 Identificatie specifieke IT aspecten o.b.v. NV COS t.a.v. de afrondingsfase 95

Bijlage 7 Relatie doelstelling, application controls en General IT Controls 98

Bijlage 8 Back-up proces 113

Bijlage 9 Toepassingsmogelijkheden data-analyse per proces 117

Inleiding

Traditioneel worden de werkzaamheden van de accountant en die van de IT-auditor vaak gezien en uitgevoerd als gescheiden processen. Maar de controlestandaarden laten er geen misverstand over bestaan: financial audit en IT zijn onlosmakelijk met elkaar verbonden, als de risicoanalyse daartoe aanleiding geeft. De accountant kan niet om de IT van de onderneming heen!

In een risicogerichte controleaanpak analyseert de accountant het risico dat de jaarrekening afwijkingen van materieel belang bevat. Hij stemt daar zijn aanpak op af, door systeem- en gegevensgerichte werkzaamheden te plannen.

Via zijn systeemgerichte werkzaamheden stelt hij vast in welke mate hij gebruik kan maken van maatregelen die de onderneming zelf heeft genomen om die afwijkingen te voorkomen of te ontdekken. Afhankelijk van de uitkomst hiervan moet hij, door gegevensgerichte werkzaamheden, voldoende aanvullende zekerheid krijgen over de kwaliteit van de verantwoording.

Bij de analyse van het risico dat een verantwoording een afwijking van materieel belang bevat, moet de accountant een brede invalshoek hanteren. Omdat IT een steeds grotere rol vervult in de bedrijfsvoering en informatieverzorging, zal hij ook de aan IT-gerelateerde risico's op een afwijking van materieel belang in kaart moeten brengen.

Wat moet de accountant doen als hij in zijn controleaanpak gebruik wil maken van beheersmaatregelen die de onderneming zelf heeft getroffen? Interne beheersmaatregelen zijn tegenwoordig vaak onderdeel van de IT van de onderneming.

Geheel handmatig uitgevoerde controles ('manual controls') komen bijna niet meer voor. Wel zien we handmatige controles nog terug als onderdeel van zogeheten 'computer dependent controls'. Een groot deel van de manual controls is vervangen door 'automated controls'. Deze controls maken onderdeel uit van applicaties die de bedrijfs- en informatieprocessen ondersteunen. In een controleaanpak die steunt op de interne beheersmaatregelen van de onderneming is het daarom bijna niet meer mogelijk om de automated controls te negeren.

Ook bij zijn gegevensgerichte werkzaamheden ziet de accountant zich geconfronteerd met de IT van de onderneming. Vrijwel alle (administratieve) gegevens worden verwerkt in een of meer geautomatiseerde systemen. Voor de gegevensgerichte werkzaamheden gebruikt de accountant de vastlegging daarvan in bijvoorbeeld administraties, documenten, dossiers, contracten en specificaties. Elke afdruk of elke schermweergave van gegevens komt tot stand via een IT-toepassing.

Hoe stelt de accountant daar de betrouwbaarheid van vast? Die vraag staat in deze uitgave centraal.

Dit rapport voorziet in de praktijkbehoefte aan een heldere beschrijving hoe een geïntegreerde aanpak, waarin IT-audit en financial audit hand in hand gaan, er uit kan zien.

Opbouw

De opbouw van dit studierapport sluit aan op de fasen van het controleproces:
1. Voorbereiding
2. Risicoanalyse en planning
3. Interimcontrole
4. Eindejaarscontrole
5. Afronding

Ieder hoofdstuk kent daarbij een vaste indeling:
- Inleiding: samenhang met andere hoofdstukken en doelstelling
- Inhoudelijke uitwerking
- Aanpak documentatie
- Aanpak communicatie

Interim- en eindejaarscontrole versus systeem- en gegevensgerichte controle

Bewust is gekozen om geen onderscheid te maken tussen systeem- en gegevensgerichte werkzaamheden. In de opbouw van dit studierapport is onderscheid gemaakt tussen interimcontrole (hoofdstuk 3) en eindejaarscontrole (hoofdstuk 4). Deze opbouw sluit aan op de gebruikelijke fasen in het controleproces. In de praktijk hoeven de stappen niet altijd plaats te vinden in de geschetste volgorde of op het beschreven moment. Dit is een keuze die iedere accountant voor zich maakt. Systeemgerichte werkzaamheden zijn in dit studierapport opgenomen in hoofdstuk 3 (“Interimcontrole”) en gegevensgerichte werkzaamheden in hoofdstuk 4 (“Eindejaarscontrole”).

Plaatsbepaling opzet, bestaan en werking van automated controls

Automated controls zijn te onderscheiden in application controls (de beheersingsmaatregelen in de geautomatiseerde processen) en General IT Controls (de randvoorwaardelijke beheersingsmaatregelen). Als onderdeel van de risicoanalyse en de planning van de controle beschrijft hoofdstuk 2 (“Risicoanalyse en planning”) hoe IT verankerd is in organisaties. Daar wordt tevens uitgelegd welke application controls we onderkennen, welke General IT Controls er zijn en hoe deze zich tot elkaar verhouden. Ook wordt aangegeven welke General IT Controls belangrijk zijn voor de controle van een verantwoording en dus in aanmerking komen voor een test op hun effectieve werking. Hoe je het bestaan en de effectieve werking kunt vaststellen van de application controls en General IT Controls, wordt beschreven in hoofdstuk 3 “Interimcontrole”.

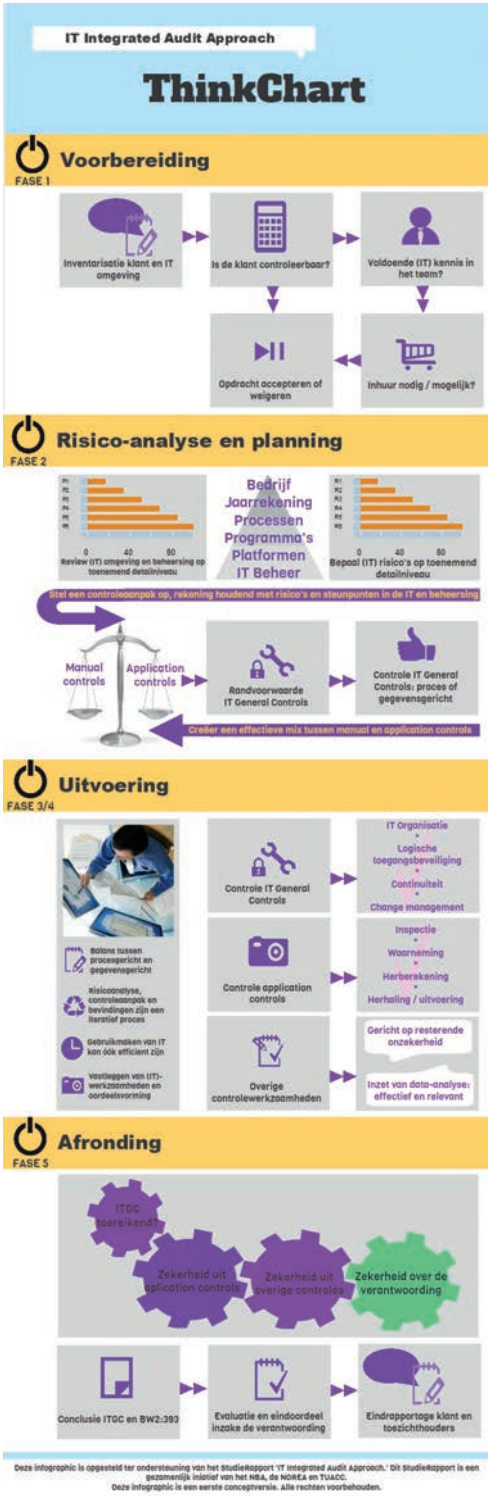
Gehanteerde symbolen

De tekst bevat veel voorbeelden en tips, te herkennen aan de volgende twee iconen:

Icoon bij een voorbeeld:

Icoon bij een tip:

Het volgende schema (de Integrated Audit +ThinkChart) geeft de samenhang weer tussen de fasen in de controle en tussen de stappen van elke fase. Het schema dient als wegwijzer voor de lezer en delen ervan komen daarom in de volgende hoofdstukken weer terug.



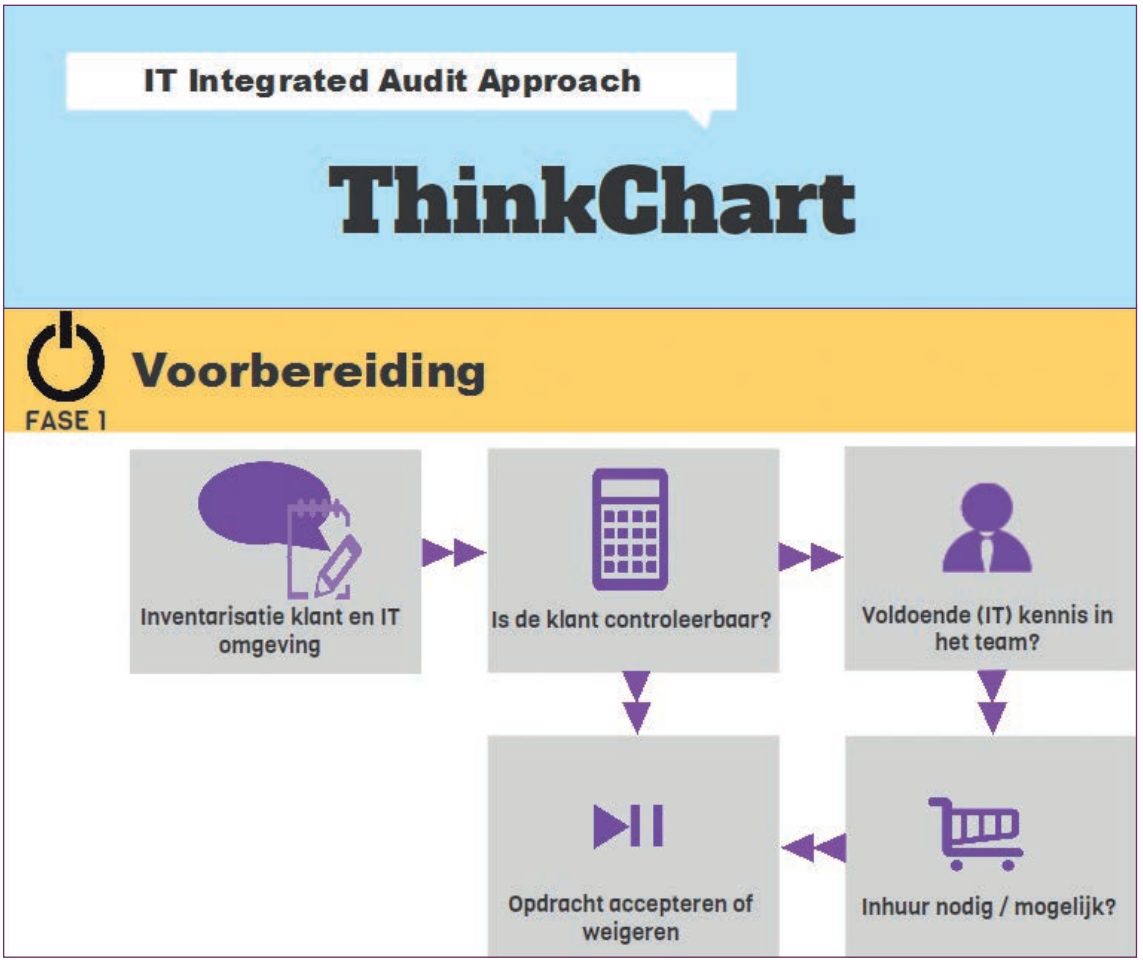
Onderdeel van de voorbereidingsfase is een algemene beoordeling van de IT-omgeving van de klant. Het resultaat hiervan draagt bij aan het vereiste begrip van de klantomgeving en vormt input voor de beoordeling van de controleerbaarheid ervan. Indien de IT-kennis van het team nog niet voldoende is om de beoordeling te kunnen uitvoeren, valt interne of externe inhuur te overwegen.

In de planningsfase wordt allereerst de omgeving van de klant nader beoordeeld op een steeds gedetailleerder niveau. Deze beoordeling richt zich onder meer op aanwezige IT-componenten, beheersing van IT en de relatie met de jaarrekening. Vervolgens worden op de verschillende niveau's risico's gedefinieerd. Voor het definiëren van de audit respons op deze risico's wordt een balans gezocht tussen manual- en application controls. Vervolgens wordt vanuit de geselecteerde application controls de diepgang van het testen van de randvoorwaardelijke General IT Controls bepaald.

Het is raadzaam de uitvoering te starten met testen van de General IT Controls zodat bij eventuele ontoereikende controls direct de controlaaanpak kan worden herzien[1]. Vervolgens worden de geselecteerde application controls getest. Aanvullend op deze controlewerkzaamheden worden overige controlewerkzaamheden uitgevoerd die noodzakelijk zijn voor het verkrijgen van voldoende zekerheid. Aandachtspunt is het inzetten van data-analyse om de gegevensgerichte controlewerkzaamheden efficiënt en effectief te kunnen uitvoeren.

De afrondingsfase vormt het sluitstuk van de uitgevoerde werkzaamheden en bevat minimaal een beoordeling van de toereikendheid van de uitgevoerde werkzaamheden[2] en de conclusies die daaruit getrokken zijn. In deze fase wordt de relatie vanuit de conclusies gelegd naar de verantwoording. Tevens wordt verslag gedaan van de relevante bevindingen aan de entiteit.

1 De infographic voorziet niet in die situaties waarin de controleaanpak tussentijds wordt herzien of bijgesteld.
2 Aanvullende werkzaamheden laat de infographic buiten beschouwing.


IT Integrated Audit Approach
ThinkChart
FASE 1
Voorbereiding
Inventarisatie klant en IT omgeving
Is de klant controleerbaar?
Voldoende (IT) kennis in het team?
Opdracht accepteren of weigeren
Inhuur nodig / mogelijk?

1. Voorbereiding

1.1 Inleiding

Inhoud en samenhang met andere hoofdstukken

In de voorbereidingsfase wordt de basis gelegd voor de uitvoering van de audit. De accountant stelt zich in deze fase de volgende vragen:

- Zijn de omstandigheden aanwezig om de opdracht zodanig uit te voeren dat een professioneel oordeel mogelijk is?
- Welke aanvullende maatregelen zouden daarvoor nodig zijn en zijn die naar verwachting te realiseren?

Voor de beantwoording van die vragen is het nodig dat de accountant op hoofdlijnen geïnformeerd is over de IT-omgeving van de opdrachtgever. Bij een complexe en grootschalige IT-omgeving zal de samenstelling van het controleteam zeer waarschijnlijk anders zijn dan in het geval van een kleinschaliger IT-omgeving. Om de juiste teamsamenstelling te kunnen inschatten, heeft de accountant enig inzicht nodig in de IT-omgeving. In de fase van risicoanalyse en planning wordt deze kennis verdiept en verder uitgewerkt. Op basis hiervan worden de risico's van een materiële afwijking in de jaarrekening onderkend en concrete werkzaamheden bepaald in respons op die risico's.

Input voor de voorbereidingsfase kan voortkomen uit eerder uitgevoerde gelijksoortige opdrachten, zoals de controle van de jaarrekening van het vorige jaar of eerder uitgevoerde vergelijkbare opdrachten.

Doelstelling

Na het lezen van dit hoofdstuk is de accountant in staat om:

- De IT-omgeving op hoofdlijnen in kaart te brengen
- De impact van de IT-omgeving op de controle in te schatten
- Te bepalen of hij bij de uitvoering van de controleopdracht over voldoende kennis en ervaring beschikt om tot een professionele afweging te komen, of dat daarvoor deskundigheid van een IT-auditor nodig is

1.2 IT-omgeving op hoofdlijnen

De IT- componenten worden op hoofdlijnen in kaart gebracht om inzicht te krijgen in de voor deze fase relevante aandachtsgebieden. Deze componenten zijn: apparatuur, systeemprogrammatuur, toepassingsprogrammatuur, organisatie, beveiliging, gegevensopslag en datacommunicatie. In bijlage 1 is de structuur van de gegevensverwerking geïllustreerd, waarin deze IT componenten en hun samenhang zijn opgenomen.

Deze componenten zijn in hoofdstuk 2 “Risicoanalyse en planning” verder uitgewerkt. In de Voorbereidingsfase gaat het er alleen om de hoofdlijnen in beeld te brengen ten behoeve van de opdrachtaanvaarding en de organisatie van de uitvoering van de opdracht.

Voorbeeld

Voorbeelden van elementen van deze inventarisatie zijn:

Processen/applicaties

- Welke bedrijfsprocessen zijn geautomatiseerd?
- Zijn deze bedrijfsprocessen geautomatiseerd in een geïntegreerde omgeving of is sprake van verschillende systemen met (complexe) interfaces?
- Welke applicaties ondersteunen de bedrijfsprocessen, voor zover relevant voor de controleopdracht?
- Zijn geautomatiseerde interne beheersingsmaatregelen in de IT systemen in hoge mate aanwezig?
- Vervangen deze geautomatiseerde interne beheersingsmaatregelen (een deel van) interne beheersing buiten de applicatie om?
- Is er sprake van standaard oplossingen, maatwerk of een combinatie hiervan?

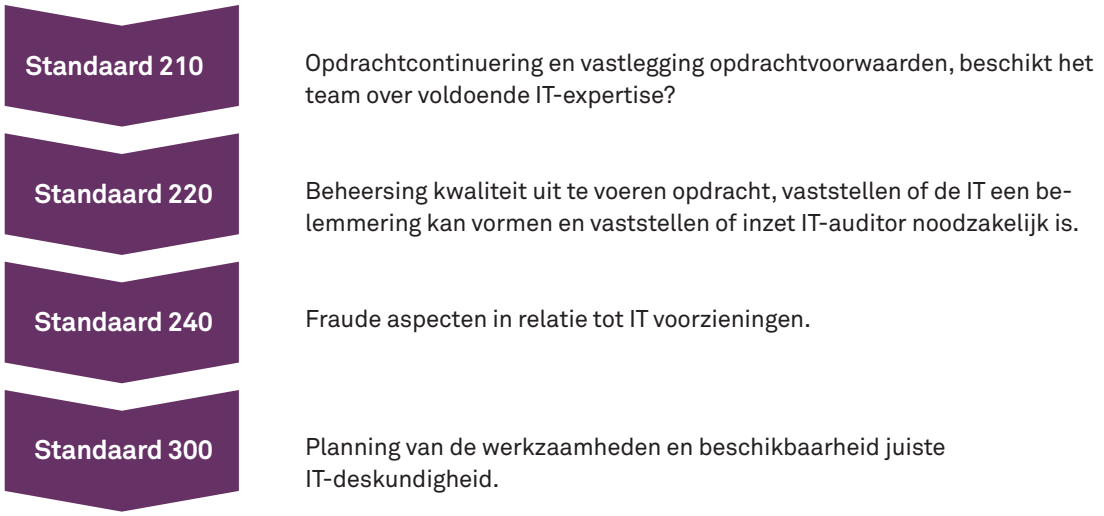
Specifieke kenmerken technische infrastructuur

- Is er sprake van een webwinkel?
- Is er specifieke wet- en regelgeving van toepassing (Wet Bescherming Persoonsgegevens)?
- Bestaan er bedrijfsrisico’s voortvloeiend uit de IT-omgeving die consequenties kunnen hebben voor de controle?
- Is de organisatie in hoge mate afhankelijk van de continuïteit van de IT-omgeving?
- Is de organisatie in hoge mate afhankelijk van de betrouwbaarheid van de IT-omgeving?
- Zijn relevante applicaties cloud-diensten?

1.3 Specifieke IT-aspecten bij de voorbereiding van de opdracht

Niet alle onderwerpen die bij de voorbereiding van de opdracht aan de orde komen hebben een raakvlak met IT. Hierna wordt nader ingegaan op een aantal onderwerpen die aandachtspunten in relatie tot IT met zich meebrengen. In bijlage 2 is per relevante controlestandaard (NV COS) aangegeven of daar specifieke IT-aspecten aan de orde zijn. Het schema hierna betreft de standaarden die van toepassing zijn in deze fase.

Figuur 1: Componenten voorbereidingsfase



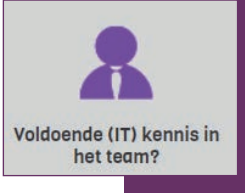
Opdrachtaanvaarding en vastlegging opdrachtvoorwaarden

Een van de overwegingen bij de opdrachtaanvaarding kan verband houden met de IT-omgeving van de opdrachtgever. De accountant vormt zich in deze fase een algemeen beeld van de uitvoerbaarheid van de opdracht. Als de IT-omgeving bijvoorbeeld zeer complex is en een grote rol speelt bij de uitvoering van de controle kan dat de uitvoering bemoeilijken. In uitzonderlijke gevallen kan de omvang en complexiteit van de IT-omgeving, in combinatie met het gebrek aan (eigen) deskundigheid, reden zijn om de opdracht niet te aanvaarden. Deze afweging zal de accountant in veel gevallen in overleg met de IT-auditor maken.

Wanneer te verwachten is dat de IT-voorzieningen een belangrijke rol zullen gaan spelen bij de uitvoering van de opdracht, is het raadzaam om dit in de opdrachtbevestiging expliciet te benoemen. Hierbij kan dan worden aangegeven dat specifieke IT-werkzaamheden uitgevoerd worden zodat de opdrachtgever zich tijdig kan voorbereiden. Dit kan gericht zijn op interviews met IT-functionarissen, beschikbaar stellen van documentatie en informatie over de werking van de interne IT-beheersingsprocessen, beoordelen van specifieke query's en dergelijke. Eigenlijk is de beschikbaarheid van personen en documentatie geen specifiek IT-aandachtspunt maar een onderwerp dat al in algemene termen in de opdrachtbevestiging wordt genoemd. Maar doordat vooral in het mkb de aandacht voor IT bij de jaarrekeningcontrole nog relatief nieuw is, kan tijdige communicatie over dit onderwerp latere discussies over nut en noodzaak helpen voorkomen.

Denk hierbij aan de implementatie van een geïntegreerde "end-to-end" oplossing die het mogelijk maakt om de workflow en autorisaties van het inkoopproces te automatiseren, waarbij de papieren stroom komt te vervallen. Hierbij is in sommige situaties specifieke IT-kennis noodzakelijk om authenticiteit, exclusiviteit en integriteit van inkoopfacturen vast te kunnen stellen.

Beheersing kwaliteit uit te voeren opdracht



Voor een goede uitvoering van de controleopdracht is een deskundig en onafhankelijk controleteam nodig. Hoewel het team daadwerkelijk wordt samengesteld in de planningsfase, is het al in de voorbereidingsfase van belang om in grote lijnen in beeld te krijgen of er belemmeringen op dit gebied te verwachten zijn - en zo ja, of en hoe die zijn weg te nemen.

In deze fase is voldoende inzicht in relevante IT-systemen nodig om de volgende vragen te beantwoorden:

- Is uitbreiding van het team met een IT-auditor nodig?
- Is IT-kennis voldoende aanwezig binnen de accountantsorganisatie om de opdracht uit te voeren?
- Vormt een eventuele beperkte beschikbaarheid van medewerkers met specifieke IT-kennis geen belemmering voor de doorlooptijd en planning van de opdracht?

Afhankelijk van de controleopdracht kan een IT-auditor met specifieke kennis ingezet worden. Specifieke kennis kan betrekking hebben op bepaalde applicaties, tools (zoals data-analyse) of technische infrastructuur (zoals lokaal netwerk, internet, cloud). Het is aan de accountant om te beoordelen welke specifieke kennis noodzakelijk is en wat de eventuele kwaliteitseisen van de IT-auditor zijn - denk bijvoorbeeld aan opleiding en certificering.

Fraude-aspecten in relatie tot IT-voorzieningen

Tijdens gesprekken met de opdrachtgever en met de leden van het team wordt een inventarisatie gemaakt van frauderisico's. Hierbij is aandacht nodig voor specifieke IT-omgevingen waarbij zich frauderisico's kunnen voordoen. Wanneer IT een belangrijke rol speelt, is de aanwezigheid van de IT-auditor bij deze gesprekken onmisbaar zodat de inventarisatie van frauderisico's de vereiste diepgang zal hebben en daarmee een effectief element van de voorbereiding is.

Het betreft hierbij ook fraude door derden. Denk hierbij aan webwinkels en betalingen via credit cards, iDEAL of Paypal, waarbij zich nieuwe vormen van "IT-fraude" zich kunnen voordoen.

Planning werkzaamheden en beschikbaarheid juiste deskundigheid

Wanneer de werkzaamheden van de controle gepland worden en de beschikbaarheid van de juiste deskundigheid voor de uitvoering van de opdracht wordt vastgesteld, is eigenlijk al geen sprake meer van de voorbereidingsfase. De opdracht is dan in feite al in de volgende fase, die in het volgende hoofdstuk aan bod komt. Toch is het van belang dat de accountant zich hiervan al in de voorbereidingsfase op hoofdlijnen een beeld vormt.

Let op wijzigingen ten opzichte van voorgaande jaren

Bedrijven in het mkb hebben de afgelopen jaren grote wijzigingen aangebracht in hun IT-voorzieningen. Goedkoper geworden hard- en software en een behoefte aan efficiency en snelle informatie hebben hier flink aan bijgedragen.In de voorbereidingsfase van een te continueren controleopdracht is het daarom belangrijk om in een vroeg stadium kennis te nemen van wijzigingen in de IT-omgeving van de klant. Wanneer bijvoorbeeld de klant is overgegaan van automatisering van afzonderlijke processen naar geïntegreerde automatisering met ERP-software, is de vraag voor de accountant wat dit voor de uitvoering van zijn controle betekent. Welke ERP-omgeving is geïmplementeerd, welke keuzen zijn daarbij gemaakt bij de eventuele herinrichting van processen en beveiliging, et cetera? Zijn essentiële interne beheersingsmaatregelen geautomatiseerd? Al in de voorbereidingsfase is het belangrijk dat de accountant zich ervan bewust is dat dit mogelijk gevolgen heeft voor de samenstelling van het team. Wellicht is het nodig om een IT-auditor met specialistische kennis van de ERP-software in te huren. Al met al zal het controleprogramma er waarschijnlijk anders uit gaan zien dan in het vorige jaar het geval was.

1.4 Documentatie

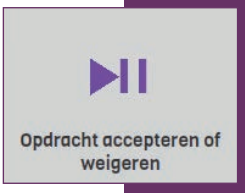
De uitgevoerde werkzaamheden, overwegingen en bevindingen die betrekking hebben op IT-relevante aspecten in de voorbereidingsfase, leg je vast in het dossier. Meld daarbij expliciet of overleg heeft plaatsgevonden met de IT-auditor, over welk onderwerp dat ging en welke adviezen de IT-auditor heeft gegeven.

De accountant trekt conclusies uit de inventarisatie op hoofdlijnen en legt die gemotiveerd vast. Daarbij geeft hij ook de consequenties ervan aan voor het vervolg van de opdracht.

1.5 Communicatie

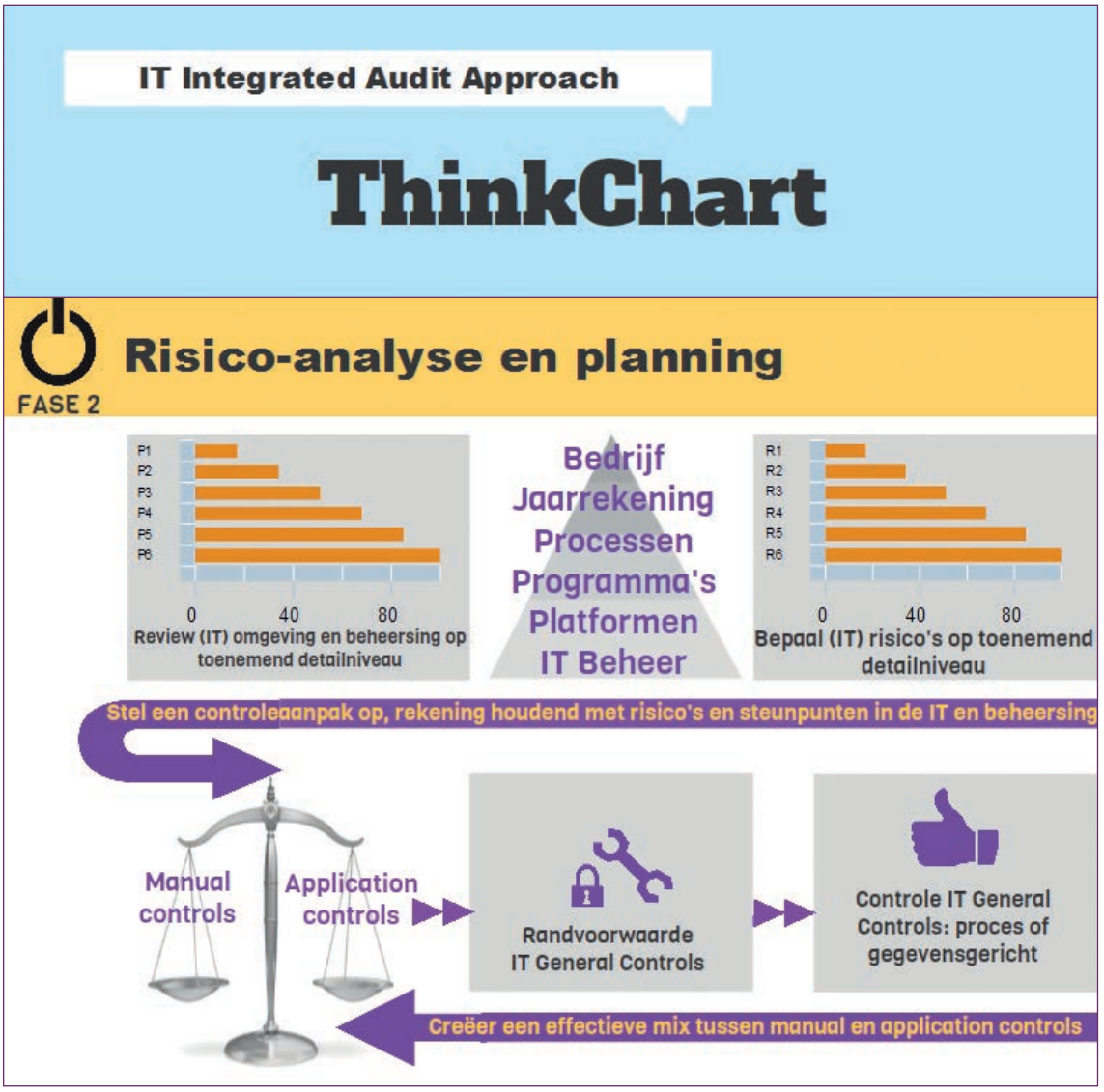
Communicatie binnen het team

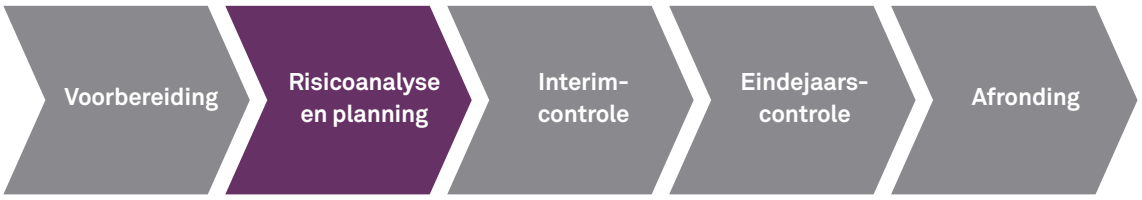
Het besluit om de opdracht te aanvaarden is pas mogelijk als de accountant (als eindverantwoordelijke) en IT-auditor (als specialist) tezamen ervan overtuigd zijn dat voldoende expertise aanwezig is om de opdracht te kunnen uitvoeren.



Communicatie met de klant

In deze fase vindt een gesprek met de opdrachtgever plaats om een eerste indruk te krijgen van de mate van automatisering. Naar aanleiding van dit gesprek dienen eventuele IT- gerelateerde opdrachtvoorwaarden te worden overeengekomen en vastgelegd in de opdrachtbevestiging.


IT Integrated Audit Approach
ThinkChart
Risico-analyse en planning
FASE 2
P1
P2
P3
P4
P5
P6
0
40
80
Review (IT) omgeving en beheersing op toenemend detailniveau
Bedrijf
Jaarrekening
Processen
Programma's
Platformen
IT Beheer
R1
R2
R3
R4
R5
R6
0
40
80
Bepaal (IT) risico's op toenemend detailniveau
Stel een controleaanpak op, rekening houdend met risico's en steunpunten in de IT en beheersing
Manual controls
Application controls
Randvoorwaarde IT General Controls
Controle IT General Controls: proces of gegevensgericht
Creëer een effectieve mix tussen manual en application controls



2. Risicoanalyse en planning

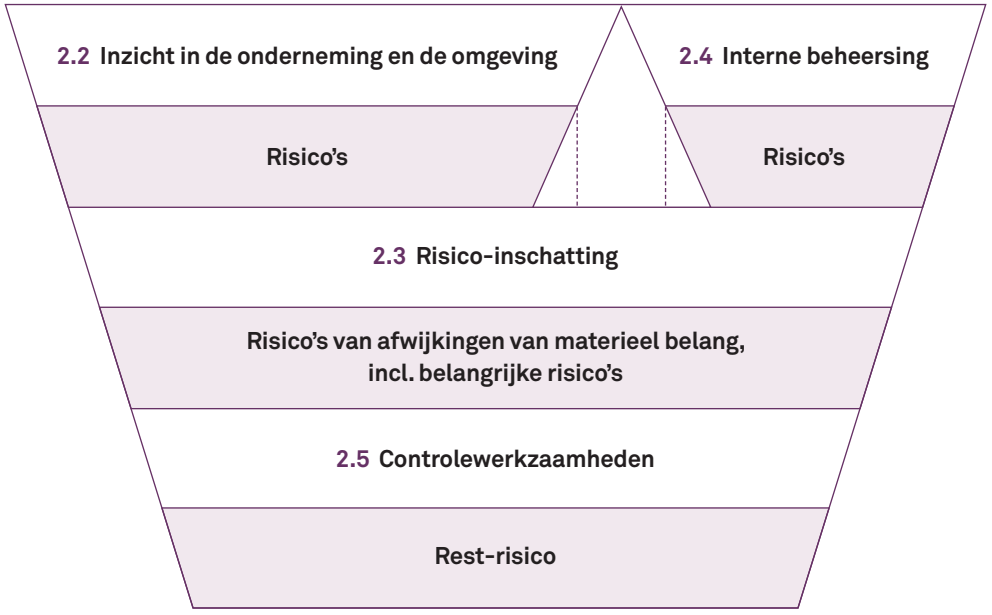
2.1 Inleiding

Inhoud en samenhang met andere hoofdstukken

In het vorige hoofdstuk zijn we ingegaan op de voorbereidingsfase, waarin de accountant op hoofdlijnen inzicht verkrijgt in de IT-omgeving. In dit hoofdstuk behandelen we de fase van risicoanalyse en planning waarbij de opgedane kennis van de IT-omgeving wordt verdiept en verder uitgewerkt. De risicoanalyse is gericht op het inschatten van risico's dat de jaarrekening een afwijking van materieel belang bevat als gevolg van fouten of fraude. Dit mondt uit in een controleprogramma. Deze fase vormt de basis voor de bepaling van de uit te voeren werkzaamheden, die worden behandeld in hoofdstuk 3 "Interimcontrole" en hoofdstuk 4 "Eindejaarscontrole".

Om een effectieve en efficiënte controle op te kunnen zetten past de accountant een risico-analytische controlemethode toe. Hiertoe bepaalt de accountant het materieel belang en voert een risicoanalyse uit. De risicoanalyse vormt de basis voor de uit te voeren werkzaamheden. Om het materieel belang te bepalen en een risicoanalyse uit te voeren, is het noodzakelijk dat de accountant kennis van de cliënt heeft. De risico-analytische methode kan het beste worden weergegeven aan de hand van het risicoanalysemodel:

Figuur 2: Risicoanalyse-model



Bron: Elementaire theorie accountantscontrole

Doelstelling

Na het lezen van dit hoofdstuk is de accountant in staat om:

- een gedetailleerde inventarisatie van de automatiseringsomgeving op te stellen;
- de risico's voortvloeiende uit de automatiseringsomgeving te identificeren;
- te zorgen voor een goede documentatie van hetgeen hiervoor is genoemd;
- een juiste mix van systeem- en gegevensgerichte werkzaamheden te plannen.

Bij het uitvoeren van deze werkzaamheden wordt waar nodig gebruik gemaakt van de kennis en ervaring van een IT-auditor of andere teamleden met relevante IT-kennis. Bij het lezen van dit hoofdstuk is het belangrijk om onderstaande goed voor ogen te houden:

Op basis van de kennis die de accountant heeft opgedaan van de huishouding, inclusief de IT-omgeving, dient hij de risico's te identificeren. De risicoanalyse start bij de business risks (potentiële risico's) om de volledigheid van risico's na te streven. Deze risico's hoeven echter niet direct invloed te hebben op de jaarrekening. De accountant zal alleen de (inherente) risico's die betrekking hebben op de jaarrekening verder evalueren. Door de huishouding zijn maatregelen getroffen om een of meerdere van deze inherente risico's te elimineren. De accountant zal bij zijn controleaanpak willen steunen op de effectieve werking van deze maatregelen. In de controle richt de accountant zich vervolgens op het afdekken van restrisico's die niet door de beheersingsmaatregelen worden afgedekt.

Met deze aanpak zijn accountants bekend en een soortgelijke werkwijze geldt voor IT-risico's en beheersingsmaatregelen om worden gaan. Dit betekent dus dat der accountant alleen die beheersingsmaatregelen in de IT-omgeving test waar hij in zijn controle op wil steunen. Het is niet de bedoeling te beginnen met een zeer gedetailleerde vastlegging van alle aanwezige systemen en alle aanwezige risico's en beheersingsmaatregelen in en rondom deze systemen. Dat zou er namelijk toe kunnen leiden dat systemen in beeld komen die niet relevant zijn voor de jaarrekeningcontrole.

2.2 Inzicht in de entiteiten haar omgeving, inclusief de IT-omgeving

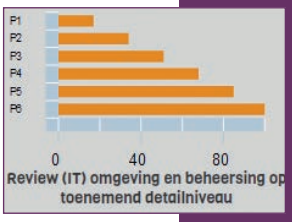
De accountant verwerft inzicht in de interne beheersing om vast te stellen op welke wijze de onderneming inspeelt op onderkende bedrijfsrisico's. Het interne beheersingssysteem bevat veelal een combinatie van handmatige en geautomatiseerde elementen. Deze geautomatiseerde elementen komen in dit hoofdstuk verder aan bod.

Voor wat betreft de IT is het in dit kader ook van belang inzicht te verkrijgen in de managementverantwoordelijkheden ten aanzien van IT, verantwoordelijkheden van de IT afdeling, beveiligingsprocedures, et cetera. Deze liggen veelal vastgelegd in een IT-plan, een beveiligingsbeleid, de organisatiestructuur en in taak- en functiebeschrijvingen.

2.2.1 Vervolg op de voorbereidingsfase

In de voorbereidingsfase (hoofdstuk 1) is beschreven welke werkzaamheden de accountant heeft uitgevoerd om een eerste indruk te krijgen van de IT-omgeving. Dit is enerzijds noodzakelijk geweest om de toereikendheid van de administratieve organisatie en interne beheersing (hierna: AO/IB) te beoordelen, anderzijds om te bepalen of specialistische kennis vereist is binnen het controleteam. Afhankelijk van deze eerste inventarisatie dient het

verder in kaart brengen van de IT-omgeving plaats te vinden door de accountant, de IT-auditor of de accountant en IT-auditor gezamenlijk. De keuze hiervoor is afhankelijk van de complexiteit van de huishouding, de IT-omgeving van de huishouding en de kennis die de accountant bezit.



2.2.2 Inzicht in de entiteit volgens de NV COS

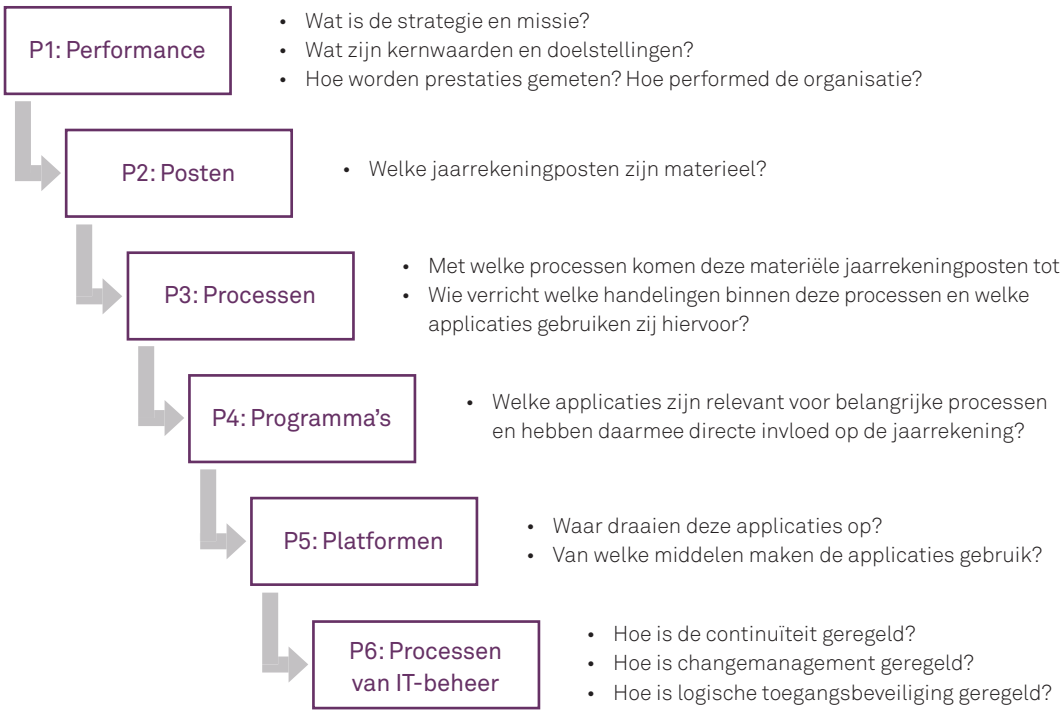
Standaard 315.18 bepaalt dat de kennis over het informatiesysteem de volgende elementen bevat:

- de transactiestromen binnen de entiteit die van belang zijn voor het financiële overzicht;
- de procedures, zowel binnen de geautomatiseerde als de handmatige systemen, waarmee de transacties tot stand worden gebracht, vastgelegd, verwerkt en in het financiële overzicht opgenomen;
- de hiermee verband houdende digitale of handmatige vastleggingen over het tot stand komen, vastleggen, verwerken en rapporteren van transacties, die de onderbouwing vormen voor de informatie en specifieke posten in het financiële overzicht;
- de wijze waarop voor het financiële overzicht van belang zijnde gebeurtenissen en omstandigheden, niet zijnde transactiestromen, worden vastgelegd in het informatiesysteem;
- het financiële verslaggevingsproces dat wordt gebruikt om het financiële overzicht van de entiteit op te stellen, met inbegrip van belangrijke schattingsposten en toelichtingen;
- interne beheersingsmaatregelen met betrekking tot journaalboekingen, met inbegrip van journaalboekingen die geen standaardjournaalboekingen zijn en worden gebruikt om eenmalige, ongebruikelijke transacties of correcties vast te leggen.

2.2.3 Het P6-model

Het P6-model kan helpen om de IT-omgeving en de bijbehorende beheersingsmaatregelen in kaart te brengen. Dit model ziet er als volgt uit:

Figuur 3: Het P6-model



Belangrijk bij de uitwerking van de verschillende niveaus is dat de diepgang en reikwijdte van de uitwerking afhangen van het verband met de aangrenzende niveaus. Met andere woorden: de uitwerking per niveau zal niet dieper of breder hoeven dan in relatie tot de jaarrekening noodzakelijk is.

Bovenstaande stappen zullen we nader toelichten, waarbij we tevens aangeven wie welke stappen kan uitvoeren:

Performance (P1)

Standaard 315 bepaalt dat de accountant inzicht verkrijgt in de entiteit en haar omgeving. Daarbij geeft Standaard 315 aan welke factoren van belang zijn. De toelichting daarbij vullen we in vanuit een gecombineerd perspectief (IT integrated financial audit):

a. **Relevante sectorspecifieke factoren, regelgeving, overige externe factoren**
De accountant stelt onder meer vast wat voor soort onderneming hij controleert (productie, handel et cetera), welke producten of diensten de onderneming in de markt zet en hoe de markt eruit ziet.

Het kan zijn dat de onderneming opereert in een zeer concurrerende markt waarbij de onderneming alleen kan overleven door continu te innoveren. De technologische ontwikkelingen rondom IT kunnen bijdragen aan de innovatie. Binnen de onderneming is hiervoor dan ook aandacht het management vereist.

Steeds meer zien we dat automatisering de wisselwerking tussen de onderneming en zijn afnemers en leveranciers ondersteunt. Een voorbeeld hiervan zijn webwinkels. De onderneming biedt een scala aan producten of diensten aan via zijn website. Afnemers kiezen op deze website de gewenste producten of diensten. Nadat de afnemer zijn keuze heeft gemaakt, gaat hij met zijn virtuele winkelwagen naar de virtuele kassa om af te rekenen. De betaling kan op verschillende manieren plaatsvinden, waaronder ook de elektronische betalingsvormen via creditcard, PayPal of iDeal. Bij gebruik van elektronische betalingsvormen heeft de onderneming een samenwerkingsverband nodig met de bedrijven die deze diensten leveren. De website en de administratie van de onderneming moeten zo zijn ingericht dat de klant kan betalen via, bijvoorbeeld, iDeal en dat de onderneming de informatie terugontvangt die nodig is om de betaling te verifiëren.

De regelgeving kan eveneens een belangrijke weerslag hebben op de IT van de onderneming. Hierbij valt te denken aan consequenties van de privacy wetgeving. Om voort te borduren op het voorbeeld van de webwinkel: de privégegevens die de afnemer invult op de website moeten zodanig beveiligd zijn, dat misbruik door ongeautoriseerde personen is uitgesloten.

b. **Aard van de entiteit**
Hierbij gaat het onder meer om inzicht te verkrijgen in de structuur van de onderneming, de wijze waarop de onderneming wordt bestuurd en gefinancierd en de investeringsactiviteiten.

Voor het IT-aspect is van belang hierbij te bepalen of de automatisering beperkt, belangrijk dan wel overheersend is.

c. **Keuze en toepassing grondslagen voor financiële verslaggeving**
De accountant stelt vast welke financiële verslaggevingsstandaarden de organisatie toege-

past en op welke wijze transacties administratief worden verwerkt. De transacties die in het boekjaar hebben plaatsgevonden, worden in boekhoudapplicaties geregistreerd. Hierbij zijn twee uitersten te onderscheiden. Het ene uiterste is een handmatige registratie: een administratief medewerker registreert een transactie in de boekhoudapplicatie aan de hand van een papieren document. Het andere uiterste is een geïntegreerde "end-to-end" oplossing zonder enige papieren stroom. Denk hierbij aan een volledig geautomatiseerde verwerking op basis van Electronic Data Interchange (EDI). Wanneer de leverancier een digitale factuur verstuurt via EDI, kan deze geheel automatisch verwerkt worden in de boekhoudapplicatie. In dat geval is dus geen administratief medewerker nodig om aan de hand van een papieren factuur de transactie te registeren. Het registreren is overgenomen door de computer.

d. **Doelstellingen en strategieën en daaruit voortvloeiende bedrijfsrisico's**
   Hierbij gaat het onder meer om de missie, doelstelling en strategie van de onderneming. Op basis hiervan kan de accountant bedrijfsrisico's identificeren, welke het uitgangspunt zijn van de risicoanalyse.

   Wat het IT-aspect betreft gaat het er hier om een beeld te vormen over het informatie- en automatiseringsbeleid. Dit beleid moet leiden tot een effectieve en efficiënte toepassing van IT. De keuzes die de onderneming hier maakt kunnen op gespannen voet staan met de beheersingsmaatregelen waarop de accountant wil steunen. Het kan bijvoorbeeld heel effectief of efficiënt zijn om alles binnen applicaties open te stellen voor alle medewerkers. Dit brengt echter wel met zich mee dat op bepaalde beheersingsmaatregelen niet gesteund kan worden.

e. **Wijze waarop entiteit financiële prestaties meet en beoordeelt**
   Hierbij gaat het om de wijze waarop kritische performance indicatoren (KPI's) voor de business zijn gedefinieerd. In het kader van de IT kan het zijn dat de onderneming KPI's heeft gedefinieerd voor de automatiseringsafdeling of de automatisering als geheel.

Posten (P2)

De accountant bepaalt welke posten in de jaarrekening materieel zijn. Hierin zijn geen specifieke IT-aspecten te benoemen.

Processen (P3)

De accountant verwerft inzicht in de processen door de AO/IB-beschrijving op te vragen en te beoordelen. Hierin dienen de volgende elementen duidelijk te zijn beschreven:

- welke transactiestromen door welke systemen lopen;
- wie welke handelingen verricht en in welk systeem dit geregistreerd of uitgevoerd wordt;
- welke relevante application controls aanwezig zijn in welk systeem.

Programma's (P4)

Bij de identificatie van specifieke IT-aspecten bij de voorbereidende werkzaamheden zijn reeds de applicaties geïnventariseerd die de bedrijfsprocessen ondersteunen. Op basis van de AO/IB beschrijving vult de accountant dit overzicht indien nodig aan. De accountant deelt de applicaties als volgt in:

- applicaties die een bedrijfsproces ondersteunen en direct invloed hebben op een of meerdere jaarrekeningposten;
- applicaties die een bedrijfsproces ondersteunen maar geen directe invloed hebben op een of meerdere jaarrekeningposten.

Het doel van de accountant mag niet uit het zicht raken: het verstrekken van een controleverklaring bij de jaarrekening. Standaard 315.18 bepaalt dat de accountant inzicht verwerft in het informatiesysteem, relevant voor de financiële verslaggeving. Om deze reden zijn alleen die applicaties relevant die een bedrijfsproces ondersteunen die directe invloed hebben op de jaarrekening.

Voorbeeld

Een applicatie waarin alleen de personalia van medewerkers vastligt, is niet relevant voor de accountant. Het helpt de Human Resource Managementafdeling maar heeft geen directe invloed op de jaarrekening. De applicatie zou wel directe invloed op de jaarrekening hebben indien hier de urenregistratie aan gekoppeld is als basis voor de facturatie. De accountant heeft dan de applicatie nodig om de volledigheid van de omzet vast te stellen.

Voor zover niet reeds geïdentificeerd in de voorbereiding, is het aan te bevelen de relevante applicaties te benoemen:

- Wat zijn de standaardapplicaties?
- Wat zijn de zelf ontwikkelde en onderhouden maatwerkapplicaties,?
- Wat zijn de extern ontwikkelde en onderhouden maatwerkapplicaties?
- Welke interfaces zijn aanwezig tussen applicaties binnen of buiten de organisatie?

Het resultaat is een overzicht van de aanwezige applicaties dat aangeeft welke processen ze ondersteunen (of welke jaarrekeningposten zij beïnvloeden) en om wat voor soort applicatie het gaat. Een voorbeeld hiervan kan zijn:

Tabel 1: Voorbeeld vastlegging applicaties

Applicatie	Processen				Soort Systeem		
	Inkoop	Productie	Verkoop	Personeel	Standaard	Intern ontwikkeld	Extern ontwikkeld
Inkoopsysteem	√				√		
Voorraadsysteem	√	√	√			√	
Productiesysteem		√			√		
Verkoopsysteem			√		√		
Urenregistratie				√			√
Electronic banking	√		√		√		

Dit onderdeel kan de accountant uitvoeren als een eerste inventarisatie. De informatie over de applicaties en hun relatie met de jaarrekening kan hij in een later stadium verder aanvullen in samenwerking met de IT-auditor.

Platformen (P5)

Om applicaties te kunnen laten functioneren, zijn platformen noodzakelijk: combinaties van hardware en systeemprogrammatuur. Platformen zijn te onderscheiden naar mainframe, midrange en PC-netwerken. Veel voorkomende platformen / besturingssystemen zijn Linux, Unix en Windows Server.

Deze stap leidt tot een beschrijving van de aanwezige infrastructuur die voor de informatiesystemen. Veelal heeft de accountant onvoldoende kennis om de risico's die hieruit voortvloeien voldoende in te schatten. Tevens is de accountant veelal onvoldoende in staat vast te stellen dat zijn beschrijving volledig is. Om deze redenen zal de accountant dit onderdeel vaak tezamen met de IT-auditor uitvoeren, dan wel voert de IT-auditor dit zelfstandig uit.

Processen van IT beheer, General IT Controls (P6)

Bij een hoog geautomatiseerde onderneming zullen procedures bestaan voor het beheer van de infrastructuur en de daarop draaiende systemen. We spreken hierbij over General IT Controls. Dit zijn de interne beheersingsmaatregelen gericht op nagenoeg alle computersystemen en bedrijfsprocessen. Hierbij valt niet alleen te denken aan de beveiliging van hard- en software, maar ook aan de IT-organisatie (beleid, procedures en monitoring).

Aan de hand van de vorige stappen in het P6 model heeft de accountant inzicht gekregen in de voor de jaarrekeningcontrole relevante applicaties en de platformen waarop die draaien. Het in kaart brengen van de General IT Controls is alleen noodzakelijk indien in de controleaanpak steunt op de IT. Daarnaast is het voldoende om alleen de werking van de relevante General IT Controls vast te stellen en is het niet nodig dit voor alle General IT Controls te doen. Meer hierover in de volgende paragraaf en in hoofdstuk 3 "Interimcontrole".

Afhankelijk van het soort organisatie (beperkte automatisering tot hoog geautomatiseerd) wordt deze stap uitgevoerd door de accountant of IT-auditor, dan wel door hen gezamenlijk.

2.3 Beheersingsmaatregelen

Interne beheersingsmaatregelen zijn manual controls, computer dependent controls of automated controls.

De automated controls zijn opgenomen in de applicaties die de processen ondersteunen, zoals beschreven bij P4 'Programma's'.

Computer dependent controls zijn een mix tussen manual controls en automated controls. Dit houdt in dat een gebruiker voor het uitvoeren van een controle een programma gebruikt. De controle wordt daarmee niet volledig uitgevoerd door de applicatie, maar ondersteunt de controle door de gebruiker. Een voorbeeld hiervan is het periodiek beoordelen van de ouderdomsanalyse debiteuren in de financiële applicatie. Bij deze beoordeling wordt indirect gesteund op functionaliteit en rapportages van de financiële applicatie.

2.3.1 Application controls

De application controls betreffen onder meer:

- Logische toegangsbeveiliging
  Dit is erop gericht ongeautoriseerde toegang tot applicaties en bestanden te voorkomen. De functiescheiding zoals beschreven in de AO/IB moet via autorisaties zijn vastgelegd in de applicaties. Dit ligt vast in een competentietabel, ook wel autorisatiematrix genoemd. Logische toegangsbeveiliging valt uiteen in:
  - Identificatie: wie zegt de gebruiker dat hij is?
    Is van belang om handelingen in applicaties te kunnen herleiden tot een individu.
  - Authenticatie: is de gebruiker wie hij zegt dat hij is?
    Hoe sterker de authenticatie, hoe meer zekerheid er is dat de handelingen in een applicatie daadwerkelijk door het individu in kwestie zijn uitgevoerd.
  - Autorisatie: welke rechten heeft de gebruiker?
    Bij applicaties gaat het hier uiteindelijk om de functiescheidingen.

De logische toegangsbeveiliging kan geregeld zijn in de applicatie zelf, waardoor elke applicatie zijn eigen autorisatiematrix bevat. Wanneer sprake is van single sign on, is de logische toegangsbeveiliging echter voor alle applicaties geregeld via de Active Directory. In dat geval is er één autorisatietabel waarin de autorisaties van alle applicaties vast liggen.

Sommige applicaties kunnen de autorisatiematrix in een overzichtelijke vorm presenteren, waardoor de accountant veelal zelf in staat is om de functiescheidingen in de applicatie te beoordelen. Kunnen applicaties dat niet of niet eenvoudig, dan is het raadzaam om vooraf ongewenste functievermengingen te definiëren en de IT-auditor te verzoeken na te gaan of deze functievermenging bestaat. Een andere mogelijkheid is om aan de hand van bestandsanalyses vast te stellen of functievermenging is opgetreden. Dit komt aan bod in hoofdstuk 3 “Interimcontrole”. Een sterke authenticatie is dan wel van belang.

Wanneer de logische toegangsbeveiliging is geregeld via de Active Directory, is het aan te bevelen om de IT-auditor in te schakelen aangezien dit enig specialisme vereist.

Naast de autorisaties in de applicatie zelf dient de beveiliging van de “onderliggende” database (bijvoorbeeld een MS SQL database) te voorkomen dat de logische toegangsbeveiliging van de applicatie wordt omzeild door rechtstreekse mutaties in de database, dus “buiten de applicatie om”. Het laatste is mogelijk omdat een gebruiker niet alleen toegang tot een database kan krijgen via de Active Directory, maar - als zijn toegangsrechten dit toelaten - ook via het gebruikersbeheer van de onderliggende database.

Bij het bepalen van de logische toegangsbeveiliging van de database gelden dezelfde uitgangspunten als bij de logische toegangsbeveiliging van applicaties.

- Invoercontroles
  - Volledigheidscontroles — Vaststellen dat geen gegevens ontbreken - bijvoorbeeld doorlopende nummering.
  - Validity check — Verzekeren dat data juist is ingevoerd en/of verwerkt. Bijvoorbeeld controle op het al dan niet aanwezig zijn van reeds in het systeem aanwezige gegevens (bijv. bij de invoer van een verkooporder de controle of het artikel bestaat.

- Field check	Juiste type: numeriek , datum of alfabetisch
- Redundancy check	Voorkomen van dubbele registraties
- Sign check	Rekenkundige juistheid
- Limit check	Verzekeren dat het onder de bovengrens blijft (bijv. kredietlimiet)
- Range check	Verzekeren dat het tussen ondergrens en bovengrens blijft (bijv. afwijking tussen bestelling en ontvangst)
- Reasonableness check	Logisch correct?

- Verbands- en totaalcontroles
  Met behulp van verbandscontroles wordt vastgesteld of een bepaald direct verband tussen twee of meer grootheden aanwezig is - bijvoorbeeld omzet en btw. Bij totaalcontroles wordt gebruik gemaakt van een door de toepassing opgebouwd controletotaal. Verschil met verbandscontrole is dat de totaalcontrole als norm een door de toepassing opgebouwd gegeven gebruikt, terwijl de verbandscontrole gebruik maakt van een door de gebruiker eerder vastgelegde directe relatie.

- Audit trail
  Voor de controle is het belangrijk dat het systeem zo is opgezet dat de route van elke transactie of gegeven door het gehele verwerkingsproces heen (van invoer tot en met uitvoer) te volgen is: de audit trail.

- Logging
  Via logging worden acties in de applicatie geregistreerd.

Op basis van uitgevoerde risicoanalyse worden de voor de jaarrekening relevante key-controls geselecteerd om te beoordelen op opzet en bestaan. Het is van belang om de opzet en het bestaan vast te stellen alvorens de risicoanalyse uit te voeren en de controleaanpak te bepalen. Op basis van de verkregen informatie uit stap P3 en P4 wordt bepaald welke application controls in opzet aanwezig zijn. Hieruit worden voor de jaarrekeningcontrole relevante key-controls geselecteerd om het bestaan ervan vast te stellen.

Het bestaan van application controls is onder meer op de volgende wijzen vast te stellen:
- inspectie
- waarneming
- externe bevestiging
- herberekening
- herhaling / uitvoering
- cijferanalyse
- verzoeken om inlichtingen

Dit is nader uitgewerkt in hoofdstuk 3 “Interimcontrole”. De accountant kan het bestaan van application controls zelfstandig dan wel in samenwerking met de IT-auditor vaststellen, maar het kan ook zijn dat de IT-auditor dit zelfstandig doet. De keuze hiervoor hangt af van de complexiteit van de IT en de kennis van de accountant.

Om de ongestoorde werking van application controls te garanderen, zijn General IT Controls noodzakelijk. Zie hiervoor de volgende paragraaf.

2.3.2 General IT Controls

Applicaties slaan data op in databases en halen er data uit op. Het soort database is afhankelijk van de applicatie. Deze databases mogen alleen vanuit de applicatie beheerd worden om de database met gegevens te vullen. Aan applicaties, databases en onderliggende infrastructuur is ook technisch beheer gekoppeld.

General IT Controls: wat zijn dat?

De General IT Controls zijn randvoorwaardelijke beheersingsmaatregelen om de ongestoorde werking van application controls te waarborgen. De betrouwbaarheid valt uiteen in de volgende componenten:

- Exclusiviteit
  De mate waarin uitsluitend geautoriseerde personen of apparatuur via geautomatiseerde procedures en beperkte bevoegdheden gebruikmaken van IT-processen.

- Integriteit
  De mate waarin het object (gegevens en informatie-, technische- en processystemen) in overeenstemming is met de afgebeelde werkelijkheid.

- Controleerbaarheid
  De mate waarin het mogelijk is kennis te verkrijgen over de structurering (documentatie) en werking van een object. Tevens omvat dit kwaliteitsaspect de mate waarin het mogelijk is vast te stellen dat de informatieverwerking in overeenstemming met de eisen ten aanzien van de overige kwaliteitsaspecten is uitgevoerd.

- Continuïteit
  De mate waarin een object continu beschikbaar is en de gegevensverwerking ongestoord voortgang kan hebben. Belangrijk aspect van continuïteit is tevens het voorkomen van dataverlies bij storingen en calamiteiten. De volgende twee onderdelen dienen te voldoen aan de vereisten van de organisatie:
  - Recovery Point objective (RPO)
    De RPO is het punt in de tijd tot waar men minimaal de gegevens moet kunnen herstellen. Het is dus de acceptabele hoeveelheid aan dataverlies uitgedrukt in tijd.
  - Recovery Time Objective (RTO)
    Een RTO is de tijd waarna een proces/middel na een onderbreking moet teruggebracht zijn op een aanvaardbaar niveau, om een onacceptabele impact op de organisatie te vermijden.

De General IT Controls zijn onder te verdelen in:

1. Management en organisatie
   - Informatie- en automatiseringsbeleid
   - Beveiligingsbeleid

2. Operationeel beheer
   Bij kleine organisaties ontbreekt vaak een aparte IT-afdeling en systeembeheerder. Wanneer bedrijven groeien, stijgt de behoefte aan een systeembeheerder. Operationeel beheer omvat:

- *Probleembeheer*
  Probleembeheer is de wijze waarop storingen, problemen en klachten ten aanzien van de informatiesystemen worden geïdentificeerd, behandeld en opgelost.

- *Wijzigingsbeheer (change management)*
  Dit is het proces van plannen, coördineren, daadwerkelijk aanbrengen en evalueren van de wijzigingen in de informatiesystemen en de verwerkingsomgeving. Change management dient er toe te leiden dat:
  - een scheiding bestaat tussen de ontwikkelomgeving en de verwerkingsomgeving;
  - wijzigingen in informatiesystemen alleen plaatsvinden indien aan de gestelde kwaliteitscriteria is voldaan;
  - wijzigingen alleen door eigenaar van de applicatie worden geautoriseerd
  - de juiste versies van informatiesystemen operationeel zijn;
  - toereikende noodprocedures aanwezig zijn.

- *Logische toegangsbeveiliging*
  Logische toegangsbeveiliging in relatie tot General IT Controls heeft betrekking op de beveiliging van het netwerk en van de besturingssystemen. Het betreft het inrichten van het netwerk en de besturingssystemen op zodanige wijze dat gebruikers uitsluitend toegang hebben tot daartoe geautoriseerde applicaties, data en overige randapparatuur. Tevens omvat het procedures om de beveiliging conform de inrichting te laten functioneren. De inrichting van het netwerk en de besturingssystemen vereist specialistische, technische kennis. Het is daarom aan te bevelen dit deel door de IT-auditor te laten onderzoeken.

- *Procesbeheer*
  Operators zijn in het algemeen verantwoordelijk voor 'het in de lucht houden van de automatisering'. Het proces rondom operationeel beheer moet daarom op juiste wijze opgevolgd worden.

3. **Continuïteit (backup en recovery, fysieke beveiliging en uitwijkregelingen)**
   Bij organisaties met een beperkte automatisering en nog veel papieren gegevensstromen kan de uitval van de systemen hinderlijk zijn maar loopt men nagenoeg geen schade op. Organisaties die in belangrijke mate steunen op hun automatisering en die vergaand gedigitaliseerd zijn, kan discontinuïteit van het geautomatiseerd systeem catastrofale gevolgen hebben. Het management dient in de besluitvorming over continuïteitsplanning de potentiële schade (voor de onderneming als geheel als gevolg van het wegvallen van de geautomatiseerde gegevensverwerking door een calamiteit) af te zetten tegen de kosten van de beveiligingsmaatregelen en de bereidheid bewust bepaalde risico's wel/niet te willen lopen.

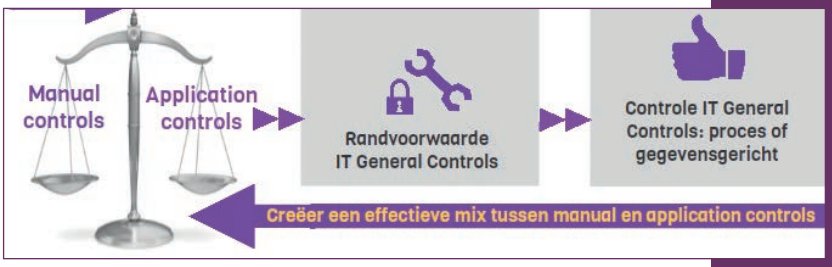
Onderzoek naar de General IT Controls

Is onderzoek naar de General IT Controls altijd nodig?

- Nee, alleen wanneer je steunt op de application controls.

Is het nodig alle General IT Controls onderzoeken?

- Nee, alleen de relevante General IT Controls. Welke dat zijn, is afhankelijk van de cliënt. Dit kun je in overleg met de IT-auditor bepalen.



ITGC: Change management

In de vorige paragraaf is aangegeven dat je het bestaan van application controls moet vaststellen voordat je de risicoanalyse uitvoert en de controleaanpak opstelt. Application controls blijven altijd hetzelfde werken, tenzij wijzigingen in de applicatie of relevante infrastructuur hebben plaatsgevonden. Indien je dus steunt op de application controls, beoordeel je van de General IT Controls tenminste het change management. Goed change management waarborgt de ongestoorde werking van application controls, zodat met de vaststelling van het bestaan van een application control tevens de werking ervan is vastgesteld.

Wat nu als je wel steunt op de application controls maar de change management is onvoldoende? In dat geval kun je mogelijk aan de hand van data-analyse de ongestoorde werking van de application control vaststellen. Wanneer je de mogelijkheid hebt om vast te stellen dat geen wijzigingen hebben plaatsgevonden, kun je ook met zekerheid stellen dat de application controls ongestoord hebben gewerkt. Dit is veelal mogelijk indien je aan de hand van het versienummer kunt vaststellen dat deze niet is gewijzigd. Indien documentatie van de problemen/incidenten aanwezig is, kun je aan de hand van deze documentatie beoordelen of zich problemen in de applicatie hebben voor gedaan, en of deze problemen zijn opgelost door wijzigingen in de applicatie door te voeren.

ITGC: Continuïteit

Continuïteit is voor een organisatie die slechts beperkt steunt op IT minder van belang dan wanneer de IT overheersend is. In een organisatie waar nagenoeg alleen de financiële administratie wordt gevoerd in een boekhoudapplicatie en waar hardcopy documentatie bewaard blijft, is continuïteit minder van belang. Indien het dan bij een storing niet mogelijk is de backup terug te zetten, zijn aan de hand van de hardcopy-documentatie alle data te herstellen. Dit kan uiteraard een behoorlijke kostenpost met zich meebrengen maar de data is niet per definitie verloren.

Door het definiëren van de zogenaamde Recovery Time Objective (RTO) wordt vastgelegd wat de vereisten zijn met betrekking tot de continuïteit per IT-systeem c.q. applicatie.

Een belangrijk onderdeel is het voorkomen van ongewenst dataverlies. Dataverlies kan in bepaalde situaties ernstige gevolgen hebben voor organisaties. Indien bij een calamiteit de laatste back-up van een ERP-systeem enkele maanden oud blijkt te zijn, kan dit desastreuze gevolgen hebben.

Een organisatie dient de Recovery Point Objective (RPO) te bepalen. De RPO is het punt in de tijd tot waar men minimaal de gegevens moet kunnen herstellen. De RTO en RPO behoren periodiek getest te worden.

Let op: geen vervanging mogelijk!

Indien application controls niet in voldoende mate aanwezig zijn, kunnen ITGC's geen compensatie bieden voor de werking van de betreffende key-control!

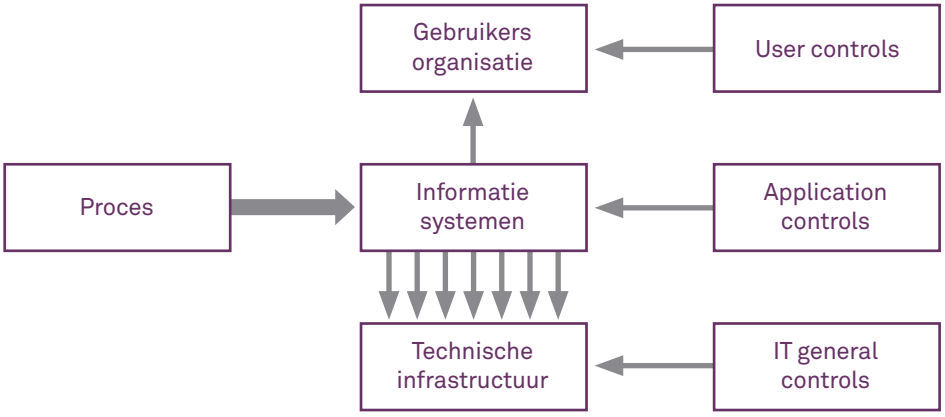
Voorbeeld

DigiNotar is een voorbeeld uit de praktijk van een organisatie waarbij de continuïteit van groot belang is. DigiNotar was een Nederlands commerciële Certificaatautoriteit dat de PKI-overheidcertificaten verzorgde voor delen van de Nederlandse overheid. Het bedrijf kwam in opspraak toen bleek dat de veiligheidscertificaten niet waterdicht waren. Als gevolg van een hack (juni 2011) konden valse certificaten worden uitgegeven waardoor de afzender van websites niet meer gegarandeerd werd. Naar aanleiding van een uitgebracht rapport zegde de overheid op 2 september 2011 het vertrouwen in DigiNotar op. Toezichthouder OPTA[3] besloot op 13 september 2011 dat de uitgegeven certificaten moesten worden ingetrokken en dat DigiNotar geen nieuwe mocht uitgeven. Kort daarna, op 20 september 2011, is het bedrijf DigiNnotar failliet verklaard. Deze casus toont aan dat bij een dergelijke organisatie de continuïteitsparagraaf in de controleverklaring nauw samen hangt met de continuïteit van de IT.

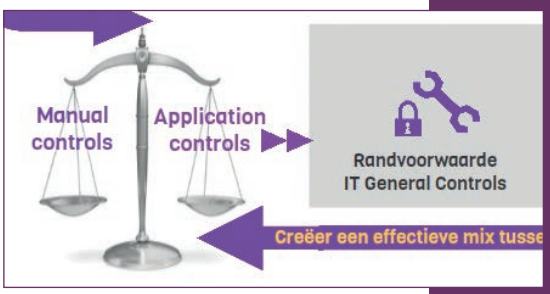
2.3.3 Relatie Application controls - General IT Controls

Application controls en General IT Controls staan met elkaar in verband. De relatie is zodanig dat General IT Controls nodig zijn om het functioneren van application controls te ondersteunen, en beiden zijn nodig om de volledige en accurate informatieverwerking te verzekeren:

Figuur 4: Relatie controls



In tegenstelling tot de traditionele controleaanpak waarbij je meerdere malen proceduretests uitvoert om de werking van een interne beheersingsmaatregel vast te stellen, hoef je een application control niet op werking te testen indien je het bestaan hebt vastgesteld. Door het bestaan vast te stellen heb je eenmaal de werking vastgesteld. Application controls blijven altijd hetzelfde werken, tenzij je veranderingen doorvoert. Hierdoor is het - indien geen wijzigingen hebben plaatsgevonden - voldoende om eenmaal de werking vast te stellen. Dit geldt alleen indien General IT Controls gedurende de gehele controleperiode goed functioneren.



3 Onafhankelijke Post en Telecommunicatie Autoriteit

General IT Controls zijn in het kader van de accountantscontrole primair relevant voor:

1. het als randvoorwaarde zorgdragen voor een ongestoorde werking van application controls;
2. het waarborgen van een minimaal niveau van beschikbaarheid van relevante IT-systemen in het kader van de continuïteit van de onderneming;
3. het waarborgen van een minimaal niveau van gegevensverwerking in het kader van de controleerbaarheid van een onderneming.

Ad 1

Als het bestaan en werking van relevante General IT Controls is vastgesteld, is daarmee de ongestoorde werking van aanwezige application controls vastgesteld. In dit geval behoeft van application controls alleen nog het bestaan te worden vastgesteld. Voor een goed oordeel is het van belang de relevante General IT Controls te bepalen op basis van die application controls die als beheersingsmaatregelen in de controleaanpak een rol spelen. De aard en omvang van de minimaal aanwezige General IT Controls is mede afhankelijk van het belang van de geselecteerde application controls. Het kan zijn dat bij de controle op General IT Controls niet op alle punten de werking valt vast te stellen zonder dat dit rechtsstreeks de werking van de application control aantast. In dat geval is de application control te beschouwen als een reguliere manual control en kun je de werking ervan op de traditionele wijze testen. Indien de werking van de General IT Controls tekortkomingen vertoont die de application controls mogelijk kunnen verstoren, kan men ervoor kiezen om via bestandsanalyse de werking van de application integraal te controleren.

Ad 2 en 3

Naast de functie van General IT Controls als randvoorwaarde voor de ongestoorde werking van application controls, spelen General IT Controls ook een rol bij de beoordeling van de continuïteit en de controleerbaarheid van de onderneming. Ook in die gevallen waarin de keuze is gemaakt op geen enkele application control te steunen dient de accountant het effect van mogelijke tekortkomingen in de General IT Controls te evalueren voor een oordeel over de continuïteitsaspecten en de controleerbaarheid van de onderneming. Conform BW 2: 393 lid 4 dient de accountant minimaal verslag uit te brengen over de continuïteit en de betrouwbaarheid van de geautomatiseerde gegevensverwerking.

Neem bij het beoordelen van de relevante application controls ook in ogenschouw op welke wijze informatie uit de systemen wordt gebruikt als managementinformatie of als brondocumenten voor de accountantscontrole.

2.4 Risicoanalyse

2.4.1 Het R6-model

De accountant voert een risicoanalyse uit zoals voorgeschreven is in Standaard 315. In de risicoanalyse legt de accountant de binnen het controleteam onderkende risico's vast en beschrijft hij welke interne beheersingsmaatregelen de entiteit hiervoor heeft getroffen. Accountants richten zich bij de risicoanalyse veelal op risico's die voortvloeien uit de omgeving van de onderneming (politieke en economische factoren) en op gebreken in de AO/IB van de onderneming. Van de accountant wordt echter tevens verlangd dat hij risico's die voortkomen uit het systeem van informatietechnologie onderkent[4]. De casus DigiNotar zoals beschreven in paragraaf 2.3.2 toont aan dat IT op zichzelf een risico kan genereren.

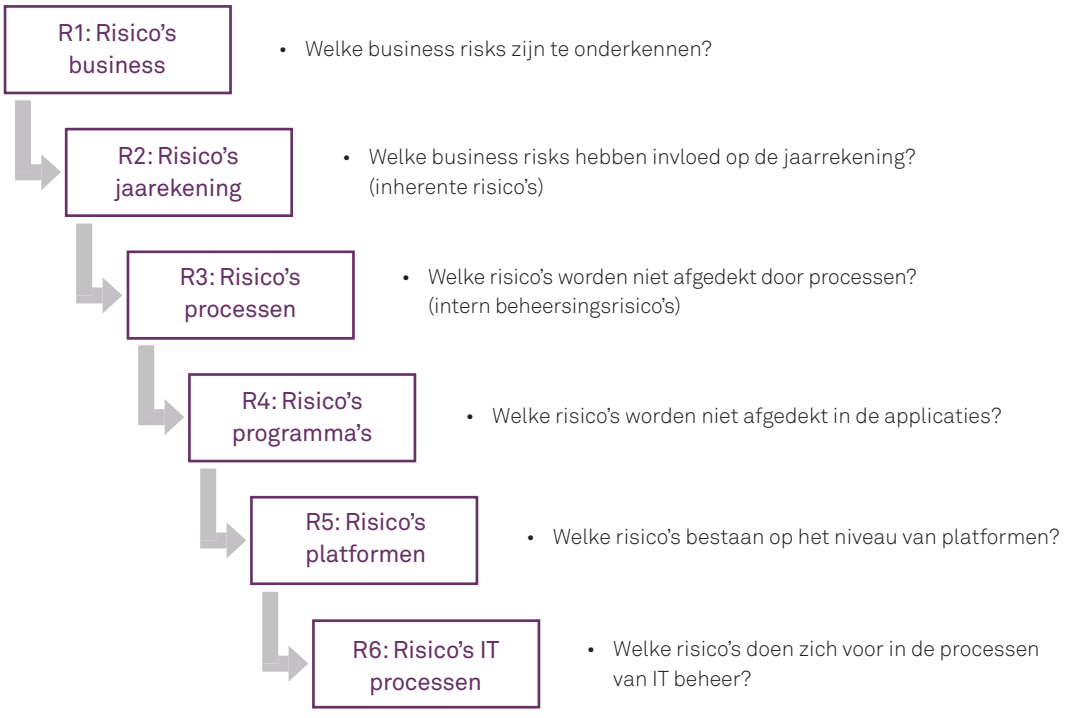
Voorbeeld

Standaard 315 geeft enkele voorbeelden die samenhangen met de geautomatiseerde gegevensverwerking[5]:

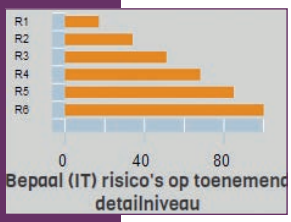
- onjuiste verwerking van gegevens;
- ongeautoriseerde toegang tot gegevens die tot gevolg kan hebben dat gegevens worden vernietigd of dat onjuiste wijzigingen worden aangebracht;
- te uitgebreide toegangsrechten waardoor functievermenging ontstaat;
- ongeautoriseerde wijzigingen van gegevens in basisbestanden;
- ongeautoriseerde wijzigingen in systemen of programma's;
- nalaten om noodzakelijke aanpassingen in systemen of programma's aan te brengen;
- ongepast handmatig ingrijpen;
- potentieel verlies van gegevens of het niet in staat zijn om gegevens indien nodig te benaderen.

Omdat Standaard 315 slechts voorbeelden geeft, is het belangrijk dat de accountant een model hanteert dat bijdraagt aan het verkrijgen van een volledig risicoprofiel. In de vorige paragraaf hebben we het P6 model gebruikt om kennis van de IT-omgeving op te doen. Ditzelfde model kunnen we gebruiken voor het evalueren van de risico's die voortvloeien uit de IT-omgeving, het R6 risicomodel:

Figuur 5: Het R6-model



4 Standaard 315, paragraaf 21
5 Standaard 315, paragraaf A56



Potentiële risico's (R1)

Een gedegen risicoanalyse start met de identificatie van de business risks. In paragraaf 2.2.1 is aangegeven dat steeds vaker een wisselwerking tussen de onderneming en zijn afnemers en leveranciers bestaat. Ondernemingen vormen daarmee steeds meer een keten. Bij het identificeren van risico's gaat de accountant na wat de gevolgen zijn van deze ketenafhankelijkheid. Om terug te pakken op het voorbeeld van de webwinkel: deze heeft (nagenoeg) geen voorraad, bestellingen van klanten leiden automatisch tot een order bij de leverancier. Wat zijn de gevolgen indien deze koppeling verstoord raakt? Of indien deze koppeling niet veilig genoeg is? Wat zijn de gevolgen voor de webwinkel indien het afrekenen via PayPal en/of iDeal niet werkt?

Posten (R2)

Vanuit de geïdentificeerde business risks bepaalt de accountant welke audit risks zijn te onderkennen. Dit zijn de business risks die aan een of meerdere jaarrekeningposten zijn te koppelen. De accountant bepaalt welke posten in de jaarrekening materieel zijn. Hier is de IT-auditor niet bij betrokken.

Processen (R3)

Op basis van de AO/IB beschrijving bepaalt de accountant welke van de geïdentificeerde risico's worden ondervangen in het stelsel van interne beheersing. Als een risico wordt gemitigeerd door de interne beheersing, stelt de accountant het bestaan van deze interne beheersingsmaatregel(en) vast. Indien het bestaan is vastgesteld, kan de accountant ervan uitgaan dat dit risico is afgedekt door de AO/IB. Hij richt zich dan op de resterende risico's.

Programma's (R4)

Van de risico's die worden gemitigeerd door de interne beheersing (uit stap 2) bepaalt de accountant welke door application controls worden gemitigeerd.

Platformen (R5)

Van de risico's die door application controls worden gemitigeerd, documenteert de accountant welke applicaties dit betreft. Van deze applicaties neemt de accountant in zijn dossier een beschrijving op van het platform waarop deze applicatie draait. De accountant overlegt met de IT-auditor of het soort platform risico's met zich mee brengt die nog niet eerder gesignaleerd zijn.

Processen van IT-beheer (R6)

Op basis van de informatie over het IT-beheer overlegt de accountant met de IT-auditor of het soort platform risico's met zich mee brengt die nog niet eerder gesignaleerd zijn.

Na het doorlopen van deze stappen heeft de accountant al dan niet tezamen met de IT-auditor de risico's in kaart gebracht die aandacht behoeven in de controle. Dit betreffen derhalve ook risico's die voortvloeien uit de IT, zoals bij R5 en R6 aan bod zijn gekomen. Deze risico's vormen de basis voor de controleaanpak.

2.4.2 Uitbesteding van IT-processen, applicaties en hardware

In het kader van inzicht in de entiteit en haar omgeving, besteedt dit hoofdstuk specifieke aandacht aan uitbesteding van IT. Steeds meer mkb- ondernemers brengen (een deel van) hun IT-omgeving in wat in meer commerciële bewoordingen "The Cloud" heet.

Cloud computing kenmerkt zich door de volgende karakteristieken:

- toegang tot applicatie en data kan alleen met een internetverbinding;
- gebruikers delen bronnen (bijvoorbeeld opslagruimte, rekencapaciteit, servers) met elkaar;
- de omgeving is naar rato van de gebruikersbehoefte flexibel op te schalen of in te krimpen;
- er is sprake van een hoge mate van zelfbediening in het beheer;
- de dienstverlening vindt plaats onder strikt gemonitorde en beveiligde condities;
- afrekenmodellen gaan uit van betaling naar gebruik en verbruik in plaats van betaling voor eigendom.

Afhankelijk van hetgeen wordt uitbesteed spreken we over Proces as a Service (PaaS), Software as a Service (SaaS) en Infrastructure as a Service (IaaS). "As a service" refereert hierbij aan de dienstverlening die de serviceverlenende partij (de serviceprovider) levert.

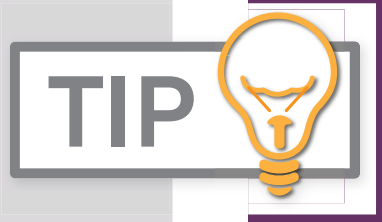
Er is een viertal varianten waarin cloudcomputing momenteel wordt aangeboden:

- Private cloud
  In een private cloud hebben alleen interne gebruikers van de eigen organisatie toegang tot applicaties en data. De opslag van de data vindt hierbij plaats in een omgeving die niet wordt gedeeld met anderen. Voorbeelden: het intranet van uw eigen organisatie, outlook mail.

- Community cloud
  In een community cloud hebben leden van de community toegang tot applicaties en data. De opslag van de data vindt hierbij plaats in een omgeving die wordt gedeeld met anderen. Voorbeelden: Facebook en Hyves.

- Hybride cloud
  Een hybride cloud is een mengvorm waarbij een deel van de applicatie en data omgeving algemeen toegankelijk is voor iedereen en een deel van de omgeving is afgeschermd voor leden van de community. De opslag van de data vindt hierbij plaats in een omgeving die deels wel en deels niet wordt gedeeld met anderen. Voorbeelden: LinkedIn waarbij gebruik wordt gemaakt van gesloten groepen. Online boekhouden.

- Public cloud
  Binnen de public cloud omgeving mag iedereen deelnemen die zich aanmeldt en heeft iedereen toegang tot de applicaties en de data. De opslag van de data vindt hierbij plaats in een omgeving die wordt gedeeld met anderen. Voorbeeld: Twitter, gmail en hotmail.

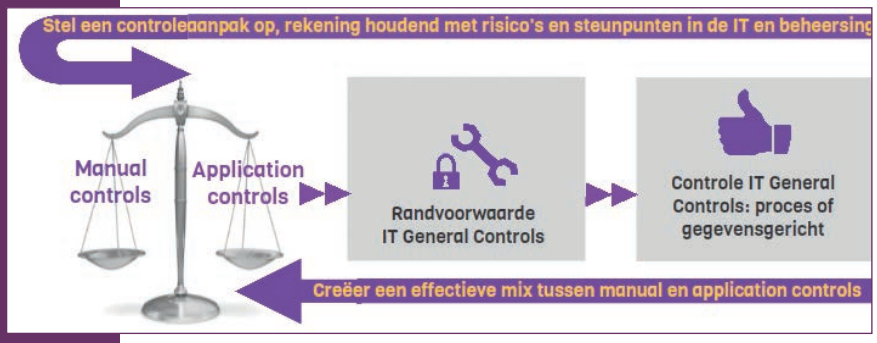


Indien er sprake is van uitbesteding van (een deel) van de IT-omgeving is het toepassen van Standaard 402 en daaraan gekoppeld Standaard 3402 aan de orde, indien de informatiestromen die verwerkt worden met de uitbestede componenten relevant zijn voor de financiële verslaglegging (zie Standaard 402.3).

Veel voorkomende voorbeelden waarin de toepassing van Standaard 3402 vereist kan zijn:
- de onderneming voert de boekhouding binnen een online boekhoudapplicatie;
- de onderneming heeft de salarisverwerking uitbesteed aan een serviceprovider;
- de onderneming heeft de vorm van een webwinkel;
- de volledige infrastructuur voor transactieverwerking wordt gehost in een extern rekencentrum.

In het algemeen geldt dat een ISAE 3402 verklaring nuttig kan zijn indien er een derde partij is die (een deel van) de AO/IB uitvoert.

De ISAE 3402 verklaring kent twee verschijningsvormen:
- **Type 1:** De verklaring beperkt zich tot de opzet van de interne beheersingsmaatregelen van de serviceorganisatie op een bepaald tijdstip;
- **Type 2:** De verklaring omvat de opzet, het bestaan en de werking van de interne beheersingsmaatregelen van de service organisatie over een bepaald tijdvak.



2.5 Controleaanpak en planning

De accountant plant de controle zo dat deze effectief en efficiënt is. Onder planning wordt verstaan:
- het vaststellen van de algehele controleaanpak;
- het ontwikkelen van een controleprogramma.

2.5.1 Controleaanpak

Op basis van de risicoanalyse en de geïdentificeerde beheersingsmaatregelen bepaalt de accountant de controleaanpak. Het vaststellen van de algehele controleaanpak omvat:

- Identificeren kenmerken van de opdracht bepalend voor de reikwijdte
  De accountant bepaalt de reikwijdte van de IT-audit aan de hand van de risicoanalyse.

- Overwegen van factoren die significant zijn voor het aansturen van de uit te voeren werkzaamheden

- Overwegen uitkomsten voorbereiding
  Indien de accountant tijdens zijn voorbereidende werkzaamheden geen contact heeft gehad met de IT-auditor, bespreekt de accountant na afronding van de voorbereiding zijn uitkomsten met de IT-auditor.

- Bepalen aard, timing en omvang benodigde middelen
  In de controleaanpak wordt de samenstelling van het controleteam beschreven. Of een IT-auditor nodig is in het controleteam, is een keuze van de accountant. Veelal zal bij een complexe IT-omgeving een IT-auditor worden toegevoegd aan het controleteam om over voldoende deskundigheid te beschikken. Echter bij een niet complexe IT-omgeving, kan de accountant ook besluiten om een IT-auditor aan het team toe te voegen. Dit zal het geval zijn indien de accountant zelf beperkte kennis heeft van IT, dan wel zich niet prettig voelt bij het zelf controleren van de IT. De controleaanpak geeft aan welk deel van de IT-audit de accountant zelf uitvoert en welk deel de IT-auditor zal uitvoeren.

  Om de controle effectief te houden is een inschatting nodig van de aan de IT-audit te besteden uren. Indien een IT-audit plaatsvindt, kunnen enkele traditionele controles vervallen om dubbel werk (en dus teveel kosten) te voorkomen. Voorbeeld: als het bestaan van een application control is vastgesteld en het change management goed is bevonden, is het niet nodig om 25 proceduretests uit te voeren op ditzelfde punt. De controleaanpak moet richting geven aan de planning door duidelijk te maken wanneer de IT-audit plaatsvindt en op welk moment de IT-auditor zijn werk zal aanvangen en afronden.

- Vaststellen rapportagedoelstellingen om de timing en de vereiste soort communicatie te kunnen plannen
  Uit de controleaanpak moet blijken op welke wijze de IT-auditor zijn werkzaamheden zal documenteren en wanneer en in welke vorm zijn bevindingen worden gerapporteerd.

2.5.2 Controleprogramma

Uiteindelijk leidt het uitwerken van de controleaanpak tot een controleprogramma waarin is beschreven welke systeemgerichte- en welke gegevensgerichte werkzaamheden worden uitgevoerd[6]. Wanneer wordt gesteund op de IT, zal in het controleprogramma moeten zijn beschreven welke automated controls en computer dependent controls worden getest bij de systeemgerichte werkzaamheden.

Bij de jaarrekeningcontrole toetst de accountant en/of de IT-auditor de volgende kwaliteitsaspecten:
- exclusiviteit
- integriteit
- controleerbaarheid
- continuïteit / beschikbaarheid

Een effectieve controle vereist dat de accountant en IT-auditor per post / proces overeenstemming hebben over de te controleren kwaliteitsaspecten en dat deze aansluiten bij de doelstellingen van de jaarrekeningcontrole.

2.6. Documentatie

Hetgeen in dit hoofdstuk is beschreven, dient door het controleteam samengevat en gedocumenteerd te worden in het controledossier. Om de audit trail overzichtelijk weer te geven, vatten we het voorgaande als volgt samen:

6 In dit studierapport gaan we uit van een mix van systeem- en gegevensgerichte werkzaamheden.

Tabel 2: Voorbeeld vastlegging risico-analyse

Proces	Applicatie	Besturingssysteem	IT-processen
Processen waaruit het risico voortvloeit en het proces waardoor de jaarrekening-post tot stand komt	Beschrijving van de applicatie die het proces ondersteunt	Beschrijving van de applicatie die het proces ondersteunt	Beschrijving van de applicatie die het proces ondersteunt

Risico	Jaarrekeningpost	Proces	Controls	Controleaanpak
Beschrijving van het risico op een afwijking van materieel belang in de jaarrekening	Posten waarop het risico betrekking heeft	Processen waaruit het risico voort-vloeit en het proces waardoor de jaarre-kening-post tot stand komt	Beschrijving van de relevante key -controls die het risico afdekken, uitgesplitst naar manuele, computer dependent en auto-mated controls. Geef hierbij aan in welke applicatie de automated controls zitten	Beschrijving op wel-ke wijze de controls getoetst worden; de toegepaste con-troleaanpak (sys-teem- dan wel gegevensgericht)

Daarnaast is documentatie vereist van de teambesprekingen die hebben plaatsgevonden.

2.7 Communicatie

Communicatie binnen het team

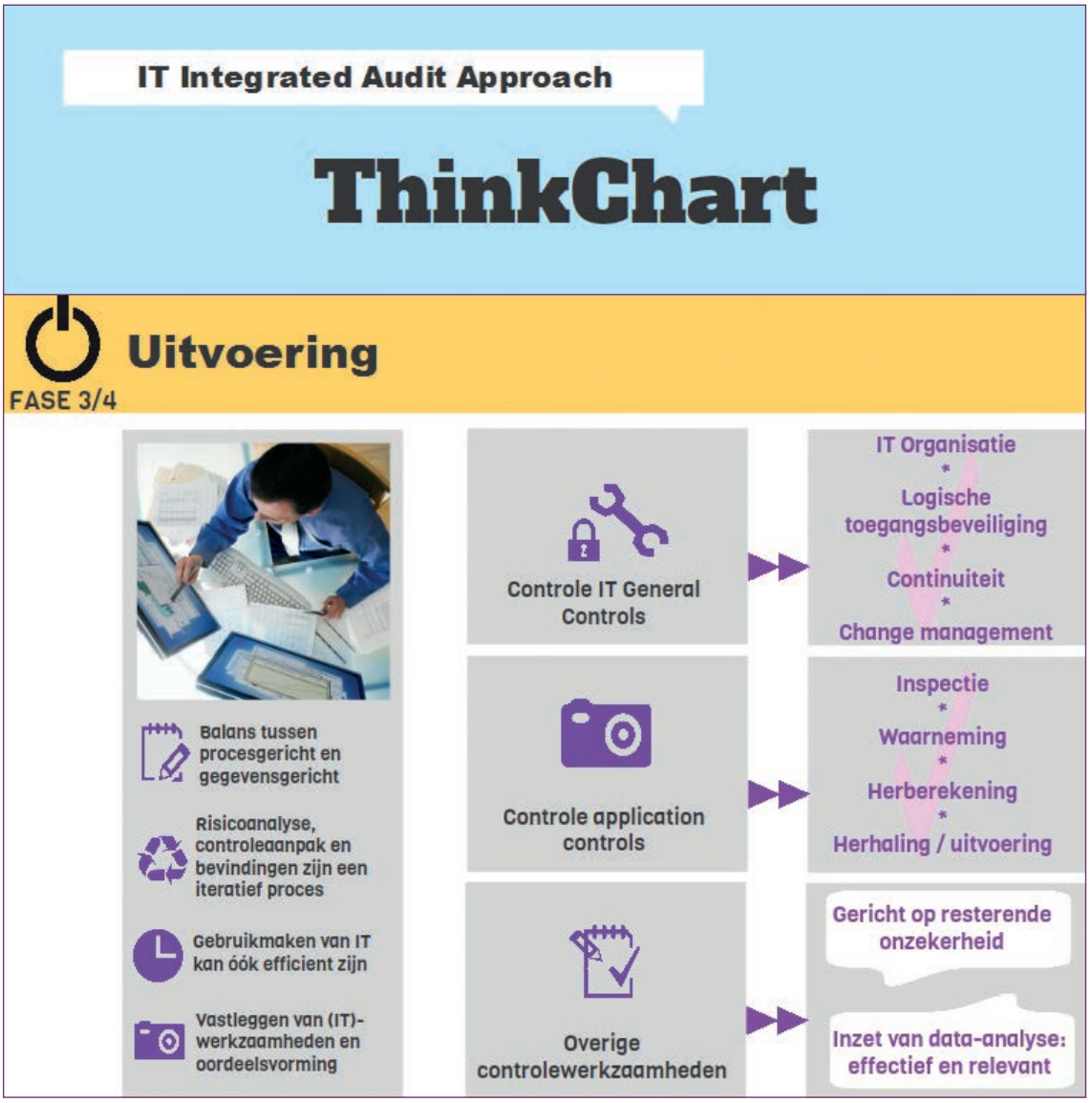
Voor de start van de controle vindt een pre-auditmeeting plaats. Bij een Integrated Audit Approach is de aanwezigheid van de IT-auditor gewenst. In de pre-auditmeeting worden de uitkomsten van de risicoanalyse besproken en de daaruit voortvloeiende controleaanpak en het controle-programma.

Communicatie met de klant

Indien sprake is van een heracceptatie van een controleopdracht, heeft het controleteam reeds inzicht in de IT-omgeving. Voor de uitvoering van de risicoanalyse is het raadzaam dat de accountant en/of IT-auditor de volgende informatie vergaart:

- Hebben veranderingen in de IT-architectuur plaatsgevonden?
- Hebben veranderingen in de IT-organisatie plaatsgevonden?
- Hebben veranderingen in samenwerking met IT-leveranciers plaatsgevonden?
- Zijn er problemen geweest in het IT-beheer?
- Welke veranderingen staan gepland voor de komende periode?

Om de werkzaamheden te kunnen uitvoeren, heeft het controleteam toegang tot gegevens nodig. De accountant moet tijdig communiceren wanneer deze toegang noodzakelijk is, en welke gegevens nodig zijn. Tevens zijn afspraken nodig met functionarissen die in aanmerking komen voor een interview.


IT Integrated Audit Approach
ThinkChart
Uitvoering
FASE 3/4
Balans tussen procesgericht en gegevensgericht
Risicoanalyse, controleaanpak en bevindingen zijn een iteratief proces
Gebruikmaken van IT kan óók efficient zijn
Vastleggen van (IT)-werkzaamheden en oordeelsvorming
Controle IT General Controls
Controle application controls
Overige controlewerkzaamheden
IT Organisatie * Logische toegangsbeveiliging * Continuiteit * Change management
Inspectie * Waarneming * Herberekening * Herhaling / uitvoering
Gericht op resterende onzekerheid
Inzet van data-analyse: effectief en relevant

3. Interimcontrole

3.1 Inleiding

Inhoud en samenhang met andere hoofdstukken

In het vorige hoofdstuk Risicoanalyse en planning, is kennis verworven van de cliëntomgeving en IT-omgeving. Tevens is vastgesteld welke interne beheersingsmaatregelen in opzet en bestaan aanwezig zijn. Hieruit is een controleprogramma ontstaan waarin de aanpak in systeem- en/of gegevensgerichte maatregelen is beschreven. Tijdens de interimcontrole worden de hierin opgenomen systeemgerichte werkzaamheden uitgevoerd door de beheersingsmaatregelen waarop gesteund zal worden te testen op werking.

In dit hoofdstuk behandelen wij de relevante aspecten voor de interimcontrole. In het volgende hoofdstuk komen de werkzaamheden met betrekking tot de eindejaarscontrole aan de orde. Dit betreffen de gegevensgerichte werkzaamheden.

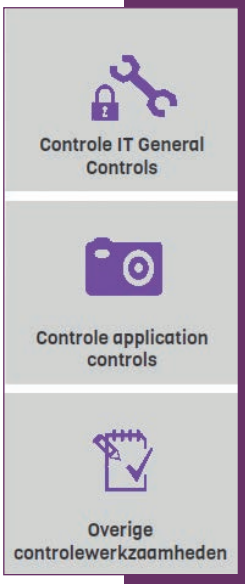
Doelstelling

Na het lezen van dit hoofdstuk is de accountant in staat om:

- de werking van de application controls vast te stellen;
- de werking van de General IT Controls vast te stellen;
- compenserende systeemgerichte of gegevensgerichte maatregelen te bepalen indien de General IT Controls niet op orde zijn.

3.2 Voorbereiding van de interimcontrole

De planningsfase zoals beschreven in hoofdstuk 2 is afgesloten met een controleprogramma waarin beschreven is welke systeemgerichte- en gegevensgerichte werkzaamheden zijn uit te voeren. Ter voorbereiding op de interimcontrole wordt bepaald welke van deze werkzaamheden reeds (deels) mogelijk zijn tijdens de interimcontrole. Vervolgens worden de noodzakelijke teamleden gereserveerd in de planning en indien van toepassing worden ook afspraken gemaakt met externe deskundigen.



Voorafgaande aan de interimcontrole wordt een zogenaamde prepare by client list opgesteld. Hierin zijn de gegevens opgenomen die het team aan het begin van de interimcontrole nodig heeft. Ook de informatie die nodig is om de werking van de General IT Controls te testen is hierop vermeld. Daarnaast is het noodzakelijk om databestanden die nodig zijn voor data-analyse op de lijst te vermelden zodat deze tijdig kunnen worden opgeleverd.

Voorbeeld

Voorbeelden met betrekking tot op te vragen prepare by client list:

- overzicht gebruikers en autorisaties
- release notes van belangrijke applicaties
- overzicht met wijzigingen indien deze worden bijgehouden

Met de cliënt worden afspraken gemaakt met wie gesproken zal worden en wanneer. De aanwezigheid van de systeembeheerder is voor de IT-werkzaamheden een belangrijk aandachtspunt. Tevens zijn praktische zaken te regelen zoals toegang tot het kantoornetwerk van de cliënt en de toegang tot de relevante IT-systemen bij de cliënt.

Ook vindt nu de detailuitwerking van de werkprogramma's voor interimcontrole plaats, voor zover dat niet reeds tijdens de risicoanalyse en planningsfase is gedaan. Bij het opstellen van de werkprogramma's zullen keuzes worden gemaakt zoals welke tools en technieken worden ingezet. Worden data-analyses op het IT-systeem van de cliënt gedraaid of wordt een dump van de gegevens opgevraagd en met pakketten zoals ACL en IDEA verder geanalyseerd? Daarnaast maken de werkprogramma's duidelijk hoeveel deelwaarnemingen nodig zijn. Dit is onder meer afhankelijk van de periodiciteit van de betreffende controls. Nadat de werkzaamheden in detail zijn vastgesteld en uitgewerkt in werkprogramma's kunnen ze verder worden voorbereid. Interviewlijsten worden opgesteld en wellicht worden vragenlijsten al voor de daadwerkelijke interim-controle naar de cliënt gestuurd ter voorbereiding. Daarnaast zullen op te vragen databestanden worden gedocumenteerd en query's worden bepaald. Mogelijkerwijs worden reeds proefbestanden opgevraagd om te bepalen of deze aan de verwachtingen voldoen zodat de werkzaamheden tijdens de interimcontrole zo effectief en efficiënt mogelijk kunnen plaatsvinden.

3.3 Uitvoeren systeemgerichte werkzaamheden gericht op key-controls

Nadat aan de hand van het controleprogramma de gedetailleerde werkprogramma's zijn opgesteld, worden de systeemgerichte werkzaamheden uitgevoerd. Deze bestaan uit lijncontroles en proceduretests:

- lijncontroles dienen om vast te stellen of de in de administratieve organisatie in opzet beschreven key-controls ook werkelijk bestaan. Een vereiste is dat de lijntest alle voorkomende situaties voldoende afdekt;
- proceduretests worden uitgevoerd om de werking van de key-controls vast te stellen.

We werken dit hierna uit voor application controls en General IT Controls.

Ter herinnering: over de application controls zeiden we in paragraaf 2.3.2 dat als je hebt vastgesteld dat een application bestaat, je tevens de werking ervan hebt vastgesteld - tenzij wijzigingen hebben plaatsgevonden.

De tabellen in bijlage 7 bevatten voorbeelden van veel voorkomende beheersingsmaatregelen per proces. Tevens is de relatie gelegd tussen controledoelstellingen, IT-auditdoelstellingen , mogelijk te testen application controls en gerelateerde te testen General IT Controls. De categorisering van beheersingsmaatregelen (manual controls, computer dependent manual controls en automated controls) is niet absoluut, maar kan variëren per onderneming en per softwareoplossing. Daarom zijn in de tabel ook bij de manual controls verwijzingen naar mogelijk te testen application controls en General IT Controls opgenomen. Op deze wijze is de tabel ook bruikbaar als een key-control in een andere categorie valt.

Let op efficiency
Bij een manual control heeft het uiteraard geen zin om naar application controls of General IT Controls te zoeken.

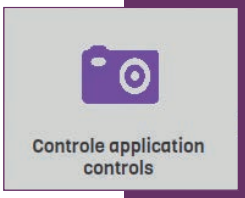
In het geval van een computer dependent control volstaat het om te kijken naar de totstandkoming van het overzicht en de kwaliteit van de General IT Controls om de betrouwbaarheid van de verkregen output vast te kunnen stellen. Alleen in het geval van een automated control is het nodig om zowel application controls als General IT Controls te testen.

3.3.1 Testen van application controls

Voor het testen van application controls kun je de volgende controlemiddelen inzetten:

- inspectie
- waarneming
- externe bevestiging
- herberekening
- het opnieuw uitvoeren
- cijferanalyse
- verzoeken om inlichtingen

Afhankelijk van de aard van de application control verschillen de testwerkzaamheden. De toepassing van deze controlemiddelen bij de IT-audit beschrijven we hierna.



Inspectie

Inspectie is vooral het aangewezen controlemiddel als een application control gebaseerd is op instellingen in het systeem. Denk bijvoorbeeld aan instellingen die bepalen wie welke rechten heeft in het systeem. Vergeet bij application controls die aan en uit te zetten zijn bovendien niet vast te stellen dat deze op het controlemoment aan staan.De werkzaamheden kun je uitvoeren door het systeem te raadplegen of door relevante tabellen met instellingen (parameters) op te vragen.

Waarneming

Voor de application controls die gebaseerd zijn op autorisaties of meteen visueel als resultaat (bijvoorbeeld een foutmelding), is het mogelijk om deze te testen via directe waarneming. Uitgangspunt is dat hierbij gewerkt wordt in de live-omgeving met live-data.

Externe bevestiging
Als de software of het beheer is uitbesteed kun je ook bij derden een opgave opvragen in de vorm van een ISAE 3402[8].

Herberekening
Als een application control gebaseerd is op rekeningkundige berekeningen, dan kun je de application control testen door de uitkomst zelf opnieuw te berekenen.

Het opnieuw uitvoeren
Een veelvoorkomende manier om application controls te testen, is door de uitvoering te herhalen. Hierbij is het van belang om zowel een situatie te testen die door de application control wordt getest, als een situatie die de application control dient tegen te houden. Voorbeeld hiervan is het testen van de 3-way match met een factuurprijs met een afwijking binnen de toleranties en een factuurprijs met een afwijking buiten de toleranties.

Cijferanalyse
Voor application controls die gericht zijn op de redelijkheid van gegevens dan wel totaal- en verbandscontroles, is cijferanalyse een geschikt controlemiddel. Het is overigens wel de vraag of je hiermee de application control test of dat je eigenlijk met gegevensgerichte werkzaamheden bezig bent. Immers, als je geen fout constateert, betekent dat nog niet per se dat de application controle gewerkt heeft.

Verzoeken om inlichtingen
Inlichtingen zullen nooit een zelfstandig controlemiddel zijn, maar ze kunnen wel richtinggevend zijn voor de inzet van de overige controlemiddelen. Komt bijvoorbeeld uit de inlichtingen naar voren dat een application control in een bepaalde release niet gewerkt heeft, dan is het zinloos om deze te testen over de betreffende periode.

Een valkuil bij het testen van application controls is dat te veel wordt gedaan. Test alleen die application controls waar de controle op steunt en richt je louter op de te bereiken controledoelstelling.

De computer dependent control vraagt bijzondere aandacht. Dit zijn handmatige beheersingsmaatregelen die gebruikmaken van informatie die het informatiesysteem genereert - het geautomatiseerde deel. Het handmatige deel zal je testen op een manier die gebruikelijk is bij manual controls. Bij de controle van het geautomatiseerde stel je vast dat de informatie betrouwbaar is. Hierbij is onder meer van belang of het een standaardrapportage of een maatwerkrapportage betreft. Standaard rapportages uit een standaard applicatie hebben normaliter een lager risicoprofiel dan zelf gebouwde rapportages. Afhankelijk van de situatie kunnen bijvoorbeeld de volgende acties worden uitgevoerd:

- sluit de verkregen rapportage aan op de (sub-)administratie of andere gecontroleerde rapportages;

8 Dit is een standaard voor standaard Third Party Assurance rapportages. Met zo'n 'derdenverklaring' kan het management van een serviceorganisatie waar een gebruikersorganisatie activiteiten aan heeft uitbesteed, aantonen 'in control' te zijn.

- ga na of er selectiecriteria zijn gebruikt voor de rapportage en of deze selecties aanvaardbaar zijn voor het doel;
- reken bewerkingen en formules in de rapportage na (bij voorkeur door de rapportage ook digitaal te controleren met controleformules);
- ga na of verkregen rapportage juist en volledig uit onderliggende brondata is opgebouwd door:
  - vanuit de brondata de rapportage te reconstrueren, of
  - de gehanteerde queries en broncodes te reviewen vanuit de kennis van de brondata en
  - systemen en de controledoelstelling.
- beoordeel of de change managementprocessen voldoende rekening houden met de impact van een wijziging op de rapportages.

Voorbeeld

Het beoordelen van een uitzonderingsrapportage over lage marges is een voorbeeld van een computer dependent control. Het geautomatiseerde deel hiervan bestaat uit de selectie van transacties voor opname in het overzicht. Dit deel van de control test je als application control.

3.3.2 Testen van de werking van General IT Controls

Zoals eerder aangegeven, is een noodzakelijke voorwaarde voor de werking van de application controls gedurende de gehele controleperiode, dat ook de relevante General IT Controls gewerkt hebben. Niet alle General IT Controls hoeven relevant te zijn voor de werking van een application control. In onderstaande tabel staat de relatie tussen application controls en General IT Controls:

Tabel 3: Relatie application en general IT-controls

	Logische toegangsbeveiliging	Wijzigingsbeheer	Continuïteit
Automated controls	*	**	
Automated controls gebaseerd op autorisaties in het systeem	**	**	
IT dependent controls	*	**	

Kort samengevat is wijzigingsbeheer altijd relevant. Voor de controls die niet gebaseerd zijn op autorisaties is logisch toegangsbeheer alleen relevant voor zover het betrekking heeft op het wijzigen van de instellingen van de applicatie.

In deze paragraaf bespreken we achtereenvolgens logische toegangsbeveiliging en wijzigingsbeheer. Tot slot behandelen we de continuïteitsmaatregelen.

Logische toegangsbeveiliging

Specifiek voor die application controls die steunen op autorisaties is het van belang om de werking van de logische toegangsbeveiliging te testen. Bij de beoordeling van maatregelen is het overigens onnodig om alle autorisaties te betrekken. Het is voldoende om de key-controls voor de minimaal vereiste functiescheiding te beoordelen. Het testen van de werking van de maatregelen vindt overeenkomstig de gebruikelijke handmatige procedure plaats. Te denken valt aan procedures voor:

- de periodieke review van alle toegangsrechten;
- het aanmaken respectievelijk wijzigen van toegangsrechten;
- het blokkeren van toegangsrechten.

Voorbeeld

Blokkeren van orders bij overschrijding van een kredietlimiet is een voorbeeld van een application control waarbij vooral wijzigingsbeheer relevant is.

Tekortkomingen in de maatregelen voor logische toegangsbeveiliging kun je in sommige gevallen ondervangen door aanvullende systeem- of gegevensgerichte werkzaamheden uit te voeren, terwijl toch nog door het systeem heen kan worden gecontroleerd. In onderstaande tabel is hier een overzicht van opgenomen:

Tabel 4: Overzicht compenserende maatregelen logische toegangsbeveiliging

	Compenserende systeemgerichte maatregelen	Compenserende gegevensgerichte maatregelen
Gebruikers hebben geen eigen account	-	-
Wachtwoorden zijn bekend, hoeven niet aangepast te worden of zijn niet complex	-	-
Geen interne periodieke review plaats van de toegekende rechten	Zelf toegekende rechten beoordelen	-
Vastleggingen over wijzigen en intrekken van rechten ontbreken	Aan de hand van logboek vaststellen wat de wijzigingen zijn geweest in toegekende rechten, respectievelijk inhoud van rollen en toegekende rollen.	-
Rechten in het systeem zijn te ruim ingesteld	Interne monitoring op uitvoeren kritische functies en handmatige autorisaties buiten het systeem	Voor key-functies via data-analyse vaststellen dat gebruikers geen handelingen hebben uitgevoerd buiten functieomschrijving

Wijzigingsbeheer

Een adequaat proces van wijzigingsbeheer is noodzakelijk om op de eerste plaats vast te kunnen stellen of er wijzigingen zijn geweest in de application controls en op de tweede plaats of de wijzigingen zijn getest en goedgekeurd door de gebruikersorganisatie. Hierbij gaat het alleen om de application controls waarop de accountant in zijn controle wenst te steunen. Voorwaarde is dat kan worden vastgesteld welke wijzigingen in de relevante applicaties hebben plaatsgevonden. In een adequaat opgezet proces zullen wijzigingen worden bijgehouden in een aparte registratie. In het mkb is dit niet altijd het geval. Daar waar met standaard software wordt gewerkt, is het mogelijk om aansluiting te zoeken bij de release-informatie van de leveranciers. Releases zijn doorgaans doorlopend genummerd zodat de volledigheid van de mogelijke wijzigingen is vast te stellen.

Om de werking van het proces van wijzigingsbeheer te testen is een proceduretest op een aantal relevante wijzigingen nodig. Vast te stellen is dat deze zijn getest, zijn goedgekeurd en de testdocumentatie beoordeeld. Het aantal uit te voeren proceduretesten bepaal je op dezelfde manier als bij overige handmatige beheersingsmaatregelen.

Voorbeeld

Autorisatie van verkooporders is een voorbeeld van een application control waarbij ook logische toegangsbeveiliging relevant is.

Tekortkomingen in het wijzigingsbeheer zijn in sommige gevallen te ondervangen met aanvullende systeem- of gegevensgerichte werkzaamheden, terwijl toch nog door het systeem heen kan worden gecontroleerd. In onderstaande tabel is hier een overzicht van opgenomen:

Tabel 5: Overzicht compenserende maatregelen wijzigingsbeheer

	Compenserende systeemgerichte maatregelen	Compenserende gegevensgerichte maatregelen
Wijzigingen worden niet geregistreerd	Bij standaardapplicaties: aansluiting zoeken bij de release notes van de leverancier, raadplegen updatehistorie. Bij maatwerk uitgevoerd door derden: aansluiting zoeken bij communicatie, kostenfacturen derden, raadplegen versielog. Intern uitgevoerd maatwerk: raadplegen transportsoftware op verplaatsingen van ontwikkel naar test en live-omgeving.	-

Vervolg tabel 5: Overzicht compenserende maatregelen wijzigingsbeheer

	Compenserende systeemgerichte maatregelen	Compenserende gegevens-gerichte maatregelen
Scheiding tussen ontwikkel, test en productieomgeving is niet op orde	Bij standaardapplicaties en extern maatwerk minder relevant. Bij interne ontwikkeling: steunen op interne vergelijkingen tussen omgevingen, logboek en toegang tot omgevingen.	-
Wijzigingen worden onvoldoende getest	Bij standaardapplicaties: vaststellen dat release notes zijn doorgenomen door cliënt. Relevante wijzigingen zelf testen, application controls verschillende keren testen.	-

Continuïteit

Continuïteitsmaatregelen richten zich op de beschikbaarheid van gegevens en het informatiesysteem in het algemeen. Deze maatregelen zijn van belang voor de jaarrekeningcontrole aangezien:

- bij systeemverstoringen de informatie waarop al interne controle heeft plaatsgevonden, kan worden teruggezet. Bij herstel van informatie op een later moment valt mogelijk niet te steunen op de interne beheersingsmaatregelen over de betreffende periode;
- bij een onderneming die sterk afhankelijk is van het informatiesysteem systeemverstoringen de continuïteit van de organisatie in gevaar kunnen brengen.

Een opmerking bij het eerste punt is dat systeemverstoringen niet relevant voor de controle hoeven te zijn indien is vastgesteld dat geen dataverlies is ontstaan. Het tweede punt (sterke afhankelijkheid) is echter wel altijd relevant. Omdat dit een toekomstgericht aspect in de jaarrekening is, zijn de continuïteitsmaatregelen belangrijk.

Continuïteitsmaatregelen richten zich zowel op het maken van backups als op het terugzetten daarvan. Belangrijke maatregelen zijn:

- maken van backups op een externe locatie;
- testen van backups;
- uitvoeren van recovery tests: vaststellen dat het informatiesysteem werkend kan worden teruggezet;
- regelen van uitwijkmogelijkheden.

Voorbeeld

Backup en recovery	
Maandelijks een integrale backup, elke dag incrementele backups.	Stel aan de hand van de logging in de backup-software vast dat de backups zijn gemaakt.
Dagelijks wordt vastgesteld of de backup geslaagd is.	Stel aan de hand van interne vastlegging vast dat vastgesteld is of de backup geslaagd is.
Backups worden bewaard op een externe locatie.	Stel aan de hand van de instellingen in de backup-software vast waar de back-up bewaard wordt.
Periodieke tests van het terugzetten van de backup (recovery test).	Stel vast dat een recovery test is uitgevoerd, beoordeel het testplan en de uitkomsten.
Broncode van maatwerksoftware is in escrow geplaatst.	Vraag van de escrow-agent een verklaring dat de (juiste versie van) de software daar is ondergebracht.
Uitwijk	
Afspraken met leveranciers over vervangende apparatuur.	Stel aan de hand van contracten vast dat deze afspraken gemaakt zijn en betrekking hebben op relevante systemen.
Fysieke beveiliging	
Toegang tot de serverruimte.	Stel door waarneming ter plaatse vast dat de getroffen maatregelen aanwezig en operationeel zijn.
Maatregelen tegen calamiteiten zoals brand, wateroverlast.	
Noodstroomvoorzieningen.	

3.4 Uitbesteding van IT processen, applicaties en hardware

Zoals beschreven in paragraaf 2.4 worden delen van de IT steeds vaker uitbesteed en dient aandacht te worden besteed aan Standaard 402 en Standaard 3402. Hieronder beschrijven we welke werkzaamheden hierbij nodig zijn.

3.4.1 Standaard 402 en de interim controle

Standaard 402 behandelt de overwegingen die voor de accountant van belang zijn als de organi-

satie een serviceorganisatie heeft ingeschakeld. Hiervan is sprake als (een deel van) de IT is uitbesteed, bijvoorbeeld door gebruik van software die via de cloud wordt aangeboden. In hoeverre hiervoor aandacht van de accountant nodig is hangt ervan af of, en zo ja in welke mate, de uitbestede diensten relevant zijn voor de financiële verslaggeving. Voor een goede risicoanalyse heb je voldoende inzicht nodig in de diensten van de serviceorganisatie. Als blijkt dat deze diensten invloed hebben op de transactiestromen of financiële administratie en/of een belangrijk onderdeel uitmaken van de interne beheersing van de gecontroleerde organisatie, dan is inzicht vereist in de beheersingsmaatregelen bij de serviceorganisatie. Dit kan bijvoorbeeld door een derdenverklaring ('third party'-rapport) over de interne beheersingsmaatregelen van de serviceorganisatie op te vragen.

3.4.2 Standaard 3402 en de interim controle

Standaard 3402 behandelt assurance-rapporten over de interne beheersingsmaatregelen bij een serviceorganisatie. Wanneer de IT is uitbesteed zal de accountant een ISAE 3402-verklaring moeten opvragen bij de service provider waar de dienst is ondergebracht. ISAE 3402 is de aan ISA 3402 gerelateerde IT-standaard. Indien de accountant een ISAE 3402-verklaring ontvangt van de accountant van de serviceprovider zijn de volgende vragen aan de orde om te bepalen of de verklaring bruikbaar is.

1. Omvat de onderzoeksperiode van het rapport het geheel of in elk geval een deel van de verslaggevingsperiode van de uit te brengen jaarrekening?
2. Is er sprake van een type 1 of 2 rapport?
3. Zijn de in de bijlage van het rapport beschreven interne beheersingsmaatregelen relevant voor de jaarrekening?
4. Is de serviceprovider impliciet of expliciet uitgegaan van interne beheersingsmaatregelen bij de onderneming zelf en zijn deze ook aanwezig?
5. Is er sprake van onderaannemers (subcontractors) bij de service provider en zijn de interne beheersingsmaatregelen van deze onderaannemers wel ('inclusive' methode) of niet ('carve out' methode) meegenomen in de ISAE 3402 verklaring van de service provider?
6. Zijn er tekortkomingen in het stelsel van interne beheersingsmaatregelen bij de serviceprovider aangegeven die relevant zijn voor materiële posten of processen in de jaarrekening?
7. Is er nader onderzoek of afstemming door of met de accountant van de serviceprovider nodig om voldoende aanvullende zekerheid te verkrijgen?

Voor het opstellen van een normenkader voor de toetsing conform ISAE 3402 wordt veelal gebruikgemaakt van gangbare raamwerken zoals Coso, Cobit, ISO 27001 en 27002, NOREA studierapport voor uitbestede ICT beheerprocessen. Het is aan te raden dat de accountant zich vergewist of de gebruikte raamwerken passen bij de mate van zekerheid die nodig is voor een controle van de jaarrekening.

Voorbeeld

Gebruik van alleen ISO 27001 of 27002 voor de toetsing biedt onvoldoende zekerheid. Deze twee raamwerken gaan uitsluitend over informatiebeveiliging en niet over de correcte verwerking van transacties.

3.5 Documentatie

Documentatie van de uitgevoerde werkzaamheden gericht op application controls zal over het algemeen bestaan uit de opgevraagde gegevens uit het systeem zoals tabellen om instellingen te beoordelen of screenshots van waarnemingen. Afhankelijk van de gebruikte controlemiddelen worden ook hardcopy-documenten aan het dossier toegevoegd.

Tabellen

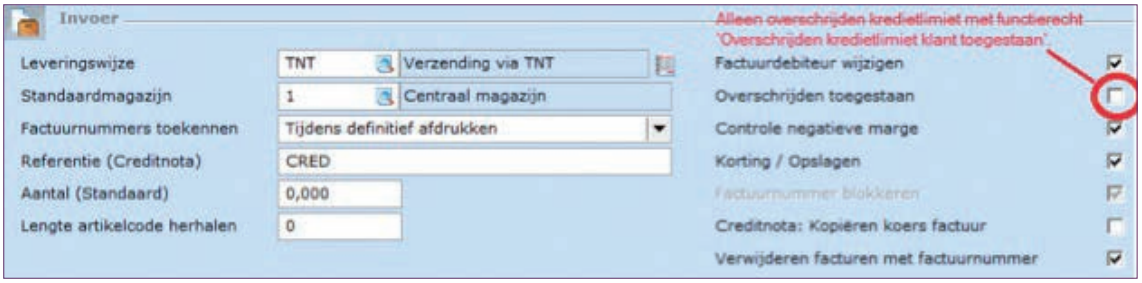
Bij het gebruik van tabellen is het van belang om een aantal praktische zaken duidelijk vast te leggen. Zo is het nodig dat de audit trail zichtbaar is, niet alleen voor controle van het verslaggevingsjaar maar ook om de controle het volgende jaar efficiënt te kunnen uitvoeren. Het gaat onder meer om:

- welke tabellen zijn opgevraagd;
- welke velden zijn geselecteerd;
- wat de betekenis is van de velden;
- welke selectiecriteria zijn gehanteerd.

Indien tabellen worden bewerkt of op een andere manier worden gepresenteerd dan het origineel (bijvoorbeeld door data-velden samen te voegen) moet ook dit voldoende zichtbaar zijn. Ter onderbouwing van de conclusies behoren in ieder geval de eindrapportages van de analyses een plaats in het dossier te krijgen.

Screenshots

Waarnemingen in het systeem worden doorgaans gedocumenteerd via screenshots. Geef voor de duidelijkheid op de screenshot de gecontroleerde aspecten aan.



Bron: Exact Software

Significante tekortkomingen

Standaard 265 geeft een definitie van '(significante) tekortkomingen'.

a. **Tekortkoming in de interne beheersing.**
   Deze bestaat indien:
   i. een interne beheersingsmaatregel op dusdanige wijze is opgezet, geïmplementeerd of operationeel is dat deze niet in staat is om afwijkingen in de financiële overzichten tijdig te voorkomen, of te ontdekken en te corrigeren; of
   ii. een interne beheersingsmaatregel ontbreekt die nodig is om afwijkingen in de financiële overzichten tijdig te voorkomen, of te ontdekken en te corrigeren

b. **Significante tekortkoming in de interne beheersing.**
   Een tekortkoming of een combinatie van tekortkomingen in de interne beheersing die, op grond van het professionele oordeel van de accountant, voldoende belangrijk is om de aandacht van degenen belast met governance te verdienen

Volgens deze definitie zijn tekortkomingen reeds in de risicoanalysefase vast te stellen omdat al van een tekortkoming sprake is als interne beheersingsmaatregelen niet adequaat zijn opgezet of geïmplementeerd. In de fase van de interim-controle richt de accountant zich op de tekortkomingen die ontstaan doordat de key-controls niet gedurende de gehele controle periode operationeel zijn.

Het is aan de accountant zelf om een afweging te maken of het een tekortkoming dan wel een significante tekortkoming betreft. Standaard 265.9 schijft voor dat de significante tekortkomingen schriftelijk worden gecommuniceerd aan degene die belast is met governance.

Deze regels voor de vaststelling van tekortkomingen gelden eveneens voor application controls en General IT Controls. De beoordeling doet de accountant in overleg met de IT-auditor, indien deze in het opdracht team is opgenomen. Indien de accountant significante tekortkomingen signaleert zal hij deze rapporteren.

Voorbeelden van tekortkomingen in de IT zijn gebreken in de logische toegangsbeveiliging die een verhoogd frauderisico met zich meebrengen of een niet beheerst proces van wijzigingsbeheer. Hierbij zal de accountant de afweging maken wat bij een specifieke cliëntomgeving minimaal mag worden verwacht.

In de risicoanalysefase heeft de accountant een controleaanpak bepaald die (deels) steunt op systeemgerichte maatregelen. Als uit de interimcontrole naar voren komt dat de geselecteerde key-controls niet operationeel zijn geweest gedurende de gehele controleperiode heeft dat gevolgen voor de risico-inschatting. Eventueel zoekt de accountant naar compenserende maatregelen. Zo niet, dan neemt het restrisico toe, wat meer gegevensgerichte werkzaamheden noodzakelijk zijn.

Actualiseren controleprogramma en rapportagebevindingen

De uitkomsten van de interimcontrole worden besproken in het team. Doorgaans vindt dit reeds gedurende de interimcontrole plaats. Op basis van de uitkomsten wordt bepaald of voor tekortkomingen in key-controls, mitigerende maatregelen kunnen worden geselecteerd of dat aanvullende gegevensgerichte werkzaamheden nodig zijn. Indien een key-control om bepaalde redenen gedurende een bepaalde periode niet operationeel is geweest, hoeven aanvullende maatregelen zich alleen op die periode te richten. Ook deze werkzaamheden zijn dan al tijdens de interimcontrole mogelijk.

Het is van belang om de uitkomsten uit de interim-controle met de cliënt te bespreken. Daarbij is het nodig om niet louter de tekortkomingen zelf te rapporteren, maar ook de oorzaak ervan te achterhalen. Dit voorkomt dat de accountant verkeerde conclusies trekt.

De aanvullende systeem- en/of gegevensgerichte controlemaatregelen worden vervolgens gepland. Door de bijstelling van de werkzaamheden is het tevens van belang om het budget aan te passen en dit af te stemmen met de cliënt.

De uitgangspunten van de risicoanalyse- en planningsfasen worden na de interimcontrole geëvalueerd en indien nodig bijgesteld. De uitkomsten van de interimcontrole zijn vervolgens het startpunt van de eindejaarscontrole. De eindejaarscontrole beschrijven we in hoofdstuk 4.

3.6 Communicatie

Communicatie binnen het team

De werkzaamheden en de benodigde gegevens dienen afgestemd te worden met de IT-auditor. Ter afronding van de interimcontrole worden de geconstateerde tekortkomingen binnen het team besproken. Daarbij is het noodzakelijk te bepalen wat de consequenties hiervan zijn voor de eerder gemaakte risicoanalyse en het opgestelde controleprogramma en ook welke gevolgen dit heeft voor de geplande werkzaamheden bij de eindejaarscontrole.

Communicatie met de klant

In deze fase is een gesprek met de opdrachtgever nodig over de uit te voeren werkzaamheden die de beschikbaarheid van enkele functionarissen vereisen. Voor de uit te voeren werkzaamheden ontvangt de cliënt een prepared by client list.

Ter afronding van de interim-controle is het aan te raden de geconstateerde tekortkomingen met de cliënt te bespreken. Na afstemming volgt rapportage van de tekortkomingen in de managementletter. De wet verlangt dat de accountant in zijn accountantsverslag aandacht besteedt aan de geautomatiseerde gegevensverwerking. Artikel 393 lid 4 BW2 luidt:

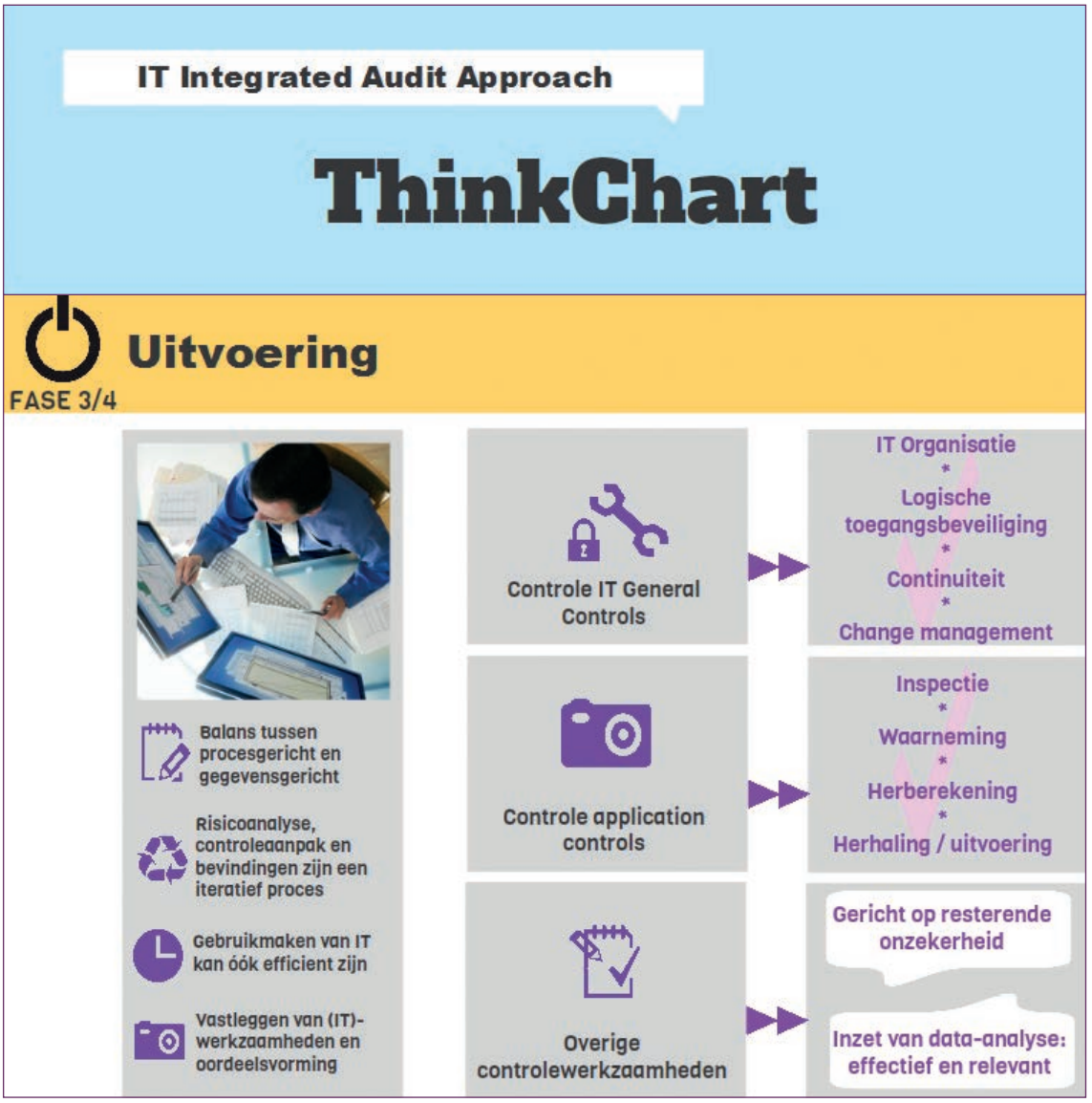
"De accountant brengt omtrent zijn onderzoek verslag uit aan de raad van commissarissen en aan het bestuur. Hij maakt daarbij ten minste melding van zijn bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking."

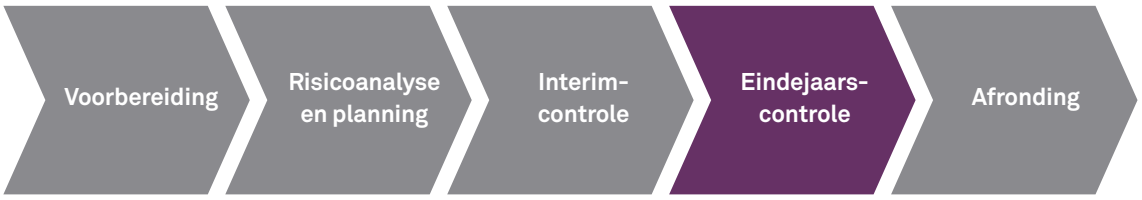
Deze bepaling is in het Burgerlijk Wetboek opgenomen naar aanleiding van de invoering in 1993 van de Wet Computercriminaliteit. Volgens Audit Alert 1 van het NIVRA uit maart 1993 is, gezien de memorie van antwoord van de Minister van Justitie aan de Eerste Kamer, met deze bepaling bedoeld dat alleen wanneer de accountant opmerkingen heeft over de geautomatiseerde gegevensverwerking, hij daarvan melding maakt in zijn verslag aan de directie en Raad van Commissarissen. De doelstelling "continuïteit van geautomatiseerde gegevensverwerking" behoort volgens de Audit Alert dan ook niet tot de reikwijdte van de jaarrekeningcontrole. Voor het oordeel over de getrouwheid van de jaarrekening is een onderzoek naar de continuïteit van de geautomatiseerde gegevensverwerking volgens deze Audit Alert niet noodzakelijk.

Dit standpunt dateert uit 1993. In de afgelopen jaren heeft de automatisering een grote vlucht genomen. Ook binnen het mkb worden de processen steeds meer geautomatiseerd. De IT heeft vanuit elk onderdeel van de bedrijfsvoering gevolgen voor de financiële verantwoording. De geautomatiseerde gegevensverwerking maakt dan ook integraal deel uit van het jaarrekeningproces en behoort in onze ogen wel tot de reikwijdte van de jaarrekeningcontrole. In het accountantsverslag is dan ook aandacht nodig voor alle relevante aspecten die de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking betreffen.

De accountant levert hiermee ook toegevoegde waarde voor zijn controlecliënt. Ook voor de controlecliënt is automatisering relatief nieuw en IT-processen zijn lang niet altijd optimaal geregeld.

Onderwerpen die in het accountantsverslag aan de orde kunnen komen, zijn onder meer:
- general IT Controls;
- toegangsbeveiliging;
- bevindingen uit het onderzoek naar de serviceorganisatie en/of ISAE 3402 rapport.


IT Integrated Audit Approach
ThinkChart
Uitvoering
FASE 3/4
Balans tussen procesgericht en gegevensgericht
Risicoanalyse, controleaanpak en bevindingen zijn een iteratief proces
Gebruikmaken van IT kan óók efficient zijn
Vastleggen van (IT)-werkzaamheden en oordeelsvorming
Controle IT General Controls
Controle application controls
Overige controlewerkzaamheden
IT Organisatie * Logische toegangsbeveiliging * Continuiteit * Change management
Inspectie * Waarneming * Herberekening * Herhaling / uitvoering
Gericht op resterende onzekerheid
Inzet van data-analyse: effectief en relevant



4. Eindejaarscontrole

4.1 Inleiding

Inhoud en samenhang met andere hoofdstukken

In het vorige hoofdstuk zijn we ingegaan op de fase van de interimcontrole, waarbij de accountant inzicht heeft verkregen over de interne beheersingsomgeving en de mate waarin hij hier in zijn controle op kan steunen. In dit hoofdstuk behandelen we de fase van de eindejaarscontrole. Dit hoofdstuk behandelt de vraag hoe de uitkomsten van de interim-controle omgezet worden naar de controlewerkzaamheden in de eindejaarscontrole.

Een belangrijk onderdeel dat hierbij aan de orde komt, is het gebruik maken van data-analyse. We bespreken de voordelen en de mogelijke valkuilen daarvan.

Doelstelling

Na het lezen van dit hoofdstuk is de accountant in staat om:

- de uitkomsten van de interim-controle over de IT aspecten te vertalen naar de controlewerkzaamheden bij de eindejaarscontrole;
- de uitkomsten van de werkzaamheden van de IT-auditor te vertalen naar een conclusie voor de financiële verantwoording;
- na te gaan welke mogelijkheden voor data-analyse er zijn en hoe data-analyse efficiënt ingezet kan worden.

4.2 Voorbereiding van de eindejaarscontrole

Nadat de systeemgerichte werkzaamheden tijdens de interimcontrole zijn uitgevoerd, bepaal je wat de gevolgen zijn voor de eindejaarscontrole. Is het nodig om de controleaanpak te wijzigen? Kunnen we nu ook minder gegevensgerichte werkzaamheden doen bij de eindejaarscontrole? Dit zijn belangrijke vragen die veel verlangen van het professionele oordeel van de accountant en het opdrachtteam.

Tijdens de interimcontrole is al veel informatie verzameld over de IT-systemen bij de cliënt. Deze kennis komt nu van pas om de controleaanpak nader toe te spitsen zodat voldoende en geschikte controle-informatie wordt verzameld om de risico's van materiële afwijkingen te mitigeren.

Wie

De IT-auditor speelt een belangrijke rol bij het inschatten van de risico's op materiële afwijking voor de financiële verantwoording. Alhoewel er veel IT-risico's kunnen zijn geïdentificeerd, hebben deze niet allemaal financiële gevolgen. De accountant en de IT-auditor bepalen samen welke gevolgen IT-risico's hebben.

In het hoofdstuk over de risicoanalyse is al aandacht besteed aan het onderscheid tussen het jaarrekeningrisico en het bedrijfsrisico. Dit onderscheid kan in de eindcontrole fase opnieuw aan de orde komen, afhankelijk van de uitkomsten van de interim werkzaamheden. Duidelijke afspraken vooraf over de onderzoeksvraag en de wijze van rapporteren voorkomen problemen in deze fase.

Naar aanleiding van zijn werkzaamheden tijdens de interim controle rapporteert de IT-auditor over zijn werkzaamheden. De basisvraag hierbij is in hoeverre de accountant op het systeem kan steunen om de geïdentificeerde jaarrekeningrisico's te mitigeren. Het is vervolgens aan de accountant om de gevolgen voor zijn verdere controlewerkzaamheden te bepalen. Professionele oordeelsvorming neemt in deze fase een belangrijke plaats in. De accountant en de IT-auditor zullen in nauw overleg de uitkomsten van de interimcontrole moeten overwegen.

In het vervolg van dit hoofdstuk gaan we nader in op deze controlewerkzaamheden.

Wat

De interimcontrole vindt meestal in het najaar van het te controleren jaar plaats. Indien de accountant tussentijds controle-informatie verkrijgt over de werking van interne beheersingsmaatregelen moet hij in ieder geval (Standaard 330.12):

- controle-informatie verkrijgen over belangrijke wijzigingen die zich na afloop van de tussentijdse periode in deze interne beheersingsmaatregelen hebben voorgedaan;
- vaststellen of er aanvullende controle-informatie moet worden verzameld over de werking van de interne beheersingsmaatregelen voor de resterende periode.

Dit geldt natuurlijk voor alle werkzaamheden die gericht zijn op de werking van interne beheersingsmaatregelen. Specifiek voor de werking van IT-gerelateerde interne beheersingsmaatregelen betekent dit dat gekeken moet worden naar de General IT Controls, waaronder wijzigingen van programmatuur en wijziging van de competentietabel(len).

Met name de kleinere organisaties zijn vaak niet zo georganiseerd dat de controle zonder meer kan steunen op de General IT Controls. Data-analyse maakt het wellicht mogelijk om alsnog vast te stellen of er ongeregeldheden hebben plaatsgevonden. Gezien de aard van data-analyse lijkt het logisch om dergelijke analyses in één keer voor het hele jaar uit te voeren. Zie het hoofdstuk over de interimcontrole voor een beschrijving van deze werkzaamheden.

Het is nodig om onder meer de volgende vragen te beantwoorden om te kunnen bepalen welke werkzaamheden in de eindcontrole nodig zijn:

- Blijken de interne beheersingsmaatregelen in de IT inderdaad zo te werken als wij hebben ingeschat? Met andere woorden kunnen wij steunen op deze beheersingsmaatregelen?
- In welke mate kunnen wij steunen op de interne beheersingsmaatregelen? Met andere woorden, welke gegevensgerichte werkzaamheden zijn nog nodig om het risico op materiële afwijkingen voldoende te mitigeren?
- Kunnen wij gebruikmaken van data-analyse voor een efficiënte(re) aanpak van de controle?

Professionele oordeelsvorming neemt een belangrijke plaats in bij het vertalen van de uitkomsten van de interimcontrole naar gevolgen voor de eindcontrole. Dit oordeel is sterk afhankelijk van de specifieke situatie bij de klant.

In de mkb-praktijk is veelal sprake van een informele organisatie. Er zijn wel afspraken en procedures maar hier zitten vaak meerdere haken en ogen aan.

Als voorbeeld nemen we het risico dat juistheid van kosten een afwijking van materieel belang vertoont. Een van de interne beheersingsmaatregelen die de onderneming hiervoor heeft getroffen, is autorisatie van betalingen. Het is denkbaar dat zich in de praktijk de volgende scenario's voordoen:

Tabel 6: Scenario's mkb-praktijk

Scenario 1	Scenario 2	Scenario 3
• Alle facturen geautoriseerd voor akkoord • Facturen worden ingeboekt door de administratie • De controller stelt betaal-advieslijst op • Directie autoriseert betalingen (en controleert betaaladvieslijst) en voert daadwerkelijke betaling uit	• Alle facturen geautoriseerd voor akkoord • Facturen worden ingeboekt door de administratie • Controller stelt betaaladvieslijst op, maar kan ook stamgegevens muteren • Directie autoriseert betalingen, voert daadwerkelijke betaling uit. Er is echter geen zichtbare controle op rekeningnummers etc	• Alle facturen geautoriseerd voor akkoord • Facturen worden ingeboekt door de administratie • Controller stelt betaaladvieslijst op, maar kan ook stamgegevens muteren • Directie autoriseert betalingen. Geen zichtbare controle op reke-ning-nummers etc. Controller voert de betalingen zelf uit

In hoeverre kan de accountant in het tweede en derde scenario steunen op de autorisatie van de directie? In het tweede scenario ziet de directie alle betalingen in ieder geval nog langskomen. De accountant kan echter achteraf niet vaststellen dat de directie die heeft gecontroleerd. In het derde scenario heeft de controller alle gelegenheid om ongeautoriseerde betalingen te doen.

Welke consequenties hebben de verschillende scenario's nu voor de aard en de omvang van de gegevensgerichte werkzaamheden? Dit is onder meer afhankelijk van het inherente risico en het interne beheersingsrisico. In combinatie met het ontdekkingsrisico van de accountant dient het accountantscontrolerisico tot een aanvaardbaar laag niveau gereduceerd te worden. Nu is het bepalen van het accountantscontrolerisico geen eenvoudige exercitie op basis van een rekenmodel dat 'zomaar even' is in te vullen. Hoe lastig ook, de accountant zal bij zijn inschatting moeten uitgaan van de specifieke situatie bij zijn cliënt.

Een alternatieve aanpak zou een primair gegevensgerichte aanpak kunnen zijn. Met behulp van data-analyse zijn er diverse mogelijkheden om de hele administratie te analyseren op onjuistheden. Hiermee is wellicht meer controlezekerheid mogelijk tegen minder kosten. In paragraaf 4.3.2 Data-analyse gaan wij hier nader op in.

De kwaliteit van het resultaat is ermee gediend als je bij het inschatten van het accountantscontrolerisico een standaardmodel hanteert. Een dergelijk model valt buiten de reikwijdte van dit boek. Verschillende controlehandboeken bieden hiervoor handvatten.

Uitkomsten

De evaluatie van de uitkomsten van de interim-controle houdt rekening met de specifieke klantsituatie en de IT-aspecten. Overleg binnen het opdrachtteam en vooral ook met de IT-auditor is hierbij van groot belang voor een goed onderbouwde uitspraak. Op basis van deze evaluatie wordt de verdere controleaanpak aangescherpt en waar nodig bijgesteld.

4.3 Uitvoeren gegevensgerichte werkzaamheden

Nadat de interne beheersingsmaatregelen binnen de IT zijn geëvalueerd en de verdere controle-aanpak is bepaald, vinden gegevensgerichte controlewerkzaamheden plaats. IT-aspecten in deze fase van de controle richten zich vooral op de mogelijkheden om gebruik te maken van gegevens die in de systemen zijn opgeslagen.

Tijdens de interimcontrole is vastgesteld in welke mate het mogelijk is om te steunen op de beheersingsmaatregelen voor de integriteit van deze gegevens. In deze paragraaf besteden wij aandacht aan verschillende controlemiddelen die gebruikmaken van deze digitale informatie.

4.3.1 Controlewerkzaamheden

De volgende tabel geeft een overzicht van de controlewerkzaamheden volgens NV COS en voorbeelden van de inzet van Computer Assisted Audit Tools and Techniques (CAATT's) daarbij.

Tabel 7: Voorbeelden inzet IT-audit tools

Werkzaamheden	Inzet IT Audit tools (bijvoorbeeld)
Inspectie	Selectie van items bij steekproeven, selecteren van items die aan specifieke criteria voldoen.
Waarneming	Geen.
Externe bevestiging	Selectie van items.
Herberekening	Controleren op mathematische juistheid.
Het opnieuw uitvoeren	Geen.
Cijferanalyse	Data-mining, vergelijkingen tussen financiële informatie, verbanden tussen verschillende datasets.
Verzoeken om inlichtingen	Geen.

Aard en timing van de te hanteren controlewerkzaamheden hangen af van de beschikbaarheid van de benodigde informatie. Zo kunnen bepaalde administratieve gegevens en overige informatie kunnen uitsluitend in elektronische vorm dan wel alleen op bepaalde plaatsen of in specifieke perioden beschikbaar zijn. Bij een entiteit die e-commerce toepast kunnen bijvoorbeeld brondocumenten zoals inkooporders en inkoopfacturen in uitsluitend elektronische vorm aanwezig zijn. Het kan zijn dat een primaire digitale registratie van bijvoorbeeld een transactie achteraf wordt gewijzigd zonder logging of audittrail. In dit soort situaties kan de accountant het noodzakelijk vinden om de entiteit te verzoeken bepaalde informatie anders of beter vast te leggen zodat hij achteraf controlewerkzaamheden kan uitvoeren.

4.3.2 Data-analyse

De gegevensgerichte werkzaamheden bij de jaarrekeningcontrole beperken zich van oudsher tot deelwaarnemingen, maar door de voortschrijdende technologie wordt het steeds effectiever en efficiënter om bestanden integraal te analyseren met audit software. Er zijn diverse gespecialiseerde audit tools op de markt, maar ook met een algemeen programma als Excel kun je al redelijk geavanceerde bestandsanalyses uitvoeren. Bij het gebruik van bijvoorbeeld Excel is het goed alert te zijn op het zelf opbouwen van de audit trail. Meer voor data-analyse beschikbare CAATT's ondersteunen dit vaak reeds in het programma zelf. Bestandsanalyses zijn in principe mogelijk als onderdeel van elke controlestrategie. De betekenis van deze werkzaamheden en de mate waarin zij bijdragen aan de te verkrijgen controlezekerheid zal echter kunnen verschillen, afhankelijk van ten eerste de vraag of onderzoek is verricht naar de opzet, bestaan en effectieve werking van de key General IT Controls en application controls en ten tweede de uitkomsten daarvan.

De grote kracht van data-analyse is dat je hiermee in een handomdraai alle gedefinieerde afwijkingen boven water haalt. Data-analyse zorgt voor een efficiëntere en effectievere controle dan wanneer je alleen de elementen toetst die, al dan niet toevallig, in je deelwaarneming vallen. Een ander voordeel is dat fouten concreter zijn aan te tonen. Bij steekproeven projecteer je de uitkomsten op de totale populatie - een extrapolatie die lastige discussies met de klant kan geven. Hij kan je verwijten fouten uit te vergroten. Bij data-analyse heb je dat probleem niet. Zo'n bestandsanalyse is te gebruiken om onopzettelijke fouten te ontdekken, maar ook om gemanipuleerde cijfers bloot te leggen of om dubbele betalingen op te sporen. De belangrijkste methoden daarvoor zijn de analyse van subsets en frequentietests.

Analyse van subsets

Een subset (deelpopulatie) is een natuurlijke groepering van gegevens. Voorbeelden zijn crediteurennummers, bankrekeningnummers, BSN-nummers en de tijdstippen waarop transacties zijn uitgevoerd. Als je het bestandsonderzoek richt op zo'n subset is de hitlist meestal kort genoeg om alle gevonden afwijkingen in detail te kunnen onderzoeken.

De subset kun je bijvoorbeeld analyseren via de volgende tests:

- RSF-test
  De RSF (relative size factor) bereken je door het grootste bedrag in de subset te delen door het tweede grootste bedrag. Hiermee kun je abnormaal hoge bedragen opsporen. Als bijvoorbeeld een factuur van 2.000 euro onjuist is geboekt als 200.000 euro en die leverancier gewoonlijk kleine facturen stuurt, geeft het bijbehorende crediteurennummer een hoge RSF.

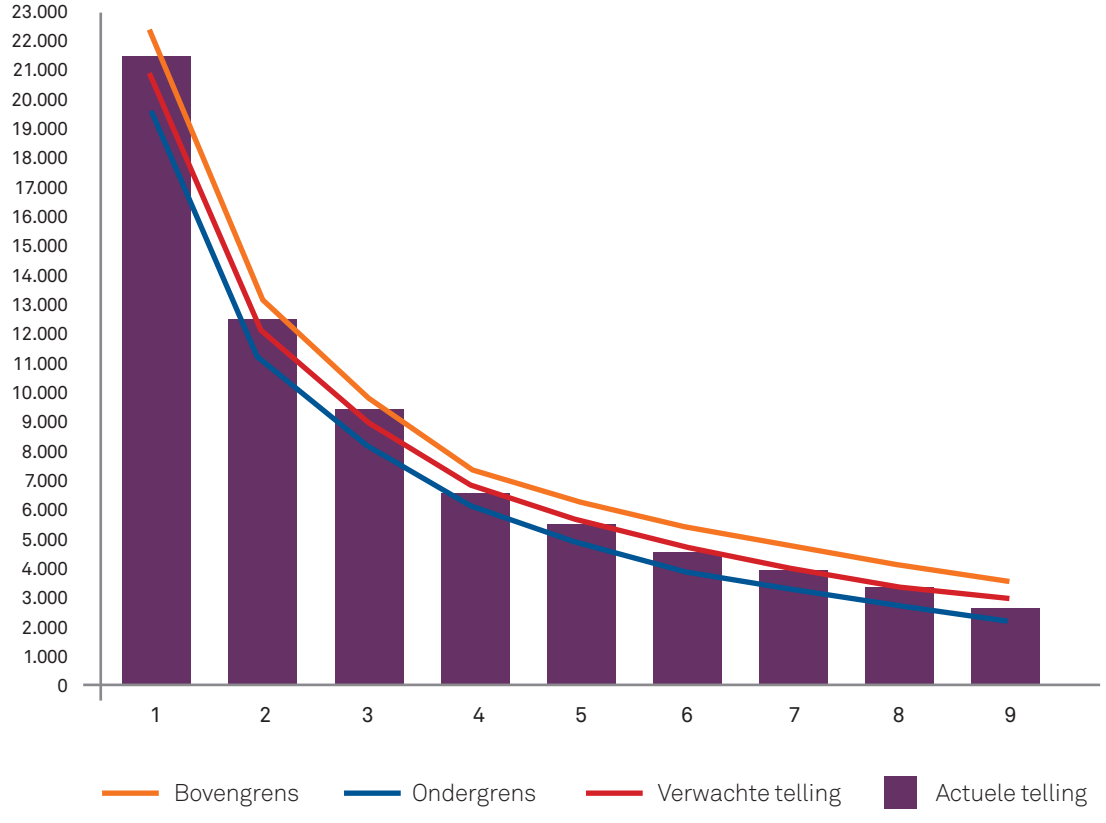
- SSD-test
  Met de SSD-test (same, same, different) kun je dubbele boekingen opsporen, zoals dubbele betalingen aan leveranciers of personeel. Dat een factuur twee keer is betaald, kan blijken uit twee betalingen die wel hetzelfde bedrag en factuurnummer hebben, maar een verschillend crediteurennummer. Dit geeft dan een SSD-score. En de SSD-score die naar voren komt bij betalingen met dezelfde datum en hetzelfde SOFI-nummer, maar verschillende bankrekeningnummers kan wijzen op een dubbele salarisbetaling.

- SSS-test
  Met de SSS-test (same, same, same) kun je identieke boekingen opsporen. Dit kunnen bijvoorbeeld dubbele betalingen zijn aan dezelfde crediteur, dubbele voorraadtellingen of dubbel geboekte verkoopfacturen.

- Frequentietests
  Bij een frequentietest vergelijk je de werkelijke frequentie waarmee een bepaald cijfer in een getallenreeks voorkomt met de verwachte frequentie. Hiermee kun je gemanipuleerde cijfers opsporen. Ieder mens heeft een voorkeur voor bepaalde cijfers en die voorkeur zal vaak ook terugkomen in gemanipuleerde reeks (vooral het cijfer 6 is berucht). Als de werkelijke frequentie sterk afwijkt van de verwachte frequentie is er waarschijnlijk geen sprake van toeval.

  De verwachte frequentie kan zijn gebaseerd op de normale verdeling of op Benford's law. Bij een normale (uniforme) verdeling ga je ervan uit dat alle cijfers even vaak voorkomen. Elk begincijfer heeft dan een verwachte frequentie van 11,1% (namelijk 1/9, want het begincijfer kan niet 0 zijn). Elk van de tweede en volgende cijfers heeft een verwachte frequentie van 10%. De wet van Benford gaat ervan uit dat de begincijfers logaritmisch zijn verdeeld. De verwachte frequentie van het cijfer 1 is dan maar liefst 30,1% en van cijfer 9 slechts 4,6%. De kans dat de gevonden afwijkingen op toeval berusten of op manipulatie, kun je statistisch bepalen met een 'goodness-of-fit' test. De belangrijkste zijn de chikwadraattoets (gebruikt door de fiscus) en de Z-waarde.

Figuur 6: Voorbeeld toepassing Benford's Law



Data-analyse in het MKB

Toenemend gemak van IT-ondersteunde gegevensgerichte controles en toenemend IT-gebruik bij het mkb bieden een schat aan kansen. Om de volledige potentie te kunnen benutten is het nodig om al op een eerder moment na te denken over de inzet van ICT-ondersteunde gegevensgerichte controles. Zeker als de controles kunnen worden herhaald en hergebruikt over bedrijfsgrenzen heen kon het wel eens sneller zijn om eerst veel gegevensgericht te controleren en daarna systeemgericht aan te vullen.

Voorbeeld

Voorbeelden van data-analyses:

- analyse van de Audit file op opvallende bedragen/posten
- analyse van logfiles
- controle op de volledigheid van gegevensbestanden door verschillende 'verzamelingen' aan elkaar te koppelen en verschillen te analyseren
- controle van dataconversies bij de implementatie van nieuwe systemen door dataset met elkaar te vergelijken
- ouderdomsanalyses debiteuren, voorraden, crediteuren
- creëren van verwachtingen ten behoeve van cijferanalyses
- cijferreeksen met elkaar vergelijken. Bijvoorbeeld periode- en filiaalvergelijking
- herhaling van interne berekeningen
- stratificatie van populaties in deelpopulaties
- selectie voor steekproeven

4.4 Documentatie

De documentatie van data-analyses is in de basis niet anders dan controle-documentatie. Standaard 230 vereist dat de accountant de controledocumentatie zo opstelt dat die voldoende is om een ervaren accountant die voorheen niet bij de controle betrokken was in staat te stellen om inzicht te verwerven in:

- de aard, timing en omvang van de controlewerkzaamheden die zijn uitgevoerd;
- de uitkomsten van uitgevoerde controlewerkzaamheden en de verkregen controle-informatie;
- significante aangelegenheden voortgekomen uit de controle, de daaruit getrokken conclusies en significante professionele oordelen die zijn gemaakt om tot die conclusies te komen.

Bij het documenteren van de aard, timing en omvang van de uitgevoerde controlewerkzaamheden leg je de volgende zaken vast:

- de kenmerken van de specifieke (getoetste) items;
- wie de controlewerkzaamheden heeft uitgevoerd en de datum van afronding;
- wie de uitgevoerde controlewerkzaamheden heeft beoordeeld en de datum en omvang van deze beoordeling.

Bij een hard copydossier wordt deze informatie veelal op de documenten geschreven. Bij digitale documenten kun je er natuurlijk voor kiezen om deze gegevens digitaal vast te leggen. Belangrijk voor de audit trail van de controlewerkzaamheden is om onderscheid te maken tussen de gegevens die afkomstig zijn van de klant en de informatie die het controleteam heeft toegevoegd. Bijvoorbeeld door gebruik verschillende kleuren te gebruiken of door verduidelijkende titels en een legenda toe te voegen. Aan te raden is om hierover organisatiebrede afspraken te maken.

Data-analyse heeft weliswaar vele voordelen bij het verzamelen van informatie en het verkrijgen van controlezekerheid, maar brengt ook nieuwe uitdagingen met zich mee. Twee daarvan zijn:

- 'Audit trail' data-analyses
- archiveren elektronische bestanden

Audit trail data-analyse

De NV COS stelt eisen aan de dossiervorming van de accountant. Data-analyses kunnen erg complex en uitgebreid zijn. Door de omvang van de gegevensbestanden is de uiteindelijke output van de analyse vaak zo omvangrijk dat deze niet altijd gemakkelijk integraal op te nemen is in het controledossier.

Een belangrijke eis is in ieder geval dat de analyse te volgen is en eventueel gereproduceerd kan worden. Dit vraagt onder meer om vastlegging van de:

- herkomst van de gegevensbestanden;
- aansluiting tussen de gegevensbestanden en de bron en waar mogelijk de jaarrekening;
- uitgevoerde bewerkingen/formules/analyse op de gegevensbestanden.

Speciale audit tools voorzien vaak in het loggen van de uitgevoerde bewerkingen. Bij analyses in een programma als Excel is dit echter niet het geval. De betrouwbaarheid van de analyse en het bewaken van de integriteit van de gegevensbron vraagt in die gevallen dan ook extra aandacht omdat het niet zeker is dat het analyseproces achteraf betrouwbaar valt te reconstrueren.

Archiveren elektronische controlebestanden

Zoals hierboven aangegeven, is reproduceerbaarheid een eis aan de onderbouwende controle-informatie voor het oordeel van de accountant. Het opnieuw opvragen van de gegevens bij de cliënt is niet gewenst. Alhoewel de cliënt zelf verantwoordelijk is voor het bewaren van zijn administratie en de onderliggende documenten en data gedurende de wettelijke bewaartermijn van zeven jaar, is het dan ook aan te raden de brongegevens te bewaren. Dit kan bijvoorbeeld door de gegevens op een dvd te branden en deze aan het hard copydossier toe te voegen.

4.5 Communicatie

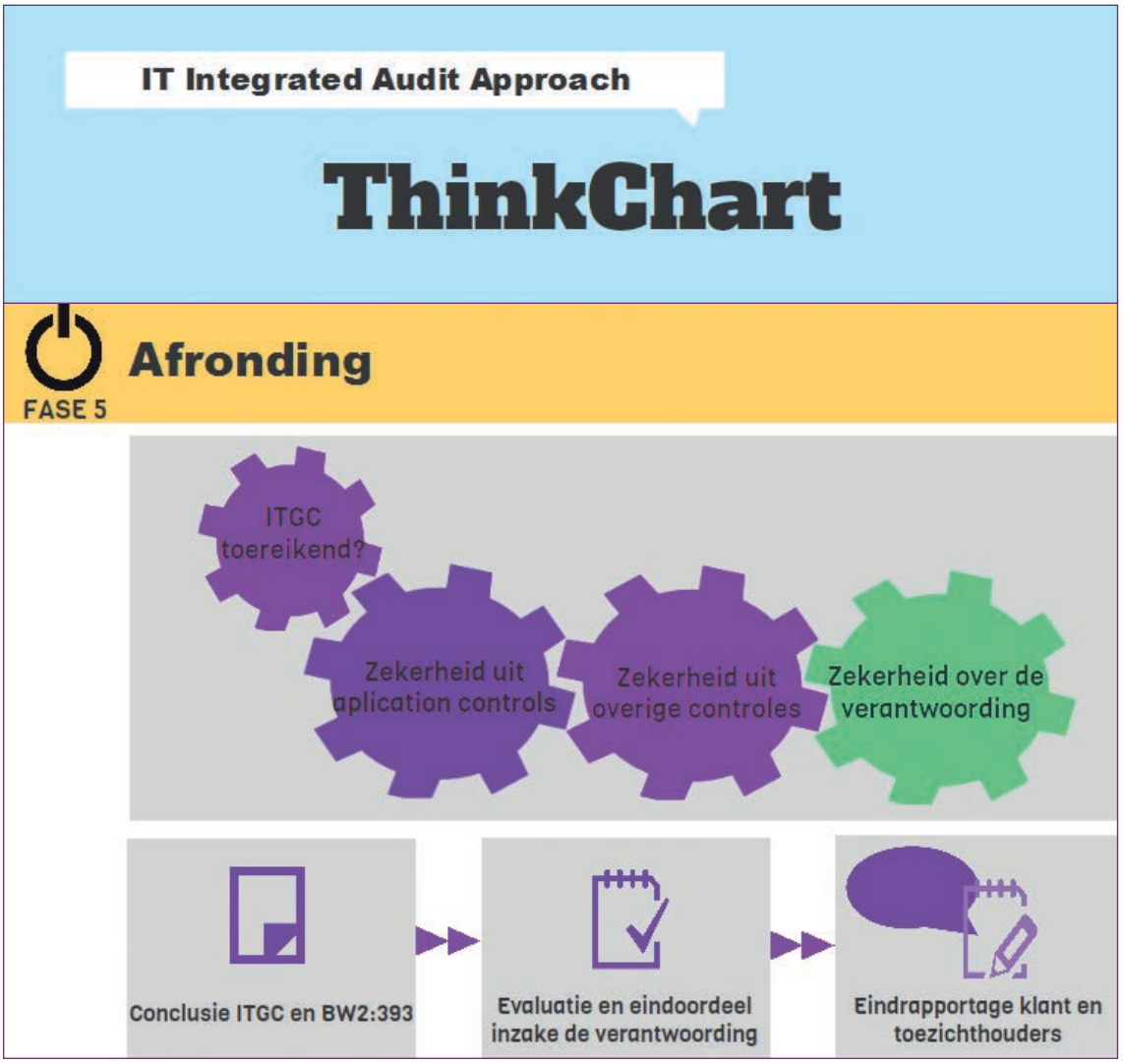
Communicatie binnen het team

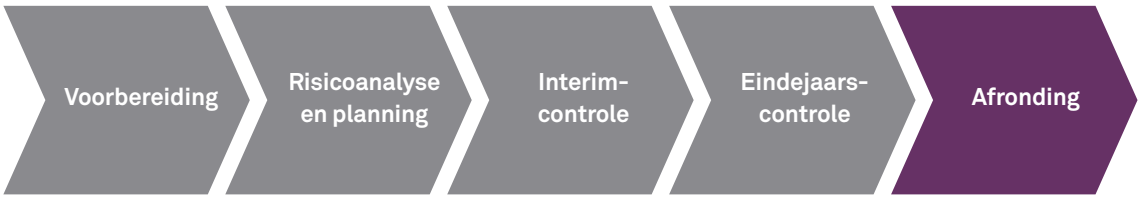
Ter afronding van de eindejaarscontrole bespreekt het team de geconstateerde tekortkomingen. Geëvalueerd wordt of voldoende controle informatie is verkregen om een oordeel te kunnen vormen omtrent de getrouwheid van de jaarrekening. Indien noodzakelijk, worden aanvullende werkzaamheden beschreven en uitgevoerd om de benodigde zekerheid te verkrijgen.

Communicatie met de klant

Een extra voordeel van data-analyses is dat de accountant hiermee beschikt over een enorme hoeveelheid data. Dit biedt de accountant mogelijkheden om deze data voor de ondernemer te ‘verrijken’. Met andere woorden, het slim analyseren, combineren en groeperen van gegevens zodat er voor de ondernemer nieuwe inzichten ontstaan. Deze kunnen vertaald worden naar adviespunten voor de klant.

De verkregen informatie uit de interimcontrole de eindejaarscontrole wordt ten slotte samengevoegd als basis voor het accountantsverslag.


IT Integrated Audit Approach
ThinkChart
FASE 5
Afronding
ITGC toereikend?
Zekerheid uit aplication controls
Zekerheid uit overige controles
Zekerheid over de verantwoording
Conclusie ITGC en BW2:393
Evaluatie en eindoordeel inzake de verantwoording
Eindrapportage klant en toezichthouders



5. Afronding

5.1 Inleiding

Inhoud en samenhang met andere hoofdstukken

In het vorige hoofdstuk zijn we ingegaan op de fase van de eindejaarscontrole waarbij de accountant in aansluiting op de resultaten van de interimcontrole gegevensgerichte werkzaamheden uitvoert om vast te stellen dat de jaarrekening geen afwijkingen van materieel belang bevat. In dit hoofdstuk behandelen we de afrondingsfase van de controle. We bespreken enkele specifieke werkzaamheden in deze fase.

Doelstelling

Na het lezen van dit hoofdstuk is de accountant in staat om afrondende procedures te voltooien.

5.2 Afronding

In de afrondingsfase vinden veelal de volgende werkzaamheden plaats:

- Beoordelen gebeurtenissen na de einddatum van de verslagperiode
- Beoordelen continuïteit
- Opvragen schriftelijke bevestigingen
- Verstrekken controleverklaring
- Administratieve afhandeling dossier

5.2.1 Beoordelen gebeurtenissen na de einddatum van de verslagperiode

De accountant beoordeelt in de afrondende fase de gebeurtenissen na de einddatum van de verslagperiode. Gebeurtenissen na de einddatum van de verslagperiode die samenhangen met IT en die een belangrijke impact hebben op de jaarrekening, zullen veelal betrekking hebben op de continuïteit van de onderneming. Als een gebeurtenis leidt tot ernstige onzekerheid over de continuïteit of zelfs tot discontinuïteit, is vermelding ervan de jaarrekening vereist.

De in hoofdstuk 2 aangehaalde casus DigiNotar illustreert dit. De gevolgen van de hack op hun veiligheidscertificaten leidde het verlies aan vertrouwen uiteindelijk tot de ondergang van het bedrijf. Ook wanneer de continuïteit van de IT niet gegarandeerd is, kan dit bij organisaties die in hoge mate steunen op IT catastrofale gevolgen hebben.

5.2.2 Beoordelen continuïteit

Herhaaldelijk hebben wij in het voorafgaande aangegeven dat de continuïteit afhankelijk kan zijn van IT, zoals ook blijkt uit het in de vorige paragraaf aangehaalde DigiNotar. Ernstige onzekerheid

over de continuïteit kan invloed hebben op de af te geven controleverklaring. Indien de onderneming in sterke mate afhankelijk is van IT, is het noodzakelijk dat accountant en IT-auditor gezamenlijk de continuïteitsrisico's inschatten.

We merken overigens in dit kader nogmaals op dat we vanuit de wet verplicht zijn minimaal over de continuïteit van de geautomatiseerde gegevensverwerking te rapporteren.

5.2.3 Opvragen schriftelijke bevestigingen

Dit kent weinig specifieke IT aspecten de accountant zal dit daarom zelf doen.

5.2.4 Verstrekken controleverklaring

Alles in overweging nemende, bepaalt de accountant als sluitstuk van de afrondende fase welke controleverklaring hij zal verstrekken. In principe heeft dan de input van IT-auditor hiervoor ontvangen om bij zijn overwegingen te betrekken.

5.2.5 Administratieve afhandeling dossier

Na het verstrekken van de controleverklaring heeft de accountant een afsluittermijn van twee maanden. In deze periode wordt het dossier klaar gemaakt voor afsluiting via activiteiten zoals het:

- vernietigen of verwijderen van achterhaalde documentatie;
- ordenen, collationeren en opnemen van kruisverwijzingen in werkdocumenten;
- aftekenen van checklists voor het samenstellen van het dossier;
- documenteren van controle-informatie die is verkregen, besproken of is overeengekomen met relevante teamleden vóór de datum van de controleverklaring.

De accountant dient zich ervan te verzekeren dat het controleteam, met inbegrip van de IT-auditor, alle relevante documentatie in het dossier heeft opgenomen ter onderbouwing van de afgegeven controleverklaring.

5.3 Documentatie

In deze fase neemt het controleteam documentatie op over de gebeurtenissen na de einddatum van de verslagperiode, naast besprekingsverslagen en een kopie van de afgegeven controleverklaring.

5.4 Communicatie

Communicatie binnen het team

Communicatie binnen het team richt zich onder meer op de overwegingen bij gebeurtenissen na de einddatum van de verslagperiode, bij de continuïteitsinschatting en bij de keuze van de af te geven verklaring.

Communicatie met de klant

Het controleteam verkrijgt van de klant documentatie over eventuele gebeurtenissen na de einddatum van de verslagperiode, plus de schriftelijke bevestiging bij de jaarrekening.

Definities & afkortingen

Accountant	Een registeraccountant of accountant-administratieconsulent. De term 'accountant' wordt in de Standaarden gebruikt om de persoon of personen aan te duiden die de controle uitvoert/uitvoeren, gewoonlijk de opdrachtpartner of andere leden van het opdrachtteam, of, naargelang van toepassing, het kantoor.
ACL	Audit analytics software; software voor data-analyse.
AO/IB	Administratieve organisatie en interne beheersing.
Apparatuur	Zie hardware
Applicatie	Een computerprogramma dat bedoeld is voor eindgebruikers. Software die bedrijfs- en informatieverzorgingsprocessen ondersteunen.
Applicatieprogrammatuur	Zie Applicatie
Application control	Handmatige of geautomatiseerde procedures die doorgaans op het niveau van een bedrijfsproces werken. Application controls kunnen preventief of detecterend van aard zijn en zijn opgezet om te zorgen voor de integriteit van de administratieve vastleggingen. Application controls hebben derhalve betrekking op procedures die worden gehanteerd om transacties of andere financiële gegevens tot stand te brengen, vast te leggen, te verwerken en te rapporteren.
Audit	Controleren van een organisatie.
Audit file	Standaard gegevensset uit het financiële grootboek.
Audit trail	Een zodanige inrichting binnen een applicatie dat de gang van elk gegeven door het gehele verwerkingsproces heen van invoer tot en met uitvoer te volgen is
Audit tool	Tool om bestanden integraal te analyseren zoals ACL of IDEA.
Automated control	Controls binnen applicaties, databases en infrastructuur, bestaande uit General IT Controls en Application Controls
Backup	Een reservekopie van gegevens die zich op een andere gegevensdrager bevinden.
Bedrijfsrisico	Zie business risk
Beheersingsmaatregel	Zie interne beheersing

Besturingssysteem	Een programma dat na het opstarten van een computer in het geheugen geladen wordt en de hardware aanstuurt. Het fungeert als een medium tussen de hardware en de computergebruiker met als opzet dat de gebruiker programma's op een gemakkelijke en/of efficiënte manier kan uitvoeren.
Beveiligingsbeleid	Verzameling van regels die de procedures en mechanismen vastlegt die de beveiliging van een systeem verzorgen en van de beveiligingsobjecten en-subjecten die bij dat beveiligingsbeleid horen.
BSN	Burger service nummer.
Business risk	Risico voortkomend uit significante voorwaarden, gebeurtenisen, omstandigheden, handelingen of het achterwege laten van handelingen, die een negatief effect kunnen hebben op het vermogen van de entiteit om haar doelstellingen te bereiken en haar strategieën uit te voeren, dan wel uit het vaststellen van ongeschikte doelstellingen en strategieën.
BW	Burgerlijk Wetboek
CAATT's	Computer Assisted Audit Tools and Techniques.
Change management	Beheersing van wijzigingen in de automatisering.
Cloud	Zie cloudcomputing
Cloudcomputing	Het via internet op aanvraag beschikbaar stellen van hardware, software en gegevens, ongeveer zoals elektriciteit uit het lichtnet.
Cobit	Framework voor het gestructureerd inrichten en beoordelen van een IT-beheeromgeving.
Computer dependent control	Mix van handmatige en automated controls.
Continuïteit van IT	Permanente beschikbaarheid van informatie en ongestoorde voortgang van de informatieverwerking; het ongestoord functioneren van computerapparatuur, programmatuur,bestanden en documentatie.
Controleerbaarheid	De mate waarin het mogelijk is kennis te verkrijgen over de structurering (documentatie) en werking van een object. Tevens omvat dit kwaliteitsaspect de mate waarin het mogelijk is vast te stellen dat de informatieverwerking in overeenstemming met de eisen ten aanzien van de overige kwaliteitsaspecten is uitgevoerd.
NV COS	Nadere voorschriften controle- en overige Standaarden,

Coso	Managementmodel dat de relaties tussen de bedrijfsrisico's en het interne beheersingssysteem identificeert .
Data-analyse	Proces van controleren, transformeren en modelleren van gegevens met als doel relevante informatie uit te lichten, hieruit conclusies te trekken en de besluitvorming te ondersteunen.
Database management system	Het programma dat de in een database opgeslagen gegevens beheert.
Deelwaarneming	Controle van een en selectie uit de populatie.
EDI	Electronic Data Interchange.
ERP	Enterprise Resource Planning.
Escrow	Een overeenkomst tussen een softwareleverancier of -distribu teur en een software-gebruiker. Daarin komen de partijen overeenkomen dat de leverancier de broncode van een software product ten behoeve van de gebruiker deponeert bij een gespecialiseerde escrow agent. De broncode wordt aan de gebruiker overgedragen op het moment dat aan bepaalde voorwaarden is voldaan.
Exclusiviteit	De mate waarin uitsluitend geautoriseerde personen of apparatuur via geautomatiseerde procedures en beperkte bevoegdheden gebruikmaken van IT-processen.
Financial audit	Controle die zich richt op de betrouwbaarheid van de financiële verslaglegging (getrouw beeld).
Frequentietest	Bij een frequentietest vergelijk je de werkelijke frequentie waarmee een bepaald cijfer in een getallenreeks voorkomt met de verwachte frequentie. Hiermee kun je gemanipuleerde cijfers opsporen.
Geautomatiseerde controle	Zie automated control
Gegevensgerichte werkzaamheden	Werkzaamheden die zijn opgezet om afwijkingen van materieel belang op het niveau van beweringen te detecteren.
Hardware	Alle fysieke componenten die in een computer een rol spelen.
IaaS	Infrastructure as a Service, een vorm van cloudcomputing.
IDEA	Naam van een softwarepakket voor data-analyse.
Informatiesysteem	Een systeem waarmee informatie over objecten of personen verzameld, bewerkt, geanalyseerd, geïntegreerd en gepresenteerd kan worden. Tot een informatiesysteem in ruime zin behoren naast de

	data en de technieken en faciliteiten om data te ordenen en te interpreteren vaak ook de ermee verbonden organisatie, personen en procedures gerekend.
Infrastructuur	Het geheel aan voorzieningen dat nodig is voor data-opslag en -transport zoals netwerken en de structuur van het internet, maar ook voor andere communicatielijnen zoals telefoonverbindingen.
Inherent risico	De vatbaarheid van een bewering met betrekking tot een transactiestroom, rekeningsaldo of in de financiële overzichten opgenomen toelichting voor een afwijking die afzonderlijk of gezamenlijk met andere afwijkingen van materieel belang is, voordat er rekening wordt gehouden met de eventuele daarop betrekking hebbende interne beheersingsmaatregelen.
Integrated Audit Approach	Geïntegreerde controleaanpak waarin IT audit en Financial audit hand in hand gaan.
Integriteit	De mate waarin het object (gegevens en informatie-, technische- en processystemen) in overeenstemming is met de afgebeelde werkelijkheid.
Interface	Een intermediair waarmee twee systemen met elkaar communiceren.
Intern beheersingsrisico	Het risico dat een afwijking kan voorkomen in een bewering met betrekking tot een transactiestroom, rekeningsaldo of een in de financiële overzichten opgenomen toelichting die, afzonderlijk of gezamenlijk met andere afwijkingen van materieel belang is, niet wordt voorkomen of niet tijdig wordt gedetecteerd en hersteld door de interne beheersing van de entiteit.
Interne beheersing	Het proces dat is opgezet, wordt geïmplementeerd en onderhouden door de met governance belaste personen, het management en andere personeelsleden met als doel een redelijke mate van zekerheid te verschaffen dat de doelstellingen van de entiteit met betrekking tot de betrouwbaarheid van de financiële verslaggeving, de effectiviteit en efficiëntie van de activiteiten alsmede de naleving van de van toepassing zijnde wet- en regelgeving worden bereikt. De term ‘interne beheersingsmaatregelen’ slaat op alle aspecten van één of meer componenten van de interne beheersing.
Interne beheersingssysteem	Zie interne beheersing
ISAE	International Standards on Assurance Engagements.
ISO	International Standardisation Organisation.

IT	Informatietechnologie: het gebruik van computers en telecommunicatiemiddelen om data op te slaan, op te halen, te verzenden en te manipuleren.
IT-audit	De werkzaamheden van een IT-auditor die zijn gericht op het uitvoeren van een assurance-opdracht, beoordeling of adviesopdracht
IT-auditor	De Register EDP-auditor (RE), ingeschreven in het register van de NOREA
IT-architectuur	Beschrijving van de inhoudelijke relaties en samenhang tussen toepassingen en gegevensverzamelingen onderling.
IT-componenten	Apparatuur, systeemprogrammatuur, toepassingsprogrammatuur, organisatie, beveiliging en datacommunicatie.
General IT Controls	Beleidslijnen en procedures die betrekking hebben op een groot aantal toepassingen en die de effectieve werking van application controls ondersteunen. Ze zijn van toepassing op mainframe-, miniframe- en eindgebruikersomgevingen. General IT controls die de integriteit van de informatie en de beveiliging van gegevens handhaven, omvatten gewoonlijk: a. de werking van het computercentrum en het netwerk; b. sanschaf, wijziging en onderhoud van systeemsoftware; c. programmawijzigingen; d. toegangsbeveiliging; e. aanschaf, ontwikkeling en onderhoud van toepassingssystemen.
IT-omgeving	Geheel aan informatiesystemen, gegevens, infrastructuur en fysieke laag (fysieke voorzieningen zoals gebouw met pasjes, airconditioning, noodstroomvoorzieningen).
IT-risico	Risico voortkomend uit het gebruik van IT.
ITGC	Zie General IT Control
Jaarrekeningrisico	Risico dat invloed heeft op de getrouwe weergave van de werkelijkheid in de jaarrekening.
Key-control	Belangrijkste beheersingsmaatregelen ten behoeve van het bereiken van ondernemingsdoelstellingen.
KPI	Kritische performance indicator
Lijncontrole	Het volgen van enkele transacties door het financiële verslaggevingssysteem.

Logische toegangsbeveiliging	Het geheel van maatregelen om gegevens te beveiligen tegen ongeautoriseerde toegang.
Maatwerkapplicatie	Applicatie op maat gebouwd op basis van specifieke functionele en technische beschrijvingen, opgesteld door de onderneming.
Manual control	Beheersingsmaatregelen die worden uitgevoerd door personen en niet rechtstreeks voortkomen uit of ondersteund worden door de geautomatiseerde omgeving.
Mkb	Midden- en kleinbedrijf
Netwerk	Het geheel van onderling verbonden computers
Netwerkbesturingsprogrammatuur	Programmatuur waarmee dataverkeer op een netwerk en de toegang van gebruikers tot systeembronnen op het netwerk zoals bestanden en printers geregeld kan worden.
NBA	Nederlandse Beroepsorganisatie van Accountants
NOREA	Nederlandse Orde van Register EDP Auditors, de beroepsorganisatie van IT-auditors.
Operating system	Zie besturingssysteem
PaaS	Proces as a Service. Een vorm van cloudcomputing.
Platform	Combinaties van hardware en systeemprogrammatuur
Proceduretest	Zie toetsingen van interne beheersmaatregelen
Query	Een opdracht aan de database om gegevens op te halen.
Recovery	Terugzetten van een backup.
Releases	Versies
Release notes	Geven aan welke wijzigingen er zijn doorgevoerd in een bepaalde versie (release) van de software.
Ontdekkingsrisico	Het risico dat de werkzaamheden die door de accountant zijn uitgevoerd om het controlerisico terug te brengen naar een aanvaardbaar laag niveau een bestaande afwijking niet zullen detecteren en die afzonderlijk of gezamenlijk met andere afwijkingen van materieel belang zouden kunnen zijn.
RSF-test	Relative Size Factor-test: het hoogste bedrag in de subset deel je door het tweede hoogste bedrag. Hiermee kun je abnormaal hoge bedragen opsporen.

SaaS	Software as a Service. Een vorm van cloudcomputing.
Server	Een computer die, of een programma dat diensten verleent aan 'clients'. In de eerste betekenis is het de fysieke computer waarop een programma draait dat deze diensten verleent.
Software	Zie applicatie
SSD-test	"Same, Same, Different"-test. Hiermee kun je dubbele boekingen opsporen, zoals dubbele betalingen aan leveranciers of personeel.
SSS-test	"Same, Same, Same"-test. Hiermee kun je identieke boekingen opsporen.
Standaardapplicatie	Applicatie die niet is aangepast aan de wensen van de onderneming.
Steekproef	Een selectie uit een totale populatie ten behoeve van een meting van bepaalde eigenschappen van die populatie.
Systeembeheerder	Verantwoordelijk voor de goede werking van een computersysteem of meerdere systemen.
Toetsingen van interne beheersingsmaatregelen	Een controlemaatregel die is opgezet om de effectieve werking te evalueren van interne beheersingsmaatregelen gericht op het voorkomen of het detecteren en corrigeren van een afwijking van materieel belang op het niveau van beweringen.
Systeemprogrammatuur	Systeemprogrammatuur zorgt onder andere voor allerlei controles bij het opstarten van de hardware. De systeemsoftware is in strikte zin van het woord wel 'software', maar is zodanig met de apparatuur verbonden dat ze vaak als één geheel worden behandeld.
Toepassingsprogrammatuur	Zie applicaties
User control	Controle op uitvoer

Literatuurverwijzingen

Boeken

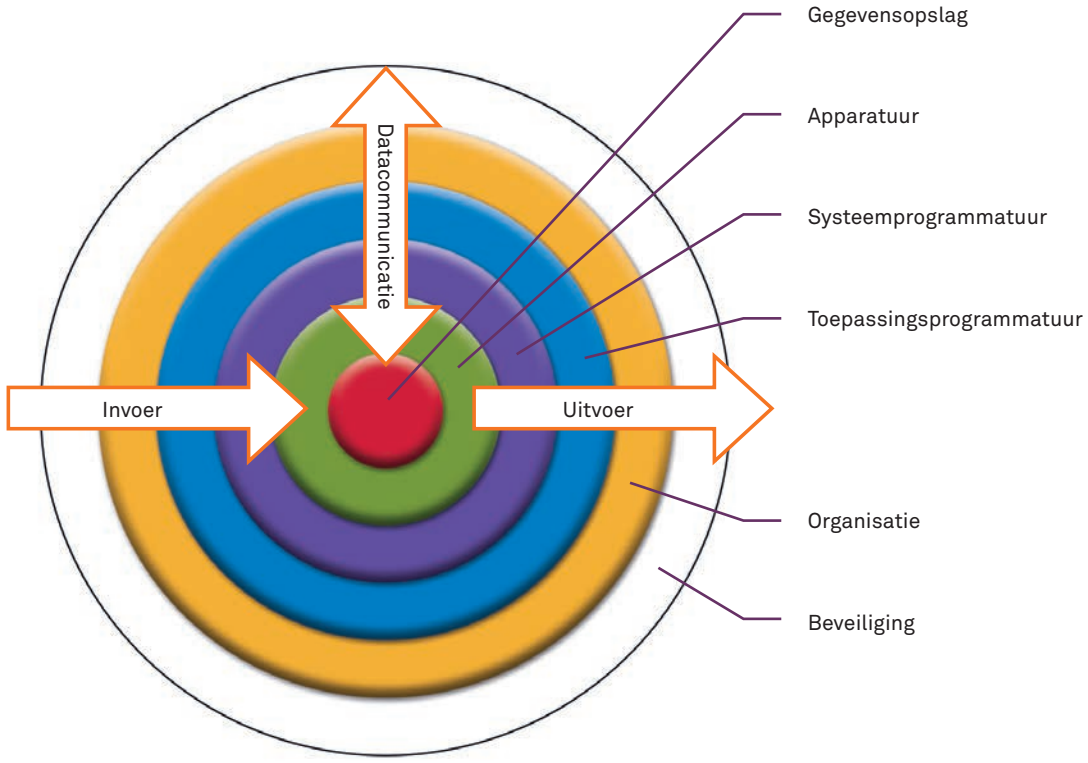
- Donkers, ir. J.A.M., M. Groesz RE en ir. J.A. Verstelle RE (1995), **Informatietechnologie: Management control van de geautomatiseerde informatievoorziening**, Deventer, Kluwer Bedrijfswetenschappen.
- Dirkx, T., M. Groesz en M. Nieuwendijk (1999), **ICT Beoordeeld; integratie automatisering in audit**, Deventer, Kluwer.
- Fijneman, R.G.A. (1999), **De betekenis en inhoud van 'jaarrekening ICT-auditing' als onderdeel van de jaarrekeningcontrole**, Tilburg, Tilburg University.
- Majoor RA, prof. dr. G.C.M., Th. Th. Heideman RA, prof. drs. J.C.E. van Kollenburg RA, W.F. Merkus RA en prof. W.P. Moleveld RA (2007), **Elementaire theorie accountantscontrole - algemene beginselen**, Groningen | Houten, Wolters-Noordhoff.
- Majoor RA, prof. dr. G.C.M., Th. Th. Heideman RA, prof. drs.J.C.E. van Kollenburg RA, W.F. Merkus RA en prof. W.P. Moleveld RA (2007), **Elementaire theorie accountantscontrole - toepassingen**, Groningen | Houten, Wolters-Noordhoff.
- NIVRA (2011), **Controle- en Overige Standaarden**, Amsterdam, NIVRA
- Westra, B.A.J., G. Folkers (2012), **Compendium Accountancy, deel 1B|COS, controle van de jaarrekening**, Amsterdam, Pentagan B.V.

Overig

- SRA-Vaktechniek (2010), **SRA Controleaanpak en Automatisering**, Nieuwegein
- NOVAA (2001), **Leidraad 12**.

Bijlage 1: IT-omgeving

Figuur 7: Structuur geautomatiseerde verwerking



Toelichting

- Apparatuur
  Dit is de hardware. Hardware functioneert niet zonder systeemprogrammatuur.

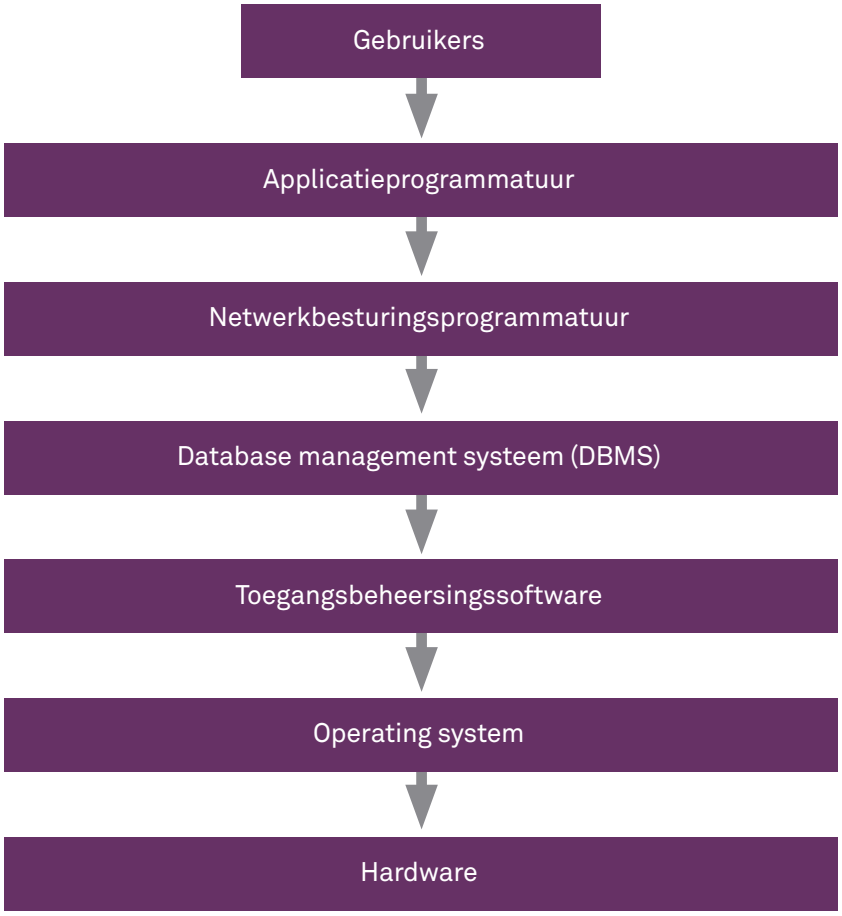
- Systeemprogrammatuur
  Systeemprogrammatuur zorgt er onder andere voor dat allerlei controles worden uitgevoerd bij het opstarten van de hardware. De systeemsoftware is in strikte zin van het woord wel 'software', maar is zo sterk met de apparatuur verbonden dat ze vaak als één geheel worden behandeld.

- Toepassingsprogrammatuur
  Een computerprogramma dat bedoeld is voor eindgebruikers. Als in de praktijk gesproken wordt over software dan wordt meestal toepassings-programmatuur bedoeld. Toepassings-programmatuur wordt ook wel aangeduid met de term 'applicaties'.

- Organisatie
  Betreft de procedures die zijn opgesteld rondom het IT beheer.

- Datacommunicatie
  Een 'computersysteem' bestaat vaak uit enkele (soms honderden/duizenden) onderling verbonden apparaten, die onderling met elkaar kunnen 'praten'. Dat praten wordt mogelijk gemaakt door netwerken (= de draden die computers verbinden) en datacommunicatie (= de uitwisseling van gegevens over die draden).

IT onderdelen



Bijlage 2: Identificatie specifieke IT aspecten o.b.v. NV COS t.a.v. de voorbereidingsfase

In onderstaand tabel is per relevante Richtlijn aangegeven of er specifieke IT aspecten aan de orde zijn bij de **voorbereidingsfase** van een audit.

Standaard	Omschrijving	IT Aspect
210 Opdrachtvoorwaarden voor controles	Deze Controlestandaard heeft ten doel vereisten vast te stellen en leidraden te geven voor: a. de voorwaarden die met opdrachtgevers worden overeengekomen aangaande de opdracht; b. de reactie van de accountant op een verzoek van de opdrachtgever tot een zodanige wijziging van de opdracht dat een lager niveau van zekerheid wordt verschaft.	Eventuele vereisten opnemen voor het onderzoek naar de automatisering; denk er ook aan contact op te nemen met de serviceprovider bij het gebruik maken van clouddiensten.
220 Kwaliteitsbeheersing voor controles	Deze Controlestandaard heeft ten doel vereisten vast te stellen en leidraden te geven omtrent de specifieke verantwoordelijkheden van het personeel van accountantspraktijken met betrekking tot de kwaliteitsbeheersingsprocedures ten aanzien van controle van historische financiële informatie, waaronder de controle van jaarrekeningen. Deze Standaard moet worden gelezen in samenhang met de Verordening Gedrags- en Beroepsregels Accountants (VGBA).	Er is voldoende inzicht nodig van relevante IT onderdelen om vast te stellen of: • IT kennis voldoende aanwezig is binnen de accountantsorganisatie om de opdracht uit te voeren; • de beschikbaarheid van medewerkers met de specifieke IT kennis geen belemmering vormt voor de planning van de opdracht; • er behoefte aan specifieke IT consultancy is; • eventueel inzet van externe deskundigheid van toepassing is.
230 Controledocumentatie	Deze Controlestandaard heeft ten doel vereisten vast te stellen en leidraden te geven met betrekking tot controledocumentatie.	Geen
240 De verantwoordelijkheid van de accountant m.b.t. fraude	Deze Controlestandaard heeft ten doel algemene uitgangspunten en noodzakelijke werkzaamheden vast te stellen en leidraden te geven omtrent de verantwoordelijkheid van de accountant voor het identificeren van het risico van fraude in het kader van een opdracht tot controle van financiële overzichten en uit te werken hoe de vereisten en leidraden in Standaard 315, “Risico’s op een afwijking van materieel belang identificeren en inschatten door inzicht te ver-	Hierbij is rekening te houden met specifieke IT-omgevingen waarbij zich fraude risico’s kunnen voordoen. Het kan ook gaan om fraude door derden. Denk hierbij aan Webwinkels en betalingen met credit cards, iDEAL of Paypal waarbij nieuwe vormen van “IT fraude” mogelijk zijn.

Standaard	Omschrijving	IT Aspect
	werven in de entiteit en haar omgeving" en Standaard 330, "Inspelen door de accountant op ingeschatte risico's" moeten te worden toegepast met betrekking tot het risico van een afwijking van materieel belang als gevolg van fraude. De vereisten en leidraden in deze Standaard dienen te worden geïntegreerd in het totale controleproces.	
260 Communicatie over controle-aangelegenheden met de met governance belaste personen	Deze Controlestandaard heeft ten doel vereisten vast te stellen en leidraden te geven voor de communicatie omtrent controle-aangelegenheden inzake financiële overzichten tussen de accountant en de met governance belaste personen van een entiteit. Deze communicatie heeft betrekking op controle-aangelegenheden voor zover van belang voor governance zoals in deze Standaard gedefinieerd. Deze Standaard geeft geen leidraden voor overleg door de accountant met partijen buiten de entiteit, zoals bijvoorbeeld externe regelgevende of verantwoordelijke instanties.	Geen
300 De planning van de controle	Deze Controlestandaard heeft ten doel vereisten vast te stellen en leidraden te geven voor de overwegingen en de werkzaamheden die gelden voor de planning van de controle van financiële overzichten. Deze Standaard is opgesteld binnen het kader van doorlopende controles. Ter aanvulling zijn in paragraaf A20 van deze Standaard onderwerpen opgenomen waaraan de accountant aandacht schenkt bij een eerste controleopdracht. In de bijlage bij deze Controlestandaard worden voorbeelden genoemd van aangelegenheden die de accountant in overweging kan nemen bij het opstellen van zijn algehele controleaanpak.	Er is voldoende inzicht nodig van relevante IT onderdelen om vast te stellen of: • de IT kennis voldoende aanwezig is binnen de accountantsorganisatie om de opdracht uit te voeren; • de beschikbaarheid van mede werkers met de specifieke IT kennis geen belemmering vormt voor de planning van de opdracht; • er behoefte aan specifieke IT consultancy is; • eventueel inzet van externe deskundigheid van toepassing is. Voorbeelden uit de bijlage: • gebruikmaken door de entiteit van serviceorganisaties • invloed van informatietechnologie, met inbegrip van de beschikbaarheid van gegevens en het verwachte gebruik van audit softwaretoepassingen.

Standaard	Omschrijving	IT Aspect
320 Materialiteit in de accountantscontrole	Deze Controlestandaard heeft ten doel vereisten vast te stellen en leidraden te geven inzake materialiteit en de relatie ervan met controlerisico.	Aandachtspunt tijdens deze fase is om vast te stellen of er specifieke eisen zijn ten aanzien van materieel belang en of deze eisen een belemmering kan vormen voor het uitvoeren van de opdracht. IT kan hierin een essentieel hulpmiddel zijn om aan de eisen van de materialiteit wel te kunnen voldoen.
600 Gebruikmaken van de werkzaamheden van andere accountants	Deze Controlestandaard heeft ten doel vereisten vast te stellen en leidraden te geven voor de accountant, die een verklaring afgeeft bij een financieel overzicht van een entiteit en daarbij gebruik maakt van de werkzaamheden van een andere accountant met betrekking tot de financiële gegevens van een of meer (groeps)onderdelen die in het financiële overzicht van de desbetreffende entiteit zijn verwerkt. Deze Standaard heeft geen betrekking op de situatie dat twee of meer accountants belast zijn met de gezamenlijke controleopdracht bij eenzelfde entiteit en op de relatie tussen de accountant en de voorgaande accountant. De vereisten in deze Standaard zijn evenmin van toepassing indien de groepsaccountant van mening is dat een financieel overzicht van een (groeps)onderdeel niet van materieel belang is. Deze Standaard is echter wel van toepassing, indien enkele (groeps)-onderdelen op zich niet, maar tezamen wel van materieel belang zijn.	Mogelijk van toepassing bij uitbesteding van (delen van) de IT.
620 Gebruikmaken van de werkzaamheden van deskundigen	Deze Controlestandaard heeft ten doel vereisten vast te stellen en leidraden te geven omtrent het gebruikmaken van de werkzaamheden van deskundigen om controle-informatie te verkrijgen.	Geen

Bijlage 3: Identificatie specifieke IT aspecten o.b.v. NV COS t.a.v. de risicoanalyse en planning

In onderstaand tabel is per relevante Standaard aangegeven of er specifieke IT aspecten aan de orde bij de **risicoanalyse en planningsfase** van een audit.

Standaard	Omschrijving	IT Aspect
240 De verantwoordelijkheid van de accountant m.b.t. fraude	Deze Controlestandaard heeft ten doel algemene uitgangspunten en werkzaamheden vast te stellen en leidraden te geven omtrent de verantwoordelijkheid van de accountant voor het identificeren van het risico van fraude in het kader van een opdracht tot controle van financiële overzichten en uit te werken hoe de vereisten en leidraden in Standaard 315, "Risico's op een afwijking van materieel belang identificeren en inschatten door inzicht te verwerven in de entiteit en haar omgeving" en Standaard 330, "Inspelen door de accountant op ingeschatte risico's" moeten te worden toegepast met betrekking tot het risico van een afwijking van materieel belang als gevolg van fraude. De vereisten en leidraden in deze Standaard dienen te worden geïntegreerd in het totale controleproces.	Hierbij is aandacht nodig voor specifieke IT-omgevingen waarbij fraude risico's zich kunnen voordoen. Het kan ook gaan om fraude door derden. Denk hierbij aan Webwinkels en het uitvoeren van betalingen met credit cards, iDEAL of Paypal waarbij zich nieuwe vormen van "IT fraude" kunnen voordoen.
260 Communicatie over controle-aangelegenheden met de met governance belaste personen	Deze Controlestandaard heeft ten doel vereisten vast te stellen en leidraden te geven voor de communicatie omtrent controle-aangelegenheden inzake financiële overzichten tussen de accountant en de met governance belaste personen van een entiteit. Deze communicatie heeft betrekking op controle-aangelegenheden voor zover van belang voor governance zoals in deze Standaard gedefinieerd. Deze Standaard geeft geen leidraden voor overleg door de accountant met partijen buiten de entiteit, zoals bijvoorbeeld externe regelgevende of verantwoordelijke instanties.	Indien uit de planningsfase belangrijke IT risico's blijken die onvoldoende zijn beheerst, communiceert de accountant dit met de organen belast met governance.
300 De planning van de controle	Deze Controlestandaard heeft ten doel vereisten vast te stellen en leidraden te geven voor de overwegingen en de werkzaamheden die gelden voor de planning van de controle van financiële overzichten. Deze Standaard is opgesteld binnen het kader van doorlopende controles. Ter	Indien blijkt dat specialistische kennis van IT noodzakelijk is, zal de accountant met de IT-auditor de controle plannen en contactmomenten inplannen.

Standaard	Omschrijving	IT Aspect
	aanvulling zijn in paragraaf A20 van deze Standaard onderwerpen opgenomen waaraan de accountant aandacht schenkt bij een eerste controleopdracht. In de bijlage bij deze Controlestandaard worden voorbeelden genoemd van aangelegenheden die de accountant in overweging kan nemen bij het opstellen van zijn algehele controleaanpak.	
315 Risico's op een afwijking van materieel belang identificeren en inschatten door inzicht te verwerven in de entiteit en haar omgeving	De doelstelling van de accountant is het identificeren en inschatten van de risico's van een afwijking van materieel belang, die het gevolg is van fraude of van fouten, op het niveau van het financieel overzicht en op het niveau van beweringen door middel van het verwerven van inzicht in de entiteit en haar omgeving, met inbegrip van haar interne beheersing, zodat een basis wordt verkregen voor het opzetten en implementeren van manieren van inspelen op de ingeschatte risico's van een afwijking van materieel belang.	In de voorbereidingsfase heeft de accountant een eerste indruk opgedaan van de IT-omgeving. De accountant verdiept zijn kennis van de IT bij de cliënt in het licht van de onderneming en zijn omgeving en doet dit vanuit het perspectief van de jaarrekening. Met het R6 model brengt de accountant de IT risico's in kaart. Voor een verdere planning brengt de accountant de beheersings-maatregelen in de IT-omgeving in kaart. Dit kan aan de hand van het P6 model gebeuren.
320 Materialiteit in de accountantscontrole	De doelstelling van de accountant is het op passende wijze toepassen van het concept van materialiteit bij de planning en uitvoering van de controle.	Op basis van de verdiepte kennis van de IT aan de hand van het P6 model, zal de accountant de materialiteit in acht nemen om de diepgang van de werkzaamheden aangaande de IT te bepalen.
330 Inspelen door de accountant op ingeschatte risico's	Het doel van de accountant is het verkrijgen van voldoende en geschikte controle-informatie over de ingeschatte risico's van een afwijking van materieel belang door middel van het opzetten en implementeren van geschikte manieren van inspelen op deze risico's.	Op basis van de geïdentificeerde risico's en aanwezige beheersingsmaatregelen in de IT-omgeving, bepaalt de accountant de algehele controleaanpak. In een controleprogramma beschrijft hij de systeem- en gegevensgerichte werkzaamheden. Hieruit blijkt welke General IT Controls en welke application controls worden getest.
500 Controle-informatie	De doelstelling van de accountant is om controlewerkzaamheden op te zetten en uit te voeren op een zodanige manier dat die het de accoun-	De accountant of de IT-auditor verzamelt documentatie van de IT.

Standaard	Omschrijving	IT Aspect
	tant mogelijk maakt om voldoende en geschikte controle-informatie te verkrijgen teneinde in staat te zijn redelijke conclusies te trekken om daarop het oordeel van de accountant te baseren.	
530 Steekproeven	Het doel van de accountant bij het gebruiken van steekproeven bij een controle is het zich verschaffen van een redelijke basis om tot conclusies te komen over de populatie waaruit de steekproef is getrokken.	De accountant bepaalt hoeveel waarnemingen worden gedaan uitgaande van een goede werking van de application controls. Ook bepaalt hij of een integrale controle wordt uitgevoerd via data-analyse.

Bijlage 4: Identificatie specifieke IT aspecten o.b.v. NV COS t.a.v. interim-controle

In onderstaand tabel is per relevante Standaard aangegeven of er specifieke IT aspecten aan de orde bij de **interim-controle** van een audit.

Standaard	Omschrijving	IT Aspect
220 Kwaliteitsbeheersing voor controles	Deze Controlestandaard heeft ten doel vereisten vast te stellen en leidraden te geven omtrent de specifieke verantwoordelijkheden van het personeel van accountantspraktijken met betrekking tot de kwaliteitsbeheersingsprocedures ten aanzien van controle van historische financiële informatie, waaronder de controle van jaarrekeningen. Deze Standaard moet worden gelezen in samenhang met de Verordening Gedrags- en Beroepsregels Accountants (VGBA).	• Deskundigheid in opdrachtteam 230.A20 • Consultatie (230.18,A21) • OKB 230.19
230 Controle-documentatie	Deze Controlestandaard heeft ten doel vereisten vast te stellen en leidraden te geven met betrekking tot controledocumentatie.	• Vastlegging elektronische controle-informatie o.a. 230.a3 • Documenteren controle-informatie elektronisch conform voorwaarden 230.9.
240 De verantwoordelijkheid van de accountant m.b.t. fraude	De doelstellingen van de accountant zijn: a. Het identificeren en inschatten van de risico's van een afwijking van materieel belang die het gevolg is van fraude; b. Het verkrijgen van voldoende en geschikte controle-informatie over de ingeschatte risico's van een afwijking van materieel belang die het gevolg is van fraude, door het opzetten en implementeren van passende maatregelen om op die risico's in te spelen; en c. Het op passende wijzen inspelen op fraude of vermoede fraude die tijdens de controle wordt onderkend.	Geen specifieke IT aspecten. De standaard is echter ook toepasbaar op risico's op afwijkingen van materieel belang als gevolg van fraude via IT. Tijdens de interim controle dient de accountant signalen die wijzen op fraude nader te onderzoeken.
250 Wet- en regelgeving	De doelstellingen van de accountant zijn: a. Het verkrijgen van voldoende en geschikte controle-informatie omtrent het naleven van bepalingen van die wet- en regelgeving die gewoonlijk worden beschouwd als zijnde van directe invloed op de vaststelling van bedragen en in financiële overzichten opgenomen toelichtingen die van materieel belang zijn;	Geen specifieke IT aspecten vermeld. Relevante specifieke wet- en regelgeving die verband houdt met IT is bijvoorbeeld de Wet Bescherming Persoonsgegevens.

Standaard	Omschrijving	IT Aspect
	b. Het uitvoeren van gespecificeerde controle-werkzaamheden teneinde bij te dragen tot het identificeren van gevallen van het niet-naleven van andere wet- en regelgeving die een invloed van materieel belang kunnen hebben op de financiële overzichten; en c. Het op passende wijze inspelen op het niet-naleven of vermoedens van het niet-naleven van wet- en regelgeving die tijdens de controle zijn onderkend.	
260 Communicatie over controle-aangelegenheden met de met governance belaste personen	De doelstellingen van de accountant zijn: a. Het duidelijk communiceren met de met governance belaste personen over de verantwoordelijkheden van de accountant met betrekking tot de controle van de financiële overzichten, alsmede over een overzicht van de geplande reikwijdte en timing van de controle; b. Het verkrijgen van voor de controle relevante informatie van de met governance belaste personen ; c. Het tijdig verschaffen aan de met governance belaste personen van observaties die voortkomen uit de controle en die significant en relevant zijn voor hun verantwoordelijkheid om toezicht uit te oefenen op het proces van financiële verslaggeving; en d. Het bevorderen van doeltreffende wederzijdse communicatie tussen de accountant de met governance belaste personen.	Verplichting te rapporteren over de continuïteit van de geautomatiseerde gegevensverwerking.
265 Het communiceren van tekortkomingen in de interne beheersing aan de met governance belaste personen en management	De doelstelling van de accountant is het op passende wijze aan de met governance belaste personen en aan het management te communiceren van tekortkomingen in de interne beheersing die de accountant heeft onderkend tijdens de controle en die op grond van het professionele oordeel van de accountant voldoende belangrijk zijn om hun respectieve aandacht te verdienen.	Tekortkomingen in de General IT Controls zijn over het algemeen onderdeel van de management-letter.
330 Inspelen door de accountant op ingeschatte risico's	Het doel van de accountant is het verkrijgen van voldoende en geschikte controle-informatie over de ingeschatte risico's van een afwijking van materieel belang door middel van het opzetten en implementeren van geschikte manieren van inspelen op deze risico's.	• Controle-informatie die tijdens tussentijdse periode of vorige periode is verkregen 330.12 en 13 (beheersingsmaatregelen) en 22 en A27 3e bullet onder c (gegevensgerichte controles)

Standaard	Omschrijving	IT Aspect
		• Toepassen audit softwaretoepassingen (330.A16) • 330.A24 en 315.30 aanpak ingeval van geautomatiseerde gegevensverwerking zonder dat er documentatie wordt vervaardigd of bewaard. • Evalueren voldoende en geschikte controle-informatie (330.26)
402 Serviceorganisaties	De doelstellingen van de accountant van de gebruiker, wanneer de gebruikende entiteit gebruik maakt de diensten van een serviceorganisatie, zijn a. Het verwerven van inzicht in de aard en significantie van de diensten die door de serviceorganisatie worden verleend en het effect daarvan op de voor de controle relevant zijnde interne beheersing van de gebruikende entiteit, dat voldoende is om de risico's van een afwijking van materieel belang te kunnen identificeren en in te schatten; en b. Het opzetten en uitvoeren van controlewerkzaamheden die op die risico's inspelen.	402.3b procedures in IT kunnen zijn uitbesteed aan een serviceorganisatie.
450 Evaluatie afwijkingen	De doelstelling van de accountant is het evalueren van: a. De invloed van geïdentificeerde afwijkingen op de controle; en b. De invloed van niet-gecorrigeerde afwijkingen, indien aanwezig, op de financiële overzichten.	Geen
500 Controle-informatie	De doelstelling van de accountant is om controlewerkzaamheden op te zetten en uit te voeren op een zodanige manier dat die het de accountant mogelijk maakt om voldoende en geschikte controle-informatie te verkrijgen teneinde in staat te zijn redelijke conclusies te trekken om daarop het oordeel van de accountant te baseren.	• Voldoende en geschikt zijn van controle-informatie (o.a. 500.7 en 9) • Relevantie en betrouwbaarheid van controle-informatie • 500.A12 - beschikbaarheid gegevens (elektronisch of alleen bepaalde periode) • 500.A13 - elektronische informatie alleen beschikbaar in bepaalde periode. • Selecteren van items ter toetsing (500.10)

Standaard	Omschrijving	IT Aspect
501 Controle-informatie specifieke items	De doelstelling voor de accountant is om voldoende en geschikte controle-informatie te verkrijgen met betrekking tot: a. Het bestaan en de conditie van de voorraad; b. De volledigheid van rechtszaken en claims waarbij de entiteit betrokken is; c. Presentatie en toelichting van gesegmenteerde informatie in overeenstemming met het van toepassing zijnde stelsel inzake financiële verslaggeving.	Geen
520 Cijferanalyses	De doelstellingen van de accountant zijn: a. Het verkrijgen van relevante en betrouwbare controle-informatie bij het gebruiken van gegevensgerichte cijferanalyses; en b. Het opzetten en uitvoeren van cijferanalyses aan het einde van de controle die een hulpmiddel vormen voor de accountant bij het komen tot een slotconclusie over de vraag of de financiële overzichten consistent zijn met het inzicht van de accountant in de entiteit.	• Betrouwbaarheid van de gegevens • Inzet softwaretoepassingen bij het uitvoeren van cijferanalyses.
530 Steekproeven	Het doel van de accountant bij het gebruiken van steekproeven bij een controle is het zich verschaffen van een redelijke basis om tot conclusies te komen over de populatie waaruit de steekproef is getrokken.	• Relevant voor uit te voeren werkzaamheden met betrekking tot werking van IT controls • Inzet softwaretoepassingen bij het uitvoeren van steekproeven
540 Schattingen	De doelstelling van de accountant is het verkrijgen van voldoende en geschikte controle-informatie over de vraag of: a. De schattingen in de financiële overzichten, met inbegrip van schattingen van reële waarde, opgenomen dan wel toegelicht, redelijk zijn; en b. De daarop betrekking hebbende toelichtingen in de financiële overzichten adequaat zijn, binnen de context van het van toepassing zijnde stelsel inzake financiële verslaggeving.	• Betrouwbaarheid van de voor de schatting gehanteerde gegevens • Interne beheersingsmaatregelen m.b.t. schattingen in IB • Inzet softwaretoepassingen bij de controle
550 Verbonden partijen	De doelstellingen van de accountant zijn: a. Ongeacht of het van toepassing zijnde stelsel inzake financiële verslaggeving eisen inzake verbonden partijen stelt, het verwerven van inzicht in relaties en transacties met verbonden partijen dat voldoende is om:	Geen specifieke

Standaard	Omschrijving	IT Aspect
	i. Frauderisicofactoren te herkennen, indien aanwezig, die voortkomen uit relaties en transacties met verbonden partijen die relevant zijn voor het identificeren en inschatten van de risico's van een afwijking van materieel belang die het gevolg is van fraude; en ii. Te concluderen, op basis van de verkregen controle-informatie, of de financiële overzichten, voor zover deze beïnvloed zijn door deze relaties en transacties: a. Een getrouwe weergave bereiken (voor getrouw-beeld-stelsels); of b. Niet misleidend zijn (voor compliance-stelsels); en b. Bovendien, waar het van toepassing zijnde stelsel inzake financiële verslaggeving eisen inzake verbonden partijen stelt, het verkrijgen van voldoende en geschikte controle-informatie over de vraag of relaties en transacties met verbonden partijen op passende wijze zijn geïdentificeerd, verwerkt en toegelicht in de financiële overzichten in overeenstemming met het stelsel.	
600 Gebruikmaken van de werkzaamheden van andere accountants	Deze Controlestandaard heeft ten doel vereisten vast te stellen en leidraden te geven voor de accountant, die een verklaring afgeeft bij een financieel overzicht van een entiteit en daarbij gebruik maakt van de werkzaamheden van een andere accountant met betrekking tot de financiële gegevens van een of meer (groeps)onderdelen die in het financiële overzicht van de desbetreffende entiteit zijn verwerkt. Deze Standaard heeft geen betrekking op de situatie dat twee of meer accountants belast zijn met de gezamenlijke controleopdracht bij eenzelfde entiteit en op de relatie tussen de accountant en de voorgaande accountant. De vereisten in deze Standaard zijn evenmin van toepassing indien de groepsaccountant van mening is dat een financieel overzicht van een (groeps)onderdeel niet van materieel belang is. Deze Standaard is echter wel van toepassing, indien enkele (groeps)onderdelen op zich niet, maar tezamen wel van materieel belang zijn.	Geen

Standaard	Omschrijving	IT Aspect
620 Gebruikmaken van de werkzaamheden van deskundigen	Deze Controlestandaard heeft ten doel vereisten vast te stellen en leidraden te geven omtrent het gebruikmaken van de werkzaamheden van deskundigen om controle-informatie te verkrijgen.	

Bijlage 5: Identificatie specifieke IT aspecten o.b.v. NV COS t.a.v. eindejaarscontrole

In onderstaande tabel is per relevante Richtlijn aangegeven of er specifieke IT aspecten aan de orde zijn bij de **eindejaarscontrole** van een audit.

Standaard	Omschrijving	IT Aspect
220 Kwaliteitsbeheersing voor controles	Deze Controlestandaard heeft ten doel vereisten vast te stellen en leidraden te geven omtrent de specifieke verantwoordelijkheden van het personeel van accountantspraktijken met betrekking tot de kwaliteitsbeheersingsprocedures ten aanzien van controle van historische financiële informatie, waaronder de controle van jaarrekeningen. Deze Standaard moet worden gelezen in samenhang met de Verordening Gedrags- en Beroepsregels Accountants (VGBA).	• Deskundigheid in opdrachtteam 230.A20 • Consultatie (230.18,A21) • OKB 230.19
230 Controle-documentatie	Deze Controlestandaard heeft ten doel vereisten vast te stellen en leidraden te geven met betrekking tot controledocumentatie.	• Vastlegging elektronische controle-informatie oa 230.a3 • Documenteren controle-informatie elektronisch conform voorwaarden 230.9.
240 De verantwoordelijkheid van de accountant m.b.t. fraude	De doelstellingen van de accountant zijn: a. Het identificeren en inschatten van de risico's van een afwijking van materieel belang die het gevolg is van fraude; b. Het verkrijgen van voldoende en geschikte controle-informatie over de ingeschatte risico's van een afwijking van materieel belang die het gevolg is van fraude, door het opzetten en implementeren van passende maatregelen om op die risico's in te spelen; en c. Het op passende wijzen inspelen op fraude of vermoede fraude die tijdens de controle wordt onderkend.	Geen specifieke IT aspecten, risico's fraude in IT benoemd in fase risico analyse.
250 Wet- en regelgeving	De doelstellingen van de accountant zijn: a. Het verkrijgen van voldoende en geschikte controle-informatie omtrent het naleven van bepalingen van die wet- en regelgeving die gewoonlijk worden beschouwd als zijnde van directe invloed op de vaststelling van bedragen en in financiële overzichten opgenomen toelichtingen die van materieel belang zijn;	Eventueel artikel 2:393 lid 4 BW inzake continuïteit geautomatiseerde gegevensverwerking, voor zover niet reeds bij de interim-controle gerapporteerd.

Standaard	Omschrijving	IT Aspect
	b. Het uitvoeren van gespecificeerde controle-werkzaamheden teneinde bij te dragen tot het identificeren van gevallen van het niet-naleven van andere wet- en regelgeving die een invloed van materieel belang kunnen hebben op de financiële overzichten; en c. Het op passende wijze inspelen op het niet-naleven of vermoedens van het niet-naleven van wet- en regelgeving die tijdens de controle zijn onderkend.	
260 Communicatie over controle-aangelegenheden met de met governance belaste personen	De doelstellingen van de accountant zijn: a. Het duidelijk communiceren met de met governance belaste personen over de verantwoordelijkheden van de accountant met betrekking tot de controle van de financiële overzichten, alsmede over een overzicht van de geplande reikwijdte en timing van de controle; b. Het verkrijgen van voor de controle relevante informatie van de met governance belaste personen ; c. Het tijdig verschaffen aan de met governance belaste personen van observaties die voortkomen uit de controle en die significant en relevant zijn voor hun verantwoordelijkheid om toezicht uit te oefenen op het proces van financiële verslaggeving; en d. Het bevorderen van doeltreffende wederzijdse communicatie tussen de accountant en de met governance belaste personen.	Geen specifieke IT aspecten / vereisten, alhoewel in deze communicatie uiteraard wel IT-punten aan de orde kunnen / moeten zijn, afhankelijk van de specifieke situatie.
320 Materialiteit in de accountants-controle	De doelstelling van de accountant is het op passende wijze toepassen van het concept van materialiteit bij de planning en uitvoering van de controle.	Geen
330 Inspelen door de accountant op ingeschatte risico's	Het doel van de accountant is het verkrijgen van voldoende en geschikte controle-informatie over de ingeschatte risico's van een afwijking van materieel belang door middel van het opzetten en implementeren van geschikte manieren van inspelen op deze risico's.	• Controle-informatie tijdens tussentijdse periode of vorige periode is verkregen 330.12 en 13 (beheersingsmaatregelen) en 22 en A27 3e bullet onder c (gegevensgerichte controles) • Toepassen audit softwaretoepassingen (330.A16) • 330.A24 en 315.30 aanpak indien geautomatiseerde gegevensver-

Standaard	Omschrijving	IT Aspect
		werking en geen documentatie wordt vervaardigd of bewaard. • Evalueren voldoende en geschikte controle-informatie (330.26)
402 Serviceorganisaties	De doelstellingen van de accountant van de gebruiker, wanneer de gebruikende entiteit gebruik maakt de diensten van een serviceorganisatie, zijn: a. Het verwerven van inzicht in de aard en significantie van de diensten die door de serviceorganisatie worden verleend en het effect daarvan op de voor de controle relevant zijnde interne beheersing van de gebruikende entiteit, dat voldoende is om de risico's van een afwijking van materieel belang te kunnen identificeren en in te schatten; en b. Het opzetten en uitvoeren van controlewerkzaamheden die op die risico's inspelen.	Dit is van toepassing indien de IT deels of geheel is uitbesteed.
450 Evaluatie afwijkingen	De doelstelling van de accountant is het evalueren van: a. De invloed van geïdentificeerde afwijkingen op de controle; en b. De invloed van niet-gecorrigeerde afwijkingen, indien aanwezig, op de financiële overzichten.	Geen
500 Controle-informatie	De doelstelling van de accountant is om controlewerkzaamheden op te zetten en uit te voeren op een zodanige manier dat die het de accountant mogelijk maakt om voldoende en geschikte controle-informatie te verkrijgen teneinde in staat te zijn redelijke conclusies te trekken om daarop het oordeel van de accountant te baseren.	• Voldoende en geschikt zijn van controle-informatie (o.a. 500.7 en 9) • Relevantie en betrouwbaarheid van controle-informatie • Door het management ingeschakelde deskundige • 500.A12 - beschikbaarheid gegevens (elektronisch of alleen bepaalde periode) • 500.A13 – elektronische informatie alleen beschikbaar in bepaalde periode. • Selecteren van items ter toetsing (500.10)
501 Controle-informatie specifieke items	De doelstelling voor de accountant is om voldoende en geschikte controle-informatie te verkrijgen met betrekking tot:	Geen

Standaard	Omschrijving	IT Aspect
	a. Het bestaan en de conditie van de voorraad; b. De volledigheid van rechtszaken en claims waarbij de entiteit betrokken is; c. Presentatie en toelichting van gesegmenteerde informatie in overeenstemming met het van toepassing zijnde stelsel inzake financiële verslaggeving.	
505 Externe bevestigingen	De doelstelling van de accountant bij het gebruikmaken van werkzaamheden inzake externe bevestigingen is het opzetten en uitvoeren van dusdanige werkzaamheden teneinde relevante en betrouwbare controle-informatie te verkrijgen.	Geen
520 Cijferanalyses	De doelstellingen van de accountant zijn: a. Het verkrijgen van relevante en betrouwbare controle-informatie bij het gebruiken van gegevensgerichte cijferanalyses; en b. Het opzetten en uitvoeren van cijferanalyses aan het einde van de controle die een hulpmiddel vormen voor de accountant bij het komen tot een slotconclusie over de vraag of de financiële overzichten consistent zijn met het inzicht van de accountant in de entiteit.	• Betrouwbaarheid van de gegevens • Inzet softwaretoepassingen bij het uitvoeren van cijferanalyses
530 Steekproeven	Het doel van de accountant bij het gebruiken van steekproeven bij een controle is het zich verschaffen van een redelijke basis om tot conclusies te komen over de populatie waaruit de steekproef is getrokken.	Inzet softwaretoepassingen bij het uitvoeren van steekproeven
540 Schattingen	De doelstelling van de accountant is het verkrijgen van voldoende en geschikte controle-informatie over de vraag of: a. De schattingen in de financiële overzichten, met inbegrip van schattingen van reële waarde, opgenomen dan wel toegelicht, redelijk zijn; en b. De daarop betrekking hebbende toelichtingen in de financiële overzichten adequaat zijn, binnen de context van het van toepassing zijnde stelsel inzake financiële verslaggeving.	• Betrouwbaarheid van de voor de schatting gehanteerde gegevens • Interne beheersingsmaatregelen rond schattingen in IB • Inzet softwaretoepassingen bij de controle
550 Verbonden partijen	De doelstellingen van de accountant zijn: a. Ongeacht of het van toepassing zijnde stel-	Geen

Standaard	Omschrijving	IT Aspect
	sel inzake financiële verslaggeving eisen inzake verbonden partijen stelt, het verwerven van inzicht in relaties en transacties met verbonden partijen dat voldoende is om in staat te zijn: i. Frauderisicofactoren te herkennen, indien aanwezig, die voortkomen uit relaties en transacties met verbonden partijen die relevant zijn voor het onderkennen en inschatten van de risico's van een afwijking van materieel belang die het gevolg is van fraude; en ii. Te concluderen, op basis van de verkregen controle-informatie, of de financiële overzichten, voor zover deze beïnvloed zijn door deze relaties en transacties: a. Een getrouwe weergave bereiken (voor getrouw-beeld-stelsels); of b. Niet misleidend zijn (voor compliance-stelsels); en b. Bovendien, waar het van toepassing zijnde stelsel inzake financiële verslaggeving eisen inzake verbonden partijen stelt, het verkrijgen van voldoende en geschikte controle-informatie over de vraag of relaties en transacties met verbonden partijen op passende wijze zijn geïdentificeerd, verwerkt en toegelicht in de financiële overzichten in overeenstemming met het stelsel.	
600 Gebruikmaken van de werkzaamheden van andere accountants	Deze Controlestandaard heeft ten doel vereisten vast te stellen en leidraden te geven voor de accountant, die een verklaring afgeeft bij een financieel overzicht van een entiteit en daarbij gebruik maakt van de werkzaamheden van een andere accountant met betrekking tot de financiële gegevens van een of meer (groeps)onderdelen die in het financiële overzicht van de desbetreffende entiteit zijn verwerkt. Deze Standaard heeft geen betrekking op de situatie dat twee of meer accountants belast zijn met de gezamenlijke controleopdracht bij eenzelfde entiteit en op de relatie tussen de accountant en de voorgaande accountant. De vereisten in deze Standaard zijn evenmin van toepassing indien de groepsaccountant van mening is dat een financieel overzicht van een (groeps)onderdeel	Geen

Standaard	Omschrijving	IT Aspect
	niet van materieel belang is. Deze Standaard is echter wel van toepassing, indien enkele (groeps)-onderdelen op zich niet, maar tezamen wel van materieel belang zijn.	
620 Gebruikmaken van de werkzaamheden van deskundigen	Deze Controlestandaard heeft ten doel vereisten vast te stellen en leidraden te geven omtrent het gebruikmaken van de werkzaamheden van deskundigen om controle-informatie te verkrijgen.	Geen

Bijlage 6: Identificatie specifieke IT aspecten o.b.v. NV COS t.a.v. de afrondingsfase

In onderstaand tabel is per relevante Richtlijn aangegeven of er specifieke IT aspecten aan de orde bij de **afrondingsfase** van een audit.

Standaard	Omschrijving	IT Aspect
560 Gebeurtenissen na de einddatum van de verslagperiode	De doelstellingen van de accountant zijn: a. Het verkrijgen van voldoende en geschikte controle-informatie omtrent de vraag of gebeurtenissen, die zich voordoen tussen de datum van de financiële overzichten en de datum van de controleverklaring en die een aanpassing van of een toelichting in de financiële overzichten noodzakelijk maken, op passende wijze in die financiële overzichten zijn weergegeven in overeenstemming met het van toepassing zijnde stelsel inzake financiële verslaggeving; en b. Het op passende wijze inspelen op feiten die de accountant bekend worden na de datum van de controleverklaring, die, wanneer zij hem op die datum bekend waren geweest, tot een aanpassing in de controleverklaring zouden kunnen hebben geleid.	Geen specifieke IT vereisten alhoewel gebeurtenissen met betrekking tot IT in dit kader wel mogelijk kunnen zijn , echter hangen deze veelal samen met continuïteit van de IT.
570 Continuïteit	De doelstellingen van de accountant zijn: a. Het verkrijgen van voldoende en geschikte controle-informatie met betrekking tot de geschiktheid van het door het management hanteren van de continuïteitsveronderstelling bij het opstellen van de financiële overzichten; b. Het concluderen, op basis van de verkregen controle-informatie, of er een onzekerheid van materieel belang bestaat met betrekking tot gebeurtenissen of omstandigheden die gerede twijfel kunnen doen ontstaan over het vermogen van de entiteit om haar continuïteit te handhaven; en c. Het vaststellen van de implicaties voor de controleverklaring.	Continuïteitsveronderstelling t.a.v. de IT, met name bij hoog geautomatiseerde ondernemingen.
580 Schriftelijke bevestiging	De doelstellingen van de accountant zijn: a. Het verkrijgen van schriftelijke bevestigingen van het management en, waar van toepas-	Geen

Standaard	Omschrijving	IT Aspect
	sing, van de met governance belaste personen dat zij van mening zijn dat zij hun verantwoordelijkheden met betrekking tot het opstellen van de financiële overzichten en de volledigheid van de verstrekte informatie aan de accountant, zijn nagekomen; b. Het ondersteunen van andere controle-informatie die relevant is voor de financiële overzichten of specifieke beweringen die in de financiële overzichten zijn opgenomen, door middel van schriftelijke bevestigingen indien deze noodzakelijk geacht worden door de accountant of indien deze op grond van andere Standaarden vereist zijn; en c. Het op passende wijze inspelen op de door het management en waar van toepassing, door de met governance belaste personen, verstrekte schriftelijke bevestigingen, dan wel op de situatie waarin het management of waar van toepassing, de met governance belaste personen, de door de accountant gevraagde schriftelijke bevestigingen niet verstrekt.	
700 Oordeel	De doelstellingen van de accountant zijn: a. Het vormen van een oordeel over de financiële overzichten op basis van een evaluatie van de conclusies getrokken uit de verkregen controle-informatie; en b. Het op duidelijke wijze tot uitdrukking brengen van dat oordeel door middel van een schriftelijke verklaring die tevens de onderbouwing voor dat oordeel beschrijft.	Geen
705 Aanpassing van het oordeel	De doelstelling van de accountant is het duidelijk tot uitdrukking brengen van een op passende wijze aangepast oordeel over de financiële overzichten, dat noodzakelijk is wanneer: a. De accountant op basis van de verkregen controle-informatie concludeert dat de financiële overzichten als geheel een afwijking van materieel belang bevatten; of b. De accountant niet in staat is voldoende en geschikte controle-informatie te verkrijgen om te kunnen concluderen dat de financiële overzichten als geheel geen afwijking van materieel belang bevatten.	Geen

Standaard	Omschrijving	IT Aspect
706 Benadrukking van aangelegenheden	De doelstelling van de accountant is, nadat hij zich een oordeel heeft gevormd over de financiële overzichten, wanneer het naar het oordeel van de accountant noodzakelijk is om als een vorm van duidelijke aanvullende communicatie in de controleverklaring, de aandacht van gebruikers te vestigen op: a. Een aangelegenheid die, hoewel deze op passende wijze is weergegeven of toegelicht in de financiële overzichten, van zodanig belang is dat deze fundamenteel is voor het begrip van gebruikers van de financiële overzichten; of b. In voorkomend geval, elke andere aangele genheid die relevant is voor het begrip van gebruikers van de controle, de verantwoordelijkheden van de accountant of de controleverklaring.	Geen

Bijlage 7: Relatie doelstelling, application controls en General IT Controls

De hieronder opgenomen lijst met beheersingsmaatregelen is niet uitputtend en/of branchegericht en is vooral bedoeld als richtinggevend voor vergelijkbare beheersingsmaatregelen.

Legenda:

Type	Afkorting	Beschrijving
Manual control	M	Handmatige controle
Computer dependent manual control	CM	Handmatige controle waarbij gebruik wordt gemaakt van door software gegenereerde output
Automated	A	Volledig geautomatiseerde controle binnen de gebruikte software applicatie

Betalingen

	IB maatregel	Type maatregel	Controledoelstelling						
			Bestaan	Waardering	Afgrenzing	Volledigheid	Juistheid	Tijdigheid	Classificatie
1	Bewaring van electronische sleutels voor geautomatiseerde betalingen	CM							
2	Interne richtlijnen voor betalingskortingen verwerkt in de software	CM					x		
3	Interne richtlijnen voor het innemen van valutaposities verwerkt in de software	CM					x		
4	Bevoegdheden in het systeem zijn dusdanig ingericht dat slechts bevoegde personen kunnen betalen	A							
5	Periodiek wordt gecontroleerd dat er geen betalingsbevoegdheid is toegekend aan niet geautoriseerde gebruikers	A							
6	De directie autoriseert alle betalingsvoorstellen alsvorens de betaling wordt verricht	A							
7	Er is sprake van voldoende functiescheiding tussen crediteurenbeheer (mutatie stamgegevens) en betalingsbevoegdheid	CM							
8	Periodieke controle op de betalingen die handmatig zijn verricht	A					x		
9	Periodieke kascontrole door de bevoegde functionaris	CM					x		
10	Het softwarematig bewaken van richtlijnen dat slechts geaccordeerde inkoopfacturen betaalbaar worden gesteld	A					x		
11	Het softwarematig bewaken van richtlijnen met betrekking tot de ontvangst van aanmaningen door medewerkers, die geen betalingsbevoegdheid hebben	A							

				IT Audit doelstelling					Application controls													IT general controls					
Autorisatie	Rechten en verplichtingen	Presentatie en toelichting		Exclusiviteit	Integriteit	Controleerbaarheid	Continuiteit		Logische toegangsbeveiliging	Volledigheidscontrole	Validity check	Field check	Redundancy check	Sign Check	Limit check	Range check	Reasonable check	Verbandscontrole	Totaalcontrole	Audit trail	Logging		Management en organisatie	Logische toegangsbeveiliging	Wijzigingsbeheer	Probleembeheer	Procesbeheer	Continuiteit
x				x					x											x	x			x	x			
x	x			x	x				x		x			x	x		x						x	x			
x	x			x	x	x			x		x			x			x						x	x			
x	x			x					x	x			x							x	x		x	x			
x				x					x	x			x							x	x		x	x			
x	x			x					x											x	x		x				
x	x			x					x											x	x		x				
					x					x	x		x	x	x	x				x	x						
					x					x				x			x	x	x								
	x			x	x				x											x	x		x				
x	x			x	x				x											x	x		x	x			

Inkopen

	IB maatregel	Type maatregel	Controledoelstelling						
			Bestaan	Waardering	Afgrenzing	Volledigheid	Juistheid	Tijdigheid	Classificatie
1	Gebruik van goedgekeurde leveranciersbestanden	A					x		
2	Gebruik van voorgenummerde bestelopdrachten	A				x			
3	Vastlegging van bestelbevoegdheden	A							
4	Onafhankelijke goedkeuring van bestellingen alvorens die worden geplaatst	A					x		
5	Onafhankelijke beoordeling van geplaatste bestellingen t.a.v. vereiste goedkeuring	A		x					
6	Onafhankelijke kwaliteitscontrole van ontvangen goederen	M	x						
7	Voornummering ontvangen inkoopfacturen	A				x	x	x	
8	Controle inkoopfacturen met bestelbonnen	CM					x		
9	Controle inkoopfacturen met ontvangstbonnen (inclusief opboeking voorraadadm.)	CM	x			x	x	x	
10	Controle inkoopfacturen met kwaliteitscontrolerapporten	CM	x			x	x		
11	Controle bijkomende kosten (vracht e.d.) met kostenfacturen	CM		x		x	x		
12	Controle op volledige (digitale) invulling blokstempel inkoop- en kostenfacturen	A				x	x		
13	Periodieke analyse prijsverschillenrekening	CM		x		x	x		
14	Periodieke analyse tussenrekeningen inkopen	CM	x			x	x	x	
15	Periodieke controle op volledigheid kortingen en omzetboni	CM		x			x		
16	Periodieke controle op openstaande bestellingen	CM				x		x	
17	Periodieke controle op openstaande goederenontvangsten	CM	x			x		x	
18	Controle op afwikkeling retouren met creditnota's	CM	x			x	x		
19	Controle op rekenkundige juistheid inkoopfacturen	A					x		
20	Controle in rekening gebrachte prijs a.d.h.v. offerte/order/geaccordeerde prijslijst	CM					x		
21	Periodieke analyse van de ontwikkeling kosten a.d.h.v. de begroting cijfers voorgaande jaar	CM				x	x		
22	Toetsing van de kosten op bedrijfseigenheid	M							
23	Toetsing van de investeringen a.d.h.v. de investeringsbegroting	M							
24	Periodieke afstemming KVA/ fysieke voorraad (inventarisatie)	CM	x			x	x		
25	Periodieke beoordeling van de rekening koersverschillen	CM					x		
26	Periodieke margebeoordeling	CM				x	x	x	

				IT Audit doelstelling					Application controls														IT general controls					
Autorisatie	Rechten en verplichtingen	Presentatie en toelichting		Exclusiviteit	Integriteit	Controleerbaarheid	Continuiteit		Logische toegangsbeveiliging	Volledigheidscontrole	Validity check	Field check	Redundancy check	Sign Check	Limit check	Range check	Reasonable check	Verbandscontrole	Totaalcontrole	Audit trail	Logging		Management en organisatie	Logische toegangsbeveiliging	Wijzigingsbeheer	Probleembeheer	Procesbeheer	Continuiteit
x				x	x	x			x	x	x	x	x							x	x		x	x				
x					x	x						x	x							x								
x				x					x	x	x			x	x					x	x		x	x				
x					x	x			x	x	x			x	x		x			x	x		x	x				
x					x	x			x		x			x									x	x				
x					x				x								x	x					x	x				
						x					x		x															
					x	x								x			x	x										
					x	x								x			x	x										
					x									x			x	x										
				x										x			x	x										
x				x		x			x		x									x	x		x	x				
					x					x								x	x									
					x					x								x	x									
					x					x								x	x									
					x					x								x	x									
					x					x								x	x									
					x					x								x	x									
					x									x			x	x	x									
					x						x			x														
					x														x	x								
					x																							
					x														x	x								
					x														x	x								

Personeel

	IB maatregel	Type maatregel	Controledoelstelling						
			Bestaan	Waardering	Afgrenzing	Volledigheid	Juistheid	Tijdigheid	Classificatie
1	Controle op blokkeren toegang tot systemen in- en uitdiensttreding met nodige documenten	CM					x	x	
2	Controle op geautomatiseerde aanmelding bij het pensioenfonds	CM				x		x	
3	Controle op volledigheid informatie in personeelsdossiers	A				x			
4	Controle op juistheid informatie in personeelsdossier	CM					x		
5	Onafhankelijke controle op naleving wet- en regelgeving (incl. CAO bepalingen e.d.)	M					x		
6	Onafhankelijke controle op tijdige afdracht loonheffing, pensioenpremies e.d.	CM					x	x	
7	Controle op bruto-netto berekeningen	A					x		
8	Controle op afloop tussenrekeningen lonen	CM							
9	Controle op correcte verwerking, ziektemeldingen, verlofkaarten en bijzonder verlofregelingen	CM				x	x		
10	Controle productiviteit / indirecte uren	CM					x		
11	Controle jobtime = shoptime per afdeling /medewerker	CM				x	x		
12	Controle uitbetaalde salarissen met elektronisch standenregister	A					x		
13	Controle op niet belaste looncomponenten in de overige kosten	CM					x		x
14	Controle op betaling juiste rekeningnummer (ook rekeningnummer fiscus)	CM					x		
15	Controle op aanwezigheid in dossier en juistheid legitimatiebewijs	CM				x	x		
16	Controle van het bankrekeningnummer a.d.h.v. gegevens personeelsdossier	CM					x		

				IT Audit doelstelling					Application controls														IT general controls					
Autorisatie	Rechten en verplichtingen	Presentatie en toelichting		Exclusiviteit	Integriteit	Controleerbaarheid	Continuiteit		Logische toegangsbeveiliging	Volledigheidscontrole	Validity check	Field check	Redundancy check	Sign Check	Limit check	Range check	Reasonable check	Verbandscontrole	Totaalcontrole	Audit trail	Logging		Management en organisatie	Logische toegangsbeveiliging	Wijzigingsbeheer	Probleembeheer	Procesbeheer	Continuiteit
x				x	x	x			x	x										x	x		x	x	x	x	x	
					x				x	x								x	x									
					x					x																		
					x					x	x		x															
	x					x												x	x									
					x	x				x								x	x									
					x					x	x		x	x			x	x	x									
					x					x	x		x				x	x	x									
	x				x	x				x	x		x				x	x	x	x	x							
					x	x				x	x		x	x			x	x	x	x	x							
					x	x				x	x		x	x			x	x	x	x	x							
x					x				x	x	x		x	x			x	x	x	x	x			x				
					x					x				x			x	x	x									
					x				x					x					x	x	x			x				
					x	x			x	x	x						x							x				
					x	x			x	x	x						x			x	x			x				

Productie

	IB maatregel	Type maatregel	Controledoelstelling						
			Bestaan	Waardering	Afgrenzing	Volledigheid	Juistheid	Tijdigheid	Classificatie
1	Autorisatie van begrote kosten aan de hand van cijfers voorgaand jaar, normale en verwachte bezetting en ervaringsnormen	M					x		
2	Autorisatie van budgetten, tarieven, prijslijsten aan de hand van gegevens voorafgaand jaar, ontvangen orders en branchegegevens	M		x			x		
3	Onafhankelijke controle op nummervolgorde van produktie-opdrachten, goederen-afgiftebonnen, gereedmeldingen	A				x	x		
4	Onafhankelijke voortgangscontrole en controle op niet tijdig gereedgemelde produktie-opdrachten	A				x	x		
5	Onafhankelijke inventarisatie en controle op aansluiting met administratie	CM	x				x	x	
6	Onafhankelijke controle op produktie-rapportering en aansluiting met planning, magazijn en administratie en analyse van verschillen	CM				x	x		
7	Onafhankelijke controle op verkoopopbrengsten van afval en uitval	CM				x			
8	Analyse afdelingsrapporten ten opzichte van budget, normen en planning	CM							
9	Onafhankelijke controle op aansluiting van ontvangsten in magazijn gereed produkt, met planning, produktie en gereedmeldingen	CM				x	x		x
10	Periodieke opstelling retrogradeberekening en analyse van efficiencyverschillen	CM				x	x		
11	Onafhankelijke periodieke toetsing werkelijk verbruik grondstoffen aan toegestaan verbruik en analyse van verschillen	CM		x		x	x		
12	Onafhankelijke controle op aansluiting van uitbetaalde uren met geregistreerde aanwezigheidsuren, urenverdeelstaat en administratie en analyse van verschillen	CM				x	x	x	
13	Onafhankelijke afdelingsgewijze nacalculatie en toetsing aan voorcalculaties en analyse prijs-, efficiency en bezettingsverschillen	CM		x		x	x	x	
14	Onafhankelijke controle op aansluiting tussen totalen van opboeking crediteuren en brutoloon met totalen van kostenverdeelstaat m.b.t. produktiekosten	CM				x	x	x	

			IT Audit doelstelling				Application controls													IT general controls					
Autorisatie	Rechten en verplichtingen	Presentatie en toelichting	Exclusiviteit	Integriteit	Controleerbaarheid	Continuiteit	Logische toegangsbeveiliging	Volledigheidscontrole	Validity check	Field check	Redundancy check	Sign Check	Limit check	Range check	Reasonable check	Verbandscontrole	Totaalcontrole	Audit trail	Logging	Management en organisatie	Logische toegangsbeveiliging	Wijzigingsbeheer	Probleembeheer	Procesbeheer	Continuiteit
X			X	X	X		X											X	X		X				
X			X	X	X		X											X	X		X				
				X	X			X			X	X				X									
				X	X			X				X				X									
				X	X			X				X				X									
				X	X			X				X				X									
				X	X			X				X				X									
				X	X			X				X				X									
				X	X			X				X				X									
				X	X			X				X				X									
				X	X			X				X				X									
				X	X			X				X				X									
				X	X			X				X				X									
				X	X			X				X				X									

Dienstverlening Uren

	IB maatregel	Type maatregel	Controledoelstelling						
			Bestaan	Waardering	Afgrenzing	Volledigheid	Juistheid	Tijdigheid	Classificatie
1	Autorisatie uurtarieven	A							
2	Autorisatie urenverantwoordingsstaten	A				x		x	
3	Autorisatie afboekingen	A				x			
4	Afstemming totaal beschikbare uren met totaal verantwoorde uren	CM			x	x			
5	Afstemming verantwoorde directe uren met gefactureerde uren	CM				x			
6	Beoordeling productiviteit per persoon en per periode	CM				x		x	
7	Onafhankelijke controle op indirecte uren	CM				x			
8	Totaalaansluiting gefactureerde omzet met productiewaarde en bijkomende kosten	CM				x	x	x	
9	Onafhankelijke controle onderhanden werkpositie per opdrachtgever en in totaliteit	CM				x		x	
10	Autorisatie uitgaande facturen	A				x		x	
11	Cijferbeoordeling op gemiddelde (behaalde) uurtarieven	CM				x		x	
12	Cijferbeoordeling op gemiddelde (behaalde) uurtarieven	CM							
13	Cijferbeoordeling overige omzet (agv bijkomende kosten) ten opzichte van de bijkomende kosten	CM				x			

Dienstverlening Capaciteit

	IB maatregel	Type maatregel	Controledoelstelling						
			Bestaan	Waardering	Afgrenzing	Volledigheid	Juistheid	Tijdigheid	Classificatie
1	Autorisatie investeringen	A				x			
2	Autorisatie tarieven	A					x		
3	Onafhankelijke leegstandscontrole	CM				x			
4	Verbandlegging met direct met capaciteit samenhangende kosten	CM				x			
5	Bewaking en periodieke inventarisatie capaciteit	CM				x			
6	Interne analyse bezettingsgraad per individueel item en per periode	CM				x			
7	Autorisatie uitgaande facturen	A				x	x		
8	Interne analyse opbrengsten/kosten/marge per individueel item en per periode	CM				x	x		
9	Autorisatie overeenkomsten met opdrachtgever	CM				x	x		
10	Onafhankelijke registratie van bezetting	A				x	x		
11	Onafhankelijke controle uitgaande facturen met bezettingsregistratie	A				x	x		

				IT Audit doelstelling					Application controls													IT general controls					
Autorisatie	Rechten en verplichtingen	Presentatie en toelichting		Exclusiviteit	Integriteit	Controleerbaarheid	Continuiteit		Logische toegangsbeveiliging	Volledigheidscontrole	Validity check	Field check	Redundancy check	Sign Check	Limit check	Range check	Reasonable check	Verbandscontrole	Totaalcontrole	Audit trail	Logging		Management en organisatie	Logische toegangsbeveiliging	Wijzigingsbeheer	Probleembeheer	Procesbeheer	Continuiteit
x					x				x	x				x			x	x	x	x	x			x	x			
x				x	x				x	x				x			x	x	x	x	x			x				
x					x				x	x				x			x	x	x	x	x			x				
				x	x	x												x	x									
					x	x												x	x									
				x	x	x												x	x									
					x	x												x	x									
					x	x												x	x									
					x	x												x	x									
x					x	x			x	x			x	x						x	x			x	x			
					x	x								x				x	x									
					x	x								x				x	x									
					x	x								x				x	x									

				IT Audit doelstelling					Application controls													IT general controls					
Autorisatie	Rechten en verplichtingen	Presentatie en toelichting		Exclusiviteit	Integriteit	Controleerbaarheid	Continuiteit		Logische toegangsbeveiliging	Volledigheidscontrole	Validity check	Field check	Redundancy check	Sign Check	Limit check	Range check	Reasonable check	Verbandscontrole	Totaalcontrole	Audit trail	Logging		Management en organisatie	Logische toegangsbeveiliging	Wijzigingsbeheer	Probleembeheer	Procesbeheer	Continuiteit
x				x	x	x			x	x				x			x			x	x			x	x			
x				x	x	x			x	x	x			x						x	x			x	x			
					x	x				x	x							x										
					x									x				x										
					x					x								x										
					x									x				x										
x				x	x	x			x	x									x	x	x			x	x			
					x									x			x	x										
x				x	x	x			x									x		x	x			x	x			
					x					x				x				x		x	x							
					x									x				x	x									

Verkopen

	IB maatregel	Type maatregel	Controledoelstelling						
			Bestaan	Waardering	Afgrenzing	Volledigheid	Juistheid	Tijdigheid	Classificatie
1	Autorisatie verkoopprijzen door directie	A				x			
2	Acceptatieprocedure bij nieuwe afnemers	CM							
3	Orderacceptatieprocedures a.h.v. bestellimieten	CM		x					
4	Controle op beschikbaarheid goederen	A							
5	Facturering op basis van ordergegevens	A				x	x	x	
6	Facturering op basis van afleveringgegevens	A				x	x	x	
7	Onafhankelijke controle van vervaardigde verkoopfacturen (c.q. creditnota's) op basis van orders, afgiftebonnen en verzenddocumenten (c.q. ontvangstdocumenten van retouren)	CM				x	x	x	
8	Onderzoek van niet tijdig ontvangen vorderingen op afnemers	CM					x	x	
9	Onafhankelijke controle op rechtstreekse leveringen door afnemers	CM				x	x	x	
10	Onafhankelijke controle op nummervolgorde van verkooporders, verzenddocumenten en verkoopfacturen	A				x			
11	Controle van de voortelling van de verstuurde verkoopfacturen met de boeking in de debiteurenadministratie	A				x			
12	Onafhankelijke controle van gehanteerde limieten	A		x			x		
13	Onafhankelijke controle op naleving afboekingsvoorschriften	CM					x		
14	Aansluiten van verantwoorde opbrengsten gesplitst naar omzetgroepen met verkoop-statistieken en analyses	CM				x	x		
15	Afgrenzing van de voorraad en de retouren	CM			x			x	
16	Onafhankelijke controle van verkochte activa	CM				x	x		
17	Marge-analyse per productgroep	CM				x	x		
18	Analyse van de geboekte kortingen/commissies per productgroep /per afnemer(groep)	CM				x			
19	Interne controle op de invoer van stamgegevens debiteuren (prijzen, korting%, bonussen)	CM				x			
20	Intern opgestelde goederenbeweging	CM				x	x		
21	Onafhankelijke klachtenregistratie / afhandeling	M		x					

				IT Audit doelstelling					Application controls															IT general controls					
Autorisatie	Rechten en verplichtingen	Presentatie en toelichting		Exclusiviteit	Integriteit	Controleerbaarheid	Continuiteit		Logische toegangsbeveiliging	Volledigheidscontrole	Validity check	Field check	Redundancy check	Sign Check	Limit check	Range check	Reasonable check	Verbandscontrole	Totaalcontrole	Audit trail	Logging		Management en organisatie	Logische toegangsbeveiliging	Wijzigingsbeheer	Probleembeheer	Procesbeheer	Continuiteit
x				x	x	x			x		x						x			x	x			x	x			
x	x			x		x			x		x						x			x	x			x	x			
x	x			x		x			x	x	x					x								x	x			
					x					x	x					x												
					x					x	x		x	x	x		x	x	x								x	
					x					x	x		x	x	x		x	x	x								x	
					x					x	x		x	x	x		x	x	x									
					x					x						x	x											
x				x	x				x	x	x						x							x				
					x					x			x					x	x									
					x						x	x		x														
					x										x			x										
x				x	x	x			x	x							x			x	x			x	x			
		x			x												x	x						x	x			
					x					x								x										
					x					x				x				x										
					x	x												x										
					x	x												x										
x				x	x	x			x	x	x	x	x	x	x	x								x	x			
					x	x												x										
	x				x	x				x							x											

Ontvangsten

	IB maatregel	Type maatregel	Controledoelstelling						
			Bestaan	Waardering	Afgrenzing	Volledigheid	Juistheid	Tijdigheid	Classificatie
1	Onafhankelijke controle op naleving voorschriften	M				x			
2	Analyse van de rekening kruisposten	CM				x	x		
3	Onafhankelijke inventarisatie van aanwezige kasgelden	CM				x	x		
4	Onafhankelijke behandeling van door debiteuren gevraagde inlichtingen	M				x	x		

				IT Audit doelstelling					Application controls													IT general controls					
Autorisatie	Rechten en verplichtingen	Presentatie en toelichting		Exclusiviteit	Integriteit	Controleerbaarheid	Continuiteit		Logische toegangsbeveiliging	Volledigheidscontrole	Validity check	Field check	Redundancy check	Sign Check	Limit check	Range check	Reasonable check	Verbandscontrole	Totaalcontrole	Audit trail	Logging		Management en organisatie	Logische toegangsbeveiliging	Wijzigingsbeheer	Probleembeheer	Procesbeheer	Continuiteit
					x										x	x	x										
					x					x								x									
					x					x				x				x									
					x					x																	

Bijlage 8: Back-up proces

Managementverantwoordelijkheden
Het proces voor identificatie van processen, applicaties en data bestanden die in aanmerking komen voor back-up is beschreven.
Identificeer alle kernapplicaties die kritisch zijn voor de ondersteuning van de bedrijfsoperatie.
Stel een testplan op om de werking van back-up en recovery processen te testen.
Benoem per proces de proceseigenaren, verantwoordelijk voor de bewaking en uitvoering van back-up en recovery.
Stel een basisniveau per bedrijfsproces vast voor de frequentie en rotatie van back-up en recovery.
Zorg voor een periodieke meting van de afwijkingen tussen basisniveau en feitelijke proceskwaliteit van het back-up en recovery proces.
Zorg voor opvolging van geconstateerde afwijkingen ten opzichte van het basisniveau.
Stel periodiek vast dat het back-up proces de juiste applicaties en data bestanden omvat en dat het back-up schema voldoet aan de continuïteitseisen van de onderneming.
Back-up operatie
Stel per geïdentificeerd bedrijfsproces vast dat:
Is beschreven op welke werkdagen en met welke frequentie er een back-up nodig is.
Er een rotatieschema aanwezig is waarin is vastgelegd met welke frequentie back-up media worden verwisseld.
Back-up software wordt gebruikt voor het inplannen en uitvoeren van back-up taken.
Back-up software wordt gebruikt om automatisch vast te leggen welke data bestanden worden meegenomen in de back-up job.
De huidige back-up instellingen zijn goedgekeurd door de applicatie en/of proceseigenaar.
De back-up software dagelijks een rapport genereert van succesvol aangemaakte back-ups en dat dit rapport door de applicatie en/of proceseigenaar wordt gemonitord.
De applicatie en/of proceseigenaar tijdig actie onderneemt op basis van de rapportage.

De back-up software automatisch een headerbestand aanmaakt op het back-up medium waarin is vastgelegd wat de inhoud, de back-up periode en de bewaartermijn van de gemaakte back-up is.

De back-up software beschikt over een overschrijfbeveiliging die er voor zorgt dat het back-up medium niet kan worden overschreven voordat de bewaarperiode is verstreken.

De back-up software beschikt over functionaliteit om het back-up rotatieschema vast te leggen.

De back-up software een foutrapportage genereert als er wordt afgeweken van het rotatieschema.

De back-up software een foutrapportage genereert als het rotatieschema niet dekkend is voor alle vooraf ingestelde werkdagen.

De back-up software zodanig is ingesteld dat ook openstaande (in gebruik zijnde) databestanden worden meegenomen in een back-up run.

Het kunnen teruglezen van back-up media regelmatig wordt getest met steeds wisselende back-up media.

Media Handling

Stel vast dat:

Back-up media, volgens een beschreven procedure buiten de onderneming in een afgesloten en brandveilige kluis worden opgeslagen.

De fysieke toegang tot het back-up medium is voorbehouden aan een beperkt aantal door het bedrijf geautoriseerde functionarissen.

Elk back-up medium is voorzien van een duidelijk voor mensen leesbare vastlegging waaruit af te leiden is welke back-up data, over welke periode, voor welk deel van het rotatieschema zijn vastgelegd.

Er steeds voldoende media buiten de onderneming worden bewaard om aan de vereiste basisafspraken voor het terugzetten van back-ups te kunnen voldoen.

Indien een externe leverancier het ophalen en retourneren van back-up media verzorgt, beoordeel dan of de contractvoorwaarden bovenstaande punten afdekken.

Logbestandanalyse door de IT-auditor

Selecteer voor de te controleren periode een set back-up logbestanden waarmee meerdere volledige werkweken worden afgedekt. Houd bij de selectie rekening met piekperiodes en vakanties.

Gebruik een data-analyse tool voor toegang tot de logfiles

Ga na of er bestanden zijn die regelmatig worden overgeslagen bij een back-up

Ga na of er back-up jobs zijn die consistent niet worden afgerond.

Ga na of er back-up jobs zijn die consistent niet worden opgestart.

Stel vast dat er gedurende de geselecteerde periode geen wijzigingen in de instellingen van de back-up software hebben plaatsgevonden.

Vergelijk de bevindingen uit de data-analyse met de rapportages van de back-up software en stel vast of deze overeenkomen.

Betrouwbaarheid van rapportages

Computer dependent manual controls maar ook de werkzaamheden van de accountant zelf maken gebruik van rapportages uit het systeem. De vraag is in hoeverre deze rapportages betrouwbaar zijn.

Aan de hand van een risicoanalyse dient bepaald te worden of en welke werkzaamheden er met betrekking tot de rapportages nodig zijn. Hierbij kunnen de volgende aanknopingspunten gelden:

- Hoe zijn de rapportages gegenereerd? Komt de informatie rechtstreeks uit de (financiële) applicatie? Betreft het een standaardapplicatie c.q. -rapportage?
- Indien het een maatwerkrapportage is, kunnen we vaststellen dat deze juist is. Als geen interne tests zijn uitgevoerd is een eigen test noodzakelijk. Is het mogelijk om te steunen op change management procedures voor de rest van het jaar?
- Is de rapportage aan te sluiten met andere informatie? Bijvoorbeeld het totaal van een ouderdomslijst aansluiten met de kolommenbalans, waardoor de juistheid en volledigheid van het saldo op de lijst is vast te stellen. De betrouwbaarheid van de ouderdom van de in de rapportage opgenomen posten wordt hiermee echter niet vastgesteld. Hiervoor zijn dan nog aanvullende werkzaamheden nodig, bijvoorbeeld het herleiden van enkele posten naar de bron.
- Betreft de lijst een (complexe) selectie van data? In dat geval kan het noodzakelijk zijn om de selectiecriteria te beoordelen.

Bijlage 9: Toepassingsmogelijkheden data-analyse per proces

Verkopen

- Confrontatie stambestand verkoopcondities met gefactureerde bedragen
- Aansluiting uitgeleverde orders met gefactureerde orders
- Aansluiting magazijnafgiften met verkoopfacturen
- Aansluiting voltooide verkooporders met verkoopfacturen
- Analyse verkooporders die niet hebben geleid tot verkoopfactuur (reden?)
- Controle doorlopende nummering verkoopfacturen
- Controle periodeafgrenzing door analyse verkopen/inkopen per periode
- Analyse verkoopstatistieken (op artikel of artikelgroep niveau; omzet, prijs, marge, hoeveelheid)
- Beoordeling boekingsgang /aansluiting BTW vanuit kruistabel dagboek /grootboekrekening
- Analyse gemiddelde factureringstermijn (datum levering/datum factuur)
- Analyse facturering door medewerkers i.c.m. competentietabel (wie heeft gefactureerd, bevoegd?)
- Analyse omzet per fee-earner/vrachtwagen/vestiging/productgroep
- Opstellen goederenbeweging (geboekte inkopen per artikel, begin/eindvoorraad; geboekte omzet per artikel; aantallen en/of waardes)
- Selectie verstrekte kortingen; analyse per medewerker, vestiging, debiteur; deelwaarneming op autorisatie
- Analyse controlerende tussenrekeningen (draaitabel, periodeverloop, bijzondere boekingen)
- Genereren van aflooplijst debiteuren (debiteuren 31/12, open per heden)

Productie

- Analyse jobtime/shoptime/projecturen
- Analyse grootboek- of projectkaarten op geboekte kosten en bijzondere boekingen
- Controle op geboekte uurtarieven (opstellen geboekte uurtarieven; vergelijking met geautoriseerde uurtarieven)
- Beoordeling over- of onderdekking aan de hand van geboekte uren per periode
- Inden niet aanwezig: opstellen projectanalyses vanuit grootboek of projectmutaties
- Controle kosten/opbrengsten na verslagperiode op projecten per balansdatum

Personeel

- Controle bankrekeningnummers/NAW stambestand personeel met bankrekeningnummers/NAW crediteurenadministratie
- Totalen uit urenregistratie confronteren met verloning / verloonde overuren
- Opstellen soll positie vast brutoloon vanuit stambestand (geautomatiseerde salaris, in- uit-dienstdatum) met verloond / geboekt vast brutoloon
- Analyse rekening nettoloon (draaitabel dagboek; afloop periode etc; bijzondere boekingen)
- Vanuit verloning Soll positie deelnemers pensioenregeling op peildatum opstellen; confronteren met opgaaf verzekeraar

Inkopen (en voorraden)

- Analyse inkopen per crediteur versus ontvangen korting/bonus per crediteur
- Analyse inkoopbestellingen die niet hebben geleid tot een inkoopfactuur
- Analyse goederenontvangsten die niet hebben geleid tot een inkoopfactuur en vice versa

- Analyse van rekening prijs- en leveringsverschillen (draaitabel dagboeken, bijzondere boekingen, periodeanalyse, verband totale inkopen per periode)
- Analyse van rekening herwaarderingen (draaitabel dagboeken, bijzondere boekingen, periodeanalyse, verband totale inkopen per periode)
- Analyse van voorraadverschillen (draaitabel dagboeken, bijzondere boekingen, periodeanalyse, verband totale inkopen per periode)
- Confrontatie waarderingsprijs in voorraadlijst met stambestand inkoop/waarderingsprijzen
- Confrontatie waarderingsprijs in voorraadlijst met gemiddelde/laatste verkoopprijzen uit facturatiedatabase
- Analyse negatieve aantallen en/of prijzen in voorraadwaardelijst
- Analyse 0-prijzen of 0-waarden in voorraadwaardelijst
- Confrontatie huidige waarderingsprijs met waarderingsprijs vorige periode (verklaring forse afwijkingen)
- Analyse grootboekrekeningen kostprijs/inkopen (draaitabel dagboek, periode, analyse per crediteur)
- Mogelijkheid stratificatie, selectie en recapitulatie voorraadinventarisatie
- Beoordeling overige bedrijfskosten op hoogte, bijzondere dagboeken en periodeverloop
- Inkopen geboekt in nieuwe verslagjaar met betrekking tot huidig verslagjaar (als laatste verkooporder verslagjaar bekend is)

Betalingen en ontvangsten

- Analyse betalingen aan niet-crediteuren door draaitabel dagboek/grootboekrekening
- Totaal betalingen uit telebankieren confronteren met rekeningnummers crediteuren/personeel
- Analyse tussenrekeningen kas, kruisposten via kruistabel (bijzondere dagboeken, bijzondere boekingen, afloop)
- Analyse verloop kas (uitzetten in grafiek: tijdig afstorten, negatieve saldi?)
- Analyse tijdstippen tussen uitboeking kas en opboeking bank/opboeking hoofdkas (sleepgevaar kas)

Automatisering

- Analyse gebruikers per mutatiecategorie in vergelijking met competentietabel/functieprofiel (indien gebruiker ook geregistreerd wordt bij mutaties)
- Bij verschillende systemen: analyse juiste en volledige synchronisatie/doorboeking batches
- Analyse diverse loggingen (indien aanwezig)