# Hoofdstuk 3 BOEK 2 Planning van controle

Planning van controle omvat: - vaststellen algehele controleaanpak

 - ontwikkelen van controleplan om controlerisico te

 reduceren

Een goede planning bevordert de effectiviteit, de verdeling van werk in het controleteam, de begeleiding en het toezicht op de leden en de beoordeling. De aard en de omvang van de planning is afhankelijk van de grootte en complexiteit van de huishouding, de eerdere ervaringen van de accountant en de gewijzigde omstandigheden tijdens de controle.

Planningsproces: 1. Cliënt acceptatie en opdrachtbevestiging

 2. Omgevingsanalyse\*

 3. Verkenning organisatie\*

 4. Signaleren bedrijfsrisico’s

 5. Initiële cijferanalyse

 6. Initiële cijferbeoordeling interne beheersing

 7. Bepaling controletolerantie

 8. Bepalen risico’s van materieel belang

 9. Bepalen controleaanpak

*\*Ad1:* ***Analyse de organisatie*** *kan door de volgende informatie:*

*Inlichtingen werknemers en management, uitvoeren cijferanalyse, waarneming ter plaatse en verificatie, besprekingen voeren met derden betrokkenen (adviseurs, taxateurs), kennisnemen van algemene economische publicaties, raadplegen jaarrekeningen vergelijkbare huishoudingen, raadplegen van documentatiecentra, interne documentatie raadplegen (notulen, managementletters, organisatiestructuren, meerjarenplannen, procedurehandboeken, functie- en taakbeschrijvingen), rapporten tussentijdse controles.*

***Analyse van de omgeving*** *kan door analyse van markt en concurrentie, seizoensgebonden activiteiten, producttechnologie, beschikbaarheid en kosten van energie, regelgevingkader, grondslagen voor administratieve verantwoording en bedrijfstakspecifieke gebruiken, belastingen, invloeden van overheidspolitiek en milieueisen, toestand economie, inflatie, herwaardering, interestpercentages en beschikbaarheid financiering.*

Ook zijn besprekingen binnen het controleteam belangrijk voor het planningsproces:

* Om inzicht te geven in het voorkomen van afwijkingen van materieel belang binnen specifieke controlegebieden waar teamleden voor verantwoordelijk zijn
* Om begrijpelijk te maken op welke wijze uitkomsten invloed hebben op andere onderdelen van de controle en andere controlewerkzaamheden

3) *Verkennen organisatie*: Belangrijk is het verkennen van de organisatie. Er dient duidelijk te zijn welke ***processen*** worden doorlopen, van initiatie van transacties tot en met verantwoording in de jaarrekening. Hiervoor dient inzicht te zijn in investeringen, financieringen, beleggingen, bedrijfsvoering en verslaggeving. Hierbij dient onderscheid te worden gemaakt in primaire en secundaire processen. Van elk proces dient een ***verslaggevingtraject*** in beeld te worden gebracht (van brongegevens tot jaarrekening).

***Primair***: inkoop, productie, verkoop, ontvangen van gelden, betalen crediteuren

***Secundair***: opvragen offertes, nemen inkoopbeslissingen, invoer bestelgegevens en ontvangstgegevens, ontvangen van facturen, vastlegging in grootboek.

Het in beeld brengen van processen is niet alleen relevant voor de risico-inschatting, maar ook voor de planning. Bij het plannen kunnen nauw samenhangende processen namelijk worden samengevoegd in een cyclus, de cycle-approach.

Zie volgende pagina voor een voorbeeld van verbanden tussen transactiecyclussen:



Voor controle op volledigheid van de opbrengstenverantwoording wordt vaak gebruik gemaakt van deze waardekringloop, waarbij dus wordt gesteund op verbanden.

4) *Signaleren bedrijfsrisico’s*: voor risico-inschatting dient de accountant het management te verzoeken om inlichtingen, een cijferanalyse te maken en te observeren en te inspecteren. Hij kan ook eerdere ervaringen gebruiken, maar dient dan eerst vast te stellen welke veranderingen zich hebben voorgedaan.

Hij dient te onderzoeken of de huishouding een ***risico-inschattingsproces*** heeft om bedrijfsrisico’s te onderkennen, deze in te schatten, ze te kunnen voorkomen en of er een proces is om te beslissen om actie te ondernemen die inspeelt op de risico’s.

Risico’s die kunnen leiden tot een ***afwijking van materieel belang*** zijn onder andere ontwikkelingen in de sector, nieuwe producten/diensten, uitbreiding activiteiten, vereisten op grond van regelgeving, gebruik van informatietechnologie, veranderingen in operationele omgeving, nieuw personeel, nieuwe informatiesystemen, snelle groei, nieuwe technologie, herstructurering en toename van buitenlandse activiteiten.

5) *Initiële cijferanalyse*: Dient voor het vaststellen van financiële ontwikkelingen, het verkrijgen van een eerste indruk omtrent de functionering van de interne organisatie, het onderkennen en analyseren van aandachtvragende onderzoeksgebieden, een indruk krijgen omtrent materieel belang en controletolerantie en het vaststellen of er sprake is van dreigende discontinuïteit.

Deze cijferanalyse is ***richtinggevend*** voor de verdere controle en kan ***vergeleken*** worden met andere perioden, verwachte resultaten en branchegegevens. Ook kunnen cijferanalyses gebruikt worden om ***verbanden*** te beoordelen, zoals tussen financiële en relevante niet-financiële informatie (loonkosten en aantal werknemers) en tussen elementen van financiële gegevens waarvan verwacht wordt dat ze aan een voorspelbaar patroon voldoen.

6) *Initiële beoordeling interne beheersing*: doel is inzicht verwerven in interne beheersingsmaatregelen die relevant zijn voor de controle. De opzet en de implementatie dienen geëvalueerd te worden. Interne beheersing kan beoordeeld worden doordat de accountant zelf operationele werkzaamheden uitvoert of inlichtingen vraagt bij werknemers en management. Ook kijkt de accountant naar ervaringen in voorgaande boekjaren.

Er dient geëvalueerd te worden hoe het management een cultuur van eerlijkheid en ethisch gedrag heeft gecreëerd en handhaaft, en of de sterke punten in de interne beheersing samen voldoende basis vormen voor andere componenten van de interne beheersing.

Relevante elementen bij het verwerven van inzicht zijn m.b.t. interne beheersing:

* Participatie van degenen belast met governance
* Opvattingen en werkwijze van management
* Organisatorische structuur
* Communicatie over handhaven integriteit en ethische waarden
* Toewijzen van bevoegdheden en verantwoordelijkheden
* Beleidslijnen en toepassing hiervan

Een sterke beheersomgeving geeft de accountant meer vertrouwen in interne beheersing van de onderneming en beperkt het frauderisico. Ook zijn minder verbeteringen nodig.

7) *Vaststellen van de materialiteit*: De accountant stelt de materialiteit vast met behulp van ***professionele oordeelsvorming***. Hij bepaalt de materialiteit voor de financiële overzichten als ***geheel***, maar als er specifieke omstandigheden zijn bij bijzondere transactiestromen, rekeningsaldi of in financiële overzichten opgenomen toelichtingen, dan kan het materialiteitsniveau ook bepaald worden op dat ***specifieke*** ***gebied***.

Vaak wordt een percentage toegepast op een meetpunt als startpunt bij het vaststelen van de materialiteit. Factoren die zo’n geschikte ***benchmark*** kunnen beïnvloeden omvatten:

* Elementen van financiële overzichten
* De vraag of er speciale aandacht dient te worden besteed aan financiële overzichten
* Aard van entiteit
* Eigendomsstructuur
* Relatieve volatiliteit van de benchmark

Voorbeelden van goede meetpunten/benchmarks zijn winst voor belasting, totale opbrengsten, brutowinst, totale lasten, eigen vermogen en intrinsieke waarde.

De ***uitvoeringsmaterialiteit*** wordt vastgesteld om de kans dat het geheel van niet-gecorrigeerde en niet-ontdekte afwijkingen in de financiële overzichten de materialiteit voor de financiële overzichten als geheel overstijgt, tot een passend laag niveau terug te brengen.

8) *Bepalen van risico’s van materieel belang*: dit dient te gebeuren op het niveau van het ***financieel overzicht*** en op ***niveau van beweringen*** wat betreft transactiestromen, rekeningsaldi en in financiële overzichten opgenomen toelichtingen. De risico’s moeten gedurende het hele controleproces onderkend worden en er moet een inschatting gemaakt worden van de risico’s en evalueren welke invloed ze hebben. Daarna dienen de risico’s gerelateerd te worden aan wat verkeerd kan lopen en moet de waarschijnlijkheid van de afwijking overwogen worden en of dit kan leiden tot een afwijking van materieel belang.

Om te oordelen of een risico een ***significant risico*** is, dient de accountant in aanmerking te nemen: - of het een frauderisico betreft

 - of het risico verband houdt met recente significante ontwikkelingen

 - de complexiteit van de transacties

 - of het risico voortkomt uit significante transacties met verbonden partijen

 - de mate van subjectiviteit bij het waarderen van de financiële informatie in

relatie tot het risico

 - of het risico betrekking heeft op significante transacties buiten de normale

verloop van bedrijfsactiviteiten

Als de accountant heeft bepaald dat er een significant risico bestaat, moeten daar tegenover interne beheersingsactiviteiten staan die op dat risico betrekking hebben en die wellicht verbeterd moeten worden.

Risico’s van afwijkingen van materieel belang worden groter als het ***management*** er direct bij ***betrokken*** is, als er ***handmatig*** wordt ingegrepen in het verzamelen en verwerken van gegevens en als er ***ingewikkelde*** berekeningen of verslaggevingprincipes gelden.

Alle bevindingen met betrekking tot het onderkennen van risico’s moeten in de controledocumentatie worden opgenomen. Het betreft uitkomsten van besprekingen met leden van het opdrachtteam, kernelementen van inzicht, de onderkende en ingeschatte risico’s en de onderkende risico’s en de daarop betrekking hebbende interne beheersingsmaatregelen.

9) *Bepalen controleaanpak*: In het controleplan wordt per post van de jaarrekening aangegeven welke risico’s worden onderkend en hoe de controle zal worden uitgevoerd zodat alle controledoelstellingen worden behaald. Vaak wordt deze aanpak eerst in hoofdlijnen uiteengezet, aangeduid als ***controlestrategie***. Daarna wordt het uitgewerkt in een ***werkprogramma***.

Bij de controles kan controle-informatie worden gebruikt over de werking van de interne beheersingsmaatregelen. Er moet echter rekening worden gehouden met relevantie van toepassing en de ouderdom van de informatie (wanneer moet de maatregel weer opnieuw getest worden?). Relevantie wordt bepaald door te kijken of zich nog belangrijke wijzigingen hebben voorgedaan sinds de laatste controle, indien die er is geweest. Dat kan door inwinnen van inlichtingen, observatie of inspectie. Als zich geen wijzigingen hebben voorgedaan, kan de accountant het ***roulatiebeginsel*** toepassen: minstens één keer per drie controles dienen de interne beheersingsmaatregelen getoetst te worden en bij iedere controle dient in ieder geval een déél van de interne beheersingsmaatregelen getoetst te worden. Hierbij mag een maatregel niet langer dan twee controleperioden ongetoetst blijven.

De accountant dient sowieso ***gegevensgerichte controles*** op te zetten en uit te voeren op transactiestromen, rekeningsaldi en in financiële overzichten opgenomen toelichtingen. Financiële overzichten dienen aangesloten en afgestemd te worden met onderliggende administraties en journaalposten van materieel belang dienen onderzocht te worden. Als de gegevensgerichte controle tussentijds wordt uitgevoerd, moet deze uitgevoerd worden in combinatie met toetsingen van interne beheersingsmaatregelen ven moeten de controles slechts uitgevoerd worden als de accountant bepaalt dat dit voldoende si en er een redelijke basis verschaft wordt voor het doortrekken van zijn controle conclusie.

Een typologie van een onderneming moet bekend zijn voordat wordt aangevangen met de planning van de controle. Zie hieronder welke typologieën er bestaan:

 - handelsonderneming

 - productieonderneming (massa/stuk)

 - agrarische en extractieve bedrijven

 - dienstverlening

 - beschikbaarstelling van ruimten

 - financiële instellingen

 - overige huishoudingen

***Stappen in controleproces tot nu toe:***

1. Opdrachtaanvaarding *haalbaarheidsonderzoek*
2. Voorbereiding controle *bedrijfsverkenning en evaluatie*

*controleomgeving*

1. Bepalen controleaanpak *onderzoek opzet en bestaan AO/IC*
2. Tussentijdse controle *controle werking AO/IC*
3. Afronding controle *evaluatie en rapportage*

# Hoofdstuk 4 BOEK 2 Planning van controle

Volgens het COSO-rapport ‘Internal control-integrated framework’ is ***interne beheersing***:

*‘een proces dat wordt geëffectueerd door directie, management en overig personeel en is ontworpen om een redelijke mate van zekerheid te verkrijgen dat de doelstellingen effectiviteit en efficiency, betrouwbaarheid van informatie, beveiliging van activa en naleving van wet- en regelgeving worden behaald’.*

De kwaliteit van interne beheersing is niet alleen meer belangrijk voor interne belanghebbenden. ***Extern belanghebbenden*** willen in plaats van retrospectieve financiële informatie steeds meer prospectieve financiële en kwalitatieve informatie, zoals over de effectiviteit van de interne beheersing. Hiervoor moet het management de opzet en de goede werking evalueren en beoordelen.

***Doel*** onderzoek interne beheersing: vaststellen op welke punten en op welke wijze bij de accountantscontrole kan worden gebruikgemaakt van de verrichtingen en uitkomsten van de interne beheersing, en ook of deze voldoet aan de minimumeisen om tot een goedkeurende accountantsverklaring te komen.

Men volgt voor de accountantscontrole een ***residubenadering***: men voert een risicoanalyse uit om potentiële fouten te ontdekken en vervolgens stelt de accountant vast of het restant aan potentiële fouten door de accountantscontrole kan worden opgevangen.

****

**COSO-model**:

Door Committee of Sponsoring Organisations (COSO). Is een ***raamwerk*** voor interne beheersing.

Inbegrepen is Enterprise Risk Management (ERM).

***Interne beheersingsmaatregelen***: administratieve procedures en maatregelen die ervoor moeten zorgen dat de richtlijnen van de leiding worden nageleefd om de gestelde doelstellingen te behalen.

*Verschil interne beheersing en externe controle = doelgroep*

Interne beheersing wordt verricht door personen binnen de te controleren huishouding, waarbij de hoogste leiding slechts gedeeltelijk een onderdeel vormt.

Externe controle reikt verder en controleert ook alle activiteiten van de hoogste leiding.

In een intern beheersingssysteem zijn een aantal **inherente** **beperkingen** aanwezig waardoor onzekerheden voer de betrouwbaarheid in het verslaggevingtraject blijven bestaan:

* Kosten van interne beheersingsmaatregelen mogen niet hoger zijn dan het daaruit te verwachten voordeel
* Meeste maatregelen zijn niet gericht op incidentele en niet-routinematige transacties
* Mogelijkheid menselijke fouten (onbewust)
* Mogelijkheid bewust niet toepassen van maatregelen door samenspanning
* Misbruik van bevoegdheden
* Maatregelen niet toereikend of niet nageleefd

Er zijn ook enkele **beperkingen** verbonden aan het **onderzoek** van de accountant:

* Hoe kun je feitelijk vaststellen of de interne beheersing heeft gewerkt? (indien controle heeft geleid tot correcties)
* Werkt de interne beheersing wel constant/voortdurend? (gehele populatie kan nooit onderzocht worden)

***Beoordeling interne beheersing:***

1. Stap 1: Beoordeling opzet interne beheersing
* Afwijkingen van materieel belang effectief voorkomen, ontdekken of herstellen door interne beheersingsmaatregelen
* Interne financiële beheersing met als doel betrouwbaarheid verslaggeving
* Eerst interne *beheersomgeving* checken om te kijken in hoeverre gesteund kan worden op interne beheersing (top-downbenadering: hoofd -> bijzaken)
* In kaart brengen *verslaggevingtraject* (backward flow: externe jaarrekening > correcties > interne jaarrekening > afsluitposten > grootboek > functionele informatiesystemen > brongegevens)
* Inzicht verwerven in *communicatie* (extern, management, governance)
* In beeld brengen functionele *informatiesystemen* die de verschillende transactiestromen en processen ondersteunen (m.b.v. output-inputschema’s, uitgebreid met een schema voor invoer-, verwerkings- en uitvoercontroles)
* Inzicht verwerven in interne *beheersingsactiviteiten* relevant voor controle, bijvoorbeeld met betrekking tot autorisatie, prestatiebeoordelingen, informatieverwerking, fysieke maatregelen en functiescheiding. Om te bepalen welke activiteiten hij gaat toetsen, kan hij een *controlecompetentiematrix* maken, waarin controledoelstellingen, risico’s en maatregelen met elkaar in verband kunnen worden gebracht. Categoriseer hierbij de maatregelen in *preventief, signalerend en repressief*.
* Beoordelen maatregelen voor het *monitoren* van de interne beheersing
* Indien aanwezig: analyseren interne *auditfunctie* (indien meer gericht op financial audit dan operationele audit, kan er gebruik van worden gemaakt voor de controle)
1. Vaststellen bestaan interne beheersingsmaatregelen
* Te controleren door verrichten proceduretests
* Bijvoorbeeld *lijncontrole*: bedrijfstransactie kiezen en nagaan of alle daaruit voortvloeiende bedrijfshandelingen in overeenstemming met de bedrijfsbeschrijving zijn verricht (ook wel cradle tot grave test of walk through test)
* Één lijncontrole per proces/cycle volstaat meestal
1. Vaststellen effectieve werking interne beheersingsmaatregelen
* Door *systeemgerichte werkzaamheden*: onderzoek van documenten, informeren naar en waarnemen van maatregelen die niet leiden tot vastleggingen en opnieuw uitvoeren van maatregelen
* Beoordeling op welke wijze maatregelen zijn uitgevoerd, consistente toepassing en door welke personen. Over afwijkingen wordt navraag gedaan.
* Indien nodig: *geautomatiseerde controletechnieken* toepassen (bestandsonderzoek, testgevallen)
* *Cijferanalyse*
* *Dual purpose tests*: het bewust combineren van gegevensgerichte en systeemgerichte controlehandelingen

***Betekenis van automatisering in het kader van interne beheersing:***

Geautomatiseerde gegevensverwerking zorgt voor *effectiviteit* en *doelmatigheid*, maar brengt ook risico’s met zich mee:

* Onnauwkeurigheid
* Ongeautoriseerde toegang tot gegevens (vernietiging of foutieve wijzigingen)
* Doorbreking functiescheiding
* Ongeautoriseerde wijzigingen in gegevens, systemen of programma’s
* Nalaten van noodzakelijke aanpassingen systemen/programma’s
* Ongepast handmatig ingrijpen
* Verlies gegevens

De geautomatiseerde gegevensverwerking moet dus *betrouwbaar* zijn, wat wil zeggen dat de informatie exclusief, integer en controleerbaar moet zijn. Daarnaast moet een dergelijk geautomatiseerd systeem *continu* zijn.

Onderscheid win beheersingsmaatregelen ten aanzien van geautomatiseerde systemen zijn:

* **General controls (algemeen)**

Indien er grote gebreken zitten in de general controls, kan de accountant ook niet steunen op de application controls. Daarom dient de kwaliteit van de general controls al in een vroeg stadium beoordeeld te worden. Hierbij kijkt men naar de organisatorische plaats van de afdeling automatisering, de gebruikte apparatuur en programmatuur, de taakverdeling, fysieke en logische toegangsbeveiliging\*, change management en problem management\*\*, testprocedures en continuïteitsaspecten.

* **Application controls (specifiek)**

Zijn geprogrammeerde beheersingsmaatregelen.

Onderscheid tussen

* geautomatiseerde en gebruikerscontroles. (vb = signalering overschrijding kredietlimiet)
* gebruikerscontrole (vb =beoordeling van deze overschrijding of de order al dan niet wordt uitgevoerd)

Ook onderscheid tussen:

* invoercontroles (autorisatie, volledigheid invoer, validatie gegevens)
* verwerkingscontroles (redelijkheid, volledigheid, volgorde, rekenkundige juistheid)
* uitvoercontroles (afwijking controletotalen, afwijkende marges, verlopen vorderingen)

\* ***logische toegangsbeveiliging*** is toegang tot programmatuur, data beschermen tegen ongeautoriseerde personen, ***fysiek*** is server in aparte serverruimte e.d.

\*\* ***change management*** is het evalueren, plannen en coördineren van de implementatie en wijzigingen in apparatuur, software en toepassingen, ***problem management*** is coördineren en stroomlijnen van probleemmeldingen, -toewijzingen en –afhandelingen.

***IT-auditors*** vormen samen een ***auditteam*** om de opzet, het bestaan en de werking van de interne beheersing in een geautomatiseerde omgeving te beoordelen. Tenminste elk jaar worden de general controles beoordeeld, dit heet ***technical audit***. Daarnaast worden ***system*** ***audits*** uitgevoerd op nieuwe of grondig herziene geautomatiseerde toepassingen om na te gaan welke application controls werkzaam zijn.

***Auditing through the computer***: bij de controle van de jaarrekening steunt men in belangrijke mate op de goede werking van de general controls en de application controls in de geautomatiseerde omgeving (goede invoer + goed proces = goede uitvoer).

Binnen een kleine organisatie is een automatiseringsomgeving meer een netwerk van computers met standaardsoftware en IT-expertise in beperkte mate. Hierbij kan voor de controle van de jaarrekening niet op de interne beheersingsmaatregelen worden gesteund.

Toch dient de accountant ook hier onderzoek te verrichten naar de opzet van geautomatiseerde systemen, maar dan in het kader van de risicoanalyse.

***Auditing around the computer***: indien in voldoende mate bronbescheiden en controleerbare vastleggingen binnen en buiten de geautomatiseerde systemen beschikbaar zijn kunnen deze gebruikt worden voor gegevensgerichte controlehandelingen zoals verificatie.

Indien automatisering **uitbesteed** wordt, kan de accountant er niet van uitgaan dat de interne beheersing adequaat is geregeld. Hij dient de risico’s in te schatten op basis van:

* aard van de verleende diensten
* aard en materialiteit van de verwerkte transacties/rekeningen
* mate waarin internactie bestaat tussen serviceorganisatie en gebruikende entiteit
* aard van relaties tussen serviceorganisatie en gebruikende entiteit

*Informatiebronnen hiervoor zijn service level agreements, gebruikshandleidingen, overzichten van systemen, rapportages van de serviceorganisatie over interne beheersingsmaatregelen en rapportages van andere accountants.*

**Communicatie over tekortkomingen interne beheersing:**

Significante tekortkomingen dienen tijdig en schriftelijk ingediend te worden bij degenen die belast zijn met governance. Ook moet dit met het management gecommuniceerd worden.

*Indicatoren voor significante afwijkingen zijn:*

* informatie die duidt op ineffectieve aspecten van interne beheersing, zoals grote transacties waarbij management een financieel belang heeft
* afwezig zijn van een risico-inschattingsproces binnen de entiteit
* informatie die duidt op een ineffectief risico-inschattingsproces
* ineffectief inspelen op onderkende significante risico’s door management
* aanpassen van eerder uitgebrachte financiële overzichten (correctie fouten)
* informatie die onvermogen van overzicht houden door management aantoont