De invloed van automatisering op AO/IC

Aanreiking van een internecontrolebegrippenkader voor geautomatiseerde bedrijfsprocessen

Drs. A.R.J. Basten RE

De Sarbanes Oxley-wetgeving en de Code Tabaksblat vragen om een diepgaander onderzoek naar de internecontrolemaatregelen. Als gevolg van deze wetgeving zal het management de effectiviteit van zijn internal-control-systeem grondig moeten toetsen en vervolgens dient de accountant ook vast te stellen dat dit systeem voldoende heeft gewerkt. In dit artikel wordt de invloed van automatisering op de internecontrolemaatregelen besproken en worden de verschillende soorten internecontrolemaatregelen aangereikt. Op basis van dit internecontrolebegrippenkader kan beter worden beoordeeld of voldoende internecontrolemaatregelen zijn getroffen binnen geautomatiseerde processen.

Inleiding

Interne controle komt de laatste jaren steeds meer in de belangstelling te staan door allerlei boekhoudschandalen en faillissementen. Interne controle heeft als doel om tijdig onvolkomenheden op te sporen en te corrigeren in de uitoefening van bedrijfsactiviteiten, alsmede het scheppen van de mogelijkheid om zo nodig nieuwe maatregelen te treffen teneinde te voorkomen dat de gesignaleerde onvolkomenheden in de toekomst weer optreden ([Star94]).

Ook internal control (a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable laws and regulations ([COSO94])) krijgt wereldwijd meer aandacht. In de literatuur is veel geschreven over de verschillen en overeenkomsten tussen deze twee begrippen. Beide begrippen hebben veel raakvlakken met elkaar; een verschil is dat interne controle zich meer richt op het controleren (van processen), en internal control meer op beheersen (van processen). Ten slotte staat ook riskmanagement weer in het spotlight, dat een duidelijke relatie heeft met interne controle en internal control.

Deze boekhoudschandalen in de toekomst zoveel mogelijk voorkomen is het doel van de Sarbanes Oxley-wet. Een onderdeel van deze wet verlangt van het management dat het de kwaliteit van het internal-controlsysteem beoordeelt en daarover schriftelijk verantwoording aflegt. Hierdoor staan deze onderwerpen weer op de agenda van management, directie en Raad van Commissarissen. Daarbij verlangt deze wet ook dat de con-

Drs. A.R.J. Basten RE
is werkzaam als ICT-auditor bij KPMG Information Risk Management. Hij heeft ruime ervaring met het reviewen van IT-beheerprocessen en het beoordelen van applicatieve toepassingen/processen binnen de financiële dienstverlening. Tevens maakt hij deel uit van de redactie van het informatiekundig magazine .ego. Daarnaast is hij als docent betrokken bij de Hogeschool Markus Verbeek te Amsterdam.

basten.fons@kpmg.nl

trolerend accountant deze verklaringen van het management beoordeelt en hierover een verklaring afgeeft, waardoor deze onderwerpen ook bij de accountantsbureaus op de agenda staan. Enkel de organisaties die aan de Amerikaanse beurs zijn genoteerd moeten aan de SOX-wetgeving voldoen. Echter, beursgenoteerde organisaties in Nederland en overheidsorganisaties ontspringen de dans niet. De wet voor behoorlijk bestuur (Code Tabaksblat) schrijft voor dat het bestuur verklaart dat de interne risicobeheersings- en controlesystemen adequaat en effectief zijn en dat het bestuur hierover een duidelijke onderbouwing geeft. Tevens dient het bestuur te rapporteren in het jaarverslag over de werking van het interne risicobeheersings- en controlesysteem.

In de reguliere jaarrekeningcontroleaanpak wordt het internecontrolesysteem meestal geanalyseerd door de interne en externe auditors en worden bevindingen hieromtrent gerapporteerd aan het management. Het onderzoek van de externe accountant naar interne beheersingsmaatregelen is beperkt en heeft niet de diepgang om daarover een afzonderlijke verklaring te kunnen afleggen ([Kuijk03]). De Sarbanes Oxley-wetgeving vraagt om een diepgaander onderzoek van het internal-controlsysteem. Als gevolg van deze wetgeving zal het management de effectiviteit van zijn internal-controlsysteem diepgaander moeten gaan toetsen en vervolgens dient de accountant ook vast te stellen dat dit systeem voldoende heeft gewerkt.

Tegenwoordig wordt een groot deel van de transacties vastgelegd in applicaties en worden allerlei rapportages met behulp van applicaties gegenereerd. Hierdoor is ook een groot deel van de interne controle (maatregelen) opgenomen in de applicaties, ofwel de internecontrolemaatregelen zijn geautomatiseerd. Een voorbeeld hiervan is een schriftelijke paraaf, die is geautomatiseerd naar een akkoordbevestiging in een applicatie. Tevens is door de introductie van automatisering op de werkplek een aantal nieuwe risico's ontstaan, waardoor nieuwe aanvullende internecontrolemaatregelen zijn benodigd. Een voorbeeld van een nieuw risico zijn gebruikers van applicaties en/of het netwerk met vergaande autorisatie, zogenaamde privileged gebruikers. In het (verre) verleden waren deze risico's niet aanwezig.

Kortom, door de introductie van applicaties is bij organisaties de set van internecontrolemaatregelen veranderd en zijn tevens aanvullende internecontrolemaatregelen benodigd als compensatie van de introductie van nieuwe risico's. Deze consequenties van automatisering voor de interne controle zijn niet nieuw, echter in veel artikelen wordt het onderscheid tussen voor en na de introductie van applicaties niet gemaakt.

Wel zijn al vele andere statements gemaakt aangaande de consequentie van de introductie van automatisering voor de interne controle. Indien de interne controle minder goed functioneert, dan moet de interne of externe controleur meer doen. Maar dat kan niet per definitie bij onvervangbare interne controles ([Blok01]). Door automatisering zijn vaak ook onvervangbare interne controles ontstaan. Overigens is deze materie zeker niet echt nieuw; Neisingh beschrijft tien jaar geleden al een eenvoudige, maar duidelijke casus waarbij een direct verband tussen de invoer en uitvoer van gegevens ontbreekt, waardoor niet meer kan worden gesteund op traditionele internecontrolemaatregelen. Indien zekerheid moet worden verkregen over de betrouwbaarheid van de uitvoer, moet de kwaliteit van de programmatuur en de integriteit van de bestanden worden vastgesteld ([Neis94]). Koedijk beschrijft in haar artikel de integratie van ICT in de jaarrekeningcontrole, en daarmee impliciet binnen de Administratieve Organisatie en Interne Controle (AO/IC) ([Koed01]). Neisingh stelt zelfs de ongedeelde verantwoordelijkheid van de RA ter discussie ([Neis01]). Jonker geeft zijn visie op de samenwerking financial auditor en EDP-auditor en Boer richt zich op ICT-aspecten bij routinematige transactieverwerking ([Jonk00] en [Boer98]). Echter, een overzicht van de verschillende soorten administratieve organisatie- en internecontrolemaatregelen die aanwezig kunnen zijn in een organisatie waarbij automatisering een belangrijke rol speelt, wordt niet uitgeschreven. Tevens zijn de onderlinge verbanden tussen de internecontrolemaatregelen vaak onduidelijk. In dit artikel wordt de invloed van automatisering op de internecontrolemaatregelen besproken en worden de verschillende soorten internecontrolemaatregelen aangereikt. Op basis van dit internecontrolebegrippenkader kan beter worden beoordeeld of voldoende internecontrolemaatregelen zijn getroffen binnen geautomatiseerde processen.

De voordelen van interne controle

Door nieuwe wetgeving en regelgeving staat internal control weer op de agenda van het management. Dit is niet alleen vanwege de boekhoudschandalen, maar ook doordat het management zich bewuster wordt van het effect van het aandacht besteden aan deze onderwerpen en de vruchten die interne controle afwerpt. Organisaties die al geruime tijd energie steken in het verder verbeteren van hun internecontrolestelsel, merken dat het management beter wordt geïnformeerd en ook beter kan sturen. Hierdoor verkrijgt de organisatie een professionelere besturing. Dit is geïllustreerd in figuur 1.
Voor een toelichting op de verschillende stages wordt verwezen naar [Gove03].

De set van controlemaatregelen

AO/IC vormen gezamenlijk het beheersingskader van een organisatie. Over beide onderwerpen zijn al vele artikelen en boeken verschenen (zie bijvoorbeeld [Jans93] en [Star94]). Administratieve organisatie kan worden

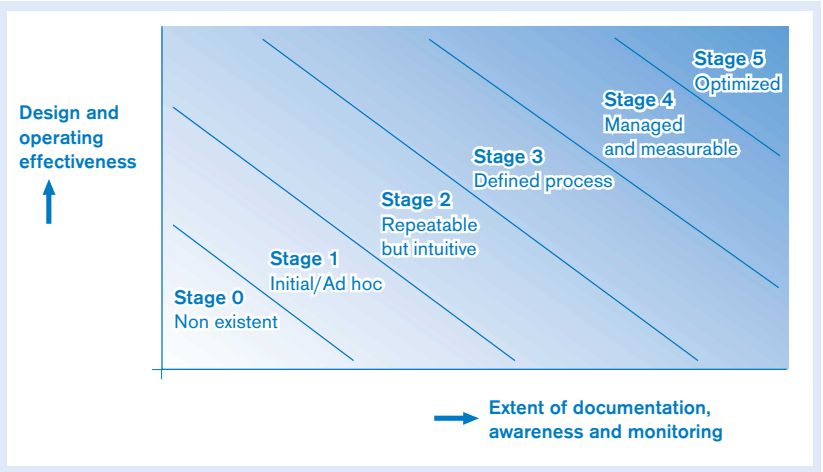
onderverdeeld naar de volgende aandachtsgebieden:
- beleid en strategie;
- procesbeschrijvingen, procedures en werkinstructies.

Interne controle (maatregelen) wordt in de literatuur vaak onderverdeeld naar organisatorische en applicatieve maatregelen. Internecontrolemaatregelen kunnen namelijk zowel in de organisatie worden belegd (bijvoorbeeld procedures, werkinstructies) als worden opgenomen in de applicaties (bijvoorbeeld applicatieve controles en autorisaties). Er is een duidelijke trend waarneembaar dat steeds meer controlemaatregelen in applicaties worden opgenomen.

Uit de dagelijkse praktijk blijkt echter dat de controlemaatregelen niet altijd expliciet worden onderverdeeld naar organisatorische en applicatieve maatregelen, waardoor onvoldoende duidelijk is wat de impact c.q. het belang is van applicaties bij het beheersingskader van een organisatie. Door dit onderscheid inzichtelijk te maken, kan beter het belang of de impact van de applicatie en de opgenomen controlemaatregelen worden ingeschat op de controleomgeving. Tevens is aangegeven of de maatregel preventief (P) of repressief (R) is. Op basis van de literatuur en de dagelijkse praktijk is de volgende verdeling totstandgekomen:

Organisatorische internecontrolemaatregelen
- Organisatorische (controletechnische) functiescheiding (P).
- Handmatige fiattering/parafering (secundaire functiescheiding) (P).
- Gebruikerscontrole (steekproef, totaalcontrole, detailcontrole, verbandscontrole, etc.), eventueel gebaseerd op een rapportage (R).
- Fysieke toegangsbeveiliging (P).

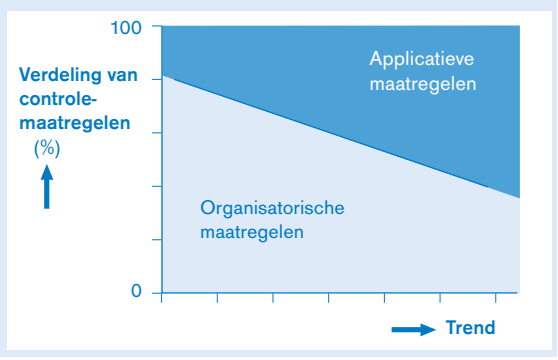
Applicatieve internecontrolemaatregelen
- Applicatieve (controletechnische) functiescheiding (P).
- Applicatieve fiattering/parafering (secundaire functiescheiding) (P).
- Applicatieve controlemaatregelen (P), bijvoorbeeld:
  - formaatcontrole (datum, elfproef, etc.),
  - verbandscontrole (journaalpost in evenwicht),
  - voorgedefinieerde waarden,
  - verplichte invoer,
  - limietcontroles (maximumbedrag of -aantal),
  - automatische nummering.
- Rapportages en verslagen (R), bijvoorbeeld:
  - verbandscontroles,
  - uitzonderlingslijsten,
  - verwerkingsverslagen (interfaces),
  - mutatieverslagen.
- Logische toegangsbeveiliging (applicaties) (P).
- Systeemconfiguratie/account mapping controls (P).
- Logging van gebruikersactiviteiten (R).



Figuur 1. Stages of Control Reliability.

Door deze verdeling te hanteren kan duidelijker worden beschreven welke soorten controlemaatregelen aanwezig zijn binnen een proces. Zoals ook figuur 2 aangeeft, is vaak alleen een combinatie van organisatorische en applicatieve maatregelen voldoende om de bijbehorende risico's te mitigeren. Denk bijvoorbeeld aan logische toegangsbeveiliging en applicatieve controles bij het aanpassen van premietabellen en het vervolgens controleren door een andere medewerker van de wijzigingen op basis van een mutatieverslag. Bij het gebruik van rapportages/verslagen voor controledoeleinden zijn twee verschillende internecontrolemaatregelen van belang. Enerzijds moet worden vastgesteld of de rapportage volledig en juist is en anderzijds moet er een adequate gebruikerscontrole (en moeten er eventuele vervolgacties) op deze rapportage zijn.

Als een duidelijke indeling wordt gehanteerd voor wat betreft internecontrolemaatregelen kan vervolgens ook worden geanalyseerd of het niet beter is om andere maatregelen te treffen die effectiever zijn. Een ander voordeel is dat duidelijker kan worden vastgesteld op welke wijze dient te worden getoetst of deze controlemaatregel effectief is. Dit wordt met een voorbeeld geïllustreerd. Bij een schade-uitkering hoger dan € 10.000 moet een fiat worden gegeven door het hoofd schadebehandeling. Dan moet worden geanalyseerd of



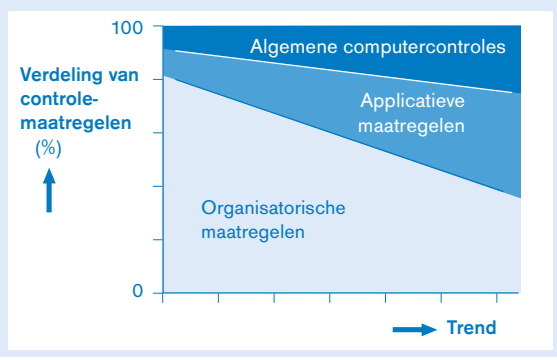
Figuur 2. Verhouding organisatorische en applicatieve interne-controlemaatregelen.

dit een organisatorisch fiat (door het zetten van een paraaf) of een applicatief fiat (afgedwongen door de applicatie) is. De applicatieve variant moet op een andere manier worden getoetst dan de organisatorische. De applicatieve variant draagt in de meeste gevallen meer controlezekerheid bij dan de organisatorische variant.

Figuur 2 geeft ook duidelijk aan dat er altijd organisatorische interne maatregelen aanwezig zullen (moeten) zijn. Een proces kan dus nooit volkomen worden beheerst door applicatieve interne maatregelen. Mede door dit feit kan ook niet worden geconcludeerd dat een proces 'in control' is, als je alleen de applicatie hebt beoordeeld. De conclusie dat een applicatie betrouwbaar is c.q. dat de applicatieve internecontrolemaatregelen effectief zijn, zegt dus niet zoveel. Het gaat om de combinatie van de applicatieve en organisatorische internecontrolemaatregelen. Andersom geldt dit in sommige gevallen niet. Niet-effectieve applicatieve internecontrolemaatregelen plus voldoende compenserende organisatorische internecontrolemaatregelen kan leiden tot een beheerst proces. Echter, vaak is een gedeelte van de applicatieve controlemaatregelen onvervangbaar (door organisatorische interne maatregelen), waardoor je dus geen oordeel over het proces kunt geven zonder de applicatieve internecontrolemaatregelen te onderzoeken.

Door deze onderverdeling van controlemaatregelen kan ook het belang van de algemene computercontroles worden bepaald. Indien veel gebruik wordt gemaakt van c.q. in grote mate wordt gesteund op interne applicatieve maatregelen, dan wordt de kwaliteit van de algemene computercontroles meer van belang. Figuur 3 geeft het toenemend belang van algemene computercontroles grafisch weer.

Kortom, het toetsen van applicatieve internecontrolemaatregelen kan niet zonder het toetsen van de algemene computercontroles; echter het gehele speelveld van algemene computercontroles hoeft niet te zijn getoetst om een oordeel te kunnen geven over de betrouwbaarheid van een applicatieve internecontrolemaatregel.



Figuur 3. Verhouding organisatorische en applicatieve interne-controlemaatregelen en algemene computer-controles.

Applicatieve internecontrolemaatregelen vormen een onderdeel van de applicatie, zodat het toetsen van een applicatieve maatregel kan worden beschouwd als het toetsen van functionaliteit van een applicatie. De wijze waarop een organisatie haar testactiviteiten en change management heeft georganiseerd, is van primair belang om de betrouwbaarheid te kunnen vaststellen van bijvoorbeeld een complexe berekening, een rapportage of een geprogrammeerde controle. Dus indien bijvoorbeeld applicatieve controles of rapportages van belang zijn is het noodzakelijk om het change management van deze maatregelen expliciet te beoordelen. Echter, indien het testtraject onvoldoende betrouwbaar (of gedocumenteerd) is, mag niet per definitie worden geconcludeerd dat de applicatieve controlemaatregelen onbetrouwbaar zijn. De beoordelaar dient dan zelf testwerkzaamheden te verrichten. Het testen van een geprogrammeerde controle of een applicatieve fiattering kan in beperkte tijd plaatsvinden. Het testen van de volledigheid en juistheid van een uitzonderingsrapportage of complexe berekening zal een grotere inspanning vereisen. Echter, het identificeren van niet voldoende geteste kritieke applicatieve internecontrolemaatregelen zou reden moeten zijn voor iedere organisatie om onduidelijkheid over de kwaliteit van deze controlemaatregelen weg te nemen. Binnen de huidige regel- en wetgeving kan een organisatie dit soort lacunes niet meer afdoen als te duur of onnodig.

Het spreekt voor zich dat indien applicatieve functiescheiding en logische toegangsbeveiliging van belang zijn, dat dan autorisatiebeheer ook dient te worden beoordeeld. Op basis van deze argumentatie kunnen de reeds gedefinieerde applicatieve interne maatregelen worden gerelateerd aan de belangrijkste algemene computercontroles. Dit is nader uitgewerkt in tabel 1.

Op basis van deze analyse kan worden gesteld dat autorisatiebeheer en change management de belangrijkste algemene computercontroles vormen bij het vaststellen of een applicatieve internecontrolemaatregel voldoende betrouwbaar is. Vanwege de hoge mate van zekerheid die benodigd is, aangaande het adequaat functioneren van de applicatieve internecontrolemaatregelen, wordt verondersteld dat het testmanagement een integraal en een belangrijk onderdeel vormt van het change-managementproces.

ICT-risico's

Door de introductie en het gebruik van applicaties zijn ook nieuwe ICT-risico's ontstaan, die ook moeten worden gemitigeerd. Doordat dit nieuwe aanvullende risico's zijn binnen een organisatie moet ook een aanvullende set van internecontrolemaatregelen worden gedefinieerd. Het belangrijkste ICT-risico is dat gegevens ongeautoriseerd worden aangepast. Hiermee wordt bedoeld dat niet via de reguliere weg gegevens worden gemuteerd, maar rechtstreeks in de database. Vaak zijn

Applicatieve maatregel	Algemene computercontrole
Applicatieve functiescheiding	Autorisatiebeheer
Applicatieve fiattering/parafering	Autorisatiebeheer & Change management (incl. Testen)
Applicatieve controles	Change management (incl. Testen)
Rapportages en verslagen	Change management (incl. Testen)
Logische toegangsbeveiliging (applicaties)	Autorisatiebeheer
Systeemconfiguratie/account mapping controls	Change management (incl. Testen)
Logging	Change management (incl. Testen)

Tabel 1. Relatering van applicatieve maatregelen aan algemene computercontroles.

applicatiebeheerders, maar ook Operating System (OS)- en databasebeheerders, in staat gegevens rechtstreeks te muteren. Indien het autorisatiebeheer niet goed is ingericht, doet zich soms ook de situatie voor dat reguliere gebruikers in staat zijn gegevens in de database te muteren. Het spreekt voor zich dat zoveel mogelijk voorkomen moet worden dat deze medewerkers in staat zijn bedrijfsinformatie te muteren, zonder dat de reguliere interne controle dit preventief voorkomt of repressief detecteert. Hierbij moet ook worden gedacht aan systeem- en/of applicatiebeheerders van softwareleveranciers, die onderhoud plegen op de applicaties van hun klanten. Hetzelfde risico is aanwezig bij het toestaan aan medewerkers om queries te draaien met mutatierechten. Kortom, het op deze wijze muteren van gegevens wordt niet voorkomen door de hiervoor besproken internecontrolemaatregelen. Indien gedetailleerde gebruikerscontroles worden uitgevoerd en/of specifieke rapportages worden gegenereerd, dan kunnen de mutaties aan het licht komen.

Ook een dataconversie van een oude applicatie naar een nieuwe applicatie vormt een nieuw ICT-risico, omdat de reguliere set van internecontrolemaatregelen de conversierisico's niet afdekt. Vaak worden in conversietrajecten gegevens verrijkt en/of worden gegevens aangepast, zodat ze opgenomen kunnen worden in de nieuwe applicatie. Hierbij ontstaat het gevaar dat gegevens ongeautoriseerd worden gemuteerd en/of dat de gegevens niet volledig worden geconverteerd.

Samengevat moeten, naast de reguliere internecontrolemaatregelen, de volgende internecontrolemaatregelen ten aanzien van de ICT worden getroffen:
- logische toegangsbeveiliging/OS en DB-maatregelen:
  - high-privileged gebruikers,
  - medewerkers,
  - derden;
- controleverslagen betreffende de dataconversie.

Indien de applicatieve maatregelen en de aanvullende op de ICT gerichte internecontrolemaatregelen een belangrijk onderdeel zijn van de totale set van internecontrolemaatregelen, dan wordt tevens van belang dat binnen de ICT-afdeling ook de administratieve organisatie is beschreven, net zoals bij de bedrijfsprocessen. De diepgang en reikwijdte van deze beschrijving moet echter in relatie staan tot de bedrijfsbrede AO-beschrijving. Indien binnen een organisatie sprake is van een beperkte AO-beschrijving, kan niet van een ICT-organisatie worden verwacht dat zij beschikt over een diepgaande AO-beschrijving.

Een AO-beschrijving van een ICT-afdeling omvat de volgende aandachtsgebieden:
- ICT-beleid en ICT-strategie;
- ICT-procesbeschrijvingen, procedures en werkinstructies.

Continuïteit

Dit artikel is tot zover gericht geweest op de waarborging van de betrouwbaarheid van de gegevens binnen een organisatie. De continuïteit van de bedrijfsprocessen en applicaties is ook een belangrijk aandachtsgebied, maar wordt in dit artikel niet uitgebreid behandeld. Onafhankelijk van het belang van applicaties en applicatieve internecontrolemaatregelen dient een organisatie een Business Continuity Plan (BCP) op te stellen. Naarmate de impact van applicaties groter wordt, wordt de afhankelijkheid hiervan in de bedrijfsprocessen ook groter. Op basis hiervan zal meer aandacht moeten worden besteed aan de ICT-hoofdstukken van het BCP, bijvoorbeeld back-ups en ICT-uitwijklocatie.

Het BCP is alleen van belang indien er zich een calamiteit voordoet. ICT kan ook in het algemeen van groot belang zijn binnen het goed kunnen functioneren van bedrijfsprocessen. Vormt de kwaliteit van de applicaties in het algemeen een continuïteitsrisico, dan worden de volgende aandachtsgebieden meer van belang:
- computer operations;
- incident management;
- system development en maintenance.

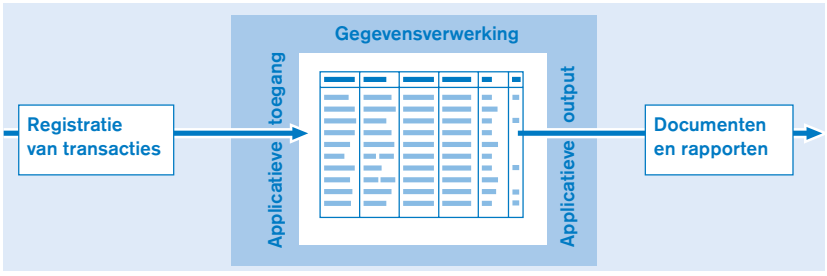
Samenstelling van het internecontrolesysteem

Door de introductie van applicaties wordt de kracht van het internecontrolesysteem bepaald door de samenhang van de organisatorische, applicatieve en op de ICT gerichte internecontrolemaatregelen, de algemene computercontroles en de continuïteitsmaatregelen. Binnen geautomatiseerde processen dienen deze vijf deelgebie-

den te worden onderzocht om tot een goed inzicht te komen van de mate waarin de risico's worden beheerst door internecontrolemaatregelen.

Totaaloverzicht

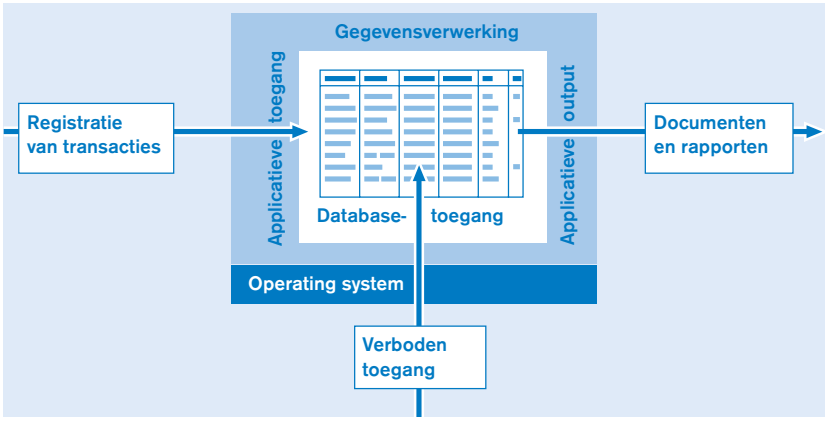
In de voorgaande paragrafen is het stelsel van internecontrolemaatregelen gedefinieerd en zijn enkele onderlinge verbanden aangegeven. Zoals gesteld is het van belang dat de totale set van internecontrolemaatregelen wordt geanalyseerd, omdat de totale set bepaalt of een proces wel of niet 'in control' is. Voor een goede begripsvorming en het verkrijgen van een totaaloverzicht wordt door middel van een grafische weergave een relatie gelegd tussen de verschillende soorten internecontrolemaatregelen. Gestart wordt in figuur 4 met het weergeven van een database en de reguliere applicatieve toegang hiertoe voor het registreren van transacties. Daar kunnen de gegevensverwerking en de applicatieve output (documenten en rapportages) aan worden toegevoegd. Dit is de basis van het registreren van gegevens en het verkrijgen van documenten en rapportages. In deze situatie is geen enkele AO/IC aanwezig.



Figuur 4. Registratie van gegevens zonder AO/IC.

Zoals reeds beschreven ontstaan door het gebruik van een applicatie nieuwe aanvullende risico's. Dit houdt in het muteren van gegevens via de niet-reguliere wijze. Deze elementen zijn toegevoegd aan figuur 4, hetgeen leidt tot figuur 5.

Figuur 5. Registratie van gegevens zonder AO/IC, met ICT-risico's.



Door het implementeren van preventieve maatregelen bij de registratie van gegevens (applicatieve toegang) en het implementeren van repressieve maatregelen bij de applicatieve output worden de operationele internecontrolemaatregelen toegevoegd. Deze preventieve en repressieve internecontrolemaatregelen komen overeen met de eerder behandelde applicatieve en organisatorische internecontrolemaatregelen. Door ook het automatiseringsgebied aan te geven, kunnen op grafische wijze zowel de organisatorische als de applicatieve maatregelen worden toegevoegd (zie figuur 6).

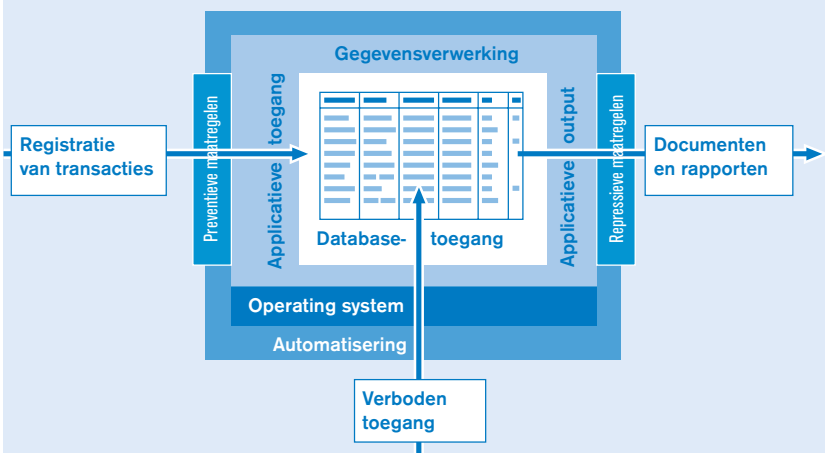
Door de omvang van de applicatieve internecontrolemaatregelen is het van belang dat ook de algemene computercontroles worden opgenomen. In figuur 7 zijn dan ook change en testmanagement en autorisatiebeheer toegevoegd als belangrijkste algemene computercontroles.

Ten slotte kunnen de AO-aandachtsgebieden worden toegevoegd, zowel de organisatorische (beleid en strategie, procesbeschrijvingen en procedures) als de ICT-aandachtsgebieden (IT-beleid en IT-strategie, IT-procesbeschrijvingen en IT-procedures).

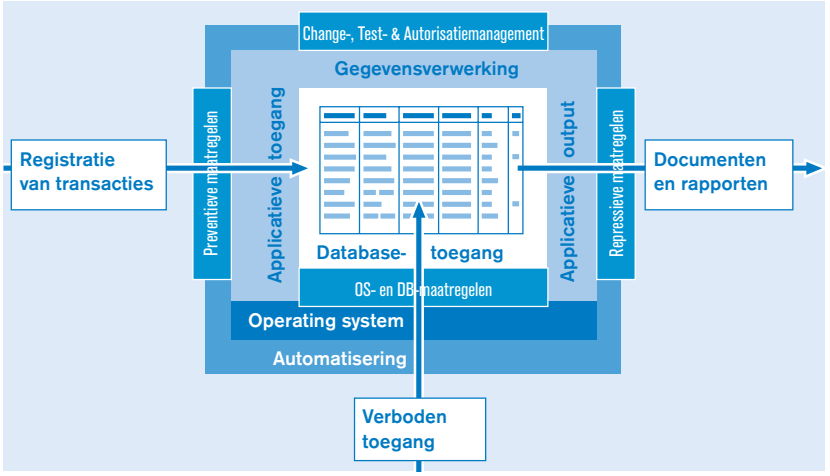
Figuur 8 geeft een overzicht van alle soorten internecontrolemaatregelen en administratieve organisatie die aanwezig kunnen zijn binnen een organisatie, waarbij automatisering een rol speelt. De elementen zijn gericht op de betrouwbaarheid van de gegevensverwerking, desgewenst kunnen de elementen voor continuïteit worden toegevoegd.

Resumé

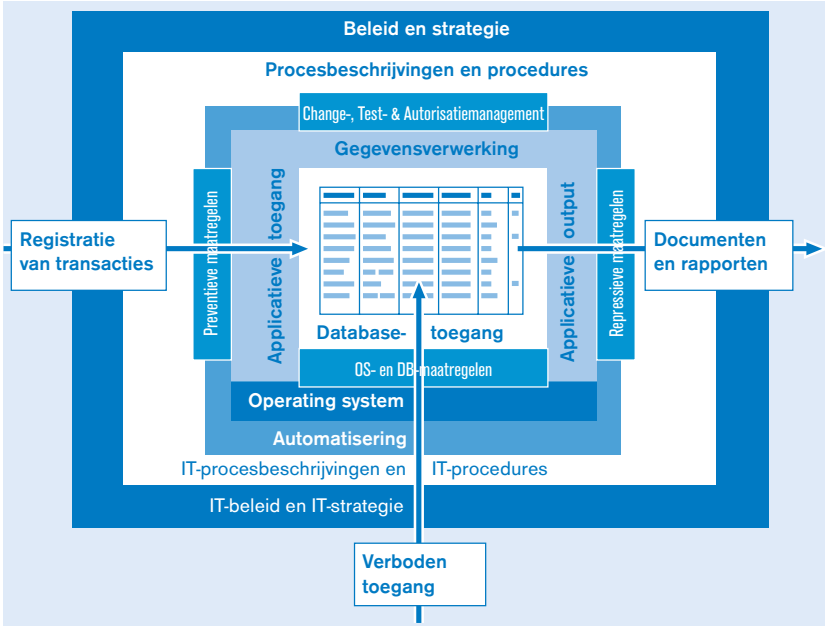
De waarde van de oude toetsingsmethodieken is qua effectiviteit gedaald, omdat de inrichting van de applicaties steeds belangrijker wordt ten opzichte van de inrichting van de organisatie. Natuurlijk moeten de traditionele beoordelingswerkzaamheden niet geheel komen te vervallen, maar vergeleken met voorheen moeten nu meer additionele beoordelingswerkzaamheden worden uitgevoerd. Bij geautomatiseerde bedrijfsprocessen kan worden gesteld dat de beoordeling van de autorisatie-instellingen belangrijker is dan de beoordeling van organisatorische maatregelen. Kortom, bij geautomatiseerde bedrijfsprocessen blijken organisatiediagrammen, taakbeschrijvingen, werkinstructies, etc. van minder betekenis te worden omdat de autorisatiematrix bepaalt of een medewerker wel of geen toegang heeft tot informatie en of deze medewerker ook informatie kan/mag muteren en/of verwijderen.



Figuur 6. Registratie van gegevens met applicatieve en organisatorische interne-controlemaatregelen.



Figuur 7. Registratie van gegevens met applicatieve en organisatorische internecontrolemaatregelen en algemene computercontroles.



Figuur 8. Registratie van gegevens inclusief AO/IC.

Literatuur

[COSO94] Committee of Sponsoring Organizations of the Treadway Commission, COSO-rapport *Internal Control – Integrated framework*, 1994.

[Bast02] A.R.J. Basten RE, *Beheersing van bedrijfsvoering*, Informatie, september 2002.

[Beek98] J.J. van Beek RE RA en A.R.J. Basten, *Inzicht in procescontrol*, Compact 1998/2.

[Blok01] Prof. J.H. Blokdijk RA, *De effectiviteit van de systeemgerichte aanpak in de accountantscontrole*, MAB, maart 2001.

[Boer98] J.C. Boer, *ICT-aspecten bij de accountants-controle van routinematige transactieverwerking*, Compact 1998/3.

[Dijk04] A.A. van Dijke, R.A. Jonker RE RA en ir. R. Ossendrijver, *Het meten van de effectiviteit van interne-controlemaatregelen*, Compact 2004/1.

[Gove03] Governance Institute, *IT Control Objectives for Sarbanes-Oxley*, 2003.

[Jans93] E.O.J. Jans, *Grondslagen van de administratieve organisatie*, 1993.

[Jonk00] R.A. Jonker RA en R.J.M. van Langen RA, *Samenwerking financial auditor en EDP-auditor*, Compact 2000/2.

[Koed01] Mw. drs. M.J.A. Koedijk RA, *De beoordeling van ICT in het kader van de jaarrekeningcontrole*, Compact 2001/3.

[Kuijk03] Dr. J.R.H.J. van Kuijk RA RC en drs. R.J. Bogtstra RA CIA, *De managementverklaringen in Sarbanes-Oxley*, Compact 2003/3.

[Neis94] Prof. A.W. Neisingh RE RA, *De invloed van informatietechnologie op de beheersing van organisaties*, Compact 1994/2.

[Neis01] Prof. A.W. Neisingh RE RA, *Ongedeelde verantwoordelijkheid RA ter discussie: IT-auditor krijgt (eindelijk) erkenning!*, Compact 2001/3.

[Star94] Prof. R.W. Starreveld RA, prof. drs. H.B. de Mare RA en prof. E.J. Joëls RA, *Bestuurlijke informatievoorziening deel 1*, 1994.

[Vree01] A. Vreeke en D.M. Hallemeesch, *Richt jij de autorisaties even in?*, Compact 2001/6.