Vertrouwen is goed … controle is beter!

Interne controle

in relatie tot COSO ERM en ICF

Wim Fennis en Jan-Pieter Schilderinck

Digitaal supplement

bij

De essentie van administratieve organisatie

Wim Fennis

Jan-Pieter Schilderinck

Tweede, herziene druk

uitgeverij coutinho

bussum 2020

Dit digitaal supplement hoort bij de tweede, herziene druk van **De essentie van administratieve organisatie** van Wim Fennis en Jan-Pieter Schilderinck.

Uitgeverij Coutinho
Postbus 333
1400 AH Bussum
info@coutinho.nl
www.coutinho.nl

ISBN: 978 90 469 0414 5
NUR: 786

Hoofdstuk 2 Control en controle

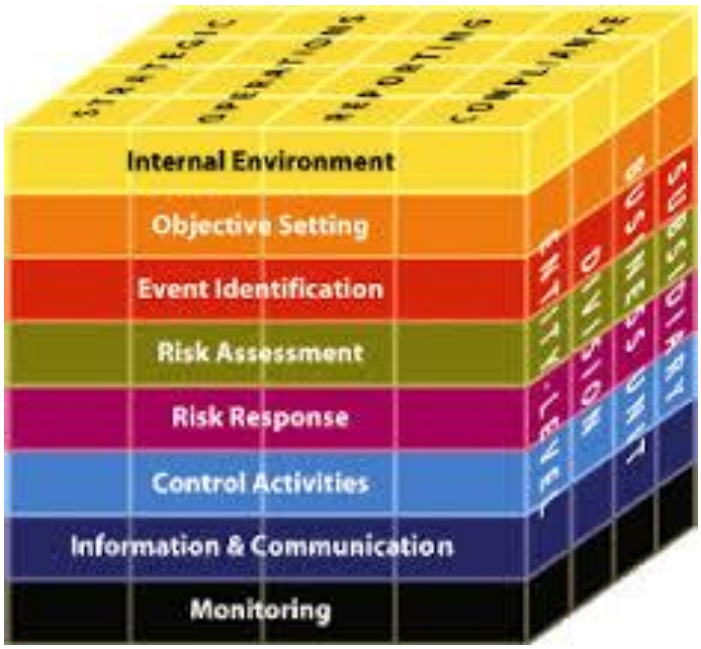
Supplement onderdeel interne controle

Interne controle in relatie tot COSO ERM

Interne controle is gericht op de bescherming van activa van de onderneming tegen ongeoorloofde handelingen. In 1992 was een aantal boekhoudschandalen aanleiding voor de oprichting van het COSO-comité, dat na onderzoek constateerde dat de externe verslaggeving van veel ondernemingen onbetrouwbaar was als gevolg van een zwak intern beheersingssysteem. Dit probleem deed zich niet alleen voor bij grote Amerikaanse ondernemingen, zoals indertijd energiemaatschappij ENRON, maar ook in Nederland, zoals de Ahold-affaire en bij ingenieursbedrijf Imtech.

Het COSO-comité heeft aanbevelingen gedaan om de integriteit, doelmatigheid en doeltreffendheid van organisatorische activiteiten te waarborgen. Het door het comité ontwikkelde managementmodel wordt het COSO-model genoemd en richt zich specifiek op de operationele besturing van functionele processen en in mindere mate op de strategiebepaling en tactische besturing.

Hieronder staat het COSO ERM-model (ook wel *Framework* genoemd) afgebeeld in de vorm van een kubus.



Figuur 1 COSO ERM-model

Doelen van de organisatie worden ingedeeld in vier categorieën:

I. *strategic*
II. *operations*
III. *reporting*
IV. *compliance*

ad. I: Het behalen van doelstellingen die vanuit de strategie worden geformuleerd.
ad II: Het effectief en efficiënt gebruiken van middelen en bedrijfsprocessen.
ad III: De betrouwbaarheid van de financiële verslaggeving weergeven.
ad IV: Het voldoen aan relevante wet- en regelgeving.

Het ERM bestaat uit acht componenten:

1. **Interne omgeving (*internal environment*)**
   Het gaat hier om het bepalen van de risicohouding door de leiding van de organisatie.
   Bijvoorbeeld: nemen we veel of weinig risico ten aanzien van bepaalde gebeurtenissen?

2. **Bepalen van doelstellingen (*objective setting*)**
   De leiding dient doelstellingen te bepalen voor de organisatie.
   Bijvoorbeeld: wel of geen marktleiderschap in combinatie met duurzaam ondernemen en winstmaximalisatie.

3. **Identificatie van gebeurtenissen (*event identification*)**
   Het bepalen van welke kritieke gebeurtenissen (zie punt 1) zich kunnen voordoen ten aanzien van marktleiderschap, duurzaam ondernemen of winstmaximalisatie.

4. **Risico-inschatting (*risk assessment*)**
   Het bepalen van de kans dat zich grote verliezen voordoen bij de uitvoering van processen.

5. **Bepalen van risico-houding (*risk response*)**
   Het gaat hierbij om de volgende acties van de leiding:

   - Accepteren > dus geen beheersmaatregelen
   - Vermijden > bepaalde acties, zoals in- en verkopen achterwege laten
   - Delen > beperkte acties doorvoeren en verliezen beperken
   - Beheersen > het nemen van effectieve beheersmaatregelen, zoals het

tegengaan van CO_2-uitstoot in het kader van duurzaam ondernemen

6. **Controleactiviteiten (*control activities*)**
   Indien wordt gekozen voor het beheersen van het productieproces dan zullen hiervoor beheersmaatregelen moeten worden geformuleerd. Bijvoorbeeld het afvangen van CO_2-uitstoot in afzonderlijke opslaglocaties of het overgaan tot schonere productiemethoden.

7. **Informatie en communicatie (*information & communication*)**
   Het is van groot belang dat de leiding richtlijnen opstelt over de wijze waarop binnen de onderneming informatie wordt verstrekt. Bijvoorbeeld via mails, interne briefings of vergaderverslagen.

8. **Monitoring**
   Hier gaat het om het bewaken van het systeem van interne beheersmaatregelen en checken of dit systeem naar behoren functioneert. Staan er seinen op geel, oranje of rood? Welke codes hanteren we en voor welke onderdelen van het bedrijfsproces?

   Opmerking:
   Het COSO Framework is niet zonder beperkingen. Er kunnen risico's optreden die niet kunnen worden voorkomen, zoals menselijk falen of externe gebeurtenissen (natuurrampen, epidemieën zoals SARS of het coronavirus, oorlogshandelingen enzovoort). Deze belemmeren het bereiken van vooraf geformuleerde doelstellingen door de leiding van een onderneming.

COSO ICF versus COSO ERM

COSO ICF (Internal Control Framework) verschilt in die zin van het ERM-model dat de categorie 'strategic' is weggevallen. Er blijven dus drie doelstellingen over, te weten:

I. ***Operations***
   Deze doelen hebben betrekking op de efficiëntie en effectiviteit van de activiteiten van de organisatie.

II. ***Reporting objectives***
   Deze doelen hebben betrekking op de interne en externe financiële en niet-financiële rapportage.

III. ***Compliance objectives***
Deze doelen hebben betrekking op het voldoen aan de wet- en regelgeving die betrekking heeft op de organisatie.

Bij COSO ICF wordt primair het 'in-controlvraagstuk' benaderd, waarbij de te bepalen strategie als uitgangspunt wordt gehanteerd. Hier ligt het accent dus met name op het beheersbaar maken van de bedrijfsprocessen. Dit model is in 2013 ontwikkeld en wordt op dit moment veelvuldig toegepast als managementinstrument bij bedrijven die COSO toepassen.
Eveneens is er een drietal componenten van de acht weggevallen in het COSO ICF-model en blijven de volgende componenten over:

1. ***Control environment***
   Het totaal aan standaarden, structuren en processen binnen de organisatie die zorgen voor het uitvoeren van de interne controles.

2. ***Risk assessment***
   Elke organisatie heeft te maken met risico's die (zo veel als mogelijk) moeten worden afgedekt of gemitigeerd. 'Risico' wordt in dit geval gedefinieerd als 'de kans dat een bepaalde gebeurtenis een negatief effect heeft op het behalen van doelstellingen van de organisatie'. Een belangrijk onderdeel hiervan is *risicotolerantie*. Aan de hand daarvan zal moeten worden bepaald in hoeverre op dit risico wel of niet moet worden ingespeeld. Een ander essentieel onderdeel is het vaststellen van doelen in verschillende delen van de organisatie. Aan de hand hiervan kunnen verschillende risico's per doel worden ingeschat.

3. ***Control activities***
   Dit zijn de activiteiten die het management uitvoert om de risico's te mitigeren die in de voorgaande stap zijn geïdentificeerd.

4. ***Information & communication***
   Om (voldoende) interne controle te kunnen realiseren is er relevante informatie van hoge kwaliteit nodig. Deze informatie moeten worden gecommuniceerd door de organisatie naar externe partijen.

5. ***Monitoring activities***
   Het is van essentieel belang dat het functioneren van bedrijfsprocessen voortdurend wordt bewaakt om er zeker van te zijn dat de controleactiviteiten goed functioneren.

Er bestaat een verband tussen de doelen van de organisatie, de componenten van interne controle die benodigd zijn om deze doelen te behalen en de structuur van de organisatie. Dit wordt weergegeven door middel van onderstaande kubus.

Figuur 1 COSO ICF-model

Vervolgens worden er 17 principes gepresenteerd die de fundamentele concepten van de vijf componenten vertegenwoordigen. Hierop wordt in het kader van de te behandelen stof niet verder ingegaan.

Hierna volgt een voorbeelduitwerking die van toepassing is op COSO ICF bij een bouwbedrijf en een aantal specifieke aandachtspunten en/of risico's van andere typen bedrijven of organisaties.
Bouwbedrijf Efficiënt en duurzaam BV ontwerpt en bouwt woningen in de randstad voor prijzen die variëren tussen 250.000 en 450.000 euro. De directie overweegt om in het kader van effectief risicomanagement over te gaan tot het hanteren van het COSO ICF Framework als beleidsinstrument voor nu en in de toekomst.
De volgende drie doelstellingen worden concreet uitgewerkt:

I. ***Operations***
II. ***Reporting***
III. ***Compliance***

Daarnaast worden de vijf componenten uit het COSO ICF-model (zie hiervoor) nader uitgewerkt door een speciale werkgroep die verantwoording aflegt aan de directie.
Een uitwerking van de drie doelstellingen en de vijf componenten kan er als volgt uitzien.

ad I:
De concrete doelen van de onderneming hebben met name betrekking op veranderende eisen in het kader van het milieu die aan materialen en bouwtechniek worden gesteld.
Voorbeeld:
Materialen moeten duurzaam zijn en voldoende isolatie in het gebouw bewerkstelligen. Verder zullen sommige materialen moeten kunnen worden hergebruikt en hiermee binnen de productiekringloop blijven.

ad II:
Het management of de directie zal periodiek moeten rapporteren over de behaalde financiële en niet-financiële resultaten, met name als het gaat om het afdekken of verminderen van risico's.
Als voorbeeld van niet-financiële risico's kunnen risico's ten aanzien van het afvoeren van milieubelastend materiaal (PFAS) worden genoemd of verontreiniging van oppervlaktewater.

ad III:
Het doel: 'voldoen aan wet- en regelgeving' zal continu moeten worden bewaakt. Wet- en regelgeving veranderen regelmatig en doen dan ook een dringend beroep op de directie om hiermee dagelijks rekening te houden.
Bouwbedrijven worden bijvoorbeeld regelmatig geconfronteerd met wijzigingen in wet- en regelgeving als het gaat om het zaken als milieu (PFAS en CO_2-uitstoot), ruimtelijke ordening (waar mag wel en waar mag niet worden gebouwd?) en geluidshinder (ligging woonwijk t.o.v. aanvliegroutes luchtvaart).

Zo zullen tevens de vijf componenten moeten worden uitgewerkt, waarbij met name het onderdeel '*risk assessment*' veel aandacht vraagt. Zeker voor een bouwbedrijf als hierboven genoemd zullen diverse risico's kunnen worden gesignaleerd.
Voorbeelden zijn:

- *leveringsrisico's van bouwmaterialen*
- *prijsrisico's*
- *kwaliteitsrisico's*
- *beveiligingsrisico's (fysiek en organisatorisch)*

- *milieurisico's (zie hiervoor)*
- *risico van technische veroudering materialen*

Recente ontwikkelingen ten aanzien van COSO
COSO ERM is in 2017 herzien en de essentie staat hieronder:
'Nieuwe COSO ERM 2017 koppelt risicomanagement aan strategie en prestatiemanagement.'

De nieuwe COSO gaat over strategie, effectiviteit en efficiëntie van de bedrijfsprocessen en de naleving van wet- en regelgeving. En dit risico gestuurd. Het geeft een kapstok voor het in kaart brengen, implementeren en verbeteren van al deze processen.
Het nieuwe COSO-raamwerk legt de nadruk op de wisselwerking tussen risico, prestatie, strategie en waarde. Het is opgebouwd uit vijf onderling verbonden thema's (uitgewerkt in principes) die essentieel zijn voor modern ERM.

Supplement bij paragraaf 2.6 'Beveiliging tegen misbruik'

In paragraaf 2.6 vermeldden wij dat er bij beveiligingsmaatregelen onderscheid gemaakt wordt tussen general controls en application controls. Daarnaast wordt nog een derde categorie onderscheiden, namelijk user controls. Deze begrippen worden hieronder nader toegelicht.

General controls
General controls zijn gericht op de beveiliging en de continuïteit van het geautomatiseerde systeem als geheel. Ze zijn onder te verdelen in een aantal groepen:

1. Organisatorische maatregelen
Hieronder vallen:
- Controletechnische functiescheiding tussen gebruiker en beheerder van het systeem; binnen de IT-afdeling moet er ook functiescheiding zijn tussen de ontwerpers van het systeem (als het ontwerpen niet is uitbesteed) en degenen die het onderhoud verrichten.
- Fysieke maatregelen die beschadiging of diefstal van de hardware tegengaan. Denk hierbij aan het plaatsen van de server in een brandvrije, gekoelde ruimte, apparatuur vastmaken dan wel in afgesloten ruimtes plaatsen.

2. Maatregelen om veroudering tegen te gaan
Voorbeelden die hierbij genoemd kunnen worden, zijn:

- *Service Level Agreements* (SLA) met de leverancier. In de meest eenvoudige vorm kunnen dit abonnementen op updates zijn, maar het is ook mogelijk om het volledige onderhoud door de leverancier te laten uitvoeren.
- In het geval van onderhoud dat in eigen beheer wordt uitgevoerd dient de organisatie te beschikken over *change-management-procedures*. Hierin wordt geregeld welke stappen gezet moeten worden bij het aanpassen van programma's of andere systeemonderdelen. Naast autorisatie vooraf is het uitvoeren van gebruikers- en acceptatietesten hiervan een onderdeel.

3. Maatregelen tegen ongeautoriseerd handelen

Hieronder vallen:

- Toegangscontrole via username-wachtwoordcombinaties. Per combinatie worden in een competentietabel alle bevoegdheden in het systeem vastgelegd.
- Logging. Dit betekent dat elk handelen van iedere gebruiker in een controlebestand wordt vastgelegd, zodat te allen tijde kan worden achterhaald wie wat gedaan heeft op een bepaald moment.

4. Maatregelen om het verlies van gegevens tegen te gaan

Te denken valt aan:

- Back-up- en recoverymaatregelen. Back-ups zijn kopieën van gegevens (of bestandsonderdelen) die bij voorkeur buiten het systeem zijn opgeslagen. Recovery wil zeggen dat je via een track vanuit een oude versie van het bestand het nieuwe bestand opnieuw opbouwt.
- Opslag in de cloud. Gegevens zijn dan buiten het eigen systeem opgeslagen. Hierop gaan we straks nader in.

5. Maatregelen tegen bedreigingen van buitenaf

Genoemd kunnen worden:

- virusscanners
- firewalls
- encryptie

Application controls

Application controls zijn controlemaatregelen die zijn ingebouwd in programma's en dus specifiek horen bij dat programma. Application controls komen heel veel voor en zijn er in verschillende soorten:

1. Vormen van invoercontrole

Enkele voorbeelden:

- Een controle of alle velden van een formulier (bijvoorbeeld bij een onlinebestelling) zijn ingevuld.
- Een controle of bankrekeningnummer en naam van de rekeninghouder met elkaar overeenkomen bij pakketten voor internetbankieren.
- Een controle of postcode klopt met adres.

2. Controles op het voldoen aan 'regels'

Voorbeelden hiervan zijn:

- Spellingcontrole bij tekstverwerkingsprogramma's (bijvoorbeeld Word).
- Controle of een journaalpost in evenwicht is bij boekhoudprogramma's.

3. Verbandscontroles

Een voorbeeld hiervan is de automatische controle in een ERP-pakket of het aantal geleverde goederen op een bepaald ordernummer gelijk is aan het aantal gefactureerde goederen op dat ordernummer.

User controls

User controls zijn controles die de gebruiker zelf uitvoert. Naarmate er meer application controls zijn, neemt het aantal user controls af.

De meeste user controls zijn minder geavanceerde vormen van invoercontroles. Bijvoorbeeld aan de hand van een papieren invoerdocument op het beeldscherm controleren of gegevens juist zijn ingevoerd. Een ander voorbeeld is een handmatig gemaakte totaaltelling vergelijken met een door de computer berekende totaaltelling.

Cloud computing

Cloud computing is een ontwikkeling die de afgelopen tien jaar een hoge vlucht heeft genomen. Het begrip is te omschrijven als het op aanvraag online beschikbaar stellen van hardware, software en gegevens. Er zijn vijf verschijningsvormen:

1. *On demand.* Daarbij wordt computercapaciteit beschikbaar gesteld. Denk bijvoorbeeld aan de opslag van gegevens.
2. *Network acces.* Eigenlijk is dat min of meer hetzelfde, maar hierbij maakt het device van de gebruiker niet uit. Dus bijvoorbeeld ook smartphones en tablets hebben toegang tot de diensten.

3. *Pooling.* Verschillende gebruikers maken gebruik van de diensten zonder dat ze last van elkaar hebben. Bij deze vorm van cloud computing is het essentieel dat de toegangscontrole goed geregeld is.
4. *Elasticity.* Dat wil zeggen snel kunnen opschalen van de capaciteit als dat nodig is. Nieuwe bedrijfsonderdelen moeten bijvoorbeeld snel van dezelfde faciliteiten gebruik kunnen maken als de bestaande.
5. *Measurement.* Hierbij wordt niet alleen capaciteit beschikbaar gesteld, maar ook het beheer wordt in handen gelegd van de aanbieder.

Een belangrijk risico voor de gebruiker van cloud computing is dat de gebruiker wel verantwoordelijk is voor de gegevens die in de cloud worden opgeslagen of verwerkt, maar niet zelf maatregelen kan nemen om deze te beveiligen. De privacy in het kader van de AVG moet gewaarborgd zijn. Het aanleggen van een firewall of het regelen van de toegang moet gebeuren door de aanbieder.
Daarom is het essentieel een SLA af te sluiten waarin al deze zaken zijn geregeld.

Van de volgende bronnen hebben we gebruikgemaakt bij dit digitaal supplement:

- *Examenopgave AIS Opgave SPD* (2017)
- Milan van den Abeele (Nijenrode University)
- Naris GRC softwaretraining