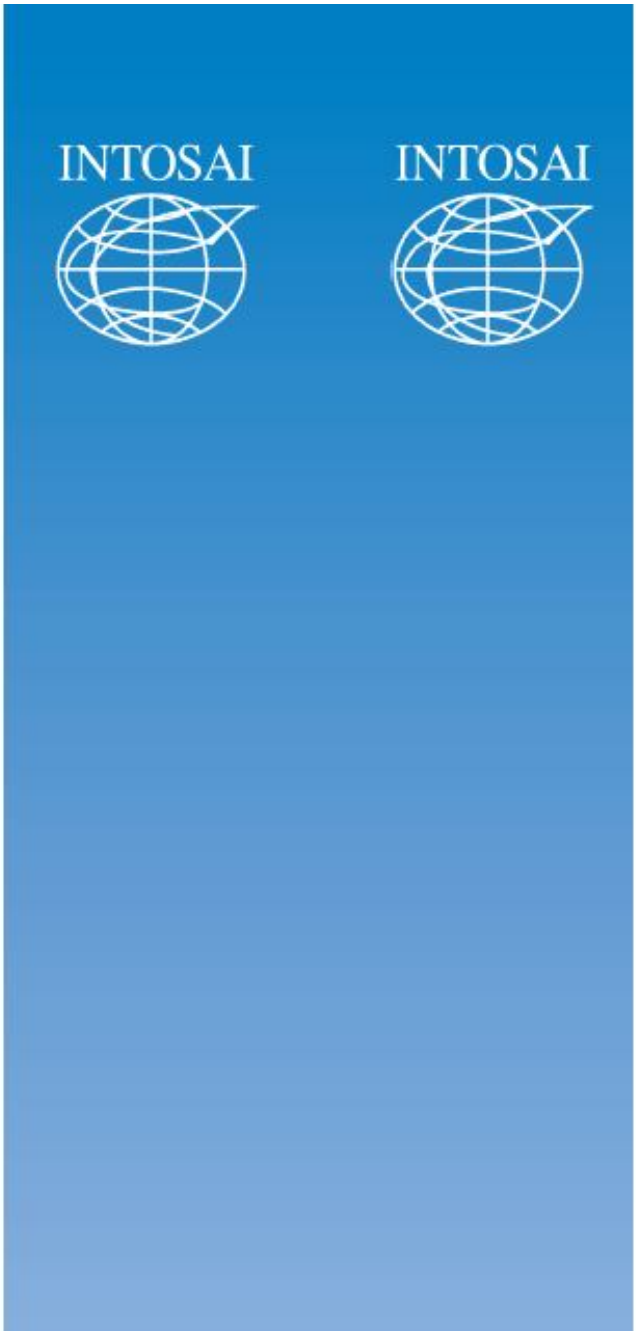


Guidelines for Internal Control Standards for the Public Sector

Internal Control Standards Committee

Fr. VANSTAPEL
Senior President
of the Belgian Court of Audit

Regentschapsstraat 2
B-1000 BRUSSELS
BELGIUM

Tel: ++32 (2) 551 81 11
Fax: ++32 (2) 551 86 22
E-mail: internalcontrol@ccrek.be

Originele versie: INTOSAI, Guidelines for Internal Control Standards for the Public Sector, 2004.
Vertaling: Adjt Raph SOMERS en LtKol Manu CAMMAERT (DG Fmn / Sec Eval)

WAARSCHUWING

Het document dat nu voor u ligt is een vertaling van het Engelstalig origineel 'Guidelines for Internal Control Standards for the Public Sector' uitgegeven door INTOSAI. Deze vertaling gebeurde op persoonlijk initiatief en dit ter ondersteuning van de toepassing van interne beheersing binnen Defensie. Het is de hoop dat deze vertaling onze Nederlandstalige collega's helpt bij het beter begrijpen van interne beheersing.

De vertaling is echter niet op maat van Defensie zodat het algemeen karakter van de standaard behouden blijft.

In geval van moeilijkheden met de interpretatie wordt er best, hoewel er ook een Franstalige versie bestaat, vertrokken vanuit de originele, Engelstalige versie.

Opmerkingen zijn steeds welkom op patrick.vanhoeserlande@mil.be.

Patrick VAN HOESERLANDE, Ir
Majoor van het vliegwezen SBH
Kabinet CHOD - Adj Director of Staff (DOS)
Kwartier Koningin Elisabeth - Eversestraat 1 - 1140 Evere
Blok 1 Lokaal A650
Tel 0032(0)2.701.3148 of 9-2400-3148
ICS intranet : http://units.mil.intra/sites/CHOD/ICS/

Inhoudstafel

Richtlijnen voor de standaard van Interne Beheersing[1]

Voorwoord

De 1992 INTOSAI richtlijnen voor de standaard van de Interne Beheersing[2] werden opgevat als een levend document vanuit de visie dat er een standaard moet worden gepromoot voor het ontwerp, de implementatie en de evaluatie van de interne beheersing. Deze visie vraagt een continue inspanning om deze richtlijnen up-to-date te houden.

De 17de INCOSAI (Seoul 2001) onderkende de dringende noodzaak voor een herziening van de richtlijnen van 1992 en er werd overeengekomen om het Committee on Sponsoring Organisations of the Treadway Commission (COSO) geïntegreerd raamwerk van de interne beheersing als basis te nemen. Daaropvolgende contacten en toenaderingen leidden tot de aanbevelingen dat de richtlijnen ook de ethische waarden moesten omvatten en dat er meer informatie over de algemene principes van de beheersingsmaatregelen t.o.v. de informatie verwerking moesten worden in verwerkt. De herziene richtlijnen houden rekening met deze aanbevelingen en zouden het begrip van de nieuwe concepten met betrekking op de interne beheersing moeten vergroten.

De herziene richtlijnen moeten ook als een levend document beschouwd worden dat in de loop van tijd ook verder zal moeten worden ontwikkeld en verfijnd om zo ook de impact van nieuwe ontwikkelingen zoals het COSO Enterprise Risk Management Framework[3] te omvatten.

De herziening is het resultaat van de inspanningen van de leden van de INTOSAI Internal Control Standards Committee. De herziening werd gecoördineerd door een task force bestaande uit leden van het comité met vertegenwoordigers van de SAI's (Supreme Audit Institution) uit Bolivia, Frankrijk, Hongarije, Litouwen, Nederland, Roemenië, het Verenigd Koninkrijk, de Verenigde Staten van Amerika en België(Voorzitter).

Een actieplan voor de herziening van de richtlijn werd overhandigd aan en goedgekeurd door de Governing Board tijdens haar 50st vergadering (Wenen, oktober 2002). De Governing Board werd op de hoogte gesteld van de vooruitgang van de herziening op haar 51st vergadering (Budapest, oktober 2003). Het ontwerp werd besproken en in principe aanvaard door het comité tijdens de vergadering van februari 2004 te Brussel. Na deze vergadering werden de richtlijnen aan alle INTOSAI leden gestuurd voor lezing en opmerkingen.

De ontvangen opmerkingen werden geanalyseerd en de benodigde wijziging werden aangebracht.

Ik wil hierbij alle leden van de INTOSAI Intern Control Standards Committee bedanken voor hun toewijding en medewerking in het volbrengen van dit project. Speciale dank gaat naar de leden van de Task Force.

De richtlijnen voor Standaard voor Interne beheersing voor de openbare sector werden ter goedkeuring voorgelegd aan de XVIII INCOSAI te Budapest 2004.

Franki Vanstapel
Senior President van de Belgian Court of Audit

1 Dit document bestond al in het Engels en het Frans.

2 'Internal Control' werd vertaald in interne beheersing, aangezien 'controle' in het Nederland seen andere betekenis heeft.

3 COSO, Enterprise Risk Management – Integrated framework, http://www.coso.org/, 2004

Voorzitter van het INTOSAI Internal Control Standards Committee.

Inleiding

In 2001 besloot INCOSAI (International Congress of Supreme Audit Institutions) een herziening te doen van de 1992 INTOSAI richtlijnen voor de Standaard voor Interne Beheersing om aan alle relevante en recente evoluties in de interne beheersing tegemoet te komen en om het concept van het COSO rapport - Internal Control-Integrated Framework- hierin te integreren.

Door het implementeren van het COSO model in deze richtlijn tracht het comité niet enkel het concept van de interne beheersing te updaten maar wil het ook bijdragen tot een beter begrijpen van de interne beheersing binnen de SAI. Het is vanzelfsprekend dat deze richtlijn het specifieke karakter van het openbare bestuur voor ogen houdt. Dit zette het comité ook aan om enkele bijkomende thema's en veranderingen mee op te nemen in de richtlijn.

In vergelijk met de COSO definities en de richtlijn uit 1992 word er nu ook aandacht besteed aan het ethische aspect van operaties[4]. Het opnemen hiervan in deze richtlijn is gerechtvaardigd omdat sedert de jaren 90 er steeds meer nadruk word gelegd op ethisch gedrag en op preventie en ontdekking van fraude en corruptie in het openbaar ambt[5]. Algemeen wordt aangenomen dat ambtenaren van de openbare diensten de bevolking een faire dienstverlening schuldig zijn en dat de budgetten goed beheerd worden. Burgers moeten een onpartijdige dienstverlening krijgen op basis van wettelijkheid en gerechtigheid. Vandaar dat ethisch gedrag een voorwaarde en steunpunt is voor het vertrouwen van de burgers en een hoeksteen is van goed bestuur.

Omdat de middelen in de openbare sector meestal gemeenschapsgelden zijn die ook voor de gemeenschap aangewend zullen worden is het nodig hier speciale aandacht aan te besteden. Het veiligstellen van deze middelen in de openbare sector is dus zeer belangrijk. Hierbij komt nog dat in de openbare sector nog veel met cash geld wordt gewerkt maar dit brengt ook met zich mee dat men niet voldoende garanties heeft over het bekomen en gebruiken van en beschikken over deze middelen. Resultaat hiervan is dat de organisaties in de openbare sector niet altijd over up-to-date rapporten over hun middelen beschikken en dat brengt hun in een kwetsbare positie. Hierdoor werd geoordeeld dat het veiligstellen van de middelen een belangrijke doelstelling van de interne beheersing moest zijn.

Zoals de interne beheersing in 1992 niet beperkt was tot het financiële en de daaraan gekoppelde administratie maar ook over het breder concept van beheersing door het management handelde, word in dit document ook het belang van de niet-financiële informatie benadrukt.

Door het veelvuldige gebruik van informaticasystemen in alle openbare diensten werd het beheersen van Information Technology (IT)steeds belangrijker en dit verklaard ook waarom er in deze richtlijn hierover een apart gedeelte werd gewijd.

IT beheersing slaat op elk van de componenten van de interne beheersing van een entiteit met inbegrip van de controle omgeving, risico inschatting, beheersingsmaatregelen, informatie en communicatie en de monitoring. Voor reden van presentatie wordt dit besproken bij de "Beheers activiteiten".

De doelstelling van het comité is om een gids te ontwikkelen voor het ontwerpen en onderhouden van een interne beheersing in de openbare sector. Openbare besturen zijn daarom ook een belangrijke doelgroep van deze richtlijn. Openbare besturen kunnen deze richtlijn gebruiken als basis voor de implementatie en uitvoering van de interne beheersing in hun organisaties.

Omdat de evaluatie van de interne beheersing een algemeen aanvaard onderdeel is van audits in de openbare besturen[6], kunnen auditoren deze richtlijn als een hulpmiddel gebruiken bij audits. De richtlijn betreffende interne beheersing met inbegrip van het COSO model kan daardoor zowel gebruikt worden

4 Operaties = alle activiteiten van Defensie, dus niet alleen de militaire operaties.

5 XVI INCOSAI, Montevideo, Uruguay, 1998

6 INTOSAI Auditing Standards

door het management van de openbare besturen[7] als een solide basis voor het beheersmodel in hun organisatie als door de auditoren als een hulpmiddel voor het evalueren van de interne beheersing. Nochtans is deze richtlijn niet bedoeld als vervanger van de INTOSAI Auditing Standards of andere relevante audit richtlijnen.

Dit document omschrijft een aanbevolen raamwerk voor de interne beheersing in het openbaar domein en is een basis voor evaluatie van de interne beheersing. Deze benadering slaat op alle aspecten van de operaties van een organisatie. Het is echter niet de bedoeling van dit document om beperkingen op te leggen of tussen te komen in de bevoegdheid van deze organisaties om wetten, reglementen of werkwijzen voor te schrijven.

Interne Beheersing binnen de openbare sector moet gezien worden in het kader van het specifieke karakter van deze organisaties; hun politieke en sociale doelstelling; het gebruik van gemeenschapsgelden; de complexiteit van hun werking (Een evenwichtsoefening tussen traditionele waarden als wettelijkheid, integriteit en openheid en de moderne waarden als doeltreffendheid en doelmatigheid.) en de brede waaier aan verplichtingen betreffende het afleggen van rekenschap.

Ten slotte moet vermeld worden dat dit document een richtlijn is. Deze richtlijn geeft geen gedetailleerde beleidslijnen, werkwijzen of procedures voor het implementeren van de interne beheersing maar biedt een raamwerk waarbinnen de entiteit zelf een gedetailleerde beheersing kan ontwerpen. Het comité is niet in een positie om deze standaard te verplichten.

Opbouw van het document

Deel 1 beschrijft het concept van de interne beheersing, met aandacht voor de beperkingen ervan. Deel 2 beschrijft de componenten van de interne beheersing. Deel 3 beschrijft de taken en verantwoordelijkheden.

In elk deel worden de beginselen eerst kort beschreven, gevolgd door meer achtergrond informatie. Er worden concrete voorbeelden aangehaald in deel 4. Ten slotte is er ook in deel 5 een verklarende woordenlijst met de belangrijkste technische termen.

7 Uitvoerend personeel is geen specifieke doelgroep. Hoewel ze beïnvloedt worden door interne beheersing en een belangrijke rol spelen in de uitvoering van de beheersing zijn ze, in tegenstelling tot het management, niet de eindverantwoordelijken voor de operaties van de organisatie die te maken hebben met interne beheersing. Hst 3 beschrijft de individuele taken en verantwoordelijkheden.

1. Interne Beheersing

1.1 Definitie

Interne beheersing is een totaalproces dat beïnvloed word door de verantwoordelijken en het personeel van een entiteit en dat ontworpen is om risico's aan te pakken en een mate van zekerheid te bieden zodat, in het streven naar de opdracht van de entiteit, de volgende algemene doelen kunnen worden bereikt:

- Ordelijk, ethisch, economisch, efficiënt en doeltreffend (effectief) operaties uitvoeren;
- Rekenschap afleggen;
- Wetten en reglementen respecteren(naleven);
- Kapitalen beschermen tegen verlies, misbruik en beschadigingen.

Interne beheersing is een dynamisch totaalproces dat permanent aangepast word aan de veranderingen waaraan een organisatie onderhevig is. De directie en het personeel van alle niveaus moeten in dit proces ingeschakeld worden om risico's[8] het hoofd te bieden en een redelijke mate van zekerheid te verkrijgen dat de opdracht en de gestelde doelen van de entiteit bereikt kunnen worden.

Een totaalproces

Interne beheersing is geen eenmalige gebeurtenis, maar een serie acties die invloed hebben op de activiteiten van de entiteit. Deze acties gebeuren doorlopend doorheen het volledige productieproces. Ze beïnvloeden en komen voort uit de manier waarop de directie de zaken leidt. Interne beheersing wordt daardoor bekeken als een bijkomende activiteit voor de onderneming en door anderen bekeken als een bijkomende last. Het interne beheersing systeem is verweven in de activiteiten van de onderneming en is het meest doeltreffend als het in de infrastructuur van de onderneming is ingebouwd als een essentieel onderdeel.

Interne beheersing kan beter worden ingebouwd dan toegevoegd. Door interne beheersing in te bouwen wordt het een deel van en geïntegreerd in de planning en de uitvoering ervan, en de monitoring door de directie.

Ingebouwde interne beheersing heeft ook belangrijke gevolgen voor de kostenbeheersing. Nieuwe beheersprocedures die los staan van de bestaande procedures verhogen de kosten. Door zich toe te spitsen op bestaande operaties en hun invloed op de doeltreffende interne beheersing en door beheersing in te bouwen in de basisactiviteiten, kan een onderneming veelal onnodige kosten vermijden.

Beïnvloeding door management en ander personeel

De bevolking van de onderneming zorgt ervoor dat interne beheersing werkt. Dit wordt bewerkstelligd door wat de bevolking binnen de onderneming zegt en doet. Bijgevolg wordt interne beheersing beïnvloed door mensen. Mensen moeten hun taken en verantwoordelijkheden en de hun grenzen van zeggenschap kennen. Omdat dit zo belangrijk is werd er een apart hoofdstuk (5) aan gewijd.

De bevolking van een onderneming bestaat uit de directie en ander personeel. De directie heeft vooral een superviserende functie, maar is ook verantwoordelijk voor het bepalen van de doelstellingen en heeft de verantwoordelijkheid over het interne beheersing systeem. Omdat het interne beheersingssysteem helpt om risico's in te schatten in de context van de doelstellingen van de onderneming, zal de directie dit interne

8 'Onzekerheid' was is deze context een betere vertaling dan 'risico' voor het woord 'risk'. Het betreft hier immers om onzekerheid die zowel een positife als een negatief effect kunnen hebben.

beheersingssysteem in plaats stellen, opvolgen en evalueren. De implementatie van het interne beheersingssysteem vergt inzet en initiatieven van de directie en intensieve communicatie tussen management en de rest van het personeel. Daarom is het interne beheersingssysteem een werkinstrument van de directie en direct gelinkt aan de gestelde doelen. In deze optiek is de directie een zeer belangrijk element van de interne beheersing. Maar al het personeel van de onderneming speelt een belangrijke rol om het systeem te laten draaien.

Interne beheersing wordt beïnvloed door mensen. Interne beheersing richtlijnen erkennen dat mensen niet altijd alles begrijpen, goed communiceren en constant presteren. Elke persoon brengt een unieke achtergrond en technische vaardigheden naar de werkvloer en heeft andere behoeften en prioriteiten. Deze realiteit beïnvloedt en wordt beïnvloed door de interne beheersing.

Het ondernemingsdoel nastreven

Elke organisatie is eerst en vooral gefocust op de verwezenlijking van zijn opdracht.

Entiteiten zijn er voor een bepaald doel. In de openbare sector is die gewoonlijk dienstverlening met een opbrengst in het openbaar belang.

Risico's het hoofd bieden

Welke ook de opdracht is, bij de uitvoering ervan komen allerhande risico's kijken. De taak van de directie is om deze te herkennen en er gepast op te reageren zodat er een zo hoog mogelijke waarschijnlijkheid bestaat om de opdracht te kunnen volbrengen. Interne beheersing kan een hulp zijn om deze risico's aan te pakken, maar het kan enkel een redelijke mate van zekerheid verschaffen met betrekking tot het vervullen van de opdracht en het behalen van de gestelde doelen.

Redelijke mate van zekerheid verschaffen

Interne beheersing kan de directie nooit absolute zekerheid bieden met betrekking tot het verwezenlijken van de gestelde doelen, hoe goed ontworpen en uitgevoerd deze ook mag zijn. Deze richtlijnen houden er rekening mee dat slechts een redelijke mate van zekerheid te verkrijgen is.

Redelijke mate van zekerheid = een bevredigende mate van vertrouwen in functie van kosten, baten en risico's. Bepalen hoeveel zekerheid redelijk is, is een kwestie van inschattingsvermogen. Met dit inschattingsvermogen moeten managers werken om de risico's die aan hun operaties gelinkt zijn en de aanvaardbare risico's bij wisselende omstandigheden te herkennen en deze risico's kwantitatief en kwalitatief te beoordelen.

Redelijke mate van zekerheid wordt ook beïnvloed door toekomstige onzekerheid en risico's en zijn door niemand met zekerheid in te schatten. Ook kunnen factoren van buiten de beheersing en invloed van de organisatie om, invloed hebben op de mogelijkheid om de gestelde objectieven te bereiken. Ook volgende factoren kunnen hun rol spelen: mensen kunnen foute beslissingen nemen; pannes kunnen gebeuren door kleine fouten of vergissingen; beheersing kan omzeild worden door corruptie van 2 of meerder personen; de directie kan het interne beheersingssysteem naast zich neerleggen. Compromissen in het beheersingssysteem worden gemaakt doordat ze ook kosten genereren.

Deze beperkingen onthouden de directie van de absolute zekerheid dat de objectieven kunnen worden gehaald.

Redelijke mate van zekerheid betekend ook dat de kosten van de interne beheersing niet de baten ervan mogen overstijgen. Beslissingen om risico's te beperken en het instellen van beheersing moeten rekening houden met de relatieve kosten en baten. Deze kosten zijn de financiële impact van de gebruikte middelen om een bepaald doel te bereiken en de economische impact van gemiste kansen door oponthoud in productie, een terugval in productiviteit of demotivatie van personeel. De baten zijn de mate waarin een risico om een doel te bereiken kunnen worden beperkt. Bv. door de mogelijkheid om fraude, verspilling, misbruik of

fouten te ontdekken te verhogen, ongepaste activiteiten te voorkomen en het naleven van voorschriften in de hand te werken.

Een interne beheersing ontwerpen, die risicomanagement en kostenbeheersing combineert vraagt dat de directie duidelijk begrijpt welke objectieven er bereikt moeten worden. Overheidsmanagers kunnen systemen opzetten met zeer strikte beheersing in een bepaald actiedomein die op andere operaties een invloed kunnen hebben. Bv. personeel kan proberen om ingrijpende beheersing te omzeilen; inefficiënte procedures kunnen vertragingen veroorzaken; te uitgebreide procedures kunnen de creativiteit en het oplossingsgericht denken van personeel indijken en de stiptheid van dienstverlening tegenwerken, kosten veroorzaken en de kwaliteit van de service doen dalen. Dus de baten van overdreven beheersing in één domein kunnen teniet gedaan worden door kosten in andere domeinen.

Bijkomend moeten ook kwalitatieve overwegingen gemaakt worden. Bv. het kan belangrijk zijn om beheersing te hebben over transacties met hoog risico en relatief kleine sommen zoals salarissen, reis- en representatie kosten. De kosten voor dergelijke beheersing kunnen relatief hoog lijken ten opzichte van de bedragen die hierdoor besteed worden, maar dit kan nodig zijn om het vertrouwen van de bevolking in deze publieke instellingen te behouden.

Bereiken van de objectieven

Interne beheersing is gericht op het bereiken van afzonderlijke maar toch verbonden doelstellingen. Deze doelstellingen worden bereikt door een veelvoud aan specifieke deel-doelstellingen, functies, processen en activiteiten.

De algemenen doelstellingen zijn:

- **Het uitvoeren van ordelijke, ethische, economische, efficiënte en doeltreffende operaties**

Ordelijk betekent: goed georganiseerd, methodisch.

Ethisch heeft te maken met morele principes. Het belang van ethisch correct gedrag en de preventie en ontdekking van fraude en corruptie in het openbare ambt is meer en meer benadrukt geworden sinds de jaren 90. Over het algemeen wordt er verwacht dat ambtenaren het algemeen belang moeten dienen op een eerlijke manier en dat ze de financiële middelen correct moeten beheren. Burgers hebben recht op een onpartijdige behandeling op basis van weten en gerechtigheid. Vandaar dat dit ethische gedrag een absolute voorwaarde is om het vertrouwen van het publiek te bewerkstelligen en de hoeksteen is voor goed bestuur.

Economisch betekent niet verkwistend of extravagant. De juiste hoeveelheid aan middelen, op de juiste plaats en het juiste moment gebruikt aan de laagst mogelijke kostprijs.

Efficiënt verwijst naar de verhouding tussen de aangewende middelen om het doel te bereiken en de gerealiseerde resultaten. Dit betekent: Minimale input van middelen om een gevraagde kwaliteit en kwantiteit te realiseren. Of een maximale productie met een vooraf bepaalde kwaliteit en hoeveelheid aan middelen.

Doeltreffend Verwijst naar het verwezenlijken van doelstellingen of de mate waaraan het resultaat voldoet aan de doelstelling of het gewenste resultaat van de activiteit.

- **Rekenschap afleggen**

Rekenschap is het proces waarbij openbare instellingen of het personeel ervan, verantwoordelijk worden gesteld voor de door hen genomen beslissingen en acties, met inbegrip van het budgetbeheer, hun eerlijkheid en andere aspecten van hun dienstverlening.

Dit zal worden verkregen door het ontwikkelen, onderhouden en openbaar maken van betrouwbare en relevante financiële en andere informatie door middel van het tijdig en eerlijk bekendmaken van die informatie aan interne en externe belanghebbenden.

Andere informatie kan betrekking hebben op het economische, efficiënte en doelgerichte aspect van de werkwijzen en operaties en op interne beheersing en haar doeltreffendheid.

- **Handelen naar de wetten en reglementen**

Organisaties moeten veel wetten en reglementen naleven. In openbare instellingen hebben deze betrekking op het bekomen en beheren van overheidsfinanciën en de manier van functioneren.

Voorbeelden zijn oa begrotingen, internationale verdragen, wetten i.v.m. correcte administratie, fiscale wetgeving, boekhoudkundige regels, milieubescherming en burgerwetgeving, belastingwetgeving en anti-fraude en anti-corruptie verdragen.

- **Kapitalen beschermen tegen verlies, misbruik en beschadigingen door verkwisting, slecht beheer, fouten, fraude en onwetmatigheden te bestrijden**

Hoewel deze vierde doelstelling als een subcategorie van de eerste kan worden gezien, moet het belang van het beschermen van de kapitalen in de openbare sector toch onderstreept worden. Dit komt door het feit dat deze middelen eigenlijk van de bevolking zijn en het gebruik ervan ten goede van de gemeenschap met speciale zorg moet worden uitgevoerd. Budgetbeheer op basis van cash geld is nog steeds wijd verspreid in de openbare sector, maar dit geeft niet voldoende zekerheid over het verkrijgen, het gebruik en de beschikbaarheid van deze middelen. Dit resulteert in het feit dat organisaties in het openbare ambt niet altijd een up-to-date zicht hebben van hun middelen en dit zorgt voor meer kwetsbaarheid. Daarvoor is het nodig om beheersing in te bouwen in de directie van de middelen vanaf hun toekenning tot het uitgeven of gebruiken ervan.

Andere middelen zoals informatie, brondocumenten en boekhoudingen zijn een sleutel tot transparantie en rekenschap van overheidsoperaties en moeten bewaard blijven. Er bestaat steeds het risico van diefstal, misbruik of vernieling van deze middelen.

Het bewaren en vrijwaren van deze data is met de opkomst van de computer nog belangrijker geworden. Gevoelige informatie opgeslagen in een computer kan vernietigd, gekopieerd, verdeeld en misbruikt worden als er geen beveiliging op toegepast wordt.

1.2 Beperkingen aan de doeltreffendheid van de interne beheersing[9]

Enkel interne beheersing alleen kan geen zekerheid geven betreffende de verwezenlijking van de gestelde objectieven.

Een efficiënt intern beheersingssysteem kan, hoe goed het ook ontworpen is en gebruikt wordt, de directie enkel een redelijke - geen absolute- zekerheid bieden over de verwezenlijking van de gestelde objectieven en de overlevingskansen van de entiteit. Het geeft de directie wel inlichtingen over de gemaakte vooruitgang of het gebrek hieraan in functie van de gestelde objectieven. Maar interne beheersing kan van een slechte manager geen goede maken. Bijkomend kunnen verschuivingen in het beleid of programma's, demografische en economische factoren buiten de beheersing van de directie het noodzakelijk maken dat de beheersing hertekend moeten worden of het verwachtingspatroon aangepast moet worden.

Een goedwerkend interne beheersing systeem verkleint het risico op het niet bereiken van de gestelde doelen. Er bestaat echter altijd de kans dat het intern beheersing systeem slecht werd ontworpen of dat het slecht word uitgevoerd.

Omdat interne beheersing afhankelijk is van menselijke factoren, is er dus steeds de kans op fouten in het ontwerp, verkeerde inschattingen of interpretaties, onbegrip, nalatigheid, vermoeidheid, verstrooiing, misbruik of inmenging.

Een andere beperkende factor is het feit dat het ontwerpen van de interne beheersing beperkt is in aanwendbare middelen. De voordelen moeten dus gezien worden in het kader van de gemaakte kosten. Een intern beheersing systeem om verlies van middelen uit te sluiten is niet realistisch en zal waarschijnlijk meer kosten dan het ooit zal kunnen opbrengen. Bij het bepalen van de opportuniteit van een bepaald beheersing systeem zal de waarschijnlijkheid van voorkomen van het risico en het potentiële effect op de entiteit mee in overweging worden genomen samen met de kosten van het invoeren van deze nieuwe beheersing.

Verschuivingen in de organisatie en de houding van de directie kunnen een diepgaande invloed hebben op de doeltreffendheid van de interne beheersing en het personeel dat deze beheersing moet uitvoeren. Bijgevolg zal de directie voortdurend moeten inschatten en bijsturen, wijzigingen doorgeven aan het personeel, en zelf ook deze nieuwe, aangepaste beheersing toepassen.

9 De beperkingen aan de doeltreffendheid van interne beheersing moet benadrukt worden om te vermijden dat er overdreven verwachtingen gecreëerd worden door verkeerdelijk begrijpen van de impact van de beheersing.

2. Componenten van de Interne Beheersing

Interne beheersing bestaat uit vijf verweven componenten:

- beheersingsomgeving
- risicoanalyse
- beheersingsactiviteiten
- informatie en communicatie
- monitoring

Interne beheersing is ontworpen om een redelijke zekerheid te verschaffen betreffende de verwezenlijking van de vooropgestelde objectieven. Vandaar dat duidelijke vooropgestelde doelstellingen een absolute voorwaarde zijn voor een doeltreffend interne beheersing systeem.

De beheersingsomgeving is de basis voor het volledige interne beheersing systeem. Het biedt de discipline en de structuur maar ook het klimaat die van invloed zijn op de algemene kwaliteit van de interne beheersing. Het beïnvloed de manier waarop strategieën en doelstellingen worden bepaald en hoe de beheersingsmaatregelen worden opgebouwd.

Wanneer duidelijke doelstellingen en een doeltreffende beheers omgeving bepaald zijn, kan de *analyse van de risico's* waaraan de entiteit kan blootgesteld worden, zorgen voor de basis voor de ontwikkeling van een gepaste strategie om deze risico's te bestrijden.

De belangrijkste strategie om deze risico's af te zwakken zijn de beheersingsmaatregelen.

*Beheersingsmaatregele*n kunnen preventief en/of curatief zijn. Curatieve acties zijn een noodzakelijke aanvulling van de interne beheersing om de gestelde doelstellingen te halen. Beheersingsmaatregelen en curatieve acties moeten een opbrengst genereren. De kosten ervan mogen de baten niet overstijgen.

Doelgerichte *informatie en communicatie* zijn van vitaal belang voor een entiteit om haar operaties uit te voeren en te contoleren. De directie heeft toegang nodig tot relevante, volledige, betrouwbare, correcte en tijdig overgemaakte informatie over interne en externe factoren. Informatie is een noodzaak in gans de entiteit om de gestelde doelen te bereiken.

Omdat interne beheersing een dynamisch proces is dat continu aangepast moet worden aan de risico's en veranderingen waaraan een onderneming blootgesteld is, moet het intern beheersing systeem opgevolgd worden zodat er steeds bijgestuurd kan worden naar aanleiding van de gewijzigde doelstellingen, omgeving, middelen en risico's.

Deze componenten bepalen de aanbevolen benadering van de interne beheersing bij besturen en leveren de basis waarop de interne beheersing beoordeeld kan worden. Deze componenten zijn van toepassing op alle aspecten van de operaties van een entiteit.

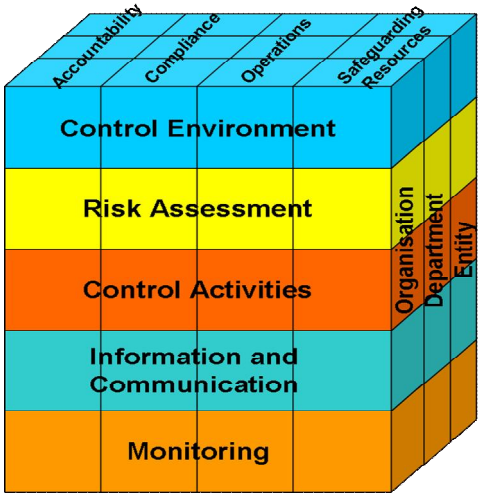
Deze componenten vormen het algemeen raamwerk. Bij de invoering ervan is de directie verantwoordelijk voor het ontwikkelen van gedetailleerde richtlijnen en werkwijzen die passend zijn voor hun organisatie en moet de directie ervoor zorgen dat deze richtlijnen en werkwijzen ingebouwd worden in de operaties van de entiteit.

Verbanden tussen algemene doelstellingen en de componenten

Er bestaat een direct verband tussen de algemene doelstellingen die uitdrukken wat de entiteit wil verwezenlijken, en de interne beheersing componenten die weergeven wat er nodig is om de doelstellingen te verwezenlijken. Dit verband is uitgebeeld in een 3-dimensionele matrix in de vorm van een kubus[10].

De 4 algemene doelstellingen – rekenschap(en rapporteren), monitoring(van wetten en reglementen), (Gestructureerd, ethisch, economisch, efficiënt en effectief) operaties uitvoeren en kapitalen(middelen) beschermen- zijn als kolommen weergegeven, de 5 componenten worden in rijen weergegeven en de entiteit met haar departementen worden in de diepte weergegeven.

Elk van de componenten "snijdt" en is van toepassing op de 4 algemene doelstellingen. Bv. financiële en niet-financiële data uit interne en externe middelen, die toebehoren aan de *informatie en communicatie* component, zijn nodig om de operaties en rapporten te beheren, om rekenschap te geven en moeten voldoen aan de relevante wetten en reglementen.



Kijkend naar de algemene doelstellingen zien we dat elk van de 5 componenten hiermee in relatie staat. Bv. bij de operaties zien we dat elk van de 5 componenten invloed heeft en belangrijk is voor de verwezenlijking ervan.

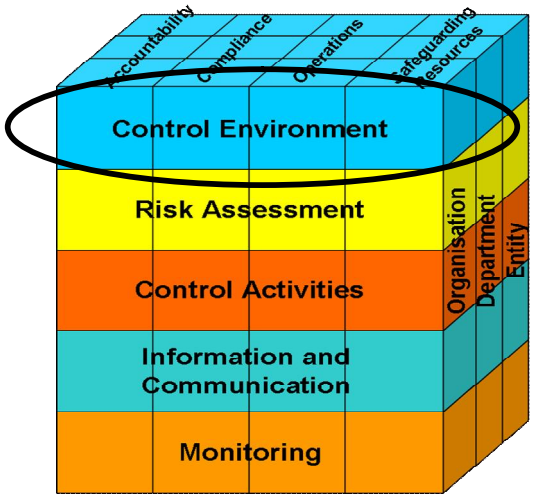
Interne beheersing is niet enkel relevant voor de entiteit maar ook voor elk van de departementen. Dit verband zien we in de 3de dimensie van de kubus die een voorstelling geeft van de organisatie in haar geheel, de entiteiten en haar departementen. Bijgevolg is elk van de cellen van de kubus van belang.

Het intern beheersing raamwerk is relevant en toepasbaar voor alle organisaties, maar de manier waarop de directie dit zal toepassen is afhankelijk van de eigenheid van de entiteit en hangt af van de specifieke karakteristieken van de entiteit. Deze zijn o.a. de organieke structuur, het risicoprofiel, het operatiedomein, grootte, complexiteit, de activiteiten en de reglementeringen. Met het in rekening brengen van de specifieke situatie van de entiteit zal de directie keuzes maken i.v.m. de complexiteit van de processen en methodes die zullen aangewend worden om de componenten van de interne beheersing toe te passen.

Het volgende deel geeft een beknopte omschrijving van de componenten met bijkomende verduidelijking erover.

10 De originele kubus werd niet vertaald en dit omwille van herkenbaarheid.

2.1 Beheersingsomgeving



De beheersingsomgeving is de basis van de organisatie en beïnvloed de toewijding aan beheersing van zijn werknemers. Het is de basis voor alle andere componenten van interne beheersing en biedt discipline en structuur.

Elementen van de beheersingsomgeving

de persoonlijke- en beroeps integriteit en de ethische waarden van de directie en het personeel, en een open, positieve houding t.o.v. interne beheersing doorheen de ganse organisatie.

Toewijding aan vakbekwaamheid

De “Tone at the Top” (de filosofie en werkwijze van de directie)

Het organigram

Human resources richtlijnen en werkwijzen.

De persoonlijke- en beroeps integriteit en de ethische waarden van de directie en het personeel

De persoonlijke- en beroeps integriteit en de ethische waarden van de directie en het personeel bepalen hun voorkeuren en waardeoordelen, die vertaald worden naar gedragsnormen. Ze moeten te allen tijde blijk geven van ondersteuning van het intern beheerssysteem doorheen de organisatie.

Elke persoon die met de organisatie te maken heeft –zowel directie als ander personeel- moet zowel op professioneel als persoonlijk vlak blijk geven van integriteit en ethische waarden en naleving van de gedragscode. Bv., het openbaar maken van persoonlijke financiële belangen, bijkomende posten en giften (door verkozen vertegenwoordigers en hoge overheidsambtenaren) en het melden van belangenvermenging.

Overheidsinstellingen moeten blijk geven van integriteit en ethische waarden, en moeten dit ook zichtbaar maken naar de gemeenschap toe door hun missie en basiswaarden. Hun operaties moeten gestructureerd, ethisch, economisch, efficiënt en effectief uitgevoerd worden. Overheidsinstellingen moeten dusdanig gestructureerd zijn dat ze hun toegewezen opdracht kunnen uitvoeren.

Toewijding aan vakbekwaamheid

Toewijding aan vakbekwaamheid gaat over het kennis- en vaardigheidsniveau dat nodig is om geordend, ethisch, economisch, efficiënt en effectief te kunnen werken en over het begrijpen van de eigen verantwoordelijkheid t.o.v. de interne beheersing.

Directie en personeel moeten hun vakbekwaamheid op een dusdanig niveau houden zodat ze een goed intern beheerssysteem kunnen ontwikkelen, implementeren en onderhouden en dat hun taken uitvoeren zodat de doelstellingen van de interne beheersing gerealiseerd kunnen worden samen met de opdracht van de organisatie. Iedereen binnen de organisatie is binnen haar eigen verantwoordelijkheden betrokken bij de interne beheersing.

De directie en kaderleden moeten hiervoor vaardigheid verwerven, onderhouden en tonen in risico-inschatting, in doeltreffend en doelgericht werken en in het begrijpen van het intern beheerssysteem zodat ze hun verplichtingen ten volle kunnen naleven.

Het aanbieden van trainingen kan bij de openbare ambtenaren zorgen voor een bewustwording van de doelstellingen van interne beheersing, de noodzaak van ethisch verantwoord werken en om vaardigheden aan te leren zodat ethische dilemma's kunnen aangepakt worden.

Tone at the top

De "Tone at the Top" (de filosofie en werkwijze van de directie)staat voor:

- dat de directie te allen tijde achter het intern beheerssysteem staat, onafhankelijk en vakbekwaam is en door voorbeeldgedrag gedreven is;
- een door de directie voorgeschreven gedragscode, waardebepalingen van vakbekwaamheid en raadgevingen die de interne beheersing ondersteunen en ethische werkwijzen ondersteunen.

Het gedrag van de directie heeft haar invloed op alle aspecten van haar acties. Haar toewijding, betrokkenheid en ondersteuning bepalen de "Tone at the top" en zorgen voor een positieve en ondersteunende houding aangaande het intern beheerssysteem van de organisatie.

Als de directie gelooft in het belang van de interne beheersing zullen de anderen in de organisatie dit voelen en zullen hierdoor de opgelegde beheersing toepassen. Bv. het oprichten van een intern audit team is een sterk signaal van de directie dat laat zien dat ze de interne beheersing belangrijk vinden.

Als echter het personeel het gevoel heeft dat beheersing niet belangrijk is voor de directie en er door de directie eerder lusteloos dan ondersteunend word gereageerd op de beheersing, dan is het bijna een zekerheid dat de beheersingsdoelstellingen niet zullen bereikt worden.

Bijgevolg is het tonen en ondersteunen van ethische verantwoord gedrag door de directie van kapitaal belang voor de doelstellingen van de interne beheersing met in het bijzonder de doelstelling van ethisch verantwoord handelen. In haar doen en laten moet de directie het voorbeeld geven door te laten zien hoe het moet en niet wat aanvaardbaar of redelijk is. De werkwijzen, procedures en daden van de directie moeten geordend, ethisch, economisch, efficiënt en effectief gedrag promoten.

De integriteit van de directie en het kader worden echter door vele factoren beïnvloed. Daarom is het noodzakelijk om het personeel regelmatig op haar verplichtingen ten opzichte van gedragscode te wijzen door voorschriften uitgevaardigd door de directie.

Waardebepalingen van vakbekwaamheid en raadgevingen zijn ook zeer belangrijk. Waardebepaling van het algemeen functioneren, moet gebaseerd worden op veel kritische factoren met inbegrip van de rol van het personeel in het uitvoeren van de interne beheersing.

Structuur van de organisatie

De structuur van een organisatie toont

- Toewijzing van gezag en verantwoordelijkheden:
- Bevoegdheden en rekenschap;
- Juiste volglijnen voor het rapporteren.

Het organigram van de organisatie definieert de belangrijkste beleids- en verantwoordelijkheidsdomeinen. Bevoegdheden en rekenschap hebben betrekking op de manier waarop deze bevoegdheid en verplichting tot afleggen van rekenschap doorheen de organisatie wordt gedelegeerd. Er kan geen sprake zijn van bevoegdheid en rekenschap zonder dat er aan rapportering word gedaan. Daarom moeten de correcte volglijnen van rapporteren worden weergegeven. Daarnaast moeten er ook bijkomende lijnen uitgetekend worden voor uitzonderlijke gevallen als bijvoorbeeld op niveau van de directie onregelmatigheden gebeuren.

De structuur kan ook een intern audit team bevatten dat onafhankelijk van de directie is en direct aan de hoogste echelons rapport uitbrengt.

De structuur wordt ook besproken in hoofdstuk 3 bij taken en verantwoordelijkheden.

Human resources richtlijnen en werkwijzen

Human resources richtlijnen en werkwijzen omvatten aanwerving en plaatsing, oriëntering, training (formeel en on-the-job) en opleiding, evalueren en raad geven, promoten (belonen), compenseren en remediëren.

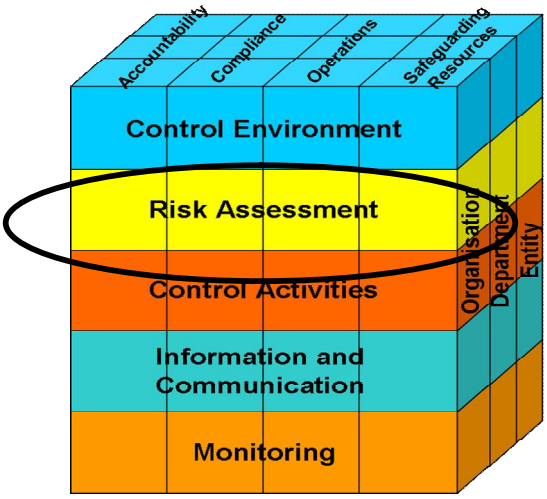
Een belangrijke factor in de interne beheersing is personeel. Competent, betrouwbaar personeel is noodzakelijk voor een efficiënte interne beheersing. Daarom is de manier waarop personeel word aangeworven, getraind, geëvalueerd, beloond en bevorderd een belangrijke factor van de Beheersingsomgeving. De beslissingen aangaande aanwerving en inplaatsstelling moeten daarom zekerheid verschaffen over de integriteit en de juiste opleiding en ervaring die vereist zijn om hun job uit te oefenen en dat de juiste formele, on-the-job en ethische training worden gegeven. Kaderleden en personeel die een goed inzicht in interne beheersing hebben en verantwoordelijkheid willen opnemen zijn van vitaal belang voor een goede interne beheersing.

Human resources management speelt een essentiële rol in bevorderen van een ethische omgeving door het aanmoedigen van professionalisme en door openhartigheid in de dagelijkse omgang. Dit laat zich zien in de aanwerving, vakbekwaamheids-evaluatie en promoties –deze moeten het gevolg zijn van verdienstelijkheid. Zorgen voor openheid in de selectieprocedures door het publiceren van de aanwervingcriteria en de openstaande betrekkingen helpt om een ethisch human resources proces te realiseren.

Voorbeelden

We verwijzen de lezer naar de Bijlage A voor voorbeelden van de doelstellingen en onderdelen van interne beheersing.

2.2 Risicoanalyse



Risicoanalyse is het identificatie- en analyseproces van risico's dat het behalen van de doelstellingen kan beïnvloeden en nodig is voor het bepalen van de gepaste reacties.

Het bevat:

(1) Risico identificatie

* Van invloed op de doelstellingen van de entiteit;

* Groot in omvang;

* Voortkomend uit interne of externe factoren zowel op vlak van de organisatie als de activiteiten;

(2) Risico-evaluatie:

* Schatten van de belangrijkheid van het risico;

* Inschatten van de waarschijnlijkheid van voorkomen;

(3) Bepalen van de risicobereidheid van de organisatie;

(4) Bepalen van de reacties:

* 4 types van reactie moeten overwogen worden: verplaatsing, tolerantie, oplossing of verwijdering. Van deze is het oplossen van de problemen het meest relevant voor deze richtlijnen omdat doeltreffende interne beheersing het beste mechanisme is om problemen aan te pakken;

* De geschikte beheersing kan bestaan uit maatregelen voor vroegtijdig ontdekken of maatregelen ter preventie van de risico's.

Omdat bestuurlijke-, economische-, industriële-, wetgevende- en uitvoeringsomstandigheden voortdurend veranderen is het van belang dat risico inschatting een voortdurend interactief proces is. Het betekent het identificeren van veranderende omstandigheden, mogelijkheden en risico's en het aanpassen van de interne beheersing om deze veranderingen op te vangen.

Zoals gesteld in de definitie kan interne beheersing enkel een redelijke mate van zekerheid bieden voor het bereiken van de doelstellingen van de organisatie.

Risico inschatting als onderdeel van de interne beheersing speelt een sleutelrol in het selecteren van de gepaste beheersingsmaatregelen. Het is het proces van identificatie en analyse van de relevante risico's voor het bereiken van de doelstellingen en het bepalen van de gepaste maatregelen.

Daarom is het bepalen van de doelstellingen de eerste vereiste van de risico inschatting. De doelstellingen moeten bepaald zijn alvorens de directie de risico's kan opsporen en de nodige maatregelen kan opstellen. Hiervoor is het nodig dat er een betaalbaar en voortdurend proces van evaluatie en aanpak van de impact van de risico's is en dat er personeel is dat de benodigde kennis en expertise heeft om de risico's te herkennen en te analyseren. Interne beheersingsmaatregelen zijn een antwoord op risico's omdat ze ontworpen zijn om de onzekerheid betreffende het bereiken van de doelstellingen in te dijken.

Besturen moeten risico's, die waarschijnlijk een impact hebben op de dienstverlening en de vooropgestelde resultaten, aanpakken.

Risico identificatie

Een strategische aanpak van risico inschatting is afhankelijk van het herkennen van risico's die van invloed zijn op de belangrijkste doelstellingen van de organisatie. Relevante risico's worden bekeken en geëvalueerd en dit moet resulteren in een aantal sleutelrisico's.

De identificatie van deze sleutelrisico's is niet enkel van belang in het kader van de aanwending van middelen in de bestrijding ervan, maar ook om de verantwoordelijken voor de aanpak aan te duiden.

De werking van een entiteit kan risico's lopen door interne en externe factoren zowel op gebied van de organisatie als haar werkzaamheden. Risico inschatting moet rekening houden met alle risico's die kunnen voorkomen.(met inbegrip van het risico op fraude en corruptie). Daarom moet risico identificatie zeer uitgebreid zijn. Risico identificatie moet een doorlopend, interactief proces zijn en is meestal geïntegreerd in het planningsproces. Het is dikwijl goed om de risico's te bekijken vanuit het vertrekpunt van een blanco blad en niet uitsluitend voort te gaan op vroegere vaststellingen. Deze aanpak vergemakkelijkt de identificatie van veranderingen in het risico profiel[11] van een organisatie die voortkomen uit veranderingen op economisch of wetgevend gebied, interne en externe omstandigheden en het invoeren van nieuwe of hertekende doelstellingen.

Het is nodig om de juiste middelen aan te wenden voor de identificatie van risico's. Twee van de meest gebruikte zijn het opleggen van een risico-evaluatie en risico-zelfanalyse.[12]

Risico-evaluatie

Om te kunnen beslissen hoe een risico aangepakt moet worden is het niet alleen noodzakelijk om te identificeren dat er een bepaald type van risico bestaat, maar ook om in te schatten hoe hoog dat risico is en wat de waarschijnlijkheid is dat het zich zal voordoen. De manier om een risico te analyseren kan zeer verschillend zijn. Vooral om dat sommige risico's moeilijk te becijferen zijn (bv. imago risico's) terwijl anderen juist gemakkelijk te becijferen zijn (financiële risico's). Voor de eerste groep is een subjectieve kijk op het risico de enige mogelijkheid. Vandaar dat risicoanalyse meer een kunst dan een wetenschap is. Nochtans zal het gebruiken van systematische waarderingscriteria de subjectiviteit van het

11 Een overzicht of matrix van de belangrijkste risico's waarmee een entiteit of afdeling mee te maken kan krijgen en dat het niveau van impact (Bv.: laag, middelmatig, hoog) weergeeft samen met de waarschijnlijkheid of zekerheid van voorkomen.

12 Opleggen van een risico analyse.
Dit is een procedure vanuit de top van de organisatie. Een team wordt samengesteld om alle operaties en activiteiten van de organisatie te bekijken in functie van de doelstellingen en hierbij de mogelijke risico's te identificeren. Het team voert gesprekken met sleutelpersoneel op alle niveaus van de onderneming om een risicoprofiel op te stellen voor de volledige omvang van de activiteiten om zo de werkwijzen, activiteiten en functies die kwetsbaar zijn te ontdekken. (met inbegrip van het risico op fraude en corruptie).

Risico-zelfanalyse
Dit is een procedure vanuit de basis van de organisatie. Elk niveau en elke afdeling van de organisatie wordt gevraagd om haar activiteiten te onderzoeken en de risico's naar boven toe te zoeken. Dit kan gebeuren via een gedocumenteerde aanpak (Met een raamwerk voor dit onderzoek door het beantwoorden van vragenlijsten) of door het aanbieden van workshops om het onderzoek te ondersteunen.

Beide aanpakken sluiten elkaar niet uit en een combinatie van inputs van bovenaf en onderuit voor de risico-evaluatie is wenselijk voor de identificatie van risico's op niveau van de afdelingen en doorheen de volledige organisatie.

evaluatieproces beïnvloeden door een raamwerk aan te reiken waardoor de evaluatie op een meer constante manier kan gebeuren.

Een van de voornaamste redenen van risicoanalyse is om de directie in te lichten over risicogebieden waarop actie moet worden genomen en hun prioriteit. Daarom zal het nodig zijn om een soort van classificatie systeem te ontwikkelen Bv.: hoog, middel of laag. Normaal gezien is het beter om niet te veel gradaties te hanteren want te veel gradaties kunnen leiden tot opsplitsingen die in realiteit niet mogelijk zijn.

Door deze classificatie kunnen de risico's geordend worden zodat er prioriteiten kunnen worden gesteld en kan er informatie aangereikt worden zodat de directie kan beslissen welke risico's aangepakt moeten worden. (Bv. risico's met een potentieel grote invloed op de operaties en met een hoge waarschijnlijkheid van voorkomen.)

Bepalen van de risicobereidheid van de organisatie

Een belangrijke factor in het bepalen van de aanpak van het risico is de risicobereidheid van de entiteit. Risicobereidheid is de mate waarin een entiteit bereid is aan het risico blootgesteld te worden alvorens ze actie zal ondernemen. Beslissingen i.v.m. met de aanpak van een risico moeten genomen worden samen met de identificatie van de mate waarin men bereid is het risico te aanvaarden.

Zowel inherente als restrisico's moeten in overweging worden genomen bij het bepalen van de risicobereidheid. Inherente risico's zijn risico's die de entiteit zou lopen zonder dat er maatregelen zouden worden genomen om zowel de impact als de waarschijnlijkheid van voorkomen te beïnvloeden. Restrisico is het risico dat blijft bestaan nadat er actie werd ondernomen.

De risicobereidheid van een organisatie zal variëren naargelang de ingeschatte belangrijkheid van een risico. Bv. een aanvaardbaar financieel verlies kan variëren naargelang de grootte van het initieel budget, de reden van het verlies, of een bijkomend risico als negatieve publiciteit. De bepaling van de risicobereidheid is een subjectief gegeven maar het is toch een belangrijke factor bij het bepalen van de algemene risicostrategie.

Bepalen van de reacties

Het resultaat van de hierboven beschreven actie is het risicoprofiel van de organisatie. Eens een risicoprofiel is opgesteld, kan de organisatie beginnen nadenken over de gepaste reacties.

Reacties op risico's kunnen in 4 categorieën ingedeeld worden. Soms kan een risico overgedragen, aanvaard of verwijderd[13] worden. In de meeste gevallen echter zal het risico behandeld moeten worden en zal de entiteit een doeltreffend intern beheerssysteem moeten ontwikkelen en onderhouden om het risico op een aanvaardbaar niveau te houden.

Het doel van het behandelen van een risico is niet noodzakelijk het wegwerken maar eerder het onder controle houden. De procedures die een organisatie uitwerkt om een risico te behandelen worden interne beheersingsmaatregelen genoemd. De risicoanalyse moet een belangrijke rol spelen in het bepalen van de geschikte interne beheersingsmaatregelen. We moeten hier opnieuw onderstrepen dat het onmogelijk is om alle risico's volledig uit te sluiten. Interne beheersing kan enkel voor een redelijke mate van zekerheid zorgen voor het bereiken van de doelstellingen van de organisatie. Entiteiten die actief aan identificatie van risico's en risicomanagement doen zijn meestal beter gewapend om snel te reageren wanneer het mis loopt en zijn ook beter in staat om op veranderingen te reageren.

13 Voor sommige risico's kan de beste oplossing het overdragen van het risico zijn. Dit kan gebeuren door een gewone verzekeringspolis, door het betalen van een derde om het risico op een andere manier over te nemen of door contractuele voorwaarden. De mogelijkheid om iets te ondernemen tegen bepaalde risico's kunnen beperkt zijn, of de kosten van eender welke actie kunnen buiten proportie zijn tegenover de potentiële voordelen van die actie. In zulke gevallen is het soms beter het risico gewoon te aanvaarden. Sommige risico's kunnen alleen op te lossen of te beheersen zijn door het stoppen van een bepaalde activiteit. In de openbare sector kan de optie om een bepaalde activiteit te stoppen erg beperkt zijn ten opzichte van de private sector. Sommige activiteiten worden door de openbare instellingen uitgevoerd omdat ze voor de private sector te veel risico's inhouden en het niet mogelijk is om de doelstelling of het resultaat, dat voor de burger nodig is, te kunnen bereiken.

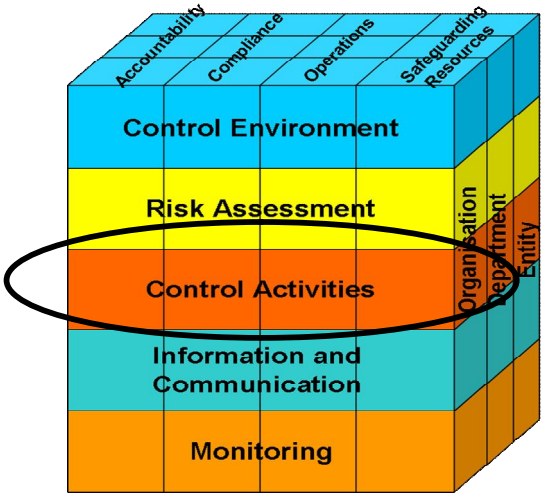
Bij het ontwerpen van een intern beheerssysteem is het belangrijk dat de beheersingsmaatregel in verhouding staat tot het risico. Geen actie ondernemen brengt een onaanvaardbaar verlies met zich mee. Meestal is het voldoende om een beheersing te ontwerpen die een redelijke zekerheid bied om het verlies te kunnen terugbrengen tot de grenzen van de risicobereidheid van de organisatie. Elke beheersing brengt kosten met zich mee en de kost van de beheersing moet in verhouding zijn tot het risico dat wordt aangepakt.

Omdat de bestuurlijke-, economische-, industriële- en wetgevende situaties en de werkingscondities constant wijzigen, zal de risico-omgeving van de organisatie ook constant wijzigen en bijgevolg zullen de prioriteiten en de doelstellingen en de hieraan verbonden risico's ook voortdurend veranderen. Basis van de risicoanalyse is een voortdurend, interactief proces om de veranderende condities te herkennen (risicoanalyse kringloop) en het nemen van de benodigde acties. Risicoprofielen en de gekoppelde beheersingsmaatregelen moeten regelmatig herbekeken en gewijzigd worden zodat er zekerheid is dat het risicoprofiel nog up-to-date is, dat de reacties op risico's nog steeds doeltreffend zijn en dat de beperkende beheersingsmaatregelen nog doeltreffend blijven op de veranderende risico's.

Voorbeelden

We verwijzen de lezer naar de Bijlage A voor voorbeelden van de doelstellingen en onderdelen van interne beheersing.

2.3 Beheersingsmaatregelen



Beheersingsmaatregelenzijn de werkwijzen en procedures die opgesteld werden om de risico's te beheersen en de doelstellingen van de entiteit te verwezenlijken.

Om doeltreffend te zijn, moeten de beheersingsmaatregelen toepasselijk zijn en zoals gepland voor de ganse periode operationeel zijn. Daarbij moeten ze kosteneffectief, veelomvattend en redelijk zijn en direct verband houden met de beheersingsdoelstellingen.

Beheersingsmaatregelen gebeuren doorheen gans de organisatie, op alle niveaus en in alle functies. Ze omvatten een gamma aan opsporings- en preventieve beheersingsmaatregelen zoals:

(1) toestemmings- en goedkeuringsprocedures;

(2) splitsing van taken (toelaten, verwerken, inbrengen, nazicht);

(3) beheer van de toegang tot middelen en data;

(4) nazicht;

(5) overeenstemming;

(6) nazicht van de werking;

(7) nazicht van de operaties, processen en activiteiten;

(8) toezicht (toewijzingen, nazicht en goedkeuring, leiding en training).

Entiteiten moeten een evenwicht zoeken tussen opsporings- en preventieve beheersingsmaatregelen.

Correctieve acties zijn een noodzakelijke toevoeging aan de beheersingsmaatregelen om de doelstellingen te bereiken.

Beheersingsmaatregelen zijn de werkwijzen en procedures die opgesteld werden om de risico's te beheersen en doelstellingen van de entiteit te verwezenlijken

Om doeltreffend te zijn moeten de beheersingsmaatregelen:

- toepasselijk zijn (de juiste beheersing op de juiste plaats en proportioneel tot het risico);
- zoals gepland voor de ganse periode operationeel zijn (steeds opgevolgd door gans het personeel en niet terzijde gelaten als het sleutelpersoneel niet aanwezig is of als de werklast verhoogt);

- kosteneffectief zijn (de kosten van het uitvoering van de beheersing mogen niet hoger zijn dan de opbrengsten die eruit voortkomen);
- veelomvattend en redelijk zijn en direct verband houden met de beheersingsdoelstellingen.

Beheersingsmaatregelen omvatten een veelvoud aan werkwijzen en procedures die zeer uiteenlopend kunnen zijn, zoals:

1. toestemmings- en goedkeuringsprocedures

Het toelaten en uitvoeren van transacties en gebeurtenissen word enkel gedaan door personen die hiervoor het gezag hebben. Toelating is het belangrijkste middel om zekerheid te hebben dat enkel door het management goedgekeurde transacties en gebeurtenissen worden uitgevoerd. Toelatingsprocedures, die uitvoerig moeten gedocumenteerd zijn en duidelijk gecommuniceerd worden aan de managers en ander personeel, moeten duidelijk vermelden onder welke omstandigheden en voorwaarden toelating mag worden gegeven. Het naleven van de voorwaarden voor toelating betekend dat het personeel handelt in overeenstemming met de richtlijnen en binnen de grenzen die door het management en de wetgever zijn bepaald.

2. splitsing van taken (toelaten, verwerken, inbrengen, nazicht)

Om het risico op fouten, verspilling en inbreuken en het niet ontdekken ervan te beperken, mag er nooit één persoon of één team het beheer over alle stappen van een transactie of gebeurtenis hebben. Taken en verantwoordelijkheden moeten systematisch toebedeeld worden aan een aantal personen om zekerheid te verkrijgen dat doeltreffende controle en evenwicht word verkregen. Deze verantwoordelijkheden omvatten het toelaten en optekenen van transacties, het uitvoeren en opvolgen of audit acties. Complotten kunnen een interne beheersingsmaatregel ondermijnen of tenietdoen. Een kleine organisatie kan echter te weinig personeel hebben om deze splitsing van taken volledig toe te passen. In zulk geval moet het management dit compenseren met andere beheersingsmaatregelen. Rotaties in de posten van tewerkstelling kunnen helpen voorkomen dat één persoon alle stappen van een transactie of gebeurtenis moet blijven uitvoeren gedurende een lange periode. Ook het aanmoedigen of verplichten van jaarlijkse verloven kunnen risico verlagend werken door de tijdelijke personeelsrotatie die ze teweeg brengen.

3. beheer van de toegang tot middelen en data

Toegang tot middelen en data is beperkt tot personen met de toelating hiervoor en die ook verantwoordelijk zijn voor de bewaking en/of gebruik van middelen. Verantwoording voor de bewaking wordt afgelegd door het bestaan van ontvangstbewijzen, inventarissen, of andere documenten die de toewijzing van deze bewaking (bescherming) documenteren en het optekening van de overdracht van de bewaking. Toegang tot de middelen beperken zorgt voor een verminderd risico op ongeoorloofd gebruik of verlies en draagt bij tot het uitvoeren van de richtlijnen van het management. De graad van beperking is afhankelijk van de kwetsbaarheid van de middelen en het ingeschatte risico op verlies of onrechtmatig gebruik, en deze kwetsbaarheid moet regelmatig opnieuw ingeschat worden. Bij het bepalen van de kwetsbaarheid van een van de middelen, moet er rekening worden gehouden met de kostprijs, overdraagbaarheid en omwisselbaarheid ervan.

4. nazicht

Transacties en belangrijke gebeurtenissen moeten nagekeken worden voor en na de uitvoering ervan. Bv., Bij de levering van goederen, moet er nagekeken worden of het geleverde aantal overeenstemt met het bestelde aantal. Nadien moet er nagekeken worden of het gefactureerde aantal ook overeen stemt met het geleverde aantal. De inventaris wordt ook gecheckt door inventariscontroles.

5. overeenstemming

Gegevens moeten op regelmatige basis nagekeken worden op hun overeenstemming met de voorhanden zijnde documenten. Bv., de gegevens van de bankrekeningen moeten in overeenstemming zijn met de rekeninguittreksels.

6. nazicht van de werking

De operationele werking van de organisatie wordt op regelmatige tijdstippen vergeleken met opgestelde standaards om de doeltreffendheid en doelmatigheid te toetsen. Indien blijkt dat deze vergelijking aantoont dat de werking niet aan de gestelde objectieven en standaards beantwoord, moeten de processen en activiteiten die werden opgesteld herbekeken worden om te bepalen of er verbeteringen moeten doorgevoerd worden.

7. nazicht van de operaties, processen en activiteiten

Operaties, processen en activiteiten moeten regelmatig nagekeken worden om er zeker van te zijn dat ze in overeenstemming zijn met de geldende reglementeringen, werkwijzen, procedures en andere vereisten. Dit nazicht van de actuele operaties van een organisatie moet duidelijk gescheiden worden gezien van de monitoring van de interne beheersing.

8. toezicht (toewijzingen, nazicht en goedkeuring, leiding en training)

Competent toezicht helpt om de objectieven van de interne beheersing te bereiken. Het toewijzen van, het toezicht op en de goedkeuring van het werk van een personeelslid omvat:

- Duidelijk communiceren van de verplichtingen, verantwoordelijkheden en de verantwoording van elk personeelslid;
- Systematisch toezicht op het werk van elk van de personeelsleden in de mate van het noodzakelijke;
- Goedkeuring van het werk op kritische ogenblikken zodat de voortgang gewaarborgd wordt.

Het delegeren van werk door een toezichthouder mag geen afbreuk doen aan de verantwoording die de toezichthouder draagt voor deze verantwoordelijkheden en taken. Toezichthouders zorgen ook voor de nodige leiding en training van hun personeel om te voorkomen dat er fouten worden gemaakt, er misbruik wordt gemaakt en dat de voorschriften van het management begrepen en uitgevoerd worden.

Bovenvermelde opsomming is geen beperkende lijst maar wel een opsomming van de meest courante preventieve- en opsporingsactiviteiten. Beheersingsmaatregelen 1 – 3 zijn preventieve acties. Nummers 4 – 6 zijn opsporingsacties. Nummers 7 en 8 behoren tot beide categorieën. Entiteiten moeten tot een evenwicht komen tussen de preventieve- en opsporingsacties waarbij er veelal een mix van activiteiten zal worden gebruikt om de nadelen van individuele controles te beperken.

Eens een beheersingsmaatregel geïmplementeerd is, is het essentieel dat er zekerheid over de doeltreffendheid ervan word verkregen. Bijgevolg moeten er bijsturingen worden doorgevoerd om de beheersingsmaatregelen aan te vullen. Het moet ook duidelijk zijn dat de beheersingsmaatregelen maar 1 component van de interne beheersing zijn. Ze moeten dan ook geïntegreerd worden met de 4 andere componenten.

Voorbeelden

We verwijzen de lezer naar de Bijlage A voor voorbeelden van de doelstellingen en onderdelen van interne beheersing.

2.3.1 Information Technologie Beheersingsmaatregelen.

Information Technology (IT) systemen vereisen specifieke types beheersingsmaatregelen. Dit bestaan uit 2 grote groepen.

(1) Algemene beheersing
Algemene beheersing omvatten de structuur, de werkwijzen en procedures die van toepassing zijn op alle of een groot gedeelte van de IT systemen van een entiteit en die helpen zorgen voor een correct functioneren ervan. Ze vormen de omgeving waarin de toepassingen werken en de beheersing gebeurt.

De belangrijkste categorieën van de algemene beheersing zijn
1- beveiligingsplanning en uitvoering doorheen de ganse structuur van de entiteit.
2- Toegangscontrole
3- Controle op de ontwikkeling, het onderhoud en wijziging van de toepassingssoftware
4- Systeemsoftware controle
5- Scheiding van taken
6- beschikbaarheid van de diensten

(2) Beheersing van de toepassingen
Beheersing van de toepassingen zijn de structuren, werkwijzen en procedures die betrekking hebben op afzonderlijk, individuele toepassingen, en staan in direct verband met individuele gecomputeriseerde toepassingen. Deze beheersing is meestal opgezet om fouten en onregelmatigheden tijdens de informatiestroom doorheen de IT systemen te voorkomen, te ontdekken en te corrigeren.

Algemene beheersing en beheersing van de toepassingen zijn met elkaar verweven en beide zijn nodig om volledige en accurate verwerking van informatie te bekomen. Omdat IT onderhevig is aan snelle veranderingen moet ook de gekoppelde beheersing constant evolueren om doeltreffend te blijven.

Met de vooruitgang van de IT zijn organisaties steeds meer afhankelijk geworden van gecomputeriseerde informatie systemen voor het uitvoeren van hun operaties en om essentiële informatie te verwerken, bij te werken en te rapporteren. Het gevolg hiervan is dat de betrouwbaarheid en veiligheid van data en de systemen om deze te verwerken, bij te werken en te rapporteren een belangrijke zorg is van het management en auditoren. Ook al zijn er voor deze informatica systemen specifieke beheersingsmaatregelen nodig, toch is IT geen “Stand-alone” beheersingsitem. Het is een integraal onderdeel van de meeste beheersingsmaatregelen.

Het gebruik van geautomatiseerde systemen voor het verwerken van informatie brengt nieuwe risico's waarmee de organisatie rekening zal moeten houden. Deze risico's zijn, onder andere, het gevolg van het uniform verwerken van transacties; automatisch geïnitieerde transacties door het systeem; mogelijke verhoging van niet gedetecteerde risico's; het bestaan, de volledigheid en het volume aan auditsporen (audit rails); de gebruikte hardware en software; en het verwerken van ongewone of niet-routine transacties. Bv., een inherent risico van het uniform verwerken van transacties is dat indien er een fout door de programmatie voorkomt in de verwerking, deze fout zich doorheen alle gelijkaardige transacties zal voordoen. Doeltreffende IT beheersing kan het management een redelijke mate van zekerheid geven dat de verwerkte informatie de gestelde beheersingsdoelstellingen zoals: volledigheid, stiptheid van rapporteren, de geldigheid van de informatie en het behouden van de integriteit van de informatie, kan vervullen.

IT beheersing bestaat uit 2 grote groepen, Algemene beheersing en beheersing van de toepassingen.

Algemene beheersing

Algemene beheersing omvatten de structuur, de werkwijzen en procedures die van toepassing zijn op alle of een groot gedeelte van de IT systemen van een entiteit en die helpen zorgen voor een correct

functioneren ervan. Ze vormen de omgeving waarin de toepassingen werken en de beheersing gebeurt. De belangrijkste categorieën van de algemene beheersing zijn:

(1) Beveiligingsplanning en uitvoering doorheen de ganse structuur van de entiteit zorgt voor een raamwerk en een voortdurende cyclus van: risico management, nieuwe ontwikkeling van veiligheidsvoorschriften, toewijzing van verantwoordelijkheden en monitoring van de correctheid van de computer-gerelateerde beheersing.

*(2) Toegangscontrole b*eperkt of ontdekt toegang tot computers (data, progamma's, uitrusting) en fysieke plaatsen waardoor deze middelen beschermd worden tegen ongeoorloofde wijzigingen, verlies en verspreiding van gegevens. Deze toegangscontrole omvat fysieke en logische controles.

*(3) Controle op de ontwikkeling, het onderhoud en wijziging van de toepassingssoftware v*oorkomt het gebruik van niet-toegelaten programma's en aanpassingen aan bestaande programma's.

*(4) Systeemsoftware controles b*eperken en registreren de toegang tot de krachtige programma's en gevoelige informatie die de computerhardware besturen en beveiligen de toepassingen die op deze platforms draaien.

(5) Functiescheiding houdt in dat werkwijzen, procedures en een organigram worden opgesteld die moeten voorkomen dat één persoon controle heeft over alle belangrijke aspecten van de computer gerelateerde operaties en die bijgevolg ongeoorloofde acties kan uitvoeren of ongeoorloofd toegang zou hebben tot data of middelen.

(6) Bedrijfszekerheid van de diensten zorgt ervoor dat bij onverwachte gebeurtenissen, de belangrijkste operaties kunnen blijven doorgaan zonder onderbreking of na een onderbreking onmiddellijk kunnen worden hervat.

Beheersing van de toepassingen

Beheersing van de toepassingen zijn de structuren, werkwijzen en procedures die betrekking hebben op afzonderlijke, individuele toepassingen, zoals: betaalmodules, inventarissen, loonadministratie, beurzen en leningen; en die ontworpen zijn voor het verwerken van data in deze specifieke toepassingen.

Deze beheersmiddelen zijn over het algemeen ontworpen om onregelmatigheden in het verwerkingsproces te voorkomen, te detecteren en recht te zetten.

Beheersing van de toepassingen en de manier waarop informatie door het systeem word verwerkt kan opgesplitst worden in drie fases.

- input: gegevens worden aanvaard en verwerkt in een geautomatiseerd formulier en ingebracht in de toepassing op een accurate en volledige wijze op het ogenblik dat het moet ingebracht worden.
- verwerking: De gegevens worden door de computer verwerkt en de bestanden worden correct geüpdatet.
- output: Bestanden en rapporten gegenereerd door de toepassing weerspiegelen de transacties of gebeurtenissen die plaatsvonden en geven het resultaat van de verwerking correct weer. De rapporten worden gecontroleerd en verdeeld aan de bestemmelingen.

Beheersing van de toepassingen kan ook gecategoriseerd worden volgens de controledoelstellingen waartoe ze behoren, met inbegrip van het feit dat de transacties en informatie toegelaten, volledig, accuraat en geldig zijn. Beheersing van de toelatingen omvat de geldigheid van de transactie en helpen ervoor te zorgen dat de transacties de gebeurtenissen over een bepaalde tijdspanne weergeven. Beheersing van de volledigheid betekend dat de transactie correct werd opgetekend en dat de gegevens juist waren. Beheersing van de accuratesse van de gegevens kan, indien niet doeltreffend, het resultaat van de bovenvermelde beheersing van de toepassingen teniet doen en ertoe bijdragen dat niet-geoorloofde transacties plaatsvinden. Dit kan ook leiden tot onvolledige en niet-correcte gegevensuitvoer.

Beheersing van de toepassingen omvatten geprogrammeerde beheersingsmaatregelen en manuele monitoring van de outputs door nazicht van de rapporten en identificatie van verworpen of ongewone items.

Algemene beheersing en beheersing van de toepassingen zijn met elkaar verweven.

De doeltreffendheid van de algemene beheersing is een belangrijke factor in het bepalen van de doeltreffendheid van de beheersing van de toepassingen. Slechte algemene beheersing zorgt voor een verminderde betrouwbaarheid van de beheersing van de individuele toepassingen. Zonder doeltreffende algemene beheersing zou de beheersing van de toepassingen kunnen worden genegeerd, omzeild of aangepast. Bv. een editor checker die voorkomt dat er te hoge aantallen werkuren worden ingebracht in een betaalmodule (bv. meer dan 24/dag) kan een sterk beheersmiddel zijn in de toepassing. Als echter de algemene beheersing toelaat om veranderingen in het progamma aan te brengen, kan deze transactie toch mogelijk gemaakt worden.

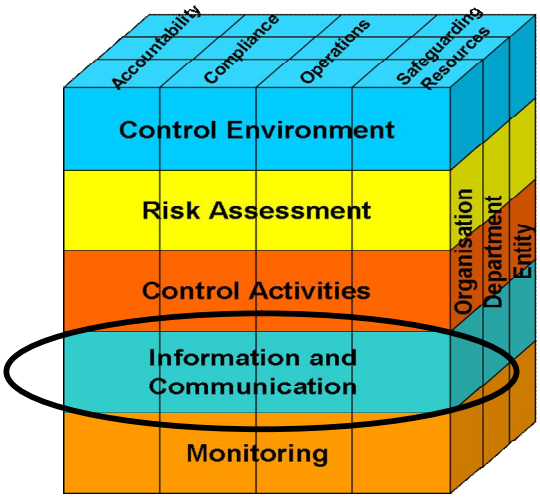
Hoewel de basisdoelstellingen van de beheersing niet veranderen, zorgen de snelle veranderingen in de IT ervoor dat er noodzaak is aan evolutie in de beheersing om effectief te blijven. Veranderingen als: de groeiende afhankelijkheid van en het vertrouwen in netwerken, krachtige computers die de eindverantwoordelijkheid van verwerking in de handen leggen van de eindgebruiker, electronic commerce en het internet; beïnvloeden de aard en de toepassing van gerichte beheersingsmaatregelen.

Meer richtlijnen in verband met beheersing van IT kunnen bekomen worden van de Information System Audit and Control Association (ISACA), in het bijzonder het ISACA Control Objectives for Information an Related Technology (COBIT) referentiekader en de handelingen van het INTOSAI IT-audit comité.

Voorbeelden

We verwijzen de lezer naar de Bijlage A voor voorbeelden van de doelstellingen en onderdelen van interne beheersing.

2.4 Informatie en Communicatie



Informatie en communicatie zijn essentieel voor het realiseren van de interne beheersing.

Informatie

Voorwaarde voor betrouwbare en relevante informatie is het onmiddellijk optekenen en correct catalogeren van de transacties en gebeurtenissen. Betekenisvolle informatie moet worden herkend, bijgehouden en gecommuniceerd in een zodanige vorm en binnen een dusdanige termijn dat het kader (leiding) hun verantwoordelijkheid binnen de interne beheersing en andere domeinen kan nemen (tijdige communicatie aan de juiste persoon). Daarom moeten zowel de interne beheersing op zich en de transacties en belangrijke gebeurtenissen volledig gedocumenteerd worden.

Informatica systemen zorgen ervoor dat er rapporten worden gemaakt die operationele, financiële en niet-financiële informatie bevatten en dat er rapporten komen over de naleving van de wetten en reglementen die ervoor zorgen dat de beheersing en de operaties kunnen worden uitgevoerd.

Het kunnen nemen van de juiste beslissingen door het management wordt sterk beïnvloed door de kwaliteit van de informatie, wat inhoud dat de informatie relevant, recent, accuraat en toegankelijk moet zijn, en tijdig moet worden doorgegeven.

Informatie en communicatie zijn essentieel voor het realiseren van alle interne beheersing doelstellingen. Bv. Het afleggen van rekenschap. Dit kan gerealiseerd worden door het ontwikkelen en onderhouden van betrouwbare en relevante financiële en niet-financiële informatie en het doorgeven van deze informatie in een eerlijk en tijdig opgesteld rapport. Informatie en communicatie over de werking van de organisatie schept de mogelijkheid om te evalueren of de operaties geordend, ethisch, economisch, efficiënt en effectief verlopen. In veel gevallen zal er informatie moeten worden verstrekt over het naleven van de wetten en reglementen.

Informatie is nodig op elk niveau van de organisatie zodat er een doeltreffende interne beheersing kan zijn en dat de doelstellingen van de entiteit kunnen worden bereikt. Daarom moet er een waaier aan pertinente, betrouwbare en relevante informatie worden gezocht, opgetekend en doorgegeven in een dusdanige vorm en binnen een dusdanige termijn dat iedereen zijn taken binnen de interne beheersing en zijn andere verantwoordelijkheden kan vervullen. Voorwaarde voor betrouwbare en relevante informatie is het onmiddellijk optekenen en correct catalogeren van transacties en gebeurtenissen.

Transacties en gebeurtenissen moeten onmiddellijk bij voorkomen opgetekend worden om ervoor te zorgen dat de informatie relevant en waardevol blijft zodat het management de juiste beheersingsmaatregelen kan doorvoeren en de juiste beslissingen kan nemen. Dit is van toepassing op het volledige verloop van gebeurtenissen of transacties (met inbegrip van het verstrekken van toelating ervan en het lanceren) en in

het catalogeren in de eindrapporten. Het is ook van toepassing op het onmiddellijk aanpassen van de documentatie zodat deze steeds relevant blijft.

Correct catalogeren van transacties en gebeurtenissen is ook noodzakelijk voor het verstrekken van betrouwbare informatie aan het management. Dit betekend het organiseren, categoriseren en bewerken van de informatie zodat deze gebruikt kan worden voor het opstellen van verslagen, schema's en financiële rapporten.

Informatica systemen zorgen ervoor dat er rapporten worden gemaakt die operationele, financiële en niet-financiële informatie bevatten en dat er rapporten komen over de naleving van de wetten en reglementen en ze maken het mogelijk om de operaties uit te voeren en te beheersen. Het systeem houdt niet alleen rekening met intern gegenereerde vormen van kwantitatieve en kwalitatieve gegevens maar ook met informatie over externe gebeurtenissen, activiteiten en voorwaarden die nodig zijn voor het nemen van de juiste beslissingen en de opmaak van rapporten.

De vaardigheid van het management op gebied van het nemen van beslissingen wordt beïnvloed door de kwaliteit van de verstrekte informatie.

Daarom moet deze informatie:

- Relevant zijn (Is deze info hier nodig?)
- Op tijd zijn (Is deze info beschikbaar als ze nodig is?)
- Recent zijn (Is dit de laatste informatie waarover we beschikken?)
- Accuraat zijn (Is deze informatie wel correct?)
- Toegankelijk zijn (Is de informatie beschikbaar voor wie ze nodig heeft?)

Om ervoor te zorgen dat de kwaliteit van de informatie en het rapporteren, het uitvoeren van de interne beheersing en verantwoordelijkheden en het opvolgen van de operaties doeltreffend en doelgericht is, moet de interne beheersing op zich, en alle transacties en gebeurtenissen, volledig en duidelijk gedocumenteerd worden (Flow-charts, beschrijvingen,....). Deze documentatie moet steeds beschikbaar zijn voor gebruik.

Documentatie van het intern beheerssysteem moet ook handelen over de structuur van de organisatie, de werkwijzen, operationele categorieën, de doelstellingen en de beheers procedures. Een organisatie moet in het bezit zijn van geschreven bewijs van de componenten van het interne beheersingsproces met inbegrip van de doelstellingen en de beheersingsmaatregelen.

De omvang van de documentatie van de interne beheersing van een entiteit hangt af van de omvang van de entiteit, de complexiteit en andere factoren.

Communicatie

Goede communicatie moet van boven naar beneden, op hetzelfde niveau (transversaal) en van beneden naar boven doorheen de volledige structuur van de organisatie lopen.

Al het personeel moet van het hoogste management een duidelijk signaal krijgen dat hun verantwoordelijkheden betreffende beheersing ernstig moeten worden genomen. Het personeel moet begrijpen welke rol ze spelen in het interne beheersingssysteem en hoe hun individuele acties het werk van anderen beïnvloed.

Er is natuurlijk ook een noodzaak aan communicatie met externe partners.

Informatie is de basis van communicatie. Deze communicatie moet voldoen aan de verwachtingen van de groep of de individuen zodat ze in staat worden gesteld hun verantwoordelijkheden doeltreffend na te komen. Doeltreffende communicatie moet in alle richtingen gaan. Van boven naar beneden, op gelijk niveau en van beneden naar boven doorheen de volledige structuur van de organisatie.

De belangrijkste communicatielijn is deze tussen het management en het kader. Het management moet steeds op de hoogte worden gehouden van de werking, de ontwikkelingen, de risico's en de werking van de interne beheersing, en andere relevante gebeurtenissen en kwesties. In deze optiek moet het management ook laten weten aan het kader welke informatie ze nodig heeft en feedback en leiding geven. Het management moet ook zorgen voor specifieke en directe communicatie i.v.m. de verwachtte gedragslijnen. Dit houdt in dat er een duidelijk standpunt moet worden ingenomen over de aanpak van, de filosofie achter en de delegatie van gezag over de interne beheersing.

Communicatie moet zorgen voor het besef van de belangrijkheid en de noodzaak aan een doeltreffende interne beheersing, het kenbaar maken van de risicobereidheid en moet het personeel bewust maken van haar taken en verantwoordelijkheden in het uitvoeren en ondersteunen van de componenten van de interne beheersing.

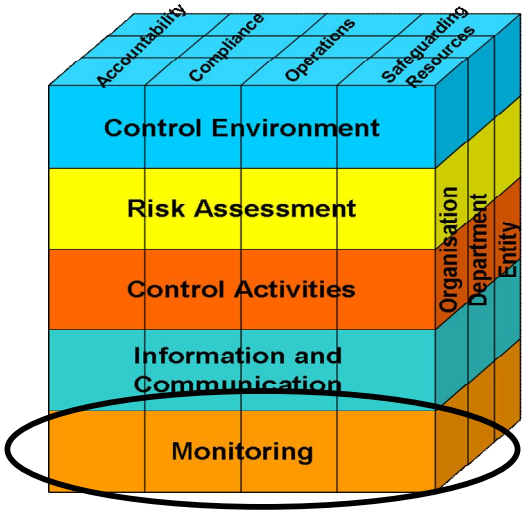
Bijkomend op de interne communicatie moet het management ook zorgen voor de juiste middelen van communicatie met en het betrekken van informatie van externe partijen, omdat externe communicatie inlichtingen kan verschaffen die een grote impact op het bereiken van de doelstellingen van de organisatie kunnen hebben.

Gebaseerd op de inlichtingen uit de interne en externe communicatie moet het management de nodige acties ondernemen en deze acties tijdig opvolgen.

Voorbeelden

We verwijzen de lezer naar de Bijlage A voor voorbeelden van de doelstellingen en onderdelen van interne beheersing.

2.5 Monitoring



Interne beheersinssystemen moeten opgevolgd worden om zo de kwaliteit van hun werking in de tijd in te kunnen schatten. Monitoring gebeurd door dagelijkse activiteiten, specifieke evaluaties of een combinatie van beide.

(1) Doorlopende monitoring
Is vervat in de normale, weerkerende activiteit van de entiteit. Het omvat de normale bestuur- en toezicht activiteiten en andere acties door het personeel genomen tijdens hun normale opdrachten.

Doorlopende monitoring heeft betrekking op elk van de componenten van de interne beheersing en omvat acties tegen een onrechtmatig, onethisch, oneconomisch, inefficiënt en niet-doeltreffend intern beheerssysteem.

(2) Aparte evaluaties
De aanpak en frequentie van de aparte evaluaties is vooral afhankelijk van de risico-inschatting en de doeltreffendheid van de doorlopende monitoringsprocedures.
Specifieke aparte evaluaties omvatten de evaluatie van de doeltreffendheid van het intern beheerssysteem en zorgen ervoor dat de interne beheersing de gewenste resultaten oplevert, gebaseerd op de vooraf bepaalde methodes en procedures. Tekortkomingen in interne beheersing moeten aan het verantwoordelijke directieniveau gemeld worden.

Monitoring moet ervoor zorgen dat de bevindingen en aanbevelingen van de audits onverwijld en adequaat toegepast worden.

Monitoring van de interne beheersing is toegespitst op de correcte uitvoering van de beheersing en op het inspelen op veranderende omstandigheden. Ook moet de monitoring onderzoeken of, in de drang naar de verwezenlijking van de opdracht van de entiteit, ook de algemene doelstellingen van de interne beheersing worden bereikt. Dit gebeurd door voortdurende monitoring, aparte evaluaties of beide zodat ze kunnen bijdragen tot de toepassing van de interne beheersing doorheen alle niveaus en onderdelen van de organisatie en dat de interne beheersing ook het beoogde resultaat bereikt.

De monitoring van de interne beheersing moet strikt gescheiden zijn van de monitoring van de operaties van de organisatie. Zoals beschreven in sectie 2.3 is dit ook een interne beheersingsactiviteit.

Doorlopende monitoring van de interne beheersing vindt plaats in het normale verloop van de dagelijkse wederkerende operaties van de organisatie. Het wordt voortdurend en in real-time uitgevoerd, reageert dynamisch op veranderende omstandigheden en is een onderdeel van de operaties van de entiteit. Hierdoor

is het doeltreffender dan aparte evaluaties en meestal ook goedkoper. Omdat aparte evaluaties meestal na de feiten plaatsvinden, zal de doorlopende monitoring meestal sneller een probleem aan het licht brengen.

De omvang en frequentie van de aparte evaluaties moet vooral afhankelijk zijn van de risico-inschatting en de doeltreffendheid van de doorlopende monitoringsprocedures. Bij het bepalen van de omvang en frequentie moet gehouden worden met de aard en mate van veranderingen en het daaraan verbonden risico zowel door interne als externe gebeurtenissen; de vakbekwaamheid en expertise van het personeel dat de remediëring en bijbehorende beheersing gaat uitvoeren en de resultaten van de doorlopende monitoring. Aparte evaluaties van de beheersing kunnen ook nuttig zijn als ze toegespitst zijn op de doeltreffendheid van de beheersing op een specifiek tijdstip. Aparte evaluaties kunnen voorkomen in de vorm van zelfevaluatie, als een herziening van het beheers ontwerp of als een directe test van de interne beheersing. Aparte evaluatie kunnen ook uitgevoerd worden door SAI, interne of externe auditoren.

Meestal zal een combinatie van doorlopende monitoring en aparte evaluaties ervoor zorgen dat de interne beheersing doeltreffend blijft.

Alle tekortkomingen die ontdekt worden tijdens de doorlopende monitoring of aparte evaluaties moeten doorgegeven worden aan die personen die in de positie zijn om de nodige acties te ondernemen. De term “tekortkoming” verwijst naar een toestand die van belang is om het bereiken van de algemene doelstellingen van de organisatie te beïnvloeden. Een tekortkoming kan daarom een reëel, potentieel of zelfs mogelijk euvel zijn, maar het kan ook een kans zijn om de interne beheersing dusdanig te verbeteren dat de waarschijnlijkheid om de gestelde doelen te bereiken groter word.

Informatie over tekortkomingen in de interne beheersing aan de juiste personen overmaken is een absolute noodzaak. Voorschriften moeten opgemaakt worden zodat er kan bepaald worden welke informatie op welk niveau terecht moeten komen om er zeker van te zijn dat de juiste beslissingen kunnen worden genomen. Regel in deze voorschriften is het feit dat een manager informatie moet krijgen over acties en gedragingen van het personeel waarvoor hij/zij verantwoordelijk is en informatie die nodig is voor het bereiken van een specifieke doelstelling.

Informatie verkregen door het verloop van de operaties wordt meestal doorgegeven via de normale kanalen, dwz de functionele verantwoordelijke en het managementniveau boven deze persoon. Er moeten echter ook alternatieve kanalen zijn voor het rapporteren van gevoelige informatie zoals illegale of niet-geoorloofde activiteiten.

De monitoring van interne beheersing betekend ook dat er procedures en werkwijzen moeten zijn die ervoor instaan dat de bevindingen uit audits en andere evaluaties adequaat en met spoed opgelost worden. Managers moeten daarom (1) onmiddellijk de bevindingen uit audits of andere evaluaties onderzoeken met inbegrip van de ontdekte tekortkomingen en de aanbevelingen van auditoren en anderen die de operaties geëvalueerd hebben, (2) gepaste acties voorschrijven als antwoord op de bevindingen en aanbevelingen uit audits en evaluaties, en (3) binnen de gestelde termijnen alle acties uitvoeren die een oplossing bieden voor de bevindingen die hun werden overgemaakt.

Het proces van bijsturing begint op het ogenblik dat de resultaten van de audit of andere evaluatie overgemaakt worden aan de directie en is pas afgerond nadat er actie werd ondernomen die (1) de vastgestelde tekortkomingen verhielpen, (2) verbeteringen aanbrachten, of (3) aangetoond hebben dat de bevindingen en aanbevelingen geen actie rechtvaardigen

Voorbeelden

We verwijzen de lezer naar de Bijlage A voor voorbeelden van de doelstellingen en onderdelen van interne beheersing.

3. Taken en verantwoordelijkheden.

Iedereen in een onderneming heeft een verantwoordelijkheid in de interne beheersing.

Managers

Zijn rechtstreeks verantwoordelijk voor alle activiteiten van de onderneming, met inbegrip van het ontwerpen, implementeren, opvolgen van het correct functioneren, onderhouden en documenteren van het intern beheerssysteem. Hun verantwoordelijkheden verschillen door hun functie in de organisatie en de karakteristieken van de organisatie.

Interne auditoren

Bestuderen en dragen bij tot de voortdurende doeltreffendheid van het intern beheersing systeem door hun evaluaties en aanbevelingen, maar ze zijn niet verantwoordelijk voor het ontwerpen, implementeren, documenteren en onderhouden van het interne beheerssysteem.

Medewerkers

Dragen ook bij tot de interne beheersing. Interne beheersing is een expliciet of impliciet onderdeel van de taken van het personeelslid. Elk personeelslid speelt een rol in het uitoefenen van de interne beheersing en zou verantwoordelijk moeten zijn voor het melden van problemen in de operaties, het niet naleven van de deontologische code en inbreuken op de werkwijzen.

Externe partijen spelen ook een belangrijke rol in het interne beheers proces. Ze kunnen bijdragen tot het verwezenlijken van de doelstellingen van de onderneming of kunnen nuttige informatie verstrekken i.v.m. interne beheersing. Ze zijn echter niet verantwoordelijk voor het ontwerpen, implementeren, juist gebruik, onderhoud of documenteren van het intern beheerssysteem van de organisatie.

Supreme Audit Institutions (SAI) (Rekenhoven)

Stimuleren en ondersteunen de verwezenlijking van een doeltreffend intern beheerssysteem bij de beleidsvoerders. De evaluatie van het intern beheerssysteem is essentieel voor de nalevings-, financiële- en productiviteits audits door de SAI. Ze delen hun bevindingen mee aan de betrokken partners.

Externe auditoren

Auditeren bepaalde overheidsinstellingen in sommige landen. Samen met hun beroepsgroeperingen geven ze advies en aanbevelingen aan de SAI.

Wetgevers en regulatoren

Vaardigen regels en richtlijnen uit i.v.m. interne beheersing. Ze moeten bijdragen tot een algemeen begrijpen van de interne beheersing.

Andere partijen

Werken samen met de organisatie (begunstigden, leveranciers, ...) met betrekking tot het verwezenlijken van de gestelde doelstellingen.

Interne beheersing wordt in de eerste plaats beïnvloed door de interne betrokkenen met inbegrip de directie, interne auditoren en het personeel. Nochtans hebben externe betrokkenen ook hun impact op het intern beheerssysteem.

De directie

Al het personeel van de organisatie speelt een belangrijke rol om het interne beheerssysteem te laten functioneren. De directie echter heeft de verantwoordelijkheid over het ontwerpen, implementeren, de monitoring van de uitvoering en de goede werking, het onderhouden en documenteren van het intern beheerssysteem. De directie kan ook raden en audit commissies bevatten, die elk een verschillende rol en samenstelling hebben en die in verschillende landen aan verschillende wetten onderhevig zijn.

Interne auditoren

Dikwijls zal de directie een intern audit team samenstellen als onderdeel van het intern beheerssysteem en dit team helpt met de monitoring van de doeltreffendheid van het intern beheerssysteem. Interne auditoren verstrekken informatie over het functioneren van de interne beheersing, vooral op het gebied van de evaluatie van het ontwerp en de werkwijze van de interne beheersing. Ze geven informatie over de sterke en zwakke punten van het systeem en geven aanbevelingen voor verbeteringen. Zij moeten onafhankelijk en objectief kunnen werken.

Voor deze redenen moet de interne audit een onafhankelijke en objectieve raadgevende en ondersteunende activiteit zijn, die een toegevoegde waarde is en de operaties van de organisatie verbeterd. Ze helpt de organisatie om haar doelstellingen te verwezenlijken door een systematische en gedisciplineerde benadering van de evaluatie en helpt de doeltreffendheid van de risicobehandelings-, beheersings- en leidinggevende processen te verbeteren.

Ook al kan de interen auditor een waardevolle leermeester en raadgever i.v.m. interne beheersing zijn, de auditor mag helemaal niet een vervanger zijn voor een goed intern beheerssysteem.

Opdat een interne auditdienst efficiënt kan werken, is het essentieel dat de auditoren, onafhankelijk van de directie, op een onbevooroordeelde en eerlijke wijze kunnen optreden en dat ze direct aan de hoogste functionaris van de organisatie kunnen rapporteren. Dit stelt de auditoren in staat om zich onbevooroordeelde opinies over hun bevindingen van het intern beheerssysteem te vormen en objectieve raadgevingen ter verbetering van de gevonden tekortkomingen te formuleren. Als professionele leidraad moeten de interne auditoren gebruik maken het Professional Practices Framework (PPF) van het IIA met inbegrip van de definities, de ethische code, de Standaard en de Practice Advisories. Ook moeten de interne auditoren de ethische code van INTOSAI volgen.

Bovenop hun taak om de interne beheersing op te volgen, kan een goed intern audit team bijdragen tot de doeltreffendheid van de externe audit door directe bijstand aan de externe auditoren. De aard, impact of timing van de externe audit kunnen aangepast worden als de externe auditdienst vertrouwen heeft in de interne auditoren.

Medewerkers

Medewerkers en ander personeel hebben ook hun invloed op de interne beheersing. Het is niet zelden het personeel van de eerste lijn die de beheers toepassingen hertekenen, verkeerdelijke beheersing herstellen en problemen ontdekken die best door dagdagelijkse taken kunnen aangepakt worden.

Externe partijen

Een tweede groep spelers in de interne beheersing zijn externe partijen als externe auditoren (SAI), wetgevers, regulatoren, en anderen. Ze kunnen bijdragen tot het bereiken van de doelstellingen of kunnen nuttige informatie verstrekken die invloed kan hebben op de interne beheersing. Nochtans zijn ze niet verantwoordelijk voor het ontwerpen, implementeren, correct functioneren, onderhoud of documenteren van het intern beheerssysteem van de organisatie.

SAI en externe auditoren

De taken van de externe partijen, in het bijzonder de SAI en externe auditoren, omvatten de evaluatie van de werking van het intern beheerssysteem en het informeren van de directie over hun bevindingen. Deze evaluatie is echter afhankelijk van het mandaat dat de externe dienst kreeg toebedeeld.

De evaluatie van de interne beheersing door de externe auditoren betekend:

- Bepalen van de impact en waarschijnlijkheid van de risico's waarvoor de interne beheersing werd ontworpen;
- Evaluatie van de waarschijnlijkheid van misbruik van middelen, niet behalen van de doelstellingen betreffende ethiek, economie, doeltreffendheid en doelmatigheid, het niet vervullen van de rekenschap, niet naleven van wetten en reglementen;
- Herkennen en begrijpen van de relevante beheersing;
- Bepalen wat er bekend is over de doeltreffendheid van de beheersing;
- Bepalen van de doeltreffendheid van het beheersingssysteem;
- Bepalen, door middel van testen, of de beheersing doeltreffend is;
- Rapporteren over de interne beheersing en overleggen m.b.t. de benodigde verbeteringen.

De SAI heeft er ook belang bij dat er sterke interne audit teams zijn. Deze audit teams zijn een belangrijk element in de interne beheersing door hun voortdurend streven naar verbeteringen in de operaties van de organisaties. In sommige landen zijn deze interne audit teams niet onafhankelijk, niet sterk of zelfs onbestaand. In deze gevallen zouden de SAI bijstand en hulp moeten bieden zodat er toch onafhankelijke interne audit teams kunnen opgericht worden en hun werk zouden kunnen uitvoeren. Deze hulp kan bestaan uit afvaardigen of uitlenen van personeel, vormingen geven, didactisch materiaal ter beschikking stellen en een methodologie en werkwijzen ontwikkelen. Dit moet gebeuren zonder dat de onafhankelijkheid van de SAI en externe auditoren bedreigd wordt.

Het SAI moet ook zorgen voor een goede verstandhouding met de interne audit teams zodat ervaring en kennis gedeeld kan worden en het werk wederzijds aangevuld en bijgestuurd kan worden. Het in rekening brengen van de opmerking van de interne audit en het erkennen van de bijdrage van het intern audit team aan het extern audit rapport is ook een middel om deze goede werkrelatie op te bouwen. De SAI moet procedures uitwerken voor het inschatten van werk van de interne audit teams om zo te kunnen bepalen in welke mate deze betrouwbaar zijn. Een sterk intern audit team kan de werklast aan de audit door de SAI verminderen en nodeloos dubbel werk vermijden. De SAI moet zorgen dat ze toegang krijgen tot de interne audit rapporten, belangrijke bankdocumenten en de aanbevelingen van het intern audit team.

De SAI moeten ook een voortrekkers rol spelen voor de rest van de openbare instellingen door binnen hun eigen organisatie een intern beheerssysteem op te richten dat met deze richtlijnen overeenkomt.

Niet enkel SAI maar ook de externe audit teams spelen een belangrijke rol door hun bijdrage aan het verwezenlijken van de interne beheers doelstellingen, vooral op het gebied van “rekenschap afleggen” en “bescherming van kapitalen”. Dit omdat externe audits van financiële rapporten en informatie alles te maken hebben met het afleggen van rekenschap en goed bestuur. Externe audits samen met niet-financiële informatie zijn voor de externe betrokkenen het belangrijkste mechanisme voor het opvolgen van de werking.

Wetgevers en regulatoren

Wetten geven een goed totaalbeeld van de definities van de interne beheersing en de te bereiken doelstellingen. Het geeft aan welke werkwijze de interne en externe betrokkenen moeten toepassen bij de uitoefening van hun taken en verantwoordelijkheden in interne controle.

Bijlage 1 Voorbeelden

Voorbeeld **Rekenschap afleggen** (1): Het departement dat verantwoordelijk is voor het beheer van veilig transport over water en zee werd georganiseerd door verschillende diensten die verantwoordelijk zijn voor het loodsen, de boeien, inspectie van de waterkwaliteit, aanmoediging van het gebruik van de waterwegen, investeringen in en onderhoud van de infrastructuur(Bruggen, kanalen en sluizen.)

Beheersingsomgeving	Risico inschatting	Beheersingsmaatregelen	Informatie en communicatie	Monitoring
Voor elk van de diensten is er een dienstdoende manager aangeduid die aan de algemene manager verslag moet uitbrengen. De dienstdoende managers hebben de vereiste vaardigheden en de toestemming om bepaalde beslissingen te nemen. Elk van hun moet ook een gedragscode ondertekenen.	Mogelijke risico's zijn aanvaringen, lekken van gevaarlijke producten en brandstoffen, breken van dijken. Als de ongelukken te wijten zijn aan nalatigheid van de betrokken dienst kan deze dienst een zware verantwoordelijkheid dragen.	Beheersingsmaatregelen die georganiseerd kunnen worden zijn het loodsen van de schepen, het plaatsen van boeien, markeringen en bakens, visuele inspectie vanuit de lucht en het nemen van waterstalen.	De informatie en communicatie kunnen gaan over het melden van aanvaringen aan andere schepen, waarschuwingen aan binnenvarende schepen i.v.m. weersomstandigheden, publiceren van de namen van de vervuilers en de mogelijke acties, en de reddingsacties die werden ondernomen.	Een monitoring van het aantal aanvaringen, milieu-inbreuken, resultaten van waterstalen samen met het vergelijken met andere landen en historische gegevens kunnen helpen om de impact en doeltreffendheid van het loodsen, het plaatsen van boeien, markeringen en bakens, de inspecties en de resultaten van de waterstalen op te volgen.

Voorbeeld **Rekenschap afleggen** (2): De manager van de sport afdeling uitte vorig jaar de doelstelling dat de sportbeoefening met 15% zou toenemen.

Beheersingsomgeving	Risico inschatting	Beheersingsmaatregelen	Informatie en communicatie	Monitoring
Vanwege de goede reputatie van de sport manager, nam de raad van bestuur deze doelstelling aan en belegde geen status meetings om de vooruitgang van de manager te bespreken. *(Deze situatie is geen voorbeeld van goed beleid)*	Door het niet specificeren van de doelen ontstaat het risico dat ze niet zullen worden gehaald. Ook ontstaat het risico dat de rapportering niet tijdig zal gebeuren omdat de manager wil wachten tot het doel -15% groei- bereikt is. Ook werd er niet bepaald hoe de groei gemeten moet worden. De betrokken manager kan zeggen dat het aantal beoefenaars met 15% steeg of het aantal uren dat de mensen aan sport doen of zelfs dat het aantal sportclubs met 15% toenam. Op deze manier vermindert de kwaliteit van de rapportering substantieel.	Het risico kan verminderd worden door correcte rapporteringslijnen uit te zetten en door een model uit te werken dat bepaald welke informatie gegeven moet worden.	Dit verslag moet op tijd uitgebracht worden en moet aan het model voldoen. Het zou de groeidoelstellingen moeten weergeven, hoe de resultaten moeten worden gemeten en waarom dit zo moet gebeuren. Alle informatie om de beweringen te staven moet aanwezig zijn.	Het verifiëren of het verslag wel of niet voldoet aan het model, welke informatie er werd verstrekt en of er nog informatie ontbreekt, kan een vorm van monitoring zijn.

Voorbeeld **Handelen naar de wetten en reglementen**: Het ministerie van Landsverdediging wil nieuwe gevechtstoestellen aankopen via een openbare aanbesteding en maakt voor deze overheidsopdracht de handelswijze en procedures bekend. Alle aanbiedingen blijven ongeopend tot het einde van de aanbesteding. Op dat ogenblik worden alle offertes geopend in aanwezigheid van de verantwoordelijke managers en enkele officiële vertegenwoordigers. Alleen deze offertes worden onderzocht en vergeleken om te beslissen welke offerte de beste is.

Beheersingsomgeving	Risico inschatting	Beheersingsmaatregelen	Informatie en communicatie	Monitoring
Het team dat deze transactie zal uitvoeren is samengesteld uit competente personen die een document ondertekenden dat ze geen financiële en relationele band hebben met de deelnemende bieders. De verantwoordelijke managers en officiële vertegenwoordigers ondertekenen dit document ook.	Een van de risico's van de openbare aanbestedingen en contracten is de voorkennis. Een van de bieders zou kennis kunnen hebben van de offertes van de andere en zou zo een winnende offerte kunnen opmaken die kan leiden tot het maken van een keuze voor een minderwaardig product. Dit kan ook leiden tot een nieuwe openbare aanbesteding omdat de gekozen onderneming niet aan de verwachtingen voldoet. Ook kunnen bieders die denken onheus behandeld te zijn schadeclaims indienen.	Om de risico's te beperken moeten er procedures opgesteld en toegepast worden die in overeenstemming zijn met de relevante wetten en bepalingen betreffende openbare contracten.	Alle procedures van toepassing op het publiceren van alle bepalingen van de overheidsopdracht, de behandeling van alle ontvangen aanbiedingen en het aankondigen van de gekozen aanbieder moeten schriftelijk gedocumenteerd worden met alle details van de te nemen acties. Bij de behandeling van de aanbiedingen moeten ook alle redenen waarom een aanbieder niet gekozen werd gedocumenteerd worden.	Een interne audit kan alle documenten nakijken en een monitoring doen van de claims.

Voorbeeld **Uitvoeren van gestructureerde, ethische, economische, efficiënte en doelgerichte operaties**.(1): Het ministerie van cultuur wil het museumbezoek doen toenemen. Om dit te verwezenlijken stellen ze voor om nieuwe musea te bouwen, cultuur-checks uit te delen aan alle inwoners en de toegangsprijzen verlagen. Om dit economisch, efficiënt en doeltreffend te doen moet het ministerie overwegen en evalueren of de gestelde doelstellingen kunnen verwezenlijkt worden door deze voorstellen en hoeveel elk van deze voorstellen zal kosten.

Beheersingsomgeving	Risico inschatting	Beheersingsmaatregelen	Informatie en communicatie	Monitoring
Het ministerie van cultuur moet zich ervan vergewissen dat haar organisatiestructuur in staat is om toezicht te houden op het ontwerpen en de bouw van de voorgestelde uitbreidingen en dat ze in staat zijn om de nieuwe musea te organiseren en uit te baten.	Het niet groeien van het aantal museumbezoeken is een van de risico's. Er bestaat ook het risico dat sommige voorstellen meer zullen kosten dan geraamd. Bv. als het verminderen van de prijs van een ticket niet resulteert in een verhoogd aantal bezoeken, zal het inkomen van het ministerie verminderen. Het bouwen van nieuwe musea zonder rekening te houden met verlichtingseisen, temperatuurcontrole en beveiliging, kan resulteren in dure bijsturingen tijdens of na de bouw.	De beheersingsmaatregelen van de hiervoor beschreven risico's kunnen een budgetcontrole zijn om de echte uitgaven te vergelijken met de gebudgetteerde bedragen, monitoring van de bouwvorderingen en het vragen van bewijzen i.v.m. extra uitgaven.	De informatie en documentatie van dit voorbeeld kan bestaan uit verslagen van vergaderingen met architecten, brandweer(i.v.m. veiligheidsvoorschriften) artiesten en andere partijen. Het kan ook verslagen bevatten van de monitoring van budgetten en de monitoring van de werkzaamheden van de bouw.	Het analyseren van de bewijsstukken voor budget.o.v.erschrijdingen, rentelasten door vertragingen in het werkverloop en betalingen zijn ook een deel van de monitoring.

Voorbeeld **Uitvoeren van gestructureerde, ethische, economische, efficiënte en doelgerichte operaties**.(2): De regering wil de landbouwactiviteit opdrijven en de levenskwaliteit in de landelijke omgeving verbeteren. Ze voorzien fondsen voor de aanleg van irrigatie en het boren van putten.

Beheersingsomgeving	Risico inschatting	Beheersingsmaatregelen	Informatie en communicatie	Monitoring
De regering moet ervoor zorgen dat ze het juiste departement heeft om de implementatie en het doorvoeren van de budgetoperatie uit te voeren en dat ze de juiste omstandigheden schept om de tijdige en doeltreffende uitvoering van het project te bewerkstelligen.	Het risico bestaat dat malafide organismen subsidies aanvragen maar deze niet voor het beoogde doel aanwenden.	Beheersingsmaatregelen kunnen zijn: - Contoleren van de kwalificaties van de organismen die een subsidie aanvragen. - On-site monitoring van de vooruitgang en controle van de rapportering i.v.m. de bouwwerken. - Controle van de uitgaven van de betrokken organismen door controle van de facturen en het uitstellen van de betaling van de subsidie(of een deel ervan) tot deze controle voltooid is.	- Voortgang rapporten die een gedetailleerd overzicht geven van de kosten, het aantal geboorde putten en het aantal geïrrigeerde hectaren. - Facturen worden opgevraagd als bewijsstukken van de gesubsidieerde kosten.	Monitoring kan bestaan uit de supervisie van het boren van de putten en de aanlag van de irrigatie kanalen en vergelijk met gelijkaardige projecten in andere landen. Opvolgen van de opbrengsten van de geïrrigeerde delen kan worden voorzien.

Voorbeeld **Kapitalen beschermen(1)**: Het ministerie van Landsverdediging heeft opslagplaatsen, militaire winkels en brandstof depots. Het is het standpunt van defensie dat de voorraden enkel aangewend mogen worden voor militaire doeleinden en niet voor private doeleinden.

Beheersingsomgeving	Risico inschatting	Beheersingsmaatregelen	Informatie en communicatie	Monitoring
De standpunten op het gebied van geschikt personeel moeten aangewend worden bij het rekruteren en het op peil houden van de personeelsbezetting van de opslagplaatsen, winkels en depots.	Het risico bestaat dat sommigen wapens willen stelen, misbruiken of verhandelen. Ook brandstoffen kunnen het voorwerp uitmaken van diefstal.	Beheersingsmaatregelen om met deze risico's om te gaan kunnen zijn; het plaatsen van omheiningen en muren rond opslagplaatsen, gewapende wachten plaatsen en bewaking van de toegangen met honden. Regelmatige inventarissen en richtlijnen dat de goederen enkel mogen afgeleverd worden als er een geschreven toestemming van een hogere officier kan voorgelegd worden kunnen helpen om de stocks te vrijwaren.	Het doorgeven van beschadigingen aan omheiningen en onregelmatigheden in de inventarissen. Goedkeuringen van inventarissen en procedures kunnen ook informatie verstrekken over dit onderwerp.	Inspectie van de omheiningen, onaangekondigde inventarissen, nagaan van stockbewegingen of zelfs het uitvoeren van een geheime veiligheidstest.

Voorbeeld **Kapitalen beschermen(2)**: Grote hoeveelheden gevoelige informatie is opgeslagen op de computers van een afdeling van het ministerie van justitie. Het belang van IT beheersing is echter genegeerd en bijgevolg zijn er veel onvolkomenheden in de IT beheersing.

Beheersingsomgeving	Risico inschatting	Beheersingsmaatregelen	Informatie en communicatie	Monitoring
De leiding moet laten zien dat ze begaan is met de vakkennis en de juiste gedragsethiek van het personeel in IT en zorgen voor een gedegen training in dit domein. Het beleid op het gebied van menselijk kapitaal speelt ook een grote rol in het verkrijgen van een positieve beheersing van de IT omgeving.	Op gebied van de algemene beheersing heeft de afdeling -geen beperking ingesteld betreffende de inzage van gegevens andere dan nodig voor het uitvoeren van de opgelegde taak. -geen doeltreffend systeem ontwikkeld om de programma's en gevoelige informatie te beschermen -geen documentatie gemaakt i.v.m. software aanpassingen -geen afsplitsing gemaakt inzake verenigbaarheid van taken -verzuimd te zorgen voor continuïteit van de dienstverlening -nagelaten haar netwerk te beveiligen tegen ongeoorloofde toegang. Op gebied van de software beheersing heeft de afdeling nagelaten toegangsmachtigingen bij te houden. *(geen goed beleid)*	De afdeling kan -zorgen voor toegangspaswoorden tot de software en controlesystemen voor fysieke toegang (Badges, Sloten, alarmen,..) -zorgen dat het onmogelijk word om in te loggen in het core-systeem voor de eindgebruikers van de software -Toegang tot het ontwikkelingsgedeelte van de software beperken tot de ontwikkelaars -logbestanden gebruiken om elke toegang (of poging tot) en elke gegeven opdracht te registreren en zodoende inbreuken te kunnen vaststellen -Zorgen voor een eventualiteiten- en rampen plan om de beschikbaarheid van kritische middelen te garanderen -firewall installeren en web server activiteiten monitoren om netwerkgebruik te garanderen.	Procedures i.v.m. software beheersing moeten aanwezig zijn en software aanpassingen moeten gedocumenteerd worden alvorens ze in gebruik te nemen. Het beleid en de taakomschrijvingen die het principes van scheiding van taken respecteren moeten ontwikkeld worden. Logbestanden die gebruikt worden om elke toegang (of poging tot) en elke gegeven opdracht te registreren moeten regelmatig overgemaakt en geanalyseerd worden.	Uitvoeren van een IT audit, een rampoefening houden, web server activiteiten opvolgen kunnen een deel zijn van de IT Beheersingsomgeving.

Bijlage 2 Woordenlijst

Algemene beheersing	- Algemene beheersing zijn de structuren, werkwijzen en procedures die nageleefd moeten worden door alle of een groot deel van de informatie systemen van de entiteit. Zij creëren de omgeving waarin de applicatie systemen en beheersing werken. - Werkwijzen en procedures die continuïteit en juist gebruik van de Computer Informatie Systemen moeten garanderen. Ze omvatten beheersing over informatica technologie management, informatica technologie infrastructuur, beveiliging en aanschaf, ontwikkeling en onderhoud van software. Algemene beheersing ondersteunen de in de applicaties geprogrammeerde beheersing. Algemene computer beheersing of Informatica technologie beheersing worden soms gebruikt als synoniem voor algemene beheersing.
Applicatie	Computer programma ontworpen om toe te laten bepaalde taken en speciale functies uit te voeren, zoals loonadministratie, inventaris beheersing, boekhouding en taak ondersteuning. Afhankelijk van de taak waarvoor het werd ontworpen kan deze applicatie gebruik maken van tekst, cijfermateriaal, grafische elementen of een combinatie van deze.
Beheersing van de toepassingen	De structuur, de werkwijzen en de procedures die toegepast worden om verschillende applicatie systemen te onderscheiden en die ontwikkeld werden om verwerking van data binnen de specifieke software te bewerkstelligen. Geprogrammeerde procedures in applicatie software en daaraan verbonden manuele procedures, ontwikkeld om de volledigheid en juistheid van informatieverwerking te verkrijgen. Zoals bijvoorbeeld : geprogrammeerde edit check van de ingebrachte data, numerieke volgorde checks en handmatige procedures om uitzonderingslijsten af te toetsen. (COSO 1992)
Audit	beheersing van activiteiten en operaties die moet uitwijzen dat deze uitgevoerd werden of in uitvoering zijn volgens de bepaalde objectieven, het budget, regels en standaards. De bedoeling van deze regelmatige beheersing is om afwijkingen welke een correctieve actie vereisen, te benoemen.
Audit comité	Commissie van de directieraad wiens taak toegespitst is op de aspecten van de financiële rapportering en de processen om de zakelijke en financiële risico te behandelen, alsook de toepassing van de relevante legale, ethische en regelgevende vereisten. De audit commissie staat de directieraad bij met een overzicht van - de integriteit van de financiële verslagen - overeenstemming met legale en regelgevende vereisten - de kwalificatie en onafhankelijkheid van de externe auditeur - de werking van het intern en extern audit orgaan. - vergoeding van de directieleden (indien er geen

	vergoedingscomité bestaat).
Audit instituut	Private firma die, onafhankelijk van hun aanduiding, samenstelling en organisatie, externe audits uitvoert volgens de wettelijke bepalingen.
Beheers actie	Beheers acties zijn de werkwijzen en procedures die gemaakt werden om risico's te beheersen en de objectieven te bereiken. De procedures die een entiteit instelt om met risico's om te gaan worden interne beheersingsmaatregelen genoemd. Interne beheersing acties zijn een antwoord op risico's omdat ze werden gecreëerd om de onzekerheid van resultaat te beperken zodra dit risico werd erkend.
beheers omgeving	De beheers omgeving bepaald de sfeer van een onderneming en beïnvloed het beheersing bewustzijn van het personeel. Het is de hoeksteen voor alle andere componenten van de interne beheersing en levert structuur en discipline.
beheersing	(1) Een voornaamwoord, gebruikt als onderwerp. Bv.: Het bestaan van een beheersing. Een werkwijze of proces dat deel uitmaakt van interne beheersing. Een beheersing kan bestaan in elk van de 5 componenten (2) Een voornaamwoord, gebruikt als xxxx. Bv.: beheersing uitoefenen. Het resultaat van werkwijzen en procedures, gemaakt om beheersing uit te voeren. Het resultaat kan wel of niet effectieve interne beheersing zijn. (3) Een werkwoord. Bv.: beheersen, regelen, uitvaardigen of implementeren van een werkwijze die beheersing beïnvloed. (COSO 1992) (4) Elke actie genomen door het management, de directieraad en andere partijen om risico´s te beheersen en om de waarschijnlijkheid te verhogen dat de gestelde objectieven en doelen worden bereikt. Het management plant, organiseert en stuurt de uitvoering van voldoende acties zodat er een redelijke verzekering gecreëerd word dat de objectieven en doelen gehaald kunnen worden. (IIA)
Belanghebbenden	Partijen die beïnvloed worden door de entiteit, zoals aandeelhouders, de gemeenschap waarin de entiteit opereert, personeelsleden, klanten en leveranciers.
besparing	De kosten van bronnen van een aanvaardbare kwaliteit nodig voor een activiteit, zo veel als mogelijk beperken. Het tijdig en aan de laagst mogelijke kostprijs verkrijgen van financiële, materiële en menselijke bronnen die kwalitatief en kwantitatief geschikt zijn.
Budget	Kwantitatieve, financiële uitdrukking van geplande activiteiten over een bepaalde termijn. Het budget wordt opgemaakt met het oog op de geplande activiteiten en het opstellen van ex post facto checks van de behaalde resultaten.
Budget beheersing	Beheersing waarbij het orgaan dat een budget heeft toegekend zich vergewist van het correcte gebruik van dit budget in overeenstemming met de ramingen, toelatingen en regelgeving.
Complot	Een gezamenlijke inspanning van personeelsleden om op frauduleuze

	wijze geld, goederen of andere bedrijfs activa te verkrijgen.
Computer beheersing	- beheersing door de computer uitgevoerd (geprogrammeerde computer beheersing in tegenstelling tot manuele beheersing. - beheersing over de verwerking van informatie met de computer bestaande uit algemene beheersing en applicatie beheersing (zowel handmatig als geprogrammeerd) (COSO 1992)
Computer Informatie Systeem (CIS)	Een CIS omgeving bestaat wanneer een computer van eender welk soort of vorm gebruikt word door de entiteit om belangrijke (financiële) informatie die van belang is voor de audit, te verwerken, onafhankelijk van het feit of deze intern in de entiteit gebeurd of door een derde.
Conformiteit aan wetten en regelgeving	- Zich schikken naar de wetten en regels die gelden voor deze entiteit. (COSO 1992) - Overeenstemming met en toepassing van de principes, plannen, wetten, regels, contracten en andere vereiste
Corruptie	(1) Elke vorm van onethisch gebruik van het openbare ambt voor persoonlijk of privaat voordeel. (2) Het misbruik van verkregen vertrouwen voor persoonlijk voordeel.
COSO	Committee of Sponsoring Organisations of the Treadway commission, een groepering van verschillende accounting organisaties. In 1992 publiceerde het een belangrijke studie over interne beheersing, getiteld Internal Control –Integrated Framework. Deze studie wordt veelal aangehaald als het COSO rapport.
Data	Feiten en informatie die doorgegeven en gebruikt kunnen worden
Documentatie	Documentatie van de interne beheersing structuur zijn het materiaal en geschreven bewijzen van de componenten van het interne beheersing proces, met inbegrip van de identificatie van de structuur van de organisatie, haar werkwijzen en de operating categories, haar gerelateerde doelen en beheersing activiteiten. Deze moeten verschijnen in documenten als management directieven, administratieve werkwijzen, procedure handleidingen en boekhoudkundige handleidingen.
Doeltreffend	Verwijst naar het verwezenlijken van doelstellingen of de mate waaraan het resultaat voldoet aan de doelstelling of het gewenste resultaat van de activiteit.
Doeltreffendheid	De mate waarin de objectieven zijn bereikt en het verband tussen de beoogde en het bereikte resultaat van een activiteit. (Intosai auditing standards) Mate waarin de beoogde objectieven werden kosten-beperkend bereikt.
Economisch	Niet verkwistend of extravagant. De juiste hoeveelheid bronnen van de vereiste kwaliteit op het juiste ogenblik aangebracht tegen een zo laag mogelijke kostprijs.
Edit checks	Geprogrammeerde beheersing die in de beginfase van het input proces foutieve invoer van data detecteren. Bv. Alfanumerieke data

	ingebracht in een numeriek veld worden door het programma verworpen. Deze geprogrammeerde beheersing kan ook toegepast worden als data van de ene naar de andere applicatie doorgestuurd worden.
Efficiënt	Verwijst naar de verhouding tussen de aangewende middelen om het doel te bereiken en de gerealiseerde resultaten. Dit betekend : Minimale input van middelen om een gevraagde kwaliteit en kwantiteit te realiseren. Of een maximale productie met een vooraf bepaalde kwaliteit en hoeveelheid aan middelen.
Efficiëntie (Rendement)	Het verband tussen het resultaat- goederen, diensten of andere- en de hiertoe aangewende middelen.(INTOSAI auditing standards) Het dusdanig gebruik van een bepaalde hoeveelheid aan financiële, menselijke en materiële middelen om een maximaal resultaat te verkrijgen. Of het beperken van middelen om een gegeven hoeveelheid en kwaliteit van resultaat te bekomen.
Eindgebruiker (in computerverwerking)	Verwijst naar het gebruik van data verwerking ontwikkeld door de eindgebruiker, meestal ontwikkeld met behulp van software pakketten. Eindgebruiker processen kunnen geraffineerde systemen zijn en een waardevol informatie middel worden voor het management. Of deze systemen voldoende getest en gedocumenteerd zijn kan twijfelachtig zijn.
Entiteit	Een organisatie, groot of klein, welke werd opgericht met een bepaald doel. Dit kan een commerciële onderneming, een Non-profit organisatie, overheidsorgaan of academisch instituut zijn. Synoniemen zijn organisatie en departement.
Ethisch	Verwijst naar de morele principes
Ethische waarden	Morele waarden die tot verantwoorde en juiste beslissingen moeten leiden. Deze waarden moeten gebaseerd zijn op wat “juist-correct” is en kunnen verder gaan dan wat wettelijk verplicht is.
Externe audit	Audit uitgevoerd door een entiteit die extern en onafhankelijk is van de geauditeerde met als doel een mening te vormen en verslag uit te brengen over de rekeningen, financiële toestand, de gegrondheid en wettelijkheid van de operaties en/of het financiële management.
Organigram Flow-charting	Diagram dat de structuur van de documenten, boeken, registers en de volgorde van verwerking ervan door de klant weergeeft. Voorstelling van de opeenvolging van procedures, informatie of documenten. Maakt het mogelijk om ingewikkelde structuren en procedures op een beknopte manier weer te geven.
Fraude	Niet-wettelijke interactie tussen twee entiteiten, waarbij de ene party de andere moedwillig bedriegt door het geven van valse informatie, om zo illegaal voordeel te verkrijgen. Dit kan door bedrog, misleiding, misbruik van vertrouwen of achterhouden van informatie.
Fysieke toegang	Bij toegang beheersing, het lijfelijk toegang verkrijgen tot een ruimte of entiteit.
INCOSAI	Congres is het hoogste orgaan van de intosai en is samengesteld uit al haar leden

Input	Ingebrachte data in een computer of het proces om data in te voeren.
Institute of Internal Auditors (IIA)	Het IIA is een instituut dat de ethische en praktische standaards opstelt, vormingen voorziet en professionalisme van haar leden stimuleert.
Integriteit	Ingesteldheid met gezonde morele principes, eerlijkheid, rechtschapenheid en de drang om juist te handelen, en om te kunnen gaan met de gevraagde waarden en verwachtingen.
Interne audit	De interne middelen waardoor het management zekerheid krijgt dat de processen waarvoor zij verantwoording moeten afleggen dusdanig uitgevoerd worden zodat er een minimale kans op fraude, vergissingen, inefficiëntie of verspilling is. Het lijkt sterk op externe audit maar het is vooral gericht op de richting die het management van de geauditeerde afdeling uit wil. Een onafhankelijke, objectieve consultatie activiteit met als doel bijkomende waarden en verbetering aan de operaties aan te brengen. Het helpt de organisatie om door een systematische en gedisciplineerde aanpak het risicomanagement, de beheersing en de beleidsprocessen te verbeteren. Om zo de doelstellingen te bereiken. Interne beheersing is een evaluatie gecreëerd in een entiteit ten dienste van de entiteit. Het behelst onder andere studie, evaluatie en monitoring van de adequaatheid en doeltreffendheid van de boekhouding en het intern beheersing systeem.
Interne audit team	(1) Afdeling of activiteit binnen een entiteit, die door het management de taak kreeg toevertrouwd om de systemen en procedures door te lichten zodat de risico's op fraude, fouten of inefficiënte werkwijzen geminimaliseerd worden. Interne beheersing moet onafhankelijk zijn binnen de organisatie en brengt rechtstreeks verslag uit aan het management. (2) Een afdeling, divisie, team van raadgevers, of andere xxx die onafhankelijke objectieve raadgevende diensten aanbrengen teneinde de operaties te verbeteren en te opwaarderen. De interne beheersing activiteiten helpen een organisatie om haar objectieven te bereiken door een systematische en gedisciplineerde aanpak van de evaluaties om zo de doeltreffendheid van het risicomanagement, de beheersing en de beleidsvoering te verbeteren.
Interne auditor(en).	Bestuderen en dragen bij tot de voortdurende doeltreffendheid van het intern beheersing systeem door hun evaluaties en aanbevelingen, maar ze zijn niet verantwoordelijk voor het ontwerpen, implementeren, documenteren en onderhouden van het interne beheerssysteem.
Interne beheersing	Interne beheersing is een totaal-proces dat beïnvloed word door het management en het personeel van een entiteit en dat ontworpen is om risico's aan te pakken en een mate van zekerheid te bieden dat, in het streven naar de opdracht van de entiteit, de

	volgende algemene doelen kunnen worden bereikt: Ordelijk, ethisch, economisch, efficiënt en effectief operaties uitvoeren Verantwoordelijk verplichting vervullen Wetten en reglementen respecteren Kapitalen beschermen tegen verlies, misbruik en beschadigingen.
Interne beheersing component	Elk van de 5 componenten van interne beheersing Deze onderdelen zijn - de interne beheersing omgeving van de entiteit - inschatting van de risico's - beheersing activiteiten - informatie en communicatie - monitoring
Interne beheersing systeem	(Proces of raamwerk) Synoniem voor de interne beheersing toepast in een entiteit.
INTOSAI	International Organisation of Supreme Audit Institutions. Beroepsorganisatie van SAI in landen van de VN of hun gespecialiseerde organismen. SAI"s spelen een grote rol in overheidsaudits en operaties door het aanmoedigen van gezond financieel management en verantwoordelijkheidszin van de besturen. INTOSAI is gesticht in 1953 en groeide van 34 landen tot meer dan 170 SAI.
Inherent risico	Het risico voor de entiteit door afwezigheid van risicomanagement kan ervoor zorgen dat er grotere risico's aankomen of dat de impact ervan vergroot.
Inherente beperkingen	Beperkingen in elk intern beheersing systeem. Ze slaan op de beperkingen in menselijk inschattingsvermogen; beperking in middelen en de kosten van de beheersing in verhouding tot de baten; het gegeven dat pech kan voorkomen en de mogelijkheid van management override en corruptie.
Logische toegang	Het toegang krijgen tot computer data. Dit kan beperkt zijn tot "alleen lezen" maar ook het recht geven om data aan te passen, nieuwe data in te voeren en te wissen.
Mainframe	Zeer performante computer ontworpen voor intensief gebruik. Mainframes worden dikwijls gedeeld door verschillende gebruikers via terminals.
Management	Bestaat uit officieren (directieleden) en andere personen die senior management functies uitoefenen. In het management zitten ook directeurs en de audit commissie maar enkele wanneer ze management functies uitoefenen.
Management proces	De acties genomen door het management om de entiteit te leiden. Interne beheersing is een onderdeel van het geïntegreerde management proces.
Management tussenkomst	Actie van het management tot het wijzigen van de procedures voor gegronde redenen. Dit is meestal nodig om het hoofd te bieden aan niet-wederkerige en buitengewone acties of gebeurtenissen en die anders door het systeem niet correct zouden zijn behandeld.
Manangement override	Het niet-legitiem veranderen van de normale procedures door het management met de bedoeling zichzelf te verrijken of de financiële

	situatie te verfraaien of het niet-naleven van de regelgeving te verdoezelen.
Manuele beheersing	Beheersing die manueel, dus niet met een computer, worden uitgevoerd.
Naleving van de regelgeving	Zich schikken naar wetten en regels die gelden voor deze entiteit (COSO 1992). Overeenstemming met en toepassing van de principes, plannen, wetten, regels, contracten en andere vereisten.
Netwerk	In IT: een groep van PC's en randapparatuur verbonden door communicatiemiddelen. Deze kunnen permanent (Kabels) of tijdelijk (via telefoon of andere verbindingen) zijn. Een netwerk kan uit slechts enkele PC's en randapparatuur bestaan maar kan ook kleine en grote PC's in een uitgebreid geografisch gebied omvatten.
Objectiviteit	Onbevooroordeelde mentale ingesteldheid die SAI, interne en externe auditoren in staat moet stellen op hun werk op een geloofwaardige manier uit te voeren en ervoor zorgt dat er geen beduidende toegevingen op de kwaliteit worden gedaan. Het betekend ook dat auditoren hun inschatting van de geauditeerde middelen niet laten beïnvloeden door anderen.
Onafhankelijkheid	(1) INTOSAI - Guidelines Public Sector (2) Definitions NL (3) vrijheid die aan een audit orgaan en haar leden word gegeven om binnen de hun gegeven macht zonder inmenging van buiten uit te kunnen werken. (4) Vrijheid van de SAI om op te treden volgens hun mandaat zonder invloed van de directie of van buiten uit. (5) De afwezigheid van factoren die de objectiviteit of de schijn van objectiviteit ondermijnen. Zulke factoren moeten behandeld worden op het niveau van individuele auditor, het engagement, het functionele en organisatorische niveau. (6) Het vermogen van de auditor om een onbevooroordeeld standpunt in te kunnen nemen in de uitvoering van zijn taak. (7) Het vermogen van de auditor om een onbevooroordeeld standpunt in te kunnen nemen in de ogen van anderen.
Ontwerp	- Plan. De manier waarop een systeem zou moeten werken, dit in tegenstelling tot hoe het werkelijk werkt. - Doel. Als in de definitie: Interne beheersing heeft als doel een zekere mate van zekerheid te bieden om de objectieven te verwezenlijken. Als het doel bereikt word kan het systeem als effectief worden beschouwd.
Onzekerheid	De onmogelijkheid om op voorhand de waarschijnlijkheid of de impact van toekomstige gebeurtenissen te kennen.
Openbare sector	Verwijst naar nationale, regionale(provincie, gewest) en lokale (gemeenten, steden) besturen en overheidsinstellingen (agentschappen, raden, commissies en ondernemingen).
Operaties	• Wat te maken heeft met de doeltreffendheid en de doelmatigheid van de activiteit van een entiteit. Met inbegrip van productiviteit, winstdoelstellingen en het

	vrijwaren van middelen. • De functies, processen en activiteiten waardoor de doelstellingen van de entiteit bereikt worden.
Opsporing beheersing	Beheersing om een ongewilde gebeurtenis of ongewild resultaat te ontdekken. (In tegenstelling tot preventieve beheersing.)
Monitoring	Is een onderdeel van de interne beheersing dat de kwaliteit van het interne beheerssysteem over de loop van tijd inschat.
Ordelijk (gestructureerd)	*Ordelijk* betekent: goed georganiseerd, methodisch.
Output	in IT: data of informatie als resultaat van computerverwerking. Bv. Grafieken op scherm of hardcopie.
Restrisico	Het risico dat blijft bestaan nadat het management op een risico heeft gereageerd.
Preventieve beheersing	Beheersing ter voorkoming van ongewilde gebeurtenissen of resultaten.
Publieke verantwoording	De verplichting van personen of entiteiten, met inbegrip van openbare besturen en organisaties die met openbare middelen werken, om rekenschap af te leggen over de hun opgelegde fiscale, bestuurlijke en werking verantwoordelijkheden en verslag uit te brengen aan hen die hun deze verantwoordelijkheden gaven.
Redelijke mate van zekerheid verschaffen	Redelijke zekerheid = een bevredigende mate van vertrouwen in functie van kosten, baten en risico's. Interne beheersing kan het management nooit absolute zekerheid bieden met betrekking tot het verwezenlijken van de gestelde doelen, hoe goed ontworpen en uitgevoerd deze ook mag zijn. Deze richtlijnen houden er rekening mee dat slechts een "redelijke" mate van zekerheid te verkrijgen is.
Risico	De mogelijkheid van een gebeurtenis die invloed kan hebben op het behalen van het beoogde resultaat.
Risicoevaluatie	Bepalen van de vermoedelijke grootte van het risico en de waarschijnlijkheid waarmee het zich zal voordoen.
Risicoanalyse	Is het proces om relevante risico's voor het bereiken van de objectieven te identificeren en te analyseren en de gepaste acties hierop te bepalen.
Risicoanalyse proces	Een voortdurend interactief proces om veranderde condities, mogelijkheden en risico's te identificeren en gepaste acties te nemen, vooral in het bijsturen van de interne beheersing. Risicoprofielen en de daaraan gekoppelde beheersings moeten regelmatig herbekeken en bijgewerkt worden zodat er zekerheid is dat het risicoprofiel actueel blijft, dat de reacties op risico's doelgericht blijven en de beheersing effectief blijven tegenover de steeds veranderende risico's.
Risicobereidheid	Het risico dat een entiteit bereid is te lopen alvorens er acties tegen dat risico worden genomen. Het risico dat een entiteit bereid is te nemen in het streven naar de uitvoering van haar visie of missie.
Risicotolerantie	De aanvaardbare afwijking van het gestelde objectief.
Risicoprofiel	Een overzicht of raamwerk van de risicofactoren waaraan de

	entiteit of het onderdeel ervan kan blootgesteld worden met inschatting van de grootte ervan,(hoog, middel, laag) samen met de waarschijnlijkheid of zekerheid van voorkomen.
SAI Supreme audit Institution	Hoogste orgaan van een land dat, onafhankelijk van de aanstelling, samenstelling en organisatie ervan, de hoogste wettelijk bevoegde instantie voor auditing is voor dat land (Rekenhof).
Scheiding van taken	Om het risico op fouten, verspilling en slechte bedoelingen en het risico van het niet ontdekken hiervan te verminderen, mag er nooit één enkele persoon of één team verantwoordelijk zijn voor alle fases (toelaten, verwerken, inbrengen, nazicht) van een transactie of gebeurtenis.
Systeem software	Software die in eerste instantie instaat voor het beheren en beheersen van de hardware en communicatiemiddelen, toegang tot bestanden en data, en de beheersing en planning van applicaties.
Systeem software beheersing	beheersing over de computerprogamma's en aanverwante software om de werking en beheersing van de verwerkings activiteiten of de computer uitrusting.
Tekortkoming	Een herkende, potentiële of reële tekortkoming, of een gelegenheid om de interne beheersing te versterken en zo een grotere mogelijkheid te creëren om de objectieven te bereiken.
Toegang beheersing	In het domein van informatie technologie, beheersing ontwikkeld om gegevens te beschermen tegen ongeoorloofde aanpassingen, verlies of verspreiding.
Veiligheidsprogramma	Programma dat de basis vormt van de structuur van de veiligheid beheersing van de entiteit en een uiting is van het engagement van het management om risico's aan te pakken. Dit programma moet het uitgangspunt zijn voor de risico inschatting, het ontwikkelen en implementeren van werkende veiligheidsprocedures en het opvolgen van de doeltreffendheid van deze procedures.
Verantwoording	Proces waarbij openbare besturen en de personen daar tewerkgesteld verantwoordelijk worden gesteld voor hun beslissingen en daden, met inbegrip van hun beheer van publieke fondsen en alle aspecten van hun takenpakket. Opdracht gegeven aan een geauditeerd persoon of entiteit zodat hij/het kan aantonen dat de toevertrouwde fondsen beheerd of gecontroleerd werden in overeenstemming met de voorwaarden waaronder deze fondsen werd toegekend.
Verwerking	In IT: Het uitvoeren van een programma door een PC
Werkwijze	Management richtlijnen i.v.m. het uitvoeren van interne beheersing. Een richtlijn dient als basis voor het uitwerken en implementeren van procedures.