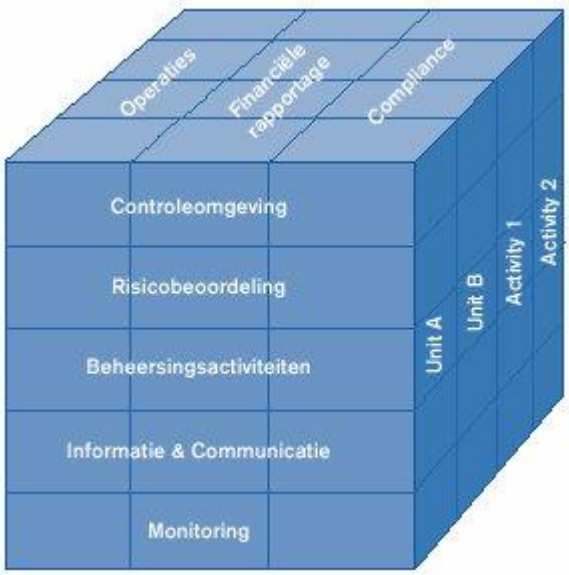
COSO

Het COSO-model is een risicomanagementmodel waarmee je kunt bepalen in hoeverre een organisatie controle heeft over de situatie, oftewel 'in control is'. Op basis van dit model kun je aanbevelingen doen om het risicomanagement te verbeteren.

Laten we eens kijken naar een voorbeeld om het gebruik van het COSO-framework te illustreren:

Stel je voor dat je werkt voor een productiebedrijf dat chips produceert; een productieproces bekend om de precisie waarmee gewerkt moet worden. Het bedrijf groeit sterk en wil ervoor zorgen dat het interne controlesysteem effectief is om risico's te beheersen en operationele efficiëntie te waarborgen.

Laten we voor de uitwerking van het risicomanagement deze casus eens leggen naast een vereenvoudigde weergave van het COSO-model om zo het model te leren kennen.



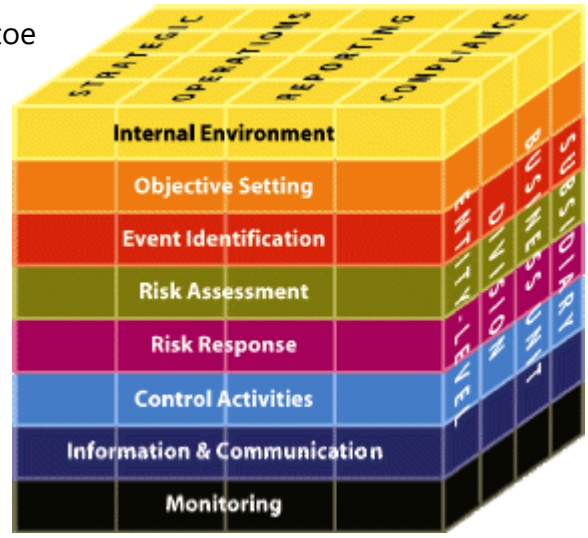
In deze casus gaan we blijkbaar in op de risico's m.b.t. op de operationele efficiency. Als je kijkt naar de bovenkant van de kubus, dan zitten we dus in de meest linker kolom 'operaties'. Je zou ook COSO kunnen gebruiken om de risico's zijn te kunnen beheersen dat de (financiële) rapportages niet betrouwbaar zouden. Dan zitten we dus in de middelste kolom van de bovenkant. Ook kunnen we proberen in control te komen op het onderwerp compliance, dat wil zeggen op de naleving van wet- en regelgeving om daarmee het vertrouwen van stakeholders te vergroten.

Kortom, de bovenzijde van de kubus gaat over het doel dat je wilt bereiken met je risicomanagement. Uiteindelijk zal een organisatie natuurlijk op alle drie doelen in control willen zijn, maar het is verstandig om niet alles in 1 keer aan te pakken en je steeds te focussen op 1 doel tegelijkertijd.

Aan de zijkant van de kubus kan je aangeven over welke entiteit je het risicomanagement aan wil pakken: is dat een specifiek bedrijfsonderdeel, afdeling of proces? In deze casus betrof het dus het productieproces. Ook hier maken we dus weer een keuze om ons te kunnen focussen, en niet alle processen tegelijkertijd op de schop te zetten.

Aan de voorzijde van de kubus zie je vervolgens een stappenplan om te komen tot risicobeheersing.

Als we vervolgens de complete COSO-kubus erbij pakken, dan zien we dat er naast de 3 al eerder genoemde doelen er nog 1 is, namelijk strategie. Een bedrijf kan ook risicomanagement toe willen passen op de strategievorming. Hoe kunnen we zorgen dat we de strategische doelen goed stellen en bereiken?



Aan de rechterzijkant heeft men ook extra suggesties toegevoegd. Je kan daarbij bepalen of je COSO wil toepassen op een specifieke business unit, een divisie, deelnemingen (subsidiary) of op welk level dan ook. In onze casus hadden we al gekozen voor het toepassen van COSO op het productieproces.

Ook de voorzijde heeft een uitbreiding ondergaan: 8 stappen i.p.v. 5. Als we de casus van het productiebedrijf eens uitwerken in 8 stappen, krijgen we het volgende stappenplan.

Stap 1: Interne omgeving / controle omgeving
Het bedrijf moet een sterke interne omgeving creëren door het bevorderen van verantwoordelijkheid binnen de organisatie. Ze kunnen bijvoorbeeld een gedragscode opstellen en communiceren naar alle werknemers om ervoor te zorgen dat iedereen op de hoogte is van de normen, en werken aan het versterken van de soft controls.

Stap 2: Doelstellingen
Het bedrijf moet bepalen welke doelstellingen zij heeft voor het productieproces, dus wat wil men bereiken in termen van effectiviteit en efficiency. In deze specifieke branche is het bijvoorbeeld van cruciaal belang dat de geproduceerde chips geen enkel defect vertonen. Immers bij chipfabricage geldt dat elke verstoring al snel een drama is omdat de chips zo klein en gevoelig zijn en de chip al snel weggegooid moet worden.

Stap 3: Identificatie gebeurtenissen
Bij stap 3 bepaalt men welke gebeurtenissen van cruciale invloed zijn om de

doelstellingen wel of niet te behalen. Denk in het geval van de chipsfabrikant aan de levering van de grondstoffen/materialen omdat dat deels schaarse metalen betreft. Maar je kan ook denken aan mankementen in het traject van kwaliteitscontrole.

Stap 4: Risicobeoordeling
Het bedrijf moet op systematische wijze de belangrijkste risico's evalueren waarmee het wordt geconfronteerd als de bij stap 3 geïdentificeerde gebeurtenissen zich voordoen. Ze kunnen bijvoorbeeld risicomanagementteams vormen om risico's te identificeren, en van die risico's de waarschijnlijkheid/kans en consequenties/impact te beoordelen.

Stap 5: Reactie op risico
Het bedrijf moet vervolgens bepalen op basis van de kans en impact beoordelen of ze een risico willen aanpakken of niet. Willen ze het misschien aanvaarden, of zich er tegen verzekeren, of volledig uitsluiten of slechts beperken. In geval van de chipsfabrikant zou heel goed kunnen dat ze bepaalde risico's bij voorkeur compleet willen uitsluiten.

Stap 6: Beheersactiviteiten
Het bedrijf moet passende beheersactiviteiten implementeren om de geïdentificeerde juiste risico-response van stap 5 te bereiken. Bijvoorbeeld, ze kunnen procedures en richtlijnen opstellen voor inkoop- en productieprocessen, kwaliteitscontroles uitvoeren op de geproduceerde chips en regelmatig onderhoud uitvoeren aan de productie-machines om daarmee 100% kwalitatief goede producten te kunnen garanderen.

Stap 7: Informatie en communicatie
Het bedrijf moet relevante informatie vastleggen en communiceren in de gehele organisatie. Dit omvat het delen van beleidsregels, procedures en andere belangrijke informatie met werknemers. Maar ook hier weer: het versterken van de soft controls; zorgen dat de binding en trots op het eigen bedrijf/werk zo groot is dat men secuur blijft werken.

Stap 8: Monitoring
Het bedrijf moet vervolgens een continu proces van monitoring instellen om ervoor te zorgen middels bijsturing dat de interne controles effectief blijven.