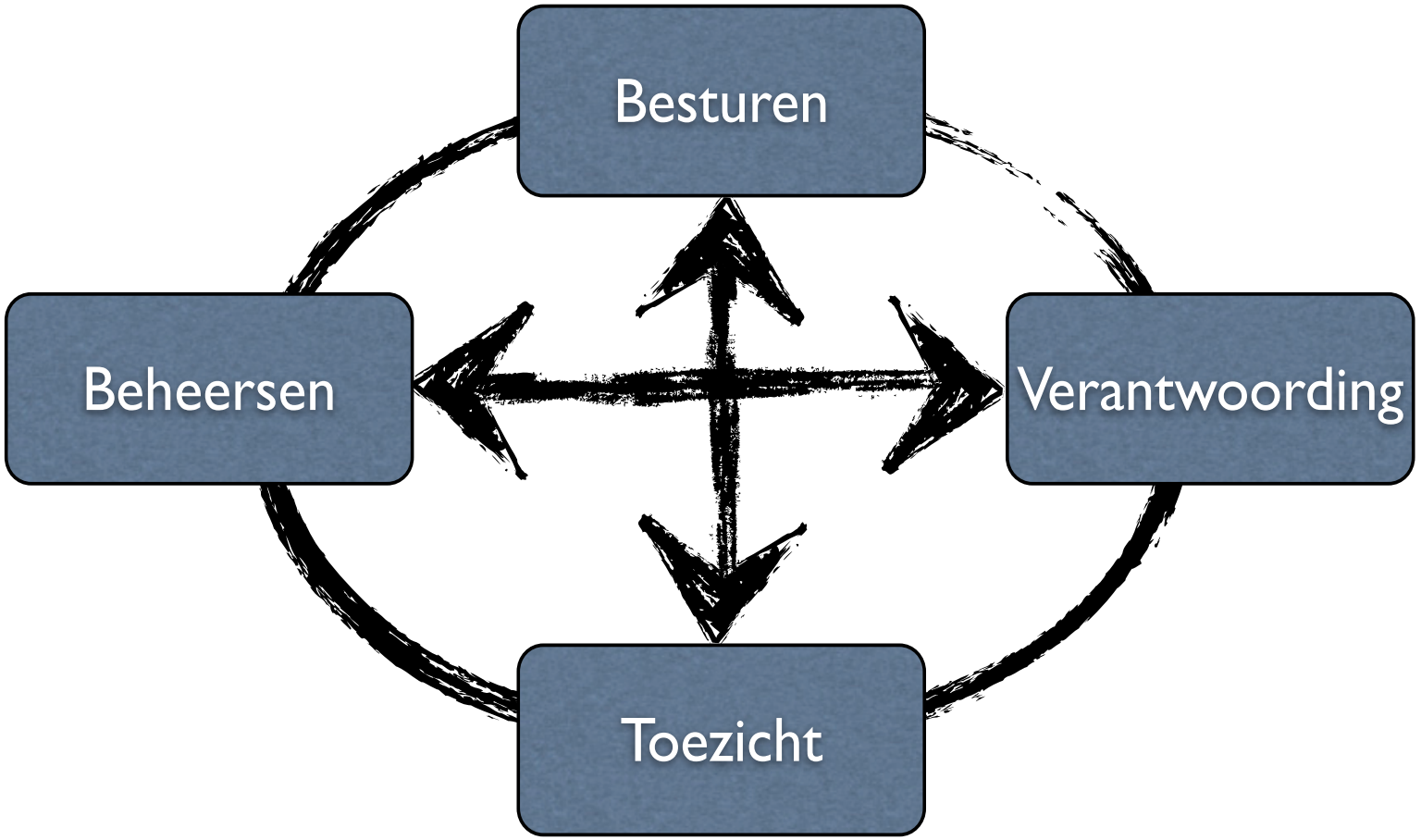
CISO/PvIB

Aspecten van informatiebeveiliging

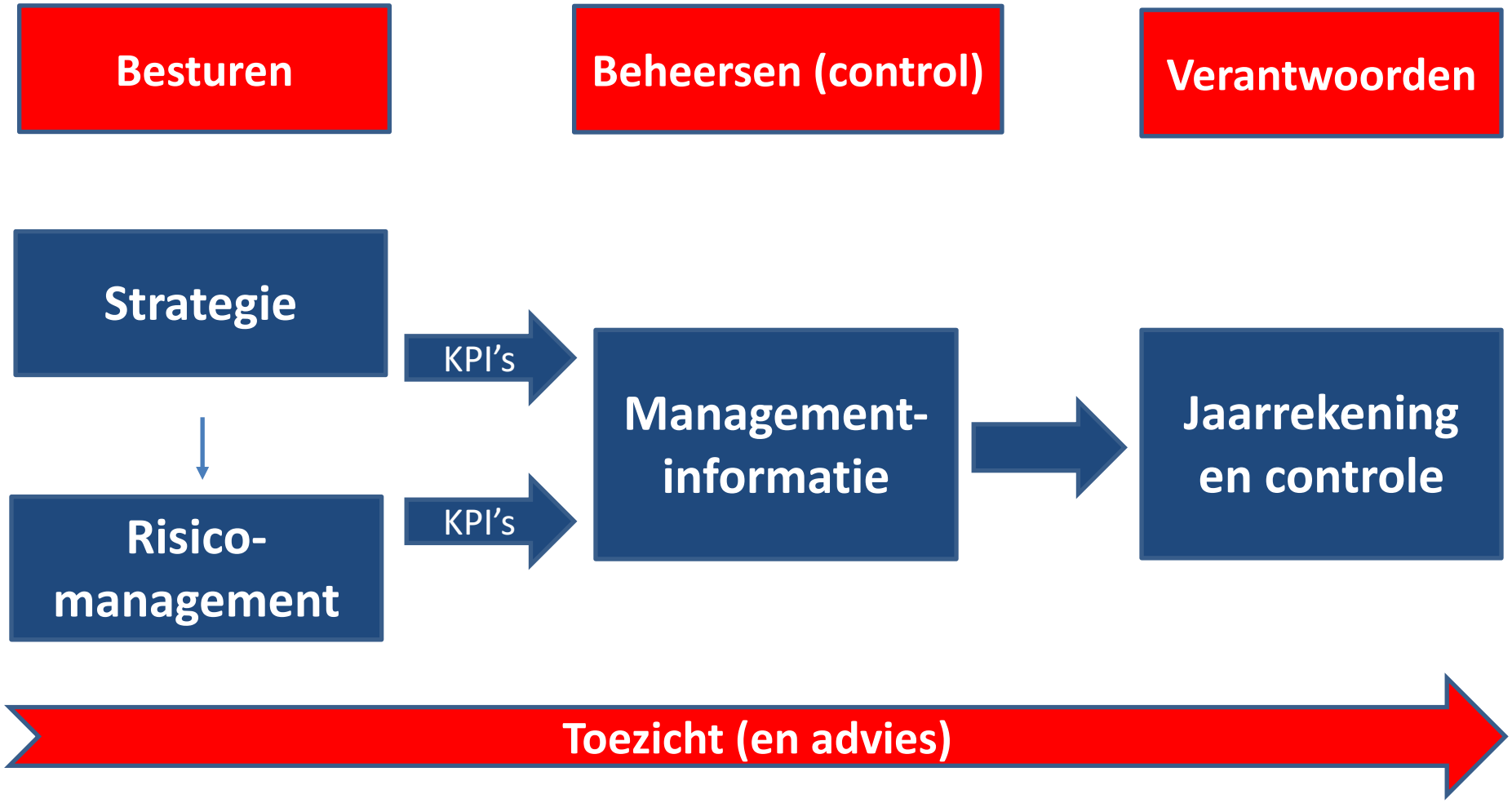
Cees in ‘t Veld

Bunnik, 29 maart 2017

Goed organisatiebestuur: Kernfuncties



Goed organisatiebestuur: modelmatig



‘In control’ (Bron: www.houseofcontrol.nl)

'In control' zijn betekent dat je je eigen organisatie goed bestuurt. En dat heeft weer alles te maken met het begrip 'voorspelbaarheid'.

Organisaties zijn omgeven met interne en externe onzekerheden (risico’s) die de realisatie van de doelstellingen in gevaar kunnen brengen.

Een organisatie is 'in control' als ze deze onzekerheden (risico’s) onderkent en maatregelen neemt zodat de organisatie voorspelbaar wordt.

‘In control’ (Bron: www.houseofcontrol.nl)

De meest voorkomende begrippen in de definities van ‘control’ zijn:

- Realiseren van doelstellingen;
- Sturing;
- Effectieve en efficiënte processen;
- Gedragsbeïnvloeding;
- Maatregelen;
- Beheersen van risico's en onzekerheden.

Een organisatie is 'In Control' als een organisatie zodanig is ingericht dat de juiste discussie op het juiste moment op het juiste niveau wordt gevoerd zodat (indien nodig) bijgestuurd kan worden om zo de doelstellingen te realiseren.

'In Control' wil dus zeggen dat de organisatie zo is ingericht dat goed bestuur mogelijk is.

Risicomanagement volgens COSO

Definitie volgens The **Co**mmittee of **S**ponsoring **O**rganizations:

- een proces bewerkstelligd door het bestuur, het management en ander personeel van de onderneming;
- toegepast bij het formuleren van de strategie binnen de hele onderneming;
- om potentiële gebeurtenissen met mogelijke invloed op de onderneming te identificeren en om risico's te beheren zodat deze binnen de risico acceptatiegraad vallen;
- om een redelijke zekerheid te bieden ten aanzien van het behalen van de ondernemingsdoelstellingen.

Risicomanagement: Definities

Risico is de kans dat een gebeurtenis plaatsvindt, vermenigvuldigd met het gevolg van die gebeurtenis, kortgezegd: risico = kans x effect.

Op basis van de risico-inventarisatie kan het **risicoprofiel** worden bepaald.

De **risicobereidheid** (de “risk appetite”) is een beeld op hoog abstractieniveau van de hoeveelheid risico dat het bestuur en het management willen lopen of accepteren bij het nastreven van hun doelstellingen.

De risicobereidheid bepaalt de aard en diepgang van de beheersingsmaatregelen.

Risicomanagement: Definities 2

We onderkennen drie categorieën risicobereidheid:

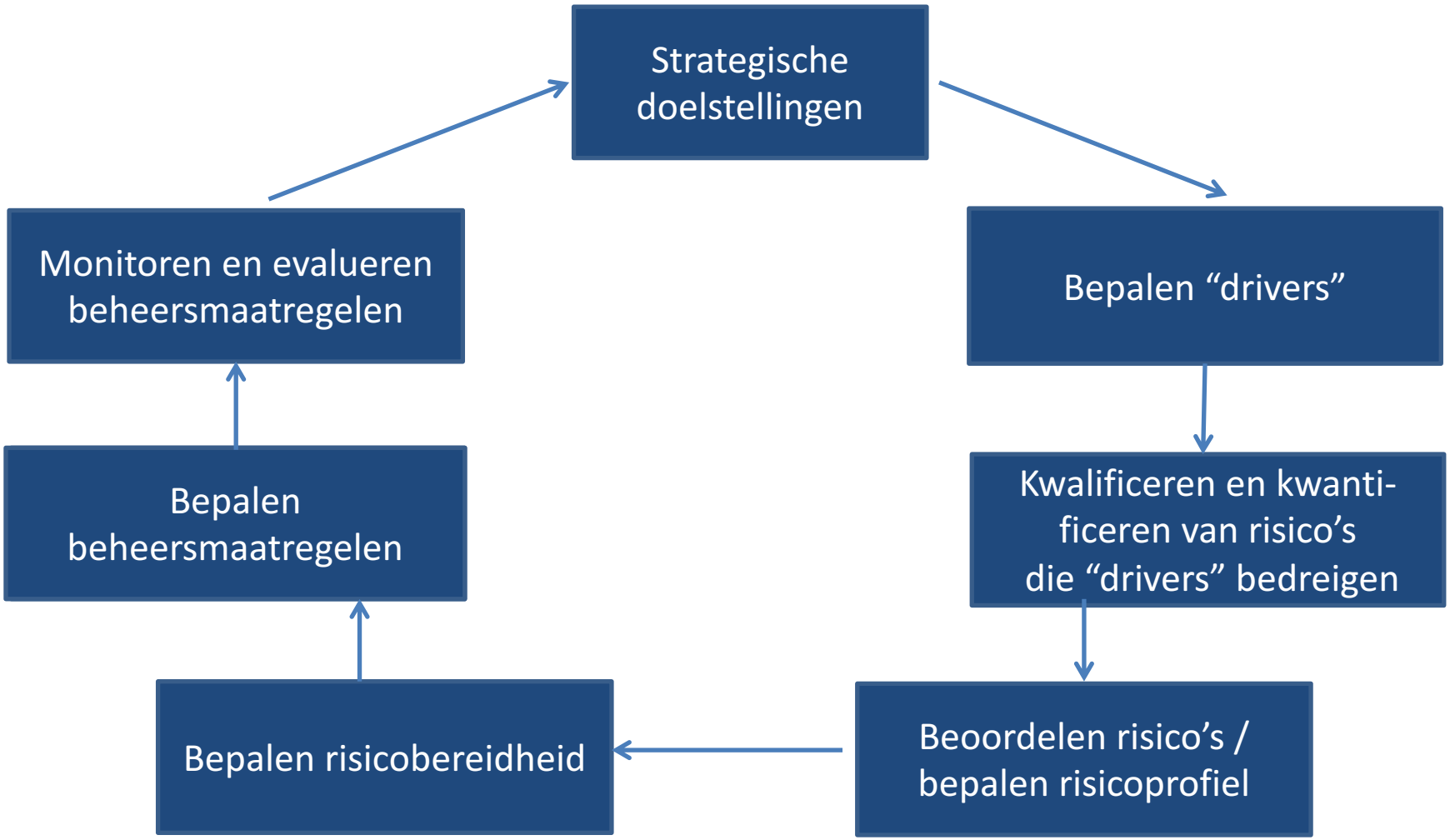
- risicomijdend
- risiconeutraal
- risicozoekend

Risicobereidheid is een keuze en is een balans tussen zekerheid en de kosten van die zekerheid.

Risico – effect beheersing = restrisico.

Het is onmogelijk om alle risico's op een bepaald moment te kennen, laat staan deze volledig te beschrijven en te beheersen. Daarom richt het risicobeheersing- en controlesysteem zich op de belangrijkste risico's.

Risicomanagement: P-D-C-A Cyclus



Risicomanagement: Voordelen

Risicomanagement:

- kan organisaties inzicht geven in wat kan gebeuren.
- stelt organisaties in staat om prioriteiten aan onderkende risico's toe te kennen en daardoor gestructureerd acties te ondernemen, waardoor lukrake acties kunnen worden voorkomen.
- maakt het organisaties mogelijk om bij besluitvorming een betere financiële afweging te maken om maatregelen te treffen.
- maakt het voor organisaties mogelijk om genomen beslissingen aangaande risico's te verantwoorden.

Risicomanagement: Nadelen

Bij onbalans tussen risico en beheersmaatregelen kan risicomanagement:

- initiatieven vertragen of blokkeren;
- verstikkend werken;
- daardoor waardecreatie in de weg staan.

Risicomanagementmodel

Beheersen van risico's

	Passief	Actief
Effect hoog	Overdragen	Vermijden/ elimineren
Effect laag	Accepteren	Reduceren
	Kans laag	Kans hoog

Reduceren

	Reduceer kans	Reduceer effect
Preventief	* Procedures * Regels en regulering * Opleiding en training	* Communicatie * Contractuele afspraken * Proces-monitoring
Repressief	* "Lessons learned"	* Garantie en service

Bron: Bedrijfsvitaliteit/Van Heeswijk

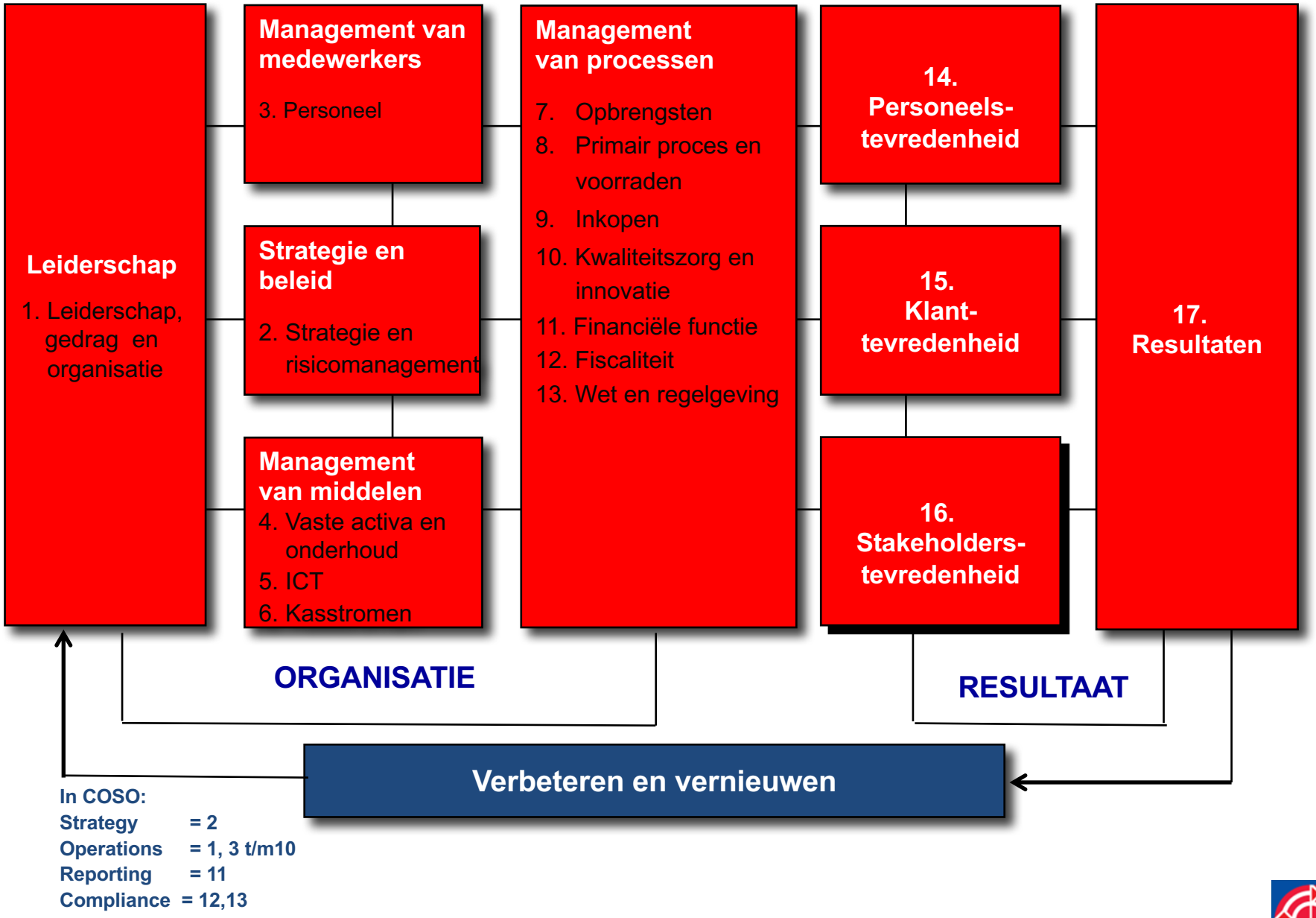
Risicomanagement - Het Interne Controle Raamwerk

Het verdient sterke aanbeveling om het beheersen van risico's (= in control zijn) beknopt vast te leggen in een beschrijving van het "Interne Controle Raamwerk" (hierna: ICR).

Het lijkt logisch om de financieel eindverantwoordelijke binnen de organisatie hierbij een belangrijke rol te geven.

Het ICR moet wel volledig maar niet te uitgebreid zijn en een duidelijke structuur volgen. De structuur is vormvrij.

INK-model



In COSO:
Strategy = 2
Operations = 1, 3 t/m10
Reporting = 11
Compliance = 12,13

Mogelijke indeling ICR 1

- Algemeen: generieke omschrijving van de onderneming (missie en visie, kernwaarden, organisatiestructuur, omvang, activiteiten, geografische spreiding).
- Gekozen risicomodel.
- Beschrijving verzekeringsportefeuille.
- Strategie (businessplan, resultaten van PESTEL-analyse, sterkte/zwakte analyse, BCG-matrix, toekomstgericht denken).
- Personeel (kwaliteit, beschikbaarheid, flexibiliteit).
- ICT-middelen (management en organisatie van de ICT, logische toegangsbeveiliging, wijzigingsbeheer, incident-/probleemmanagement, fysieke beveiliging, back up en herstel, uitwijk).
- Overige middelen (huisvesting, machines en installaties, voorraden, financieringsmiddelen).

Mogelijke indeling ICR 2

- Processen (verkopen, inkopen, productie/primair proces, kwaliteitszorg, innovatie, communicatie).
- Financiële functie en rapportage.
- Voldoen aan wet- en regelgeving (governance structuur, ingeregelde bevoegdheden, opmaken en deponeren jaarrekening, fiscale zaken, juridische zaken, contractbeheer, algemene voorwaarden, fraudebeleid e.d.).
- Personeelstevredenheid.
- Klanttevredenheid.
- Stakeholdertevredenheid.
- Resultaten.

Voordelen ICR 1

Voordelen van het Interne Controle Raamwerk

- De opsteller(s) van het ICR worden gedwongen om organisatiebreed nog eens na te gaan hoe het ook alweer zat met de interne controle en de monitoring daarvan.

- Het kennisnemen van het ICR door interne belanghebbenden als bestuurders , MT-leden en adviseurs/commissarissen/toezichthouders draagt bij aan de bewustwording bij betrokkenen en verbetert daardoor ook de signalering van risico's met "Kans hoog, effect hoog".

Voordelen ICR 2

Voordelen van het Interne Controle Raamwerk

- Het ICR kan desgewenst worden gedeeld met externe stakeholders als financiers of partijen waarmee strategisch wordt samengewerkt.

- Door het ICR periodiek (bijvoorbeeld jaarlijks) opnieuw te herijken en vast te stellen ontstaat een levend document dat, nadat het eenmaal is opgesteld, eenvoudig is te onderhouden. Tevens blijft daardoor de kennis binnen het management actueel.

Informatiebeveiliging (1)

- Managementinformatie en externe verantwoording spelen een belangrijke rol in goed organisatiebestuur
- Informatie & Communicatie Technologie (hierna: ICT) is vandaag de dag onmisbaar en niet meer weg te denken
- Daarmee zijn een adequate beheersing van informatie en ICT-omgeving basisvoorwaarden voor de continuïteit van de onderneming
- Incidenten rond informatiebeveiliging zijn aan de orde van de dag (Hillary Clinton, Kadaster enz. enz.)
- De wetgever probeert het tempo bij te houden met nieuwe regelgeving (privacy, zorgplicht, meldingsplicht)

Informatiebeveiliging (2)

- Uit recente onderzoeken onder bestuurders en commissarissen blijkt zowel het onderkennen van het belang van ICT als de kennis van ICT in totaliteit bezien bij beide groepen vaak ver onder de maat is.

- De komende vijf jaren is sprake van een verwachte golf van innovaties in de nanotechnologie, de medische technologie en de biotechnologie en de opkomst van verregaand gedigitaliseerde exponentiële organisaties.

- Door de toenemende omvang en invloed van ‘big data’ wordt het belang van informatiebeveiliging nog belangrijker

- Menselijk gedrag is een zwakke schakel in het beheersen van risico’s

Informatiebeveiliging (3)

De vraag is: hoe verder?

INK - model ICT

In COSO: S = Strategy, R = Reporting, C = Compliance, overige = Operations

Toekomstgericht denken 1

Het krachtenveld waarin organisaties opereren verandert voortdurend en ook steeds sneller.

Ontwikkelingen op het gebied van globalisering, techniek, demografie, sociale media, duurzaamheid en regelgeving zijn ingrijpend en raken elke organisatie.

Denken in risico's vanuit opgedane ervaringen dekt daarom niet per definitie alle risico's!

Toekomstgericht denken 2

Toekomstgericht denken is daarmee een essentieel onderdeel van risicomanagement geworden. Hierdoor worden belangrijke ontwikkelingen tijdiger gesignaleerd en is er meer tijd om op ontwikkelingen te reageren door risico's preventief te reduceren.

Hoe breder het toekomstgericht denken binnen de organisatie is belegd, hoe sterker de signalerende en preventieve werking ervan.

Toekomstgericht denken 3

Hulpmiddelen:

- het periodiek opstellen/actualiseren van PEST-analyse, BCG-matrix, sterkte/zwakte analyse;
- scenariodenken;
- alert zijn op faillissementsrisico's;
- het periodiek reflecteren op de levensfase van de onderneming;
- alert zijn op frauderisico's;
- het kennis nemen van publicaties van trendwatchers en sectorrapporten;
- het delen van ervaringen met branchegenoten;
- benchmarking;
- het bijwonen van bijeenkomsten.

Stappenplan risicomanagement 1

1. Beleg risicomanagement bovenin uw organisatie.

2. Introduceer een risicomanagementmodel dat passend is voor uw organisatie.

3. Ontwikkel op een gestructureerde wijze toekomstgericht denken in uw organisatie.

4. Integreer risicomanagement in uw bestaande planning & control cyclus (begrotingsprocedure, kritische sturingsindicatoren, management informatie, managementoverleg, actie/bijsturing, jaarverslag).

Stappenplan risicomanagement 2

5. Evalueer periodiek uw verzekeringsportefeuille.

6. Beschrijf het Interne Controle Raamwerk, actualiseer dit periodiek en neem gestructureerd actie op gesignaleerde leemten.

7. Besteed in het Interne Controle Raamwerk specifiek aandacht aan afwijkende organisatie-onderdelen.

8. Zorg voor goede ‘soft controls’.

Bijlage

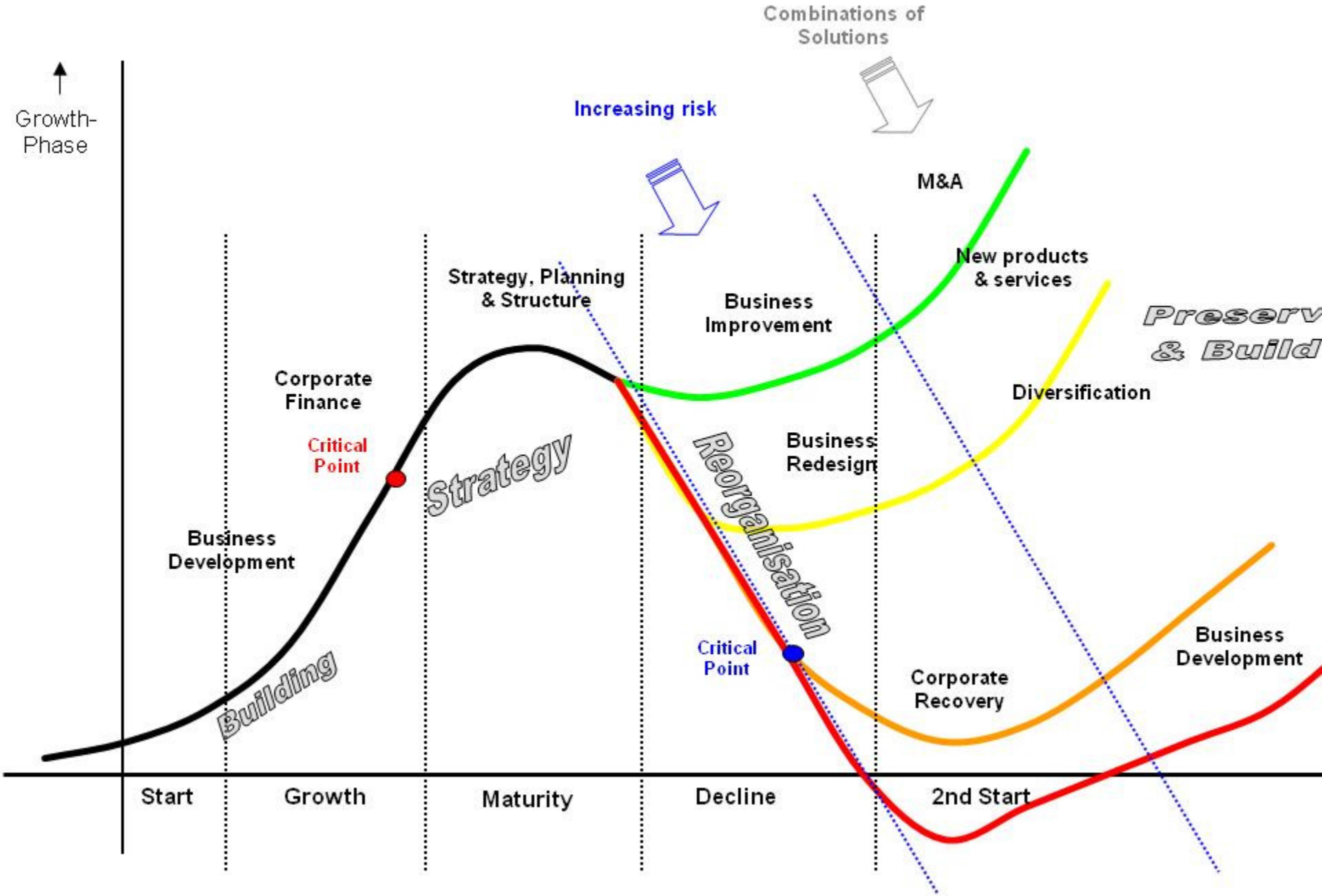
Risicofactoren:

- Faillissement
- Levenscyclus van de onderneming
- Fraude

Risicomanagement

Tien belangrijke oorzaken van faillissementen

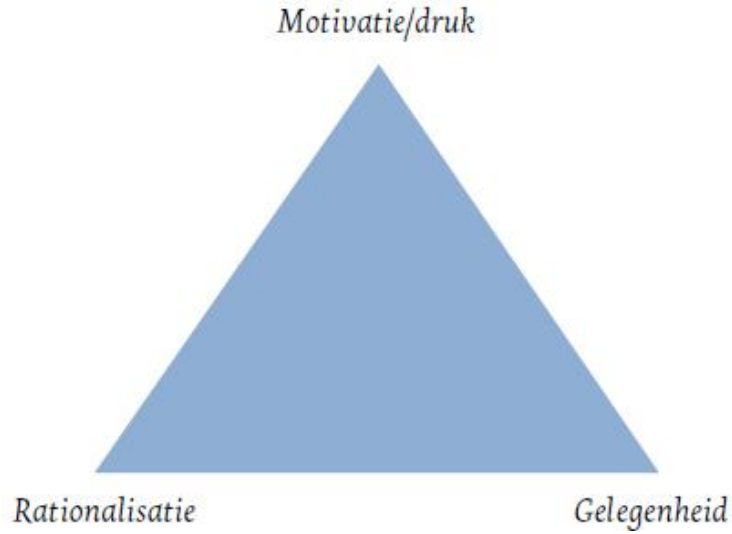
1. Wanbeheer, slecht management of een gebrek aan visie
2. Onvoldoende kapitaal
3. Wie niet kan rekenen, gaat failliet
4. Wanbetaling of faillissement van de klant
5. Slechte economie
6. Vraaguitval en omzetdaling
7. Minder snel krediet
8. Veranderende markt en concurrentie
9. Calamiteiten en ziekte
10. Wijziging wet- en regelgeving


Combinations of Solutions
Increasing risk
Growth-Phase
M&A
New products & services
Strategy, Planning & Structure
Business Improvement
Preserv & Build
Corporate Finance
Diversification
Critical Point
Strategy
Business Redesign
Reorganisation
Business Development
Critical Point
Business Development
Corporate Recovery
Building
Start
Growth
Maturity
Decline
2nd Start

Risicomanagement - Fraude 1

Fraude = een opzettelijke handeling door één of meer leden van het management, met governance belaste personen, werknemers of derden, waarbij gebruik wordt gemaakt van misleiding teneinde een onrechtmatig of onwettig voordeel te verkrijgen
(COS 240)

Fraudedriehoek:



Risicomanagement - Fraude 2

Voorkomen van fraude:

- Duidelijk stelsel van regels en procedures(waaronder een gedragscode gekoppeld aan arbeidscontract)
- Invoeren van effectieve (interne) controle
- Adequate scheiding van functies en verantwoordelijkheden
- Mogelijkheden tot melden en rapporteren van fraude
- Training en opleiding
- Indien jaarrekeningcontrole: dialoog met accountant