

WHITEPAPER

Het enterprise risk management raamwerk

"Concrete aanbevelingen om jouw ERM raamwerk efficiënt in te richten"

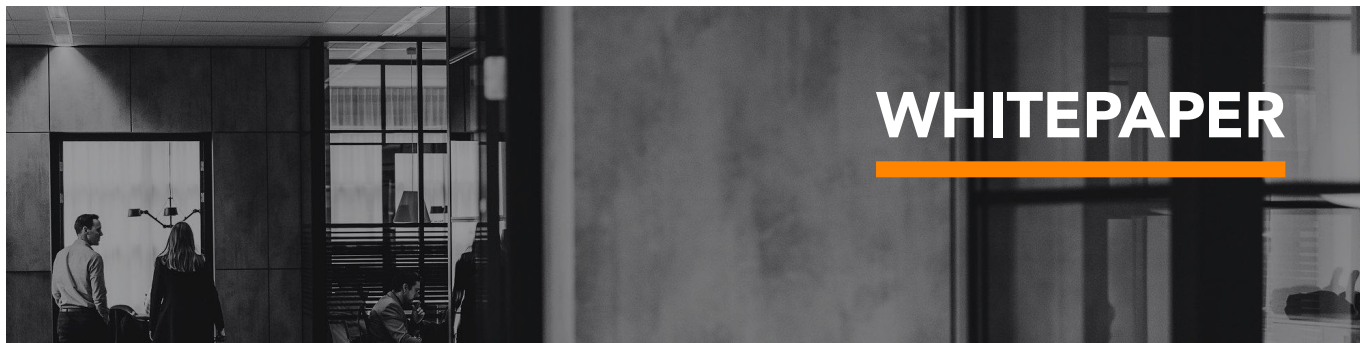
*“Inrichten
en actualiseren
is een grote uitdaging”*

Een Enterprise Risk Management (ERM) raamwerk. Voor financiële dienstverleners niet alleen de fundering voor een effectief werkend risicomanagement systeem, maar ook de meest kosteneffectieve en duurzame manier om compliant te zijn aan veranderende wet- & regelgeving. Natuurlijk op voorwaarde dat deze goed is ingericht en up-to-date is gehouden. Pas dan voegt het optimaal waarde toe voor de organisatie en haar stakeholders.

Helaas vormt het inrichten en actualiseren tot op heden de grootste uitdaging voor organisaties. Bij het inrichten en herijken ontbreekt vaak een concrete visie op het ERM raamwerk. Daarnaast zijn generieke ERM raamwerken (COSO/ISO) geïmplementeerd zonder deze op maat te maken voor de organisatie. Hierdoor is het ERM raamwerk onvoldoende in staat om op een efficiënte wijze om te gaan met wijzigende wet- en regelgeving of om opkomende risicogebieden (bijvoorbeeld cyberrisico's en klimaatrisico's) binnen het ERM raamwerk te positioneren. Dit zorgt uiteindelijk voor extra werk, frustratie en verwarring bij zowel de eerste als de tweede lijn.

Gelukkig hebben wij een aantal concrete aanbevelingen. In dit whitepaper bespreken we daarom:

- 1. De uitdagingen waar verzekeraars mee worstelen bij het inrichten van hun ERM raamwerk**
- 2. Waar deze uitdagingen vandaan komen;**
- 3. Waar organisaties rekening mee dienen te houden bij de volgende herijking van het ERM raamwerk.**



WHITEPAPER

ERM ONDER DE LOEP BIJ DE TOEZICHTHOUDER

De financiële crisis van 2008 liet kwetsbaarheden en tekortkomingen zien in veel van de toen opgestelde ERM-raamwerken. Met name in de manier waarop organisaties deze implementeerden. Er werd namelijk te weinig nadruk gelegd op risicocultuur en de rol van risicomanagement. De raamwerken waren vooral toegespitst op het voldoen aan wet- & regelgeving en op de behoefte van accountants en auditors. Deze beperkingen werden steeds nadrukkelijker zichtbaar naarmate er meer wettelijke vereisten rondom risicomanagement van kracht werden. In plaats van het gehele ERM raamwerk te moderniseren, hebben veel organisaties slechts onderdelen uit het ERM raamwerk aangepast. Hierdoor blijft het een uitdaging om het raamwerk te laten voldoen bij elke nieuwe wijziging in wet- en regelgeving.

Toezichthouders streven naar een grotere mate van volwassenheid in de financiële sector. Geen vreemde gedachte, gezien risicomanagement al zeker 10 jaar vergrote aandacht krijgt. In 2011 keek DNB al naar integraal risicomanagement in de financiële sector. In 2018 publiceerde DNB de 'Good Practice Risicomanagement Verzekeraars in 2018' als onderdeel van een groot onderzoek rondom risicomanagement in de praktijk. Nu, in 2020, start DNB met een nieuw onderzoek naar risicomanagement bij verzekeraars. Dit wordt bekeken vanuit Pilar II uit het Solvency II raamwerk, wat inhoudt dat de verzekeraar een geïntegreerde en brede blik heeft op de beheersing van risico's en daarbij de onderlinge samenhang tussen risico's kent. De verwachting van DNB is dat verzekeraars de risicobeoordeling en beheersing op een consistente manier doen. Het onderzoek vormt daarbij de aanzet voor DNB om het risicomanagement van een verzekeraar op een meer integrale en structurele manier te beoordelen. DNB onderzoekt ook hoe nieuwe risicogebieden als cyberrisico's, klimaatrisico's en de langdurig lage rente worden meegenomen in het risicomanagement van de verzekeraar. Ondanks dat de sector zeker vooruitgang boekt, is het nog maar de vraag of alle gaten uit het onderzoek van 2018 gedicht zijn.

PROBLEMEN IN DE PRAKTIJK

We schetsen de top 10 problemen en uitdagingen waar organisaties in de praktijk tegenaan lopen.

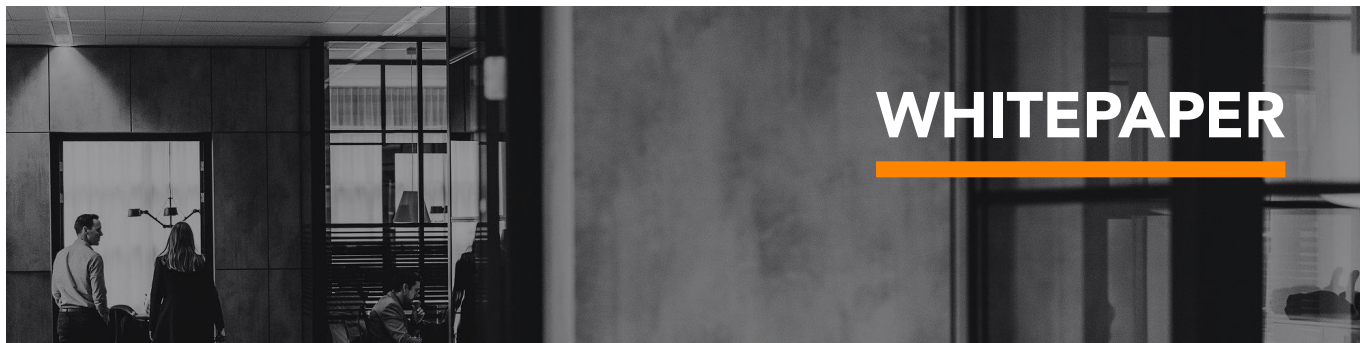
De onderstaande voorbeelden maken duidelijk dat er een verbeteringslag mogelijk is als het gaat om de implementatie en uitvoering van een risicomanagement raamwerk.

- 1. Afstand.** Het principe van 3 Lines of Defense heeft één belangrijk negatief gevolg: een gecreëerde afstand met de business. Deze afstand zorgt ervoor dat de tweede lijn vaak laat wordt aangehaakt bij vraagstukken en incidenten. Soms kan de afstand zo oplopen dat de tweede lijn wordt gezien als een 'vinkjesloket' dat liever wordt vermeden.
- 2. Beslissingen.** Een ander gevolg van deze afstand is dat de tweede lijn onvoldoende wordt meegenomen in de werkzaamheden van de business. Hierdoor is de 2e lijn onvoldoende op de hoogte van wat er speelt en de mogelijke risico's. De business moet de 2e lijn voldoende aanhaken, zodat de informatiestroom de goede kant op gaat en het management tijdig in de gelegenheid is om te kunnen bijsturen.
- 3. Risicocultuur.** Dit is vaak een onderbelicht of ontbrekend onderdeel in het ERM raamwerk waardoor de operationele effectiviteit van processen en controls feitelijk enkel op papier getoetst worden. Neem bijvoorbeeld het proces van incidentenmelden. Dit kan helder ingericht zijn, maar dit betekent niet automatisch dat er een risicocultuur is om dit te ondersteunen. Wanneer er zich bijvoorbeeld een risico heeft voorgedaan, is het voor de business vaak niet de hoogste prioriteit om dat te melden bij de ERM-er. Hier speelt mee dat de business vaak geen zin heeft in extra gedoe en vragen en dit als 'straf' ervaart.

- 4. Administratie.** Wanneer de focus van het ERM raamwerk vooral op aantoonbare controle ligt, zorgt dit voor een grote hoeveelheid administratieve vastlegging. De eerste lijn ervaart dit als een bureaucratische last wanneer het niet duidelijk is welk doel of voordeel dit voor hen heeft. Ook voor de tweede lijn kan deze administratieve vastlegging het doel voorbij streven.
- 5. Data achterstand.** Data is power. Dit lijkt de nieuwe slogan te zijn voor veel financiële instellingen. Uiteraard gaat risicomanagement daarin mee door meer en meer datagedreven te werk te gaan. Echter, zonder geschikte tools is het lastig om de juiste informatie in real-time op te halen. Het gevolg: verwarring en frustratie bij zowel de eerste als tweede lijn doordat er verschillende versies van bijvoorbeeld een risicodossier in omloop zijn.
- 6. Informatiestromen overload.** Wanneer het ERM raamwerk niet of onvoldoende is ingericht, heeft dit ook een negatieve impact op dataverzameling. Risicosignalen komen van alle kanten en worden op verschillende plekken behandeld en opgeslagen. Hierdoor kan het lastig worden de juiste verbanden te maken en het identificeren van de oorzaken van problemen/gebeurtenissen kost hierdoor veel tijd.
- 7. Eilandjes.** Niet alleen de business heeft last van 'silo denken'. De gehele 2e lijn heeft er last van. Zeker bij grotere organisaties zien we vaak een splitsing in de behandeling van risico's: ORM, ERM, FRM, Compliance risk, Legal risk, GDPR, Anti-Fraude, MLRO, noem het maar op. Iedere afdeling heeft een stuk van de puzzel. Dit maakt een pragmatisch en goed geïmplementeerd ERM raamwerk nog belangrijker.

8. **Complexiteit.** Een gevolg van te veel afdelingen en onderwerpen maakt het moeilijk een doordachte risicomanagementstructuur neer te zetten met de juiste informatiestromen en beslismomenten. Laat staan dat deze ook door zowel management als de 1e lijn goed gedragen en begrepen worden. Vooral voor kleine en middelgrote organisaties is het lastig om voldoende tijd te vinden om alles op een juiste wijze te verbinden. Daarnaast zijn er vaak meerdere tweede lijn rollen bij één persoon belegd.
9. **IRM.** De steeds belangrijkere rol van IT voor vele bedrijven vertaalt zich ook door naar een noodzaak voor IT risicomanagement. Dit specialistische onderdeel is vaak onvoldoende meegenomen in het ERM raamwerk, en er daadwerkelijk invulling aan geven blijkt lastig. In de praktijk blijven de bijbehorende vacatures daarom vaak lang oningevuld.
10. **De riskmanager.** Veel risicomanagement raamwerken zijn ontstaan vanuit een audit achtergrond. Het is dan niet gek dat de invulling van de taken van een riskmanager voorheen betekende dat processen en beheersmaatregelen op papier beoordeeld moesten worden. Tegenwoordig staat informatie ophalen vanuit de business (bijvoorbeeld door Risk Control Self Assessments) centraal. De verzameling van rollen en kwaliteiten van de riskmanager is daarom met de tijd steeds uitgebreider geworden. Met name op het vlak van operationeel risicomanagement komen er steeds meer onderwerpen en verwachtingen bij. Daarnaast moet de riskmanager ook meer interacteren met de 1e lijn.

De onderliggende oorzaak voor de benoemde praktijk problemen ligt grotendeels in het feit dat organisaties gebruik maken van compleet verouderde ERM raamwerken, het bestaande ERM raamwerk slechts beperkt gemoderniseerd hebben of er niet in geslaagd zijn om het ERM raamwerk specifiek voor de organisatie te maken tijdens de implementatie.



WHITEPAPER

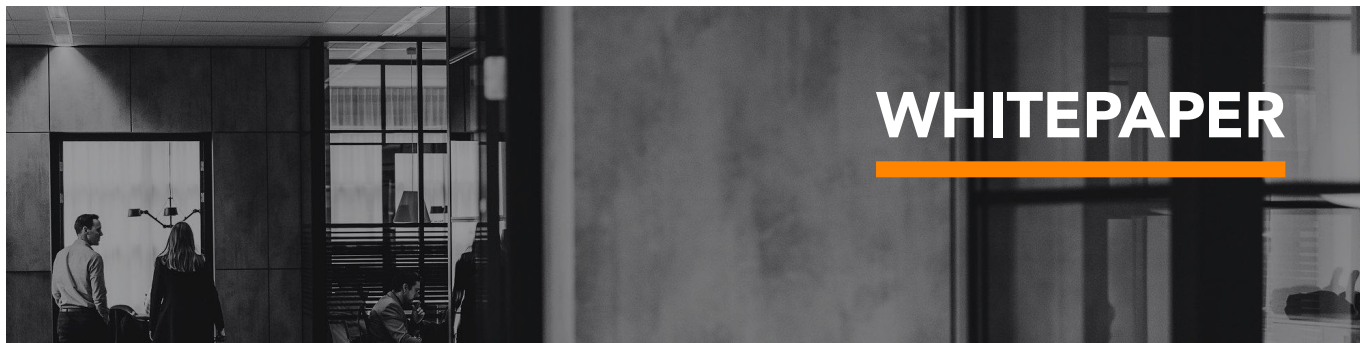
In de praktijk worden dit soort problemen vaak individueel opgelost. Hierdoor ontstaan nieuwe problemen omdat er onvoldoende oog is voor de onderlinge samenhang in het raamwerk. Het is waarschijnlijk effectiever en efficiënter om het hele ERM raamwerk eens goed tegen het licht te houden en te herijken.

HERIJKEN ERM RAAMWERK

Het beheren van risico's om zodoende je doelstellingen te behalen is geen nieuwe benadering. Veel organisaties doen dit allang. Echter, door de toegenomen complexiteit van organisaties en de omgevingen waarin zij opereren is het lastiger geworden om op een consistente wijze het risicomanagement toe te passen in de gehele organisatie.

Het gebruik van complexe en uitgebreide raamwerken kan ervoor zorgen dat je al met 1-0 achterstaat voordat je begint met de implementatie van het raamwerk en het betrekken van de 1e lijn. De beschreven problemen in de praktijk worden veelal gecreëerd doordat er te weinig of zelfs geen aandacht aan wordt besteed in de 'oude' (ERM) risicomanagement raamwerken. Of doordat organisaties er beperkt in slagen om de nieuwe raamwerken te implementeren op een manier die werkt voor hun specifieke organisatie.

Aspecten als governance, risicocultuur en toepasbaarheid vallen of staan met een goede implementatie van het raamwerk. Voordat deze praktisch ingezet kan worden en daadwerkelijk waarde toevoegt, is het belangrijk dat er een goed begrip is van het raamwerk. Een andere belangrijke randvoorwaarde voor succes is de uitvoerbaarheid van het raamwerk. Dit is namelijk essentieel om de informatiestromen beheersbaar te houden en op een efficiënte manier te kunnen aantonen dat de business in control is van het risicolandschap en de benodigde beheersmaatregelen.



WHITEPAPER

Governance en cultuur zijn belangrijke aspecten bij het updaten en actualiseren van het raamwerk. Beiden worden dikwijls vergeten of overgeslagen omdat het lastige onderwerpen zijn. Voldoende aandacht bevordert juist eigenaarschap en verantwoordelijkheid bij de 1e lijn. Denk hierbij ook aan de gewenste kwaliteiten van je 2e lijn. Met andere woorden: “de nieuwe riskmanager” – iemand die proactief de business in gaat en meer als sparringpartner wordt gezien. Tenslotte is er een transitie gaande naar data gedreven risicomanagement waarbij de 2e lijn meer als business partner fungeert i.p.v. een auditor of een ‘vinkjes loket’.

Ben je na het lezen van dit whitepaper geïnspireerd geraakt om je ERM raamwerk te updaten? Denk dan vooral aan deze aspecten:

- Kijk kritisch naar de kwaliteiten van de risicomanager zelf, de persoonlijkheid. Kijk naar pro- activiteit, meedenkend, overtuigingskracht en sociale vaardigheden.
- Kennis van de branche zelf moet niet onderschat worden, dit zorgt voor goede inhoudelijke discussies en een scherpe definitie van de risico's.
- Zorg voor een consistent, duidelijk en praktisch gebruik van het raamwerk. Betrek bij het updaten ook voldoende de 1e lijn om de behoeftes en de werking in de praktijk mee te nemen. Zo creëer je eigenaarschap.
- Probeer Control Testing zo efficiënt mogelijk te maken, duidelijke regels op te stellen met betrekking tot vastlegging en de juiste tooling te gebruiken als ondersteuning.
- Implementeer een risicocultuur check – een vragenlijst om de risicocultuur in het bedrijf te meten.
- Houd rekening met een continu veranderend landschap en een voortdurende toename aan wet- & regelgeving. Zorg ervoor dat het ERM raamwerk dynamisch genoeg is om deze veranderingen aan te kunnen.



WHITEPAPER

MEER WETEN?

Behoeftte aan een sparringpartner of iemand die even meedenkt van buitenaf? Bel ITDS.



EDSKE SMIT

SENIOR BUSINESS CONSULTANT

E E.SMIT@ITDS.NL