De nieuwe lente!

https://creativecommons.org/licenses/by-sa/3.0/

Onze taal geeft weer wie we zijn en …… hoe we de wereld in kijken.

Als de 'internal auditor' (ook) 'Trusted Advisor' (Maister, 2000) wil zijn, moeten we meer dan vertrouwen winnen: we zullen dezelfde taal moeten spreken als degenen wiens vertrouwen we waard willen zijn.

Onze IIA-inc. President en CEO Richard Chambers geeft aan dat we vijf woorden en frasen moeten vermijden: 'failed', inadequate', 'ineffective', 'we found' en 'it appears'.[i] Wij denken dat we het ook niet moeten hebben over wat er allemaal *fout* kan gaan, laat staan over 'naderend onheil'. Toch start daarmee de eerste IIA-nl column, op persoonlijke titel geschreven door een IIA-bestuurslid. Oké, hij spreekt ook van 'enablers' (instaat stellers), maar zelfs de 'enablers' worden meestal verwoord in 'risico's'.

Wat is het toch dat management control activiteiten: het economisch alloceren van middelen, het juiste meten en motiverend communiceren (Anthony 2004)[ii], steeds worden uitgedrukt in risico's en het treffen van controlemaatregelen om risico's te 'mitigeren'?
Uit de column 'Winter is coming': "De IAF dient naast het identificeren van het risico-universum ook rekening te houden met de enablers van een internal auditplan. De tien onderstaande enablers geven richting aan het internal auditjaarplan."

Als oefening en eerste stap in ons streven te worden gezien als 'Trusted Advisor' pogen we de 10 onderwerpen uit de column 'Winter is coming' te verwoorden gebaseerd op een management control-visie zonder risico-jargon. In een andere column zijn we dieper ingegaan op wat verder minimaal nodig is om als (internal) auditor enige kans te gaan maken op de titel 'Trusted Advisor'.

Onderstaand hebben we links de 10 punten uit de column geplaatst en rechts onze bewerking ervan. Op www.MCAudit.nl vindt u meer over de Trusted Advisor.

Na de omhelzing door accountants en controllers van COSO-IC als control-model zijn in eerste instantie financieel managers, maar uiteindelijk ook topmanagement gewend geraakt aan 'de risicotaal'. Zelfs HR-managers lijken zich er inmiddels bij neer te hebben gelegd. CEO's zien het mogelijk als een mooi oefen-moment voor het gesprek met de toezicht-houder. (CEO's zijn vaak heel goed in staat hun taalgebruik aan te passen als dit de organisatie ten goede komt.) Maar na een periode van voornamelijk positieve effecten op de (financiële) beheersing van veel organisaties, leeft nu breed de opvatting dat het 'voorspelbaarheidsdenken' is doorgeslagen. Ook the Committee of Sponsoring Organizations (COSO) zelf vraagt in de meest recente versie van ERM nadrukkelijk om risicomanagement te zien als een middel en de focus te richten op performanceverbetering. Risicomanagement mag wat ons betreft weer gewoon 'management' heten! Managers moeten weer zelf management-keuzes kunnen maken op basis van management-analyses. Risicomanagers kunnen dan weer terug in de tweede lijn; dus acterend als ondersteuners van managers. Misschien hun functietitel wijzigen in Risicomanagementonder-steuners?

Links: 'Winter is coming'; IIA-column 2019	**Rechts: 'De nieuwe lente!'**
1. Strategie en strategierealisatie Koppelt de IAF het internal auditjaarplan voldoende aan de realisatie van de strategie en doelstellingen van de organisatie? Worden de key-risico's in kaart gebracht die strategierealisatie in de weg staan? Groot risico is dat het management en het eerste lijnsmanagement zich blindstaren op de korte-termijndoelstellingen en daarbij het groter geheel uit het oog verliezen.	1. Strategie en strategierealisatie Koppelt de IAF het internal auditjaarplan voldoende aan de realisatie van de strategie en doelstellingen van de organisatie? Gebruikt management de organisatie 'assets' op de juiste manier om de doelstellingen te realiseren? Zijn de vooronderstellingen duidelijk en de randvoorwaarden voor de strategierealisatie voldoende geoperationaliseerd? Ook de relatie tussen korte en lange termijn doelstellingen is belangrijk.
2. Risicobereidheid (risk appetite) Zijn risicotolerantie en -bereidheid kwantitatief bepaald? Wat is het maximale risico per (deel)gebied dat de hoogste leiding wil nemen en de organisatie kan dragen – bijvoorbeeld de afgesproken bankconvenanten met de kredietverstrekkers? Sommige risico's moet je accepteren, andere risico's vragen om actie (verminderen, vermijden of overdragen). Wees dus voorbereid op een dynamische risico-aanpak, maar bepaal ook de grenzen.	2. Kritieke succesfactoren Is voldoende concreet uitgewerkt welke factoren moeten worden gerealiseerd en welke niet mogen worden overschreden om de doelen tijdig te realiseren? Is dit waar mogelijk vertaald naar subdoelen, (deel)verantwoordelijkheidsgebieden, (sub)processen of afdelingen? Sluit dit aan bij de geaccepteerde onzekerheid in de uitgangspunten en verwachtingen? Is management zich ervan bewust dat 'not everything that counts can be counted'? (Vrij naar Einstein.) Juist het analyseren van de ontwikkeling in kwalitatieve elementen maakt dat management leert van de effecten van hun aanpassingen en komt tot effectieve managementinformatie.
3. Risico-identificatie Wat zijn de grootste risico's voor de organisatie? Wat is de impact van deze risico's en hoe waarschijnlijk zijn ze? Hoe zijn ze met elkaar verbonden en wat is de (gecalculeerde) snelheid van een verandering van deze risico's? Een aantal 'laag geclassificeerde' risico's die met elkaar zijn verbonden, kunnen in samenhang alsnog voor een grote impact zorgen. Misschien een open deur, maar het is belangrijk om het tweedimensionale risico-identificatieproces te vervangen door het moderne vierdimensionale risicomanagementmodel.	3. Stuurinformatie en concurrentiefactoren (SWOT) Managementinformatie moet niet gebaseerd zijn op wat fout kan gaan, maar op wat nodig is om waar mogelijk voorspelbaar, maar persé ook gericht op verbetering de doelen te realiseren. Medewerkers die weten wat hun afnemers verwachten en wat die onder kwaliteit verstaan, vormen randvoorwaarden voor het onderkennen dat de ingeslepen werkwijzen niet meer voldoen. Voorts of het aanpassingsvermogen van hun bedrijfsproces de kwaliteit van de hen aangeleverde 'grondstoffen' nog aankan. Medewerkers hebben dus overzicht nodig én het vertrouwen dat beargumenteerd afwijken van de standaard door hun manager wordt gewaardeerd. Mits de laatste er proactief bij wordt betrokken én wordt geleerd van de effecten van die afwijkingen.
4. Risicoanalyse en -beoordeling Door 'what-could-go-wrongs' en 'what-if' scenario's te formuleren en de mogelijke financiële, veiligheids- en reputatieconsequenties door te rekenen, weet de organisatie hoe groot de gevolgen kunnen zijn. Hoe vaak analyseren en beoordelen de hoogste leiding en de eerste lijn de key-risico's? Worden stress-testing en scenarioplanning toegepast? Hoe effectief kan de organisatie risico's managen? Door een 'continuous' assessment in te plannen met de risicomanagementfunctie, zijn de hoogste leiding en de eerste lijn beter voorbereid, wat de kans op onaangename verrassingen verkleint.	4. Flexibiliteit en aanpassingsvermogen Topmanagement stelt de organisatiedoelen vast mede op basis van inzicht in het aanpassingsvermogen van de organisatie. Het heeft overzicht over de productwensen en de verandering daarin én over de kwaliteit die toeleveranciers bieden. De eigen organisatie als schakel daartussen optimaliseren is de eigen opdracht. Dat vereist ondernemerschap, motivatie van de medewerkers door het bieden van uitdagingen en het schenken van tijd, middelen en vertrouwen dat daar goed mee wordt omgegaan. Dit verlaagt de beheerskosten en vergroot de effectiviteit van de organisatie als geheel. Voorts continu meten en analyseren, zodat die schaarse middelen regelmatig kunnen worden herverdeeld. Zonder analyse wordt vertrouwen blindvertrouwen in plaats van slimvertrouwen (Covey[iii]).
5. Eigenaarschap Wie heeft het 'eigenaarschap' voor de key-risico's, wie is verantwoordelijk voor wat en wie rapporteert	5. Eigenaarschap Wie heeft het 'eigenaarschap' van de beoogde resultaten voor de klanten? En zijn de doelstellingen

aan wie? Als de risico's zijn benoemd, is het raadzaam om hieraan – per risico – een functie te koppelen die de risico´s continu in de gaten houdt, beheerst en significante uitkomsten rapporteert aan de hoogste leiding.	goed en volledig vertaald naar de onderliggende lagen? Wie zorgt dat de meest recente analyse-uitkomsten de juiste verantwoordelijken bereikt? Voorkom dat managementinformatie als individuele kennis tot macht leidt! Voorkom dat naar bezitters van informatie wordt gekeken als verantwoordelijken. Creëer geen extra besluitlagen met risicobeoordelaars en compliance-vastleggers. Zie informatievergaring en -deling als organisatie brede verantwoordelijkheid.
6. Cultuur, gedrag en soft controls Zijn er ´blinde vlekken´ die om aandacht vragen? De organisatiecultuur, het gedrag van medewerkers/management en soft controls drukken een groot stempel op de effectiviteit van risicomanagement. Denk daarom goed na in hoeverre de organisatie bijvoorbeeld transparant of conflict mijdend is. Onder andere voorbeeldgedrag ('tone at the top'), uitvoerbaarheid, bespreekbaarheid, transparantie en handhaving zijn elementen in het 'DNB cultuurhuis' om als toezichthouder of IAF toe te zien op cultuur en soft controls.	6. Organisatieklimaat en -gedrag Zijn technisch- en sociaal-organisatorische controls in balans om het organisatieklimaat te realiseren die het topmanagement voor ogen staat? Wat is er nog nodig om ideeën en potentiele conflicten aan de oppervlakte te krijgen en van te leren? Ontwikkelingen in de wijze van samenwerking tussen en binnen de organisatie-lagen moeten een aandachtspunt zijn van alle organisatieleden. Interne afspraken ontstaan door en zijn afhankelijk van goede onderlinge samenwerking. Wanneer de zelfopgelegde druk om het goede te doen voor de organisatie op medewerker-, team- of afdelingsniveau afneemt zal de oorzaak daarvan worden onderzocht en zijn er wijzigingen nodig. Idealiter ontstaan deze 'van onderuit' de organisatie door nieuwe afspraken en andere werkwijzen. Vaak zijn herverdelingen nodig, bijvoorbeeld wanneer er plaatselijk gebrek is aan tijd, menskracht, kennis of flexibiliteit. Voorkóm dat de toezichthouder of IAF moeten toezien op 'cultuur' en 'soft controls'.
7. Risicorapportages Aan welke eisen moet de risicorapportage voldoen? In hoeverre worden de rapportages gebaseerd op kwantitatieve meetinstrumenten en data-analyse? Hier doen continuous auditing (CA) en continuous monitoring (CM) intrede. Beslissingen kunnen het beste genomen worden als de organisatie over voldoende feiten en toekomstgerichte informatie beschikt. Maak daarom heldere risicorapportages die aansluiten bij de informatiebehoefte van de hoogste leiding.	7. Managementinformatie Aan welke eisen moet managementinformatie voldoen? In hoeverre worden de rapportages gebaseerd op trendanalyse van zowel kwalitatieve als kwantitatieve gegevens? Naast gestructureerde analyses is het vrij analyseren van opgeslagen gegevens belangrijk; het kan tot nieuwe kennis en inzichten leiden. Veelvuldig moet worden geconcludeerd dat 'de echte' gegevensverwerking sterk afwijkt van 'de verwachting' zoals beschreven in procedures en handboeken! Maak daarom heldere rapportages die aansluiten bij de informatiebehoefte op alle organisatieniveaus.
8. Calamiteiten Is de organisatie voldoende voorbereid op extreme gebeurtenissen en grootschalige risk events? Neem crisisplannen, BCM, DRP en cyberpreventieplannen opnieuw onder de loep: passen ze nog bij de huidige interne en externe eisen, maar ook bij de verwachtingen van de hoogste leiding?	8. Scenario-analyses Is de organisatie voldoende voorbereid op ontwikkelingen die op basis van trendanalyse niet te verwachten zijn? Externe (maar soms ook interne) ontwikkelingen kunnen kansen bieden voor organisaties die er al wat rekening mee hadden gehouden. Zwaar negatieve gebeurtenissen zijn dan in een concurrerende markt relatief minder ongunstig dan voor de concurrent. Bedenk en werk uit hoe in denkbare situaties moet worden gehandeld.
9. Black swans en third party risks Houden de hoogste leiding en IAF voldoende rekening met risico's met een extreem kleine kans en waarschijnlijkheid, maar met een catastrofale impact? Of met risico's die liggen bij en beheerst worden door derde partijen zoals leveranciers, partners, (onder)aannemers en ketenpartijen? Deze risico's hebben als belangrijk kenmerk dat ze zeer	9. Believe and Interactive control system (Simons 2000)[iv] Organiseer een klimaat waarin zélf blijven nadenken over de (nog) ondenkbare situaties en daar gezamen-lijk de dialoog over aangaan wordt aangemoedigd. Denkbare extreme situaties die bijna nooit voorkomen vereisen een duidelijke keuze en wees transparant over de situatie die de organisatie-leiding accepteert indien ze zich voordoen; zowel intern als extern. Trap

moeilijk in te schatten zijn. Veel organisaties zullen vele risico's als onmogelijk of 'buiten hun bereik' achten en deze risico's daarom niet meenemen in de beheersings- en internal auditplannen.	niet in de valkuil van het buiten de organisatie brengen van verantwoordelijkheden die eerder intern niet konden worden beheerst. Schade-clausules zullen niet snel ook de imagoschade dekken.
10. Oversight van risicomanagement Heeft de hoogste leiding een volwassen risicomanagementfunctie in huis om integraal de risico's te overzien? Zijn de eerstelijns management control, het risicomanagement en de internal auditfunctie complementair aan elkaar? Om risico's goed in te schatten, moeten de hoogste leiding en de three lines of defense de business, de sector en de impact van veranderingen helder en continu in kaart hebben.	10. Overzicht over kansen en bedreigingen Managementafwegingen over de inzet van middelen vinden als vanouds plaats op basis van de inschatting van ontwikkelingen en de kans dat het opofferen van de middelen tot meerwaarde zal leiden. Dit hoort op alle niveaus te gebeuren in de mate van detail dat past bij het managementniveau. Deze managementverant-woordelijkheid afschuiven op een stafmedewerker staat haaks op goed bestuur. Ondersteuning organiseren in de vorm van een 'facilitator', 'aanjager', 'informatieverzamelaar' of 'coach' gebeurt idealiter tijdelijk; tot het moment dat het weer een algemeen geaccepteerd onderdeel is van management op alle niveaus.

De 10 punten uit 'Winter is coming' omvatten natuurlijk niet wat er allemaal onder management control moet worden verstaan. Met het formuleren van de teksten in de rechter kolom raakten we weer enthousiast over de theorieën van Simons, Maister, Quinn, Hofstede, … allemaal ontstaan in de vorige eeuw. En hoewel we in de 21e eeuw alsmaar roepen dat alles sneller verandert en flexibiliteit en beweeglijkheid noodzakelijk zijn om die verandering te kunnen bijbenen, blijven we auditen en adviseren vanuit het 'voorspelbaarheidsdenken': het mitigeren van risico's met heipalen en beton. Waar Simonsv met zijn 'Interactive control system' ons in 1995 probeerde duidelijk te maken dat management control ook het continue ter discussiestellen van de strategie betekent, vragen wij om 'geformaliseerde beleidsdocumenten' en 'de aantoonbare werking' van 'the three lines of defense'.
We gaan het anders doen. We moeten het anders gaan doen. Op naar een ontwikkeltraject voor de 'Trusted Advisor'.

Ook deze blog is natuurlijk op persoonlijke titel geschreven, maar het geeft de ideeën weer van een groeiend aantal beroepsgenoten.

Ron de Korte RA RE RO CIA is Partner van ACS Partners te Doorn.
Hij begeleidt 2e en 3e lijns afdelingen in hun professionalisering, bijvoorbeeld door training in en ondersteuning van audits/ onderzoeken en het verstevigen van de onderzoeks-, rapportage en adviesvaardigheden.

[i] Chambers. R., (2017), Trusted Advisors; Key attributes of outstanding internal auditors, IIA-incorporate, USA.

[ii] Anthony, R. and Govindarajan, V. (2004), Management Control Systems, 11th ed., McGraw-Hill, Boston, MA.

[iii] Covey S.M.R., The speed of trust, Business Contact, 2008.

[iv] Simons, R. (2000), Performance Measurement and Control Systems for Implementing Strategy, Prentice-Hall, Upper Saddle River, NJ

[v] Simons, R. (1995). Levers of Control: How managers use innovative control systems to drive strategic renewal. Boston: Harvard Business School Press, USA.