July 2014 Dutch Chapter

IOR Newsletter

This is the second edition of the Newsletter of The Dutch Chapter of the Institute of Operational Risk .This publication is designed to help keep members and non-members informed of developments within the ORM discipline and the activities of the Dutch Chapter of the IOR particularly. Should you like further information about any of the issues raised in this newsletter, or have any suggestions about how we can improve the content or design, please do not hesitate to contact the Editorial team at the following address: IOR@axveco.com

Dit is de tweede editie van de Nieuwsbrief van de Nederlandse tak van het Institute of Operational Risk. Deze nieuwsbrief is bedoeld om leden en geinteresseerden op de hoogte te houden van de ontwikkelingen in het vakgebied en van de activiteiten van de Nederlandse tak van het IOR in het bijzonder. Mocht u naar aanleiding van deze nieuwsbrief nadere informatie wensen of opmerkingen en of suggestie hebbeb om tot een verdere kwalitieitsverbetering te komen, dan nodigen wij u graag uit deze te richten aan het communicatie team via: IOR@axveco.com

Introduction

Alex Dowdalls

Head of Dutch Chapter IOR

It is my pleasure to present the second newsletter of our Dutch chapter of the Institute of Operational Risk (D-IOR).

We have been operational for only 9 months yet we have already achieved a great deal in this short period of time. We have held three major events - kindly hosted by BinckBank, SNS REAAL and KAS Bank - with up to 55 participants, we have our first corporate members now on board and we have established the D-IOR as a platform to share views for Operational Risk managers in The Netherlands.

This is a great time to be in operational risk – the tradition view that risk management centres around credit, market, liquidity and insurance technical risk is shifting as a result of the growing realization that people remain at the heart of failures – not just policies or models. It is no surprise to see increased supervisory attention on risk culture and behaviours which in my view is *the* new frontier for risk management in the coming years.

If we consider the recent DNB supervisory vision 2014-2018 for the finance sector, then we see the migration to the European Single Supervisory Mechanism (SSM) taking form, raising the bar on regulatory supervision for both large and smaller institutions. Basel III, Solvency II, CRD IV and AIFMD are becoming a reality. DNB will be implementing a new system for collecting and analysing regulatory data with the intention of enhanced impact on behaviours within institutions and identification of key risks across the sector. There will be more focus on integrity and transparency with the aim of improving the risk culture.

In the industrial, energy, transport, health and food sectors we have experienced major operational incidents where people have been killed, injured or inadvertently infected – in these sectors, improved operational risk management can save lives. We encourage more participation from risk managers and internal auditors in these sectors in D-IOR activities.

The IOR is moving from strength to strength and has adopted the corporate membership programme which further increases its outreach in the profession. The principles of incorporation were revised to reflect the corporate membership and to encourage professional education. A team is also actively exploring the establishment of an academically accredited qualification for Operational Risk Management – more on this topic later!

For now I am delighted that you are participating in our events or at least reading our newsletter. I look forward to welcoming you to our next event at Achmea Conference Center in Zeist on 2 October, 2014 and to welcoming you into the IOR as an individual or corporate member.

Alex

Other industries

According to the outcome of the survey held after the event at Kas Bank N.V. there is a clear interest in learning how operational risk is perceived in other industries.

Despite the fact only financial institutions need to hold capital against operational risks, it is obvious that with a creative mind any industry is exposed to the event types (on level I) as defined under the Basel II Accord.

In one of our future events we will invite risk managers from other industries to speak about their experiences with regard to the operational risks their company encounter and the way they deal with it.

One the risk that is getting a lot of attention nowadays is cyber risk. Cyber risk is an animal with many heads and creates different kind of exposures. Hacking, Data or ID theft, DDos attacks, Espionage, system failure are just examples of this,

In this respect it is quite interesting to see what the impact is on the global military or defense ministries around the world.

On www2.deloitte.com you can find the following report:

"**'Global Defense Outlook 2014"**

In the report that deals with the defense spending of the top 5O countries there is a clear attention for cyber threats.

Cyber operations emerge as a global threat and based upon an analysis of reported cyber attacks the threat appears to consist primarily of criminal activities and data theft, vandalism and resource hacks than attacks against infrastructure.

Based upon the number of attacks mentioned in the report (f.e. South Korea 95.000 daily hacking events against military computer networks in 2009 and according to the Chinese Defense Ministry 144.000 attacks monthly) the spending to avoid and defense against cyber attacks shall grow substantially.

India recently announced a plan to train 500.000 cyber warriors by 2017 and to impose mandatory cyber security audits.

The financial industry is highly exposed to cyber threats and the challenge is how to stay one step ahead in securing the business.

Andere industrieën

Looking at the aforementioned report it is obvious that the costs related to achieve this will be very substantial creating the need for a cross-industry cooperation.

We expect this topic to be addressed at a future event.

D-IOR

****

Uit de survey die aan het einde van het evenement bij Kas Bank N.V is gehouden, kwam naar voren dat er behoefte is te leren hoe in andere industrieen met operationele risico"s wordt omgegaan.

Hoewel alleen financiele instelligen kapitaal moeten aan houden voor operational risk, is het duidelijk dat met wat fantasie feitelijk alle industrieen bloot staan aan de risico's zoals die onder het Basel II Akkoord (op level I) zijn gedefinieerd.

Voor een van de volgende bijeenkomsten zullen we een risk managers uit andere industrieen uitnodigen te spreken over hun ervaringen met operationele risico's in hun bedrijf en de wijze waarop men daarmee omgaat.

Het Cyber risico is een van de risico's die bijna dagelijks in de pers wordt genoemd. Cyber aanvallen komen in vele gedaanten voor en brengen verschillende risico's met zich mee. Hacking, data en identiteits diefstal, Ddos aanvallen, spionage, systeem uitval zijn slechts enkelen voorbeelden.

In dit verband is het interessant te zien wat deze risico"s betekenen voor de wereldwijde defensie industry.

Op www2.deloitte.com staat het navolgende rapport:

*"**Global Defense Outlook 2014"***

In dit rapport dat met name gaat over de militaire uitgaven in de top 50 landen is veel aandacht voor cyber.

Cyber activiteiten ontwikkelen zich tot een wereld wijde bedreiging en op basis van publiek beknde cyber attacks lijkt het erop dat het in beginsel meer om criminele activiteiten te gaan, diefstal van data, vandalisme en hacking dan een werkelijke aanval op de systemen.

Op basis van cijfers die bekend zijn gemaakt over cyber aanvallen (zoals bijvoorbeeld in Zuid-Korea waar in 2009 dagelijks 95.000 aanvallen waren op het militaire computersysteem en in China wordt het defensie met 144.000 aanvallen per maand geconfronteerd) zullen de uitgaven om zich te beschermen tegen deze aanvallen enorm stijgen.

Zo heeft India recentelijk aangekondigd voor 2017 500.000 "cyberwarriors" te hebben opgeleid, maar tegelijk voor ook cyber audits verplicht te gaan stellen.

Ook de financiele wereld is zeer kwetsbaar voor cyber aanvallen en het is een grote uitdaging om de aanvallers een stap voor te blijven.

Kijkend naar het eerder vermelde rapport en de ontwikkelingen, dan zullen de kosten die gemaakt moeten worden om de stap voorsprong te behouden substantieel zijn. Hierdoor ontstaat er wellicht een nodzaak en goede aanleiding om dit industrie overschrijdend aan te pakken.

Op een volgend evenemen zal dit wellicht al aan de orde komen.

D-IOR

Risk Appetite

Risks appetite in het DNB ORM onderzoek, hoe nu verder?

Op 8 mei 2014 heeft DNB de Nieuwsbrief Banken mei 2014 gepubliceerd. In deze nieuwsbrief is prominent aandacht besteed aan de toestand van het operationeel risicobeheer bij banken. Dit is gedaan op basis van een onderzoek onder een beperkt aantal banken.
DNB heeft veel aandacht besteed aan de naleving van de FSB principes, vooral op het gebied van Risk appetite.
Gebleken is dat de onderzochte banken voortgang maken met de naleving van de FSB principes, maar dat er ook nog de nodige lacunes zijn. DNB constateert onder meer het volgende:

- Veelal ontbreekt een duidelijke Risk Management Statement
- De Risk Appetite Statements zijn incompleet, omdat hierin niet alle materiele risico's van het business model zijn opgenomen. Een is get gebruik van derivaten of provisie gedreven activiteiten
- Onvoldoende uitgewerkt is de vertaling van het Risk Appetite Statement voor niet-financiele risico's naar de praktijk van de bedrijfsvoering. Denk bijvoorbeeld aan limieten voor compliance
- De aansluiting van de (top down) Risk Appetite op de (bottom up) vast gestelde limieten schiet tekort. Het risicoprofiel kan niet goed worden afgezet tegen de Risk Appetite, mede door bovenstaande punten.
- Daarbij ontbreekt een totaalbeeld van de risico's, wat een tijdige bijsturing van de risicovolle activiteiten in de weg kan staan.
- Banken wegen Risk Appetite mee in de besluitvorming over strategie en bedrijfsmodel, maar doen dat nog onvoldoende expliciet, zo beoordeelt DNB.
- Het Risk Appetite Framework is voor de interne auditfunctie nog nauwelijks een punt van onderzoek.

DNB gaat ervan uit dat banken blijven werken aan de verbetering van hun risicobeheer en daarbij rekening houden met de FSB principes.

De risk appetite is ter sprake gekomen in het overleg van de core committee leden van D-IOR.

Het lijkt D-IOR een goed idee om een inventarisatie te doen van die banken die recentelijk door DNB in de steekproef over de staat van het Operationeel risicobeheer betrokken zijn geweest. De inventarisatie is bedoeld als opmaat voor een gezamenlijk onderzoek naar de bestaande opzet en werking van risk appetite ts zoals genoemd in de FSB principes, om zo vast testellen waar de mogelijke lacunes liggen die DNB heeft genoemd. Het gezamenlijke onderzoek moet dan leiden tot verbeterpunten waar alle banken , waarvan de ORM Managers die lid zijn van D-IOR voordeel bij kunnen hebben.

Belangstelleden voor dit onderzoek, dat zal worden opgezet en uitgevoerd in een werkgroep van D-IOR, kunnen zich opgeven bij Koos Vegting Core member D-IOR.

Koos Vegting
Risk Manager at Kas Bank N.V.
Via : IOR@axveco.com

Risks Appetite under the DNB ORM survey, next steps?

On May 8, 2014 the DNB has issued its newsletter "Banken May 2014". The main topic of this letter was the current situation with respect to operational risk management. The overview was based upon a survey carried out at a limited number of banks. Much attention was paid to the way the banks followed the FSB principles on risk appetite.

Although progress is made with becoming compliant with the FSB principles, DNB still noticed some deficiencies:

- *Lack of a clear Risk Management Statement*
- *Risk Appetite Statements are incomplete. Not all the risks of the business model are taken into account*
- *The implementation of the Risk Appetite Statement for non-financial Risks in the day to day business model is insufficient (f.e. limits for compliancy)*
- *The (top down) Risk appetite for the (bottom up) established limits is not fully attuned. It is difficult to map the risk profile against the risk appetite.*
- *The lack of an overall risk profile, reduces the possibility to adjust high risks activities in time*
- *The DNB is not completely satisfied with the way banks implement the risk appetite in their strategy and business model*
- *The internal audit function is hardly involved in the risk appetite framework*

According to DNB, banks will not only be required to improving risk management continuously, but also to follow the FSB principles.

The topic Risk-Appetite was on the agenda of recent the D-IOR core team meeting.

In view of the foregoing, the D-IOR believes it is in the interest of all to combine and to analyze the outcome and experiences of the recent DNB survey.

This exercise will be the starting point for a mutual project to analyzing the current situation with regard to the appetite frameworks and risk appetite statements under the FSB principles and to understand and identify the gaps DNB has found.

The outcome of this survey should lead to a priority list of improvements where all banks – with ORM Managers who are member of the D-IOR, can benefit from.

D-IOR will set up and orchestrate a special workgroup and should you be interested to participate please contact Koos Vegting, Core member of D-IOR.

Koos Vegting
Risk Managerat Kas Bamk N.V.
Via: IOR@axveco.com

Outcome survey event at Kas Bank / Uitkomst enquete evenement bij Kas Bank

After the event, held at the premises of Kas Bank in Amsterdam on May 21, 2014 some 20 attendees responded to the request to completing the questionnaire.
The key note speakers, Kris Wulteputte and Simon Ashby received high notes for their contribution and the overall rating of the event was above expectation, thanks also to the excellent hosting by Kas Bank. From a core team D-IOR perspective, it was encouraging to see a lot of new attendees, representing 15 different companies. 16 attendees have indicated to apply for a membership and 8 attendees have shown interest to writing an article for the next Newsletter. ORM in other industries and unexpected event management were amongst the topics mentioned most to be on the agenda for a future event

Aan het einde van het evenement dat werd gehouden op het kantoor van de Kas Bank in Amsterdam op 21 mei jongstleden , is aan de deelnemers gevraagd een enquete formulier te willen invullen. Zo'n 20 aanwezigen hebben daar gehoor aan gegeven.
De beide sprekers, Kris Wulteputte en Simon Asby hebben een hoge waardering voor hun bijdrage gekregen en het evenement als geheel voldeed meer dan verwacht, mede ook door goede zorgen van Kas Bank. Het core team van D-IOR was uitermate verheugd een flink aantal nieuwe aanwezigen te mogen verwelkomen, die gezamenlijk meer dan 15 bedrijven vertegenwoordigden. Van de aanwezigen dit het formulier hebben ingevuld zouden 16 lid worden terwijl 8 hebben aangegeven een artikel te willen schrijven in de volgende Nieuwsbrief. ORM bij andere industrieën en het het omgaan met onverwachte calamiteiten werden genoemd als onderwerpen voor een volgend evenement.

Venue and date of next event / Locatie en datum volgende evenement

The upcoming event will be held at the Achmea Conference Centre, Handelsweg 2, 3070NH Zeist, on October 2nd 2014. The theme for the day will be announced on the IOR webpage, on the IOR linkedin page and via e-mail for those who are registered at IOR@axveco.com

Op 2 oktober 2014 zal het volgende evenement plaatsvinden in het Achmea Congres Centrum, gelegen aan de Handelsweg 2 , 3070 NH Zeist. Het thema voor deze bijeenkomst zal worden bekend gemaakt op de IOR webpage, op de IOR linkedin pagina en via een e-mail, aan bij IOR@axveco geregistreerde personen.

European Banking Authority/ EBA

On June 12, 2014 the European Banking Authority launched "A consultation on draft Regulatory Technical Standards (RTS) on assessment methodologies for the Advanced Measurement Approach for operational risk" (See www.eba.europa.eu)

The purpose of the paper is to ensuring uniform application by institutions in the European Union and to avoiding inconsistencies in the determination of institutions risk profile. Based upon these Regulatory Technical Standards the competent authority will only grant permission to use the AMA where institutions can prove that all relevant qualitative and quantitative requirements set out in the RTS are met.

The proposed regulation is divided into 8 chapters, with amongst others:

In Chapter II

- Operational risk events related to legal risk, market risk and fraud in the Credit area
- The scope of operational risk loss

In Chapter III

- Governance Structure, Operational Risk Governance and Management
- The Risk Management function and
- Senior Management involvement

In Chapter IV

- The 4 AMA elements, internal loss data, external data, scenario analysis and Business Environment and the Internal Control factors
- Insurance and other Risk Transfer Mechanism
- Capital allocation
- Parallel running

Chapters V, VI, VII are dealing with the Data Quality and IT Infrastructure, the Use test and the Audit and Internal Valuation.

In the accompanying documents under header 5, sub 5.2 there is an overview of questions for consultation. Any comment should be submitted to the EBA before September 12, 2014. Following the consultation, the EBA will review the RTS proposals to ensure that they take into account any changes arising from the consultation process. EBA must submit the draft to the European Commission by the end of 2014. At the end of the process this Regulation will enter into force on the 20th day following that of its publication in the Official Journal of the European Union and will be binding in in all Member States.

NCSC

Via het Nationaal Cyber Security Centrum (NCSC) kunt u op de hoogte blijven van de laatste ontwikkelingen op het gebied van computer beveiliging.

Het NCSC valt onder de Nationaal Coordinator Terrorism Bestrijding en Veiligheid van het Ministerie van Veiligheid en Justitie.

De missie is: “het bijdragen aan het vergroten van de weerbaardheid van de Nederlandse samenleving in het digitale domein en daarmee aan een veilige en open stabiele informatiesamenleving.””

Op www. ncsc.nl kunt u zich aanmelden om op de hoogte gehouden te worden van de laatste ontwikkelingen.

Through registration at the National Cyber Security Centrum (NCSC) you can stay updated on the latest developments on computer security.

The NCSC reports to the “National Coordinator for Terrorism Bestrijding en Veiligheid” a unit of the Ministry of Security and Justice.

The mission statement: to contribute to an increasing resilience of the Dutch Society in a digital domain and thus a secure, open and sustainable information society.

Registration to be kept updated on the latest developments:

www.ncsc.nl

The Dutch Chapter team

Dick van Male (ING) is toegetreden tot het core team van de Nederlandse afdeling van het IOR. Het team dat toeziet op de dagelijkse gang van zaken bestaat nu uit de navolgende leden:

Dick Van Male (ING) joined the core team of the Dutch Chapter of the IOR. The team dealing with the day-to-day challenges consists of:

-Marca Schotsgerrits	Rabobank
-Erik Obbink	SNS REAAL
-Fulco Neijmeijer	Achmea
-Radboud Lubbers	Independent
-Koos Vegting	Kasbank
-Paul van Dijk	Independent
-Dick van Male	ING
-Alex Dowdalls	Axveco

***** Sharda Poelloe en Jeffrey van Poppel zullen hun activiteiten voor D-IOR overdragen aan nieuwe core team leden. De Voorzitter en de andere leden van het core team danken haar voor hun waardevolle bijdrage.

** Sharda Poelloe and Jeffrey van Poppel will transfer their core team activities to new core team members.*

The chairman and the members of the team are very grateful for the contributions Sharda made.

Membership IOR

Het IOR en zijn Nederlandse tak zetten zich in voor de verdere ontwikkeling en verbetering van de ORM functie.
Om de doelstelling te kunnen bereiken is een breed draagvlak van belang.
Door lid te worden van de IOR draagt u actief bij aan deze ontwikkeling.

Naast het persoonlijk lidmaatschap bestaat er ook de mogelijkheid om als bedrijf een lidmaatschap te nemen.

Op de webpage van het IOR kunt u zich aanmelden.

www.ior-institute.org

The IOR and its Dutch Chapter put effort in developing and improving the ORM function.
It is obvious that a widespread support is necessary to achieving the objectives. By joining the IOR as member you actively support the idea about the IOR.

Just recently the IOR has introduced, next to an individual membership, a corporate member ship.

To register as a member please look at:

www.ior-institute.org

To Contact the Dutch Chapter

For questions about the activities of the Dutch Chapter, the upcoming events, the newsletter or memberships and or information about possibilities to hosting events or sponsor certain activities please contact: *IOR@axveco.com*

Voor vragen aangaande de activiteiten van de Nederlandse Afdeling, evenementen, de nieuwsbrief of het lidmaatschap en of de mogelijkheid om eventueel als gastheer te kunnen optreden op toekomstige evenementen en mogelijkheden om als sponsor op te treden kunt u terecht bij: *IOR@axveco.com*

Disclaimer