June 2017

IOR Newsletter

THE INSTITUTE OF OPERATIONAL RISK

Welcome to this edition of the Newsletter of the Institute of Operational Risk. This publication is designed to help keep members and non-members informed of developments within the industry and also within the IOR itself. If you would 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: info@ior-institute.co.uk

In this issue

IOR Launches Certificate in Operational Risk Management (CORM)

The Institute is delighted to announce the launch of our externally accredited qualification, the Certificate in Operational Risk Management. After much blood sweat and tears, over many months by many practitioners, the CORM launched on the 18th May 2017.

With interest from over 50 applicants in the pipeline, both individuals and corporates, and covering diverse locations such as New York, India, Netherlands, UAE, Germany, Indonesia, Malaysia and of course the UK, it's fair to say that there is an appetite for the qualification. This initial launch has been carefully managed so that we can support students as they engage with the new technology and processes prior to fully scaling up to a more widely marketed launch later in the year.

The CORM is designed to provide benefits to anyone in a role involving the management of operational risks. It involves studying key concepts related to operational risk management and then passing an independent exam to demonstrate that understanding. It can also give organisations and regulators a basis for evidencing the competency of individuals and teams and that they can rely on their understanding of sound operational risk management tools and techniques.

The CORM is accredited by ATHE an awarding body regulated by the Office of Qualifications and Examinations Regulation (Ofqual). It has been assessed at QCF Level 4 (pre foundation degree) in the UK and at EQF Level 5 within Europe.

Full details, including pricing and how to apply, can be found at https://www.ior-institute.org/education/certificate-in-operational-risk-management

This is truly a game changer for the Institute on our continued journey of becoming the professional body of choice for operational risk practitioners. The CORM has only been possible due to the support and effort of the core team and those 30 or so volunteer members who also made contributions along the way. In acknowledging all of the many individuals involved in our education development, the Institute would like to specifically thank the following for finally getting the CORM launched:

- Project Management – Lotfi Baccouche and Iris Fenn
- Steering Committee – John Thirlwell, Elena Pykhova, George Clark, Dr. Simon Ashby, Dora Grant, Manoj Kulwal and Stephen Murgatroyd, with earlier Steer Co members Ravi Gupta, Mike Finlay and Jacky Cumberland making contributions before work commitments prevented their continued involvement.
- Suppliers – Eko Ltd, N4PS Ltd, ATHE and APMG

So what's next?
This is the start of the Institutes development of education programmes. We will draw breath and maximise the opportunity from CORM over coming months but the objective is to continue to develop a range of qualifications and options.

More immediately, we are continuing to develop the technology support so that we can further minimise manual processes and improve the student experience.

The new committees which will both maintain business as usual such as exam banks, workbook content, supplier oversight and independently provide oversight of standards such as result adjudication, complaints and breaches of academic standards are in place and operative. Membership of both committees is a mix of experienced practitioners and academics.

We will market the CORM more actively once we have student feedback and take on board any improvements identified. All members will have a role to play in bringing this to the attention of their networks and providing support to the Institute.

IOR Launches new membership system

At the AGM we announced the intention to upgrade the technology which supports our membership processes. This was to improve the application process for corporate memberships, reduce manual interventions and processes and importantly, provide self service tools to local chapters such as improved management information.

This programme was successfully delivered during May 2017 while at the same time moving to a more stable and long term core platform. Not an easy task but one that was well managed by Stephen Murgatroyd as Director, Operations.

We are in the final stages of ensuring that all of the data is robust and has been transferred accurately. Once confirmed Stephen will start to develop the opportunities available for use by our Chapters.

Although few members may directly see the benefits of this investment it is a critical step in improving the Institutes future capability and professionalism.

IOR evaluating its membership benefits

The Institutes fee structure has changed little since the IOR launched in 2004 and we recognise that individuals and corporates have a choice as to which bodies they join and how they spend their money. With that in mind we are constantly looking at the benefits of membership and to maximise the potential for choosing the IOR. The launch of our CORM is key part of that value proposition.

Over the coming months, selected members may be asked to take part in short surveys. These will be driven by analysis undertaken by Manoj Kulwal, our Director for Marketing. We have already started to analyse our webpage access for example.

Similarly we will look to add member benefits where we can, working with selected partners to improve the range of options. We have already announced the introduction of GoCardless for membership renewals. This allows members to automatically renew each year.

Very soon we will launch a new jobs page which will be managed in conjunction with YourMembership. This will provide both corporate and individual members the opportunity to post and find recruitment and career opportunities specifically related to operational risk. Watch our website for details.

We also recognise that sometimes members cannot either access or attend local chapter events. We are developing a series of webinars that will be available to all members so that they too can benefit from others views, opinions and experiences. Visit IOR Events website to register for upcoming webinars.

Similarly we know that the Sound Practice Papers are a key member benefit. These member pages are often the most searched or accessed. We intend to refocus in this area.

In the meantime, if members have any thoughts on how we can improve the membership experience, whether that is process or benefits, then please contact: info@ior-institute.org

Chapters

Changes are coming to the England and Wales Chapter

After two years at the helm of the Chapter, Jonathan Birrell-Gray is now off to pastures new. Jonty has a long history with the Institute and we can only be thankful for all his hard work and wish him the best for the future.

But life goes on and so does the E&W Chapter with former Council Director Jimi Hinchliffe taking over as the new Chairman. Jimi, together with the other Chapter Committee members, will be working hard over the coming months on a range of initiatives to enhance the support and benefits we provide to our members.

What can members expect from us?

Our members' interests are at the centre of everything we do.

We aim to deliver real value for money by offering high quality events, including workshops and seminars presented by top industry professionals (most of them are free of charge for members - see our website for upcoming events). We will keep you updated on material

regulatory developments through briefings, insight papers and a new chapter newsletter and we will seek your input to IOR responses to regulatory consultations. We aim to strengthen our membership base so you can make the most of networking opportunities.

We also want to be closer to you and get in touch more often via social media (watch this space!) and the main IOR website. Of course, we will also want to hear back from you about the things you like and where we can improve. Let's talk!

What comes next?

In April, we partnered with MERJE, a niche recruitment firm, for a breakfast event on risk culture at the Balls Brothers, London. Speakers from HSBC shared their experience on assessing and embedding risk culture to a hall packed with engaged members and guests. Looking forward, we are partnering with Xactium, a Risk Management software vendor, to provide access to IOR members to some high-quality events on risk appetite and risk assessment in Leeds and London. We are also working with MUFG to host a session on operational risk capital in response to the recent comments from Jamie Dimon, Peter Sands and in the context of the SMA. We will keep you posted on these and other initiatives as they progress.

So, fellow members, changes are coming. Get in touch, get on-board, and let's make the England & Wales Chapter better and stronger.

Updates from the International Chapters

It's been another busy year already for our Chapters, with a number of events already taking place covering many different topics with plenty more events planned for the remainder of the year.

Recent events commenced in Nigeria with a conference held in December attended by 48 delegates.

March was a busy month with the German Local Chapter held a Quant Workshop attended by their Regulator, their first event of the year. This was closely followed by a Round Table in Hong Kong hosted by PwC, with topics for discussion including Banks' Risk Culture framework, Governance, Risk Management Practice and Conduct Risk Indicators. Finally, at the end of March the Bank of Nigeria hosted a one day Session.

The most recent event was held in Germany, an Operational Risk Forum whose agenda included wide ranging topics such as, Operational Risk Classification Benefits and Limits, Linkages between Risk Culture and Management of Operational Risks, Behavioural Risk Management. Operational Risk and Internal Controls.

Over 100 experts from banks, insurance and the consulting sector discussed current challenges in Operational Risk Management. Representatives from national and international supervisors provided information about the latest regulatory OpRisk topics as

well as OpRisk initiatives on an EU/EBA level. Mainly the presentation of the new regulatory requirements for IT (BAIT), which were recently published in Germany, resulted in a very lively discussion. Planning is already underway for the next OpRisk forum for the German speaking area which will take place on 16th May 2018

Events to look out for

Many of our Local Chapters are now taking a well-earned break for the summer period but the calendar for the remainder of the year is already filling up with events as follows:

- 13th July 2017: Our England and Wales will run a breakfast session on "Fixing Op Risk Capital" places are limited to 50 people.
- 11th – 17th September 2017: The South Africa Local Chapter has arranged a visit to England which will include a Colloquium and Seminar hosted jointly by the IOR Council and the England and Wales Chapter.
- 13th September 2017: The England & Wales will run a one day event with the agenda including a Loss Events Masterclass, The Regulatory Agenda, Sound Practice Guidelines, Cyber Risk and Culture, Conduct and Behaviours.
- 14th September 2017: The German Local Chapter will run an Operational Risk Quant Workshop in Bonn.

In the pipeline:

- Deloittes have agreed to host an event for the Scottish Chapter and both parties are currently in discussion to agree a date for the event.
- The Hong Kong Chapter are currently planning to sponsor a Student Event in partnership with the Risk Management Association.

Hopefully this has given you some insight into the activities in the various Local Chapters and we will provide you with a further update on the planned events later in the year.

If you wish to join any of the above events full details can be found on our website at https://www.ior-institute.org/ior-events/upcoming-events

OpRisk Ideas Spotlight:

In this section of the newsletter, operational risk practitioners share their ideas with the community. In this edition, Adesh Rampat challenges the traditional view of risk assessment that covers analysis of probability and impact.

This article was first published on Continuity Central's website dated April 7th 2017.

Most risk equations include the standard approach of probability and impact. Nowadays, with the changing threat landscape, a new approach to the risk equation should be looked at. In this article I will explain why adding resilience and incident response to the risk equation provides a more useful and measurable metric.

Standard risk equations use probability and impact to calculate the extent of a particular risk, often displaying the result in a risk matrix. However, such an approach neglects two important aspects from an organizational perspective: resilience and incident response. To rectify this I propose a new approach, as follows:

Risk = Impact x **Resilience/Incident Response**

This equation allows for risk to be easily understood especially when it comes to the level of incident response required to address an event. It also assists in the assessment process as to the critical areas to focus on in today's constantly changing threat landscape.

When an organization is hit by a cyber attack, for example, the probable questions that are asked include:

- What is the impact?
- What systems within the network has the attack penetrated?
- Is our current incident response plan effective?

Resilience and incident response have been specifically brought into this equation primarily because organizations must have resiliency and incident response built in to the security framework – these are not nice to have – they are a must have.

Let's analyze what this equation is about:

Impact: this is the effect on the organization due to the occurrence of a risk.

Resilience: organizational resilience against threats. This must take into consideration the following:

- Ability to deal with the effects of a natural disaster – this will include the relocation of systems and staff required to have the organization functioning within a reasonable period of time.
- Ability to withstand the effect of technology related threats such as distributed denial of service attacks (DDOS). Resiliency in this area would range from employing sufficient bandwidth to 'cushion' such an attack to recognizing a threat through the use of monitoring systems.

- Conducting periodic penetration tests (both on the external perimeter and internal network) to understand where vulnerability exists and implementing the necessary fixes.
- Employing user awareness programs, to combat, for example, against Ransomware and other social engineering threats.

Measuring resilience can be broad ranging; however, the organization needs to determine what is important to ensure a risk-based approach that is focused on protecting all its 'crown jewels'. Through its security operations center (SOC), an organization can determine how to assess and respond to threats as they emerge because of its continuous monitoring processes thereby building its resiliency and, more so, a strong security posture.

Incident response: the time it takes for an organization to respond to an attack in the event that its systems have been penetrated or have been hit by a natural disaster. An organization must have a sound incident management plan which it can use to be able to recover within the shortest possible time.

Measurements

For measuring each of the variables in the equation (impact, resilience and incident response) a scale of 1 to 10 can be used:

- 0-2 Low
- 3-5 Medium
- 6-8 High
- 9-10 Critical

Let's look at two hypothetical examples as to how this equation can be applied:

Example 1
The organization is reviewing its ability to withstand a DDOS attack. The questions that can be asked are:

- What is the impact of this attack on the organization if systems deemed critical are affected?
- Can the organization's IT infrastructure withstand such an attack (resiliency)?
- In the event that the organization's systems have been penetrated, how sound is the incident response?

Applying the risk equation:

- **Impact**: High (6-8)
- **Resilience**: Medium (3-5) the organization has determined that its perimeter defense / defence is adequate; however, it may need to make some improvements.
- **Incident response**: Medium (3-5) the organization already has an incident response plan, however it has determined that this plan requires some modification to ensure that its business continuity mechanisms are adequate.

Taking the low ends of the scale for each of the variables, the overall risk can be calculated as follows: 6 x 3 / 3 = 6

Therefore, the organization's overall risk to a DDOS attack considering the three variables is rated as HIGH.

Example 2
In the following example an organization is looking at its internal controls to determine effectiveness against fraud. The questions that can be asked are:

- What is the impact to the organization of an employee committing fraud?
- Are the organization's IT internal controls and procedures sound enough to prevent fraud?
- In the event that the organization's systems and procedures have been compromised, how sound is the organization's incident response?

Applying the risk equation:

- **Impact**: High (6-8)
- **Resilience**: High (6-8) the organization has completed a risk assessment on its systems and procedures and determined that is has a number of recommendations to implement.
- **Incident response**: High (6-8) the organization's incident response plan does not cover incidents relating to fraud and requires major modification to ensure that its business continuity mechanisms are adequate enough to deal with this incident.

Taking the low ends of the scale for each of the variables, the overall risk can be calculated as follows: 6 x 6 / 6 = 6
The organization's overall risk in dealing with a fraud related incident considering the three variables is rated as HIGH.

Conclusion

It is to be noted that this equation requires a great deal of analysis when determining the value to apply for each factor. Let's say for example when analyzing an event and the risk to the organization is critical, the organization's infrastructure resilience cannot handle the impact of this event so this is also rated as critical. If this is the case then the organization must have a sound incident response plan to handle this event or else face a disaster.

With this new approach to calculating risk, organizations can have a much clearer view as to the risks faced when its resilience and incident response are being tested.

About the Author

Adesh Rampat currently works for a financial institution and has 28 years of experience in the IT industry including 10 years in operational risk management. He can be reached at adeshpcs@gmail.com

Disclaimer

The content of this document is the property of the Institute of Operational Risk (IOR).

Care and attention has been taken in the preparation of this document but the IOR shall not accept any responsibility for any errors or omissions herein. Any advice given or statements or recommendations made shall not in any circumstances constitute or be deemed to constitute a warranty by the IOR as to the accuracy of such advice, statements or recommendations. The IOR shall not be liable for any loss, expense, damage or claim arising out of the advice given or not given or statements made or omitted to be made in connection with this document.

The IOR recognises copyright, trademarks, registrations and intellectual property rights of certain third parties whose work is included or may be referred to in this document.

The content of this document does not constitute a contractual agreement with the IOR. The IOR accepts no obligations associated with this document except as expressly agreed in writing. The information contained in this document is subject to change.

Promoting and Developing the Discipline of Operational Risk Management