UPDATE

The official newsletter of the Institute of Operational Risk

JULY 2018

Certificate in Operational Risk Management (CORM) Wins Major Industry Award

Accepting the award are IOR Chair, George Clark (centre) and Elena Pychova (right) former Director of Education for the IOR. With Tom Osbourn, Editor, Risk Management. (left)

The Institute of Operational Risk are delighted to announce that our Certificate in Operational Risk Management (CORM) has won the prestigious "Industry Initiative of the Year" award at the Risk.net Operational Risk Awards ceremony held on the 12th June. The award recognises the Institute's significant achievement in designing and delivering an internationally available and externally accredited qualification in Operational Risk Management.

"This award was built in-house and is a recognition of the quality, competency and dedication of the many volunteer members who contributed. We are a small but growing professional body and are humbled by this recognition from our peers" George Clark, Chair of Council at the Institute said after receiving the award.

"It demonstrates the rapid success of CORM since its initial targeted launch in May 2017 and full launch to market in February 2018," added Elena Pykhova, IOR Director of Education, who received the award with George. "We currently have around 150 students who have taken or are registered to take the award and we know that, across multiple countries, many more are discussing doing so."

Although George and Elena represented the Institute in receiving the Award, the Institute wishes to acknowledge all those who made a contribution to the development of the qualification, especially over the last 3 years. Sadly, there are far too many to mention here but you know who you are. The Institute is indebted to all of its members who have played even a small part in this outstanding success.

OperationalRisk Awards 2018 Winner

The Institute of Operational Risk Industry initiative of the year

If you would like to become a member or find out more about our qualification (you may even want to sit it yourself) then please visit www.ior-institute.org or contact us at info@ior-institute.org. We look forward to hearing from you!

IN THIS ISSUE

THE INSTITUTE OF OPERATIONAL RISK

IOR Newsletter is published quarterly by the Institute of Operational Risk. We are working to keep members and non-members informed of industry developments and of the IOR itself. If you would like further information about any of the issues raised here or would like to provide feedback, we invite you to contact the Editorial team at info@ior-institute.org

Culture Risk Management – is this new frontier for Operational Risk Management Practices and what can be learnt from developments in the supervision of Culture and Behaviours?

Enda Twomey | Head of Irish Chapter | Institute of Operational Risk

The author, **Enda Twomey**, is currently the local Chapter Head of our Irish Chapter.
These views are personal to the author and do not represent the view of any other party.

Introduction

The classic definition of Operational Risk is "The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events." This points to the role of operational risk managers have in managing the risks that can arise from people's behaviours and this being of particular importance in areas such as conduct risk amongst others.

Operational risk managers also have a key role in not just the enhancement of risk management frameworks and governance but also in driving improvement in underlying risk culture which forms the basis of appropriate risk behaviours. A question which arises as operational risk practice further develops is: "What is the role of operational risk managers in managing people's risk when the behaviours in question affect the organisation more generally and the wider underlying organisational culture? "

The Dutch Model

One of the more interesting areas in organisational culture has been the developing regulatory approach to the supervision of culture and behaviours in financial institutions. This work has been pioneered by the Dutch Central Bank ("DNB") and consists of its approach to the supervision of culture and behaviours (the "Dutch Model"). As operational risk managers are asked to assist in the application of risk management techniques to culture risk, it is useful to look at the Dutch Model more closely to see what the model can tell us in approaching the management of culture and behaviours.

So what is the Dutch model and how is it being applied?

The DNB's mission statement is that it "seeks to safeguard financial stability" and further outlines that "In light of that mandate, we must keep a close eye on anything that may put that this financial stability in jeopardy. Naturally, this includes a financial Institution's behaviour and culture". In 2010, the DNB increased the number of supervisory staff which specialised in assessing behaviours and culture and built its expertise in this area.

Underlying Premises of Dutch Model

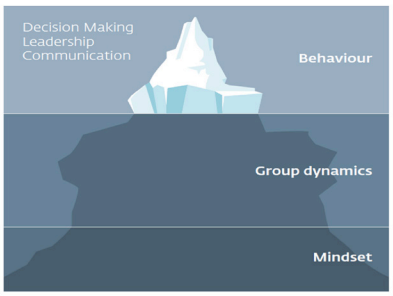
The underlying premises of the approach are stated as follows:

1. Increasing rules and regulations contributes to the perception of being in control but there are limits to what can be achieved;
2. The strong connection between the perceived behaviours and culture within financial institutions and the public's trust in the financial sector; and
3. Behaviours and culture are part of sound business operations – there is a need to identify on an institution-wide view and related mission statement on appropriate behaviours and culture and have effective processes to identify and manage behaviours and culture.

The Iceberg Metaphor

The DNB explains its approach though the use of the following iceberg metaphor:

Figure 3.1 DNB's supervisory model on behaviour and culture



The metaphor is used to show the distinction between what is directly observable i.e. behaviours and what can only be observed indirectly i.e. group dynamics. The behaviours focussed upon are leadership, communications and decision-making. Group dynamics is defined as "the interaction between different positions and patterns within a group and between groups which affects overall group effectiveness". The deepest level of the organisation is the "mind-sets", which are defined as the deeply held beliefs and values which often guide group dynamics and individual behaviours.

This approach assesses the risks attaching to leadership, decision making, communication and group dynamics, and consideration is given as to whether the behaviours and the underlying group dynamics are systematic or coincidental. Once these risks have been identified and assessed, then the next steps are ensuring that any risky and unsound behaviours and behavioural patterns are changed.

In addition (and of particular interest to operational risk managers) the DNB has also developed techniques in assessing how a financial institution approaches the risks arising from:

1. Its capacity to effect change;
2. The effectiveness and sustainability of its cultural change programmes; and
3. The enhancement of its error management culture.

Conclusion

The approach adopted by the DNB is novel and is attracting wide interest. It provides a systematic view based on decades of organisational psychology research as to what good leadership, communication, decision-making and group dynamics look like. The learnings from this approach are of particular interest to conduct and operational risk managers, but of course are also applicable to all areas of risk management.

It also poses the question for the future of operational risk management practices i.e. how should those practices be further developed to support the management of risks arising in the area of culture and behaviours?

Legacy FinTech software - too risky to replace?

EKO is the Institute's technology partner.
This article provides some insight gleaned from many years supporting a wide and varied client base.

Why avoid Risk?
FinTech is understandably a risk-averse industry. No-one wants to lose sleep worrying about avoidable risks to their finances or to their business. Using IT to reduce needless risk in financial services might be said to be doing some good in the world - at least we and our clients sleep better!

Legacy systems
Traditional financial service providers have been using FinTech since long before the word was even coined. Banking, trading, insurance, and risk management were early adopters in harnessing the power of IT. Consequently, financial service providers can have generations of software spanning decades co-existing in their systems.

Such a complex mix of new and legacy software can carry an unpalatable level of risk when upgrading components.

Within complex IT system infrastructures the risk/reward ratio of replacing a legacy system can make leaving well alone look like a good choice. At the same time, choosing not to replace a legacy system risks incurring what is known in IT as technical debt. Over time technical debt can accumulate to the point of making a system unmaintainable - effectively 'painting yourself into a corner'.

To mitigate long-term risk, your IT providers should give guidance on technical debt - typically system maintenance should include budget for regular paying down of technical debt. A mature long-lived system will generally benefit from keeping up with useful developments in computer science, such as new hardware, systems architecture or coding paradigms.

Any change to code carries risk, and good IT providers utilise multi-disciplinary approaches to managing changes safely, whether at macro or at micro level.

Strategic sense-making
Seeing the big picture and making sense of complex systems is not easy. Systems theory has spawned decision-making tools such as the legendary Dave Snowden's Cynefin framework (https://hbr.org/2007/11/a-leaders-framework-for-decision-making), which helps manage change by first categorizing by complexity the changes being considered. Each level of complexity - obvious, complicated, complex or chaotic - represents a different risk profile, and each has its own set of best practices for change management.

Behaviour Driven Development (BDD)
A major source of risk in IT is that business stakeholders and developers often effectively speak different languages - bridging the gap between natural language and technical language can be a challenge.

BDD is an agile software delivery methodology which meets this challenge by prioritizing a collaborative approach to delivering business objectives. All stakeholders - including developers and testers - share an understanding of a project's vision and goals, and regular timely conversations between stakeholders are the mainstay of the development process. Users' needs are captured as Acceptance Criteria in near natural language, readable by non-technical stakeholders. Large monolithic deployments are avoided, and instead features are prioritized and deployed in repeated short-cycle deliveries to detect misunderstandings early. In this way, the risks and attendant costs of late rework is minimized.

Chaos Monkey
This colourful risk management concept originated at Netflix, and is a tool which intentionally disables components of computer systems to test software's ability to tolerate failures, while remaining resilient and maintaining quality of service.

Central to this approach is a comprehensive test suite hierarchy, spanning low-level unit tests, through systems integration and 'real world' tests. Test platforms reduce project risk because they are intentionally written separately from the underlying system under test, and tests can be run automatically and continuously. Testing therefore provides a platform-agnostic means of ensuring code meets all specified business behaviour and remains robust and resilient.

A comprehensive test suite offers a means to change any part of a codebase safely, with assurance that unintended consequences will be identified early by regression tests.

Too risky to replace?
FinTech services have a unique set of risk characteristics that can make any software changes liable to cause sleepless nights.

Nevertheless, judicious use of risk mitigating technologies can give confidence that the right tools are being used, the right user stories are being implemented, and the right tests are being run.

As developers, when together with stakeholders we tick all those boxes, the peace of mind achieved feels wonderful. A culture of considered, continuous, comprehensive testing means arguably any piece of software can be upgraded safely.

At Eko, we regularly run workshops to discover the risks and engineer a path to a solution. If you'd like to engage in one of these workshops you can contact us via:
http://www.ekouk.com/contact

Chapter activity

The England & Wales Chapter Events

Hannah Chung | Local Chapter Committee | England and Wales

From left to right: Mark Spicknell, Tony Blunden, Michael Grimwade, Tom Osborn, and Patrick McConnell.

In May 2018, The England & Wales Chapter organised an event exploring the 'Current and Future Challenges for Operational Risk Managers'.

Highlights

- A cultural shift is required as banks have been reactive rather than proactive following the raft of prominent scandals experienced over the last decade. They continue to operate in this "firefighting" mode, responding to regulation instead of looking beyond to define an end state that truly provides the link between risk and reward.
- As organisations implement new technology, the importance of sandboxing and robust testing has been highlighted by the recent TSB on-line banking issues. Additionally, organisations need to ensure the right skillset exists within their Operational Risk Management functions to assess, challenge and monitor the rise in new technology risks.
- Operational Risk Management need to be fully plugged in and proactively engaged with particular attention given to areas of the organisation where growth is actively pursued. Where control frameworks underpinning this growth aren't robust and adequately supporting the businesses' growth strategies, it isn't hard to predict where the next biggest operational risk event might occur.

Discussion points included:

Culture

- Culture has been linked to a number of prominent scandals experienced over the past decade. These operational risk events, ranging from LIBOR manipulation, FX fixings, PPI mis-selling, tax and AML misconduct, have highlighted how organisation culture plays a significant role in contributing to these events. They stem from bad practices being repeated, imposed and accepted within organisations and proliferating across the banking industry.
- Where cultural issues remain unfixed, the panel debated whether the removal of operational risk loss events from a firm's historical data for the disposals of businesses is justified. Ultimately, organisations need to ensure cultural issues are addressed as part of their incident remediation.

The Rise of Technology Risk

- Blockchain, Artificial Intelligence and other emerging FinTech advancements requires Operational Risk Managers to have increased awareness and engagement to understand the new risks introduced as a result of these capabilities.
- Highlighted by the ongoing TSB incident in 2018, strategic technology risks are one of the most important operational risks as banks look to replace their legacy systems to meet their customer needs and remain competitive.
- The recent banking problems associated with TSB's on-line banking application illustrate the criticality of technology risk and the importance of sandboxing and robust testing prior to introducing technology changes into the live environment.
- Further, their problems were exacerbated by external attacks with fraudsters exploiting the organisation's vulnerabilities to take advantage of customers. These events highlight the importance of operational resiliency and the need for this to be high on the management agenda.
- The rise of technology risks has also highlighted increased "talent risk" faced by organisations to employ Technical Specialists with the appropriate technology skills and expertise required. Given the breadth and scope of operational risks faced by organisations, management need to regularly assess whether the skills and experience of its second line operational risk managers appropriately match the key risks faced by the organisation.

Top 10 Operational Risks for 2018

- The Top 10 operational risks for 2018 was designed to offer a reflection of the industry's top concerns with respect to non-financial risk at a given point in time.
- Further details on the methodology and aggregation from the survey are available in the field guide published on Risk.net.

The Panel

Tony Blunden, Head of Consulting, Chase Cooper
Michael Grimwade, International Head of Operational Risk, MUFG Securities
Dr Patrick McConnell, Honorary Fellow at Macquarie University Applied Finance Centre
Mark Spicknell, RBS Head of Operational Risk
Moderator: Tom Osborn, Desk Editor, Risk management, Risk.net

We are grateful to our corporate member RBS for hosting the event and to our speakers for making the time to present their views.
The presentation materials by Dr Patrick McConnell are available to our Members on the Institute of Operational Risk website.
More commentary on Tom Osborn's update of the latest annual operational risk survey can be found here.

The New Risk Awards Are Here! Get Recognition Where It Is Due!

Edward Sankey FIOR

CIR Risk Management AWARDS 2018

This year again the IOR is sponsoring of the Risk Awards. These Awards have rewarded successful examples of fine practice over many years.

The operational risk community has had many leading and successful instances of excellent practice. These might be new training programmes, risk reporting systems, techniques in risk analysis, control strategies, response planning and project implementations. There is no doubt that operational risk is developing the art and practice of risk management with new solutions.

Probably because one is so close to one's work day-by-day it is not seen to be the fine example and even innovation that it is when compared to general practice.

Last year one of the winners was Adam Seager of Argo, a past Director of the Institute. He had the great pleasure of accepting the award from comedian Lucy Porter! He won "Operational Risk Initiative of the Year".

If you are working in a firm, this is a great way to celebrate an individual and/or the team, together with enjoying the great Awards Dinner celebration with the team and guests.

If you work for a consultancy, you may have a fine new service to that deserves an award. And/or – you might propose to a client that an entry is made of a successful project you have worked on, providing an excellent special benefit for your client!

The organisers have set up a number of categories, and I'm sure you would be able to find a suitable class to enter it in. Preparing an entry is not onerous. The submission is max. 1000 words. It is extremely unlikely that the entry will require disclosure of sensitive information about your firm.

For more information, see http://www.cirmagazine.com/riskmanagementawards/index.php (see the video!) The categories are on: http://www.cirmagazine.com/riskmanagementawards/categories.php.

With a submission required of just 1,000 words or less, into which illustrations can be added, it will be easy to meet the submission deadline of 13 July.

My advice is identify the advance or the innovation (or a Risk Manager of note) and start writing. The words will come!

Our members do great work, and if I as a past judge can advise on how to go ahead – choosing the topic or writing it, I would be pleased to for the sake of getting some IOR wins!

TAKE YOUR CAREER TO THE NEXT LEVEL WITH CORM

THE CERTIFICATE IN OPERATIONAL RISK MANAGEMENT (CORM) FROM THE IOR

For anyone managing operational risks, this course represents the **Gold Standard** to developing a common understanding amongst OpRisk practitioners as well as providing assurance to organisations through independent certification.

For individuals, the CORM certification demonstrates employee commitment and professional knowledge to employers and peers.

The comprehensive study programme over 9 study topics covers fundamentals, management, appetite, practitioner tools and regulatory treatment of operational risk.

This course has been created and is delivered by The Institute of Operational Risk and is accredited by ATHE and regulated by OfQual.

More details are available at: **www.ior-institute/CORM**

Certification offers:

- Industry accreditation
- Team confidence
- Assurance to governance
- Professional development
- Peer recognition
- Common understanding

OperationalRisk Awards 2018 Winner — The Institute of Operational Risk Industry initiative of the year

Course fee:

£550 (plus VAT)
includes all materials and exam fee

plus
1 year IOR Associate Membership*
*new members only

Enrol now for 2018 at www.ior-institute.org/CORM

THE INSTITUTE OF OPERATIONAL RISK

Promoting and Developing the Discipline of Operational Risk Management

www.ior-institute.org | Tel: 01920 443818 | info@ior-institute.org