In association with

ORIGAMI RISK

CIR
CONTINUITY INSURANCE & RISK

Enterprise risk management roundtable

In association with ORIGAMI RISK

Roundtable

ERM: Putting a face to the name

Our panel of experts reflect on the challenges involved in establishing ERM programmes, and on how they are leveraging resources to improve outcomes

John Hurrell: What challenges do you face when it comes to implementing ERM within your organisations?

Josh Newsum: The main challenge we face is how to create an efficient ERM programme and process and deliver actionable results to the board.

Neil Almond: There are number of issues with implementing ERM in a large, established corporation. Scale is a significant factor: the sheer number of people that you have to interface with in order to get the necessary information makes for quite a challenge in itself. Establishing a motive for implementing ERM should be a key consideration, for example, greater surety of achieving strategic goals and/or looking to improve governance.

Rebecca Cope-Lewis: Our current search at Serco for an ERM system has led us to ask ourselves what precisely an ERM system should look like, and what should it actually do for us? And that's a challenge in itself!

Danny Pollard: A key challenge for me has been establishing the communication and flow of information through our business with regards to risk. Our current approach, using Excel, did work initially but as we have grown and become complex, this no longer works, so we're about to look at dedicated ERM software.

The biggest challenge has been helping management to step out of their very intense day-to-day operational duties and to recognise, which they are doing, that some of the solutions that have been 'good enough' to date on a divisional basis are now being outgrown by the business as a whole as we have grown and become more complex and that we need to adopt the scalable solutions that we are now working to implement.

Iain Pickard: One cannot look at risk in silos because very often the most toxic risks are combinations, and to address this you've got to understand the connections between them.

David Lanfranchi: Working with silos is inevitable within an agency-based business like ours. We have a lot of different companies doing a lot of different things. Getting them to recognise the structured approach to understanding risk is difficult enough. We are currently in the early stages of structuring our ERM. It's a steep learning curve at the moment, and we're achieving buy-in gradually.

Alejandro Carvajal: As the HS2 project is a joint venture, a key challenge for us is around integration. We've got the people, the governance and the systems, but we are trying to make them work

Roundtable

Participants:

Chair: John Hurrell, Senior Advisor, **Strategia Worldwide**	**Sunnie Luthra,** Risk & Capital Actuary, **International General Insurance**
Neil Almond, Insurable Risk Manager, **Tesco**	**Iain Pickard,** Co-Founder & Managing Partner, **Strategia Worldwide**
Alejandro Carvajal, Risk Manager, **Skanska**	**Danny Pollard,** Internal Risk Auditor, **Irwin Mitchell**
Rebecca Cope-Lewis, Group Risk & Programmes Manager, **Serco**	**Simon Spurr,** Group Head of Risk & Capital, **International General Insurance**
James D'Arcy, Senior Consultant, **Aon Risk Solutions**	**Andrew Duttine,** Sales Executive, **Origami Risk**
Mike Hopkinson, Senior Group Risk Manager, **Kier**	**Josh Newsum,** Senior Practice Lead for ERM, **Origami Risk**
David Lanfranchi, Risk Manager, **CSM Sport & Entertainment**	**Neil Scotcher,** Client Service & Sales Executive, **Origami Risk**

alongside one another on a project-by-project basis.

Simon Spurr: Risk is at the heart of what we do – whether it's investing or underwriting, and one of our challenges involves bridging quantitative and qualitative, which is very complicated.

Additionally, a lot of operational risks overlap with insurable risks. For example if we fail to record or model our risk exposures correctly, it becomes a very difficult problem when we attempt to rely on our modelling outputs.

Andrew Duttine: A lot of the work we do with clients is around fixing issues with data being in silos – to help build the information businesses need to make good, informed decisions.

Sunnie Luthra: I focus on a very narrow area of ERM, specifically quantifying the financials of a risk.

Mike Hopkinson: One of the challenges is translating ERM information into good business decision-making information. As my focus is strategic and operational risk, I'm very passionate about trying to get frontline risks communicated throughout the business to the senior management level. It's what I call the 'golden thread' – not easy, but an interesting challenge! When it comes to silos, one of the biggest potential challenges is meshing together operational risk silos, functional risk silos and data silos.

James D'Arcy: Our work on ERM has changed dramatically from the design and implementation of frameworks to now much more ad hoc, focused and very detailed projects.

Working for an insurance broker, one of the additional challenges that I face is differentiating between non-insurable risk, insurable risk and how the two can affect each other. Having that conversation with can be difficult, with clients and with colleagues. We also experience the same challenges as others do in getting access to the right people to have the discussion about risk and how risk affects strategy – the 'golden thread', as you say.

Neil Scotcher: I've implemented a lot of solutions for a lot of organisations, and everybody has a different view of how ERM should be done. As a solutions provider, my key challenge is trying to understand how a client sees things.

Understanding the drivers

Hurrell: What is abundantly clear is that everyone has a slightly different view of where ERM fits within their organisation, as well as very different views on its actual definition. Let's assume for the discussion that ERM is an integrated process for managing risk throughout the organisation, joining operations and strategy and being managed within a board-approved framework.

To get a sense of momentum and direction, do you think ERM is getting more traction today compared with three years ago? And how do you see that changing over the coming years – both for regulated and non-regulated enterprises?

Hopkinson: We are absolutely seeing more traction, driven by external market and sector factors and a heightened government focus on construction businesses. There is now a greater expectation of where we need to be.

Spurr: I agree that external factors are at play here as well as legislation and compliance, which are driving ERM up the agenda. We have certain obligations when it comes to having a formalised

Roundtable

risk system. At the same time, though, there is a growing recognition that there is value in it.

Luthra: In the insurance industry, the primary driver for ERM has been Solvency II and the industry has spent a lot of money becoming compliant. Seeing this, the board now wants to know how the company can get value out of this exciting thing, since they're paying so much money for it! So we are now beginning to look in greater detail at some of the individual aspects of ERM and how they come together – to find out what the underlying message is.

Cope-Lewis: That's exactly where we are. We've just joined our insurance department with our risk and compliance functions and that's helping to us to better connect these two functions, and that wider scope is really key.

At Serco, we have senior level commitment to the work of the risk function and that buy-in helps enormously.

I think we have to be careful that we don't create an expensive cottage industry on the frontline, however. Achieving the right balance can mean the difference between ERM being seen as an enabler, or as just another expensive function that sits on the side.

Hurrell: If ERM sits on the side it's not ERM anymore…

Almond: There's definitely more momentum behind ERM today, but we are at a stage now where it's got to prove itself, beyond simply ticking the compliance box. For retailers that could include successfully hitting strategic objectives or the avoidance of loss, financial or otherwise. It's worth adding at this point that the likelihood of landing ERM in one perfectly in one hit, is low. To make it work, you have to accept that it could be an iterative process.

Demonstrating ROI

Hurrell: How indeed does ERM prove itself? Now that we have progress and momentum, how do you prove the ROI? With corporate objectives often financially driven, how do you prove the payback of ERM, when it is reducing the likelihood of a negative outcome, as opposed to creating a positive, bankable outcome? How are you demonstrating that ERM warrants the continued support and leadership of the board in the absence of an easy-to-identify financial return?

"The problem with ERM is that sometimes you can become a victim of your own success"

Luthra: The problem with ERM is that sometimes you can become a victim of your own success. We stop bad things from happening; but when nothing bad happens, questions are raised about our relevance.

Pickard: Risk management in general can be viewed as two sides of the same coin – stopping bad things happening, and enabling opportunity – helping the business to do the things that perhaps they would not otherwise have been able to do. A clear understanding of risk helps us understand and manage it, providing the confidence to go forward and develop new areas of business.

Hopkinson: That's quite true. One of my strongest allies is our innovation director, and that relationship is really key to my work.

Carvajal: One of my previous employers began implementing ERM to support an IPO. Having established that whole process, they are now able to really understand the benefits of the programme in highlighting strengths and weaknesses. As a result, they have a much more realistic view of the business than they did five years ago, which I think is a great example of integrational gain.

Roundtable

Newsum: It is indeed objectives – and what might get in the way of those objectives – that really resonates with boards and committees today. And that's new thinking compared with the last decade, which used to be very focused on risks and their impact on the business; whereas now boards want to know how an event impacts objectives and how that plays into risk appetite and risk tolerance. They want to be sure they are making smart decisions that consider risk posture versus the actual level of risk. This is where we're starting to see a value shift.

Luthra: The risk function at a previous employer of mine developed a reputation of being 'blockers', which should not happen. We should instead be considered as enablers, thinking through the risk with the individual functions and not trying to impose our opinion on them.

Spurr: While our ERM process continues to develop, it's already being seen as an enabler. We have been able to demonstrate the benefits of ERM and modelling through better decision making, ultimately leading to impacts on the bottom line.

I'm also a big believer in highlighting success where you can, such as showing how cyber defences stymie attacks on a daily basis. If this risk was not managed, we would be in a much worse position.

D'Arcy: At the same time, I think there is a risk that ERM itself can provide a false sense of security.

Board involvement and ROI

Hurrell: Board leadership is seen to be critical to any successful ERM enterprise. Surveys conducted among the Airmic membership and such studies as a recent Cass Business School Report support the view that ERM is more likely to succeed within the organisation when it has buy-in and impetus from the top. Has anyone seen any examples of this in practice? To what extent have your boards taken the leadership position in ERM? Do you feel supported by the board or is it a bit of an uphill struggle?

Spurr: You have to respect people's time. The board is tremendously busy and the full pack that goes into a typical quarterly board meeting is over an inch thick. I have trimmed my section down to around 10 pages. Respect their inability to understand all the minutiae; whether you're building tunnels or houses or whether you're doing sports events or whether you're an insurance company, the goal of the board is to ensure adequate challenge and review of the work – not to be experts in all of it. Give them some confidence but don't overburden them with difficult to understand risk registers that dumb things down to tick a box. Instead have a deep conversation about one or two bits once a quarter, rather than drowning them in a sea of data.

Hopkinson: Yes, we certainly have that level of engagement with the board. But you've got to continue to demonstrate ROI, otherwise they may lose the passion for it. That, for me, has been one of the key drivers for ongoing engagement and improvement..

Lanfranchi: That's got to be the approach, from my point of view. When we're looking at individual events, we do an awful lot of work around What If scenarios. It's perhaps not the textbook ERM process, but nonetheless it is a meaningful discussion about how we make something as good as it can be.

Scotcher: What clients often want from ERM software is a system that tells them 'what if', when they have not actually got the data for what's happening right now. Often you have to start by understanding what data you've got before you can look at trying to figure out 'what if'.

Roundtable

Hurrell: It seems to me that risk maps are quite good at looking at external sources of risk, but are not very useful for looking at what's going on within an organisation, and being able to critically assess particular problems. Almost every week there's a big data breach – which nine times out of 10 is down to an internal systems failure; and yet risk maps are still externally focused. They feel very comfortable talking about bad things that will happen from the outside, but very uncomfortable about things that might happen as a result of what's going on within the organisation, due to some failure of management or other disconnect. How can organisations more effectively assess risks from within?

Hopkinson: When we first started our ERM journey about three years ago, we drew in risk champions from each of our business units and found exactly what you have described: they were all very happy to highlight external risks. Now we have introduced group functions that have oversight across the whole business, and this new matrix approach has had a really positive effect, because it means assumptions are challenged.

Cope-Lewis: Again, I see my role here as a facilitator, recognising that culture has to be set from the top.

Pollard: Do risk functions even have the courage to challenge an 'elephant in the boardroom'? Would I have the courage to put a scenario on the table around the mislabelling of a sandwich, for instance? No, because it would be so obvious. It would seem inconceivable that that such a simple thing would be missed.

Hurrell: Airmic's 'Roads to Ruin' research found that in 19 of the 20 catastrophic failures they studied, including BP, AIG and HSBC, it was known within the organisation that something was badly was wrong, but it had just not reached the decision-making level.

Cass Business School recommends a twofold approach to dealing with this challenge. The first is about having a whistleblowing, or similar procedure; the secondly, was to empower people to say something – at all levels of the organisation, and particularly the front-line.

"There is a definite distinction between the business intelligence and actuarial data that go into an ERM system"

The value of good data

Hurrell: Given the growing recognition of the value of data, what is being done to improve its use, analysis and deployment?

Almond: You have to be pragmatic. You have to understand your data. Unless you understand and have absolute confidence in the integrity of your data, you may as well not bother. The analysis of bad data is probably one of the most dangerous things we can do as a business.

Luthra: Supplementing that with industry-wide data can be helpful but it can be a double-edged sword if it has its own issues – if it is incomplete, out of date or just irrelevant.

The other issue is that, quite frequently, data is backward-looking not forward-looking. What has happened has happened. Agree that you might learn from it, to some degree. But the important question is what might happen in the next five, 10 or 15 years that will take the company down? There is no data for that. So that needs to be considered, and the only way to achieve that is through discussion.

And if there is a challenge of scale, AI or RPA can come in here, but it still

Roundtable

needs the human touch when it comes to the important job of communicating what it actually means.

Almond: I totally agree. And for that reason you have to keep control of what you're doing with the data and how it's being interpreted.

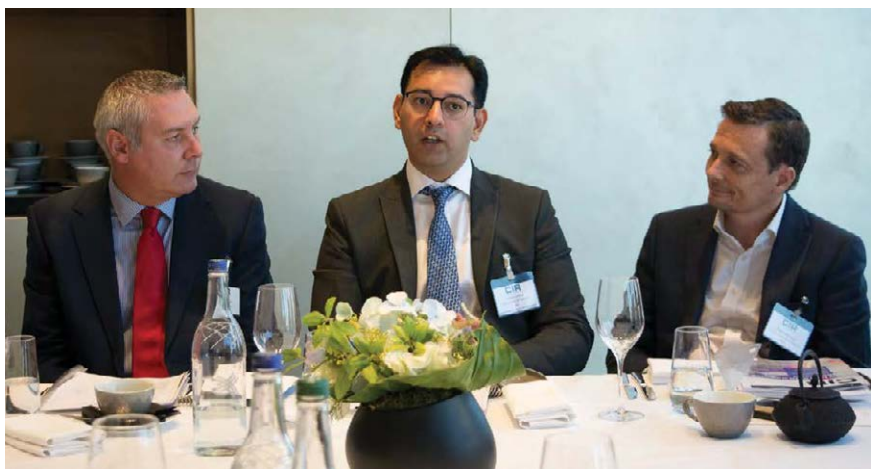
I do a lot of work with actuaries and have observed that when statistical models are used, real-world business intelligence can sometimes be overlooked.

Luthra: Actuaries are usually backward looking while risk managers are more forward looking. The two views complement each other, but they should not merge into one. There are two different personalities that need to work together.

Lanfranchi: I think that occasionally approaches to modelling can be oversimplified. A small data set will only produce nonsense. Complex modelling is, as its name suggests, quite complex and requires a decent dataset, and will produce a result that may bear some resemblance to what will actually happen.

Cope-Lewis: I think you've got to look back because that helps to inform going forward. It should be used to inform going forwards, so if an event does happen, you learn from that event and put in place measures to ensure that if a similar event occurs it doesn't impact as much as it might otherwise.

This is about risk appetite and how much risk you are willing to take. In my view, that approach is more useful sometimes. I think you've got to accept that at some point, something is going



to happen; someone is going to do something – and it comes down to people, in the end.

Lanfranchi: You can produce all the models you like but if you can just have a conversation with the teams that understand the risk, then you can put in place a series of mitigating measures that are probably not too expensive, probably not to complicated, and will probably work… most of the time. That is probably better than analysing it to death and presenting it to the board with page of papers they won't read anyway.

Carvajal: For me ERM is more about collaboration and communication.

Hopkinson: You have to have good data and understand how good it is. But actually, I think at times even poor data can be helpful, if it's used as a catalyst for conversation… It's back to Simon's earlier comment around having those in-depth conversations and discussions.

Spurr: I agree, because I think much of the information that goes into an ERM system is more subjective. It might well result in a number, but somebody has made a judgement call in there somewhere. There is a definite distinction between the actuarial data and business intelligence information that goes into an ERM system.

Hurrell: What models or standards are you using internally or for compliance purposes? Or are you taking a completely different approach to the way you implement ERM?

Almond: Slavishly applying one standard might be the wrong approach, but sometimes you just have to start somewhere. At least everyone starts off singing from the same hymn sheet.

Cope-Lewis: Standards are good for ensuring you are roughly in the right ballpark, at very least.

Whilst I have a background that includes quality management, I'm not an advocate for slavishly adhering to standards. I believe that as risk professionals it is our duty to understand and know that information, but to choose an approach and do what is right for your business. Then what your business needs becomes your model. I think that is the right approach and

Roundtable

it will look slightly different for every company. We can show compliance with ISO 31000 if we need to, which we sometimes do.

Pollard: As a baseline we are working towards ISO 31000, but that only tells you so much. The risk management process and framework should be custom-made for the business.

As an internal risk auditor, I've come to understand all the different areas and how complex they are, which helps enormously. I've built on ISO 31000 and incorporated it into what we do on a day-to-day basis but also included other aspects from other standards such as COSO. You have to adapt standards to fit your own organisation its unique challenges.

Carvajal: In terms of the maturity of our framework, I'd say it's probably in development. We have some challenges when it comes to integrating with some of the Network Rail frameworks, technologies and models, but we're getting there and we are certainly taking the best from what we are learning.

Pickard: We don't follow any standards. We like to have our own standard. Standards are great because they're a handrail, but we've got to be careful they don't become a straitjacket. We would encourage people to look at risk differently, comprehensively – to take an outside-in as well as an inside-out view.

Spurr: I want to implement something that is sufficiently simple and meaningful that it can be explained to the people on the frontline – in other words, it makes sense to the people who are actually taking the risk. There is a real danger that we over-engineer a lot of this.

Lanfranchi: I think that's fair to say. We find ISO 31000 useful from a vocabulary perspective, as well as for consistency and structure. Then you can use it as a baseline and adapt it for your own use. We have a very unique business where we are doing a lot of creative things. We have to think about those very carefully.

Luthra: You have to remember that not every risk can be quantified. My job primarily is to analyse the risks, quantify them, put a number to them, and then start a discussion about whether this number is right and what went behind the calculations to bring us to that number.

You cannot have just the discussion or just the number. You need to have the combination of both, because without the numbers nobody will be interested. Quantification is important, but not the end – it's the start.

Hopkinson: I'd echo that view. I'd also like to add that our own framework continues to evolve and it will continue to evolve, but while it's not based on one specific standard, it does take best practice from different sources, including COSO and ISO.

Newsum: We speak to a lot of customers who believe at first that they need to be tied to a particular standard or framework, only to find that such a rigid approach often leads to a programme that doesn't end up being overly successful for them.

Origami's position is that we are fairly framework or standard agnostic. Instead we focus on developing the right type of risk culture within the organisation, identifying the risks and creating a programme that's really scalable and sustainable for that organisation.