StrategicRISK

November 06

ROUNDTABLE 2006

OPERATIONAL RISK

Sponsored by:

HUGH JAMES

PRICEWATERHOUSECOOPERS

Operational Risk

An introduction to the StrategicRISK roundtable discussion by **Lee Coppack**

Semantics bedevils risk management. What do we mean by the terms we so often use? And do we mean the same thing? The first question for the participants in this roundtable was – what do we mean by operational risk?

It quickly emerged that there is a dividing line between financial services companies, like banks, and other businesses. Financial institutions must use the risk definitions supplied by regulations, like Basel II, while businesses that are not subject to the same type of prescription have flexibility in how they define types of risk. The most appropriate definitions may be ones that they devise themselves to take account of their individual circumstances.

Indeed, there was an argument that organisations could avoid categorising risks altogether if they use enterprise wide risk management (ERM). ERM, it was said, allows an organisation to group and manage its risks in whatever way it finds useful, for example by functional headings, like IT, supply chain or property.

Transparency and communication emerged as critical components of risk management. With large companies operating in different sectors and many different countries, you cannot otherwise see how an action in one part of the business could affect other elements. There was a general view that organisations need someone in a senior position with an enterprise-wide perspective to champion risk management, whether or not the person carries the title chief risk officer. Having board members with experience of the industry and its intrinsic risks is also valuable.

The role of internal audit and its relationship with risk management came in for discussion. They should work together with the organisation's view of risk driving internal audit, which in turn provides independent assurance that the policies and programmes are in place and working.

The words of Donald Rumsfeld turned out to be unexpectedly appropriate when it comes to managing operational risks, for fraud and collusion and the behaviour of traders and sales reps (known unknowns) are among the most difficult to deal with and potential doomsday scenarios (unknown unknowns) among the most difficult to imagine.

Ultimately, the group felt that where possible bespoke definitions of operational risk to suit individual companies are good, but that an enterprise wide approach that concentrates on managing, instead of naming, risks is even better.

Lee Coppack, Market Analyst, StrategicRISK

Roundtable participants

Geoff Taylor, chairman AIRMIC and director of risk management Europe, Middle East and Africa, Nike, who chaired the discussion

Terry Cunnington, director group risk management, Euronext

Milan Milovanovic, European risk and insurance manager, Hertz

Lee Needham, insurance manager, Barclays

Simon Perry, director, PricewaterhouseCoopers (PWC)

Hugh Price, head of insurance, Hugh James

Chuck Teixeira, a director at PwC who leads the integration of risk and control frameworks

Operational Risk

GEOFF TAYLOR: Our topic today is operational risk, and the first thing that springs to my mind is, what is operational risk? It seems that we have multiple different definitions. The financial institutions tend to see market and credit risk as their core business, and everything else is operational risk. Whereas I think in the corporate world we tend to see things more in three different categories. There is the financial risk because, yes, we hedge currency and that is done by treasury. There is the general business risk: how much should we sell, can we sell this or not sell it? Then all the support function pieces tend to be lumped together as operational risk, but we don't necessarily deal with that operational risk in an integrated way.

So do we have a definition of operational risk? Or is it still going to be individual to different industries? If we don't agree what operational risk is, it is going to be very interesting to see how regulators or other stakeholders might try and influence the agenda on operational risk, so I open that to comment.

TERRY CUNNINGTON: Although I am in financial services, Euronext is not a bank. Therefore, we don't have market risk and credit risk. We could argue that as our business is running markets, the market risk is our operational risk, but we don't have an operational risk approach. We have enterprise wide risk management (ERM). There is a huge overlap between that and what other people regard as operational risk, but we are in the process of having a more top down ERM approach and bringing in elements of operational risk, bringing in more of a bottom up approach as well.

LEE NEEDHAM: For banks, Basel II which is the new regulatory standard, contains a definition of operational risk, For banks, that is the definition they have to follow. It is not elective. That said, your earlier comment was more or less correct; operational risk is anything other than market and credit. There are a couple of exclusions in Basel II; it doesn't pick up strategic risk or reputation risk.

SIMON PERRY: I'd like to see corporates outside financial services sectors that aren't being regulated and so given a regulated definition of operational risk, develop their own risk categories and their own definitions of what is operational risk in their own language.

HUGH PRICE: The way a lawyer would do these things is making sure we get the advice right every time and try to eradicate mistakes or errors. In other words, we see it in terms of negligence claims. You get it right if you keep your client content, because you have given them the right advice in the right way. That is how I see operational risk, quite distinct from strategic risk,

which is the business going forward, the high helicopter view.

GEOFF TAYLOR: How do you then fit in things like people risk, in terms of key people, health and safety, security of your operations? Where does that sit?

HUGH PRICE: The core is getting the advice right, but then obviously with that you have got to make sure people are properly trained, they are properly supervised, given the skills set that they need to give that advice to the client. Health and safety, that all has to be taken into account because that is part of the operation. You have got to make sure the workplace is safe for your people and the environment is right for your people to generate the work and advice and they have skills that you want them to have.

CHUCK TEIXEIRA: A lot of times you see operational risk defined as the loss that results from internal and external activities. For things such as health and safety, key people risk and all those types, it's what happens if all these people walk out the door tomorrow or if this building gets destroyed. What is the consequence? What is the probability of those things happening? It all gets tied to this concept of loss.

MILAN MILOVANOVIC: Looking at the attendees of this meeting today, most of whom are from financial services, I tried to think of something that was common and the one thing we do have in common is operational risk. So how do you define it? I came to the conclusion that the best way to round-robin the definition of operational risk is to give it the heading 'effective and efficient use of resources and the management and monitoring of that'. That would embrace most of what we would deem as being operational, headcount, staffing, health and safety, those sorts of things. Collectively, effective and efficient use of resources is how I would describe operational risk.

GEOFF TAYLOR: I kind of subscribe as well to the fact that you have to tailor-make your definition to where you are and driving a common definition, as Basel II has tried to do, may not be the right way.

LEE NEEDHAM: Basel II is very prescriptive. It has a general definition. It then actually categorises risks into seven risk types, which are then further sub-divided. For a bank, the two biggest risks are internal and external fraud, because banks deal in money and people steal money, but if you are an airline, people stealing money is probably not your biggest operational risk. Therefore, I think trying to come up with a common language across the industries would be quite difficult unless it was very generic and then you are losing something.

GEOFF TAYLOR: I am not totally familiar with Basel II, but do they put themselves into the risk because they are regulating?

LEE NEEDHAM: Yes, regulatory risk is a category. It's in there. Look at what has happened to the online betting agencies in the last few days. Changes in regulation can completely destroy your business overnight, so clearly it is a risk to be aware of.

GEOFF TAYLOR: To mention a point on reputational risk, I work for a corporate which has a reasonable brand presence and we trade a lot on brand, so how the consumers, the public and other stakeholders perceive it is very important. I am not sure whether we see that as an operational risk or not, because I think how it is managed is really different depending upon different parts of the business. Should it be part of operational risk or shouldn't it? I think it is not necessarily a risk in itself anyway. There are other risks that affect your reputation, so it is more a consequence of management and other risks.

TERRY CUNNINGTON: In my view where you have a regulated industry, and especially banks, where you don't have a choice in the matter, that is one thing, but where you haven't, why tie yourself down by saying you are operational risk? Why not just say you are risk management, and it doesn't matter what is included or not, as long as the responsibility is clear within the organisation.

In our organisation we have seven higher categories that break down further, those seven are business operations, technology, extended enterprise because you have dependency upon third parties, we have legal and regulatory risks, we have product and brand, we have resources – that includes property, financial and people risks – and we have strategic risk. Does it really matter what you say is operational risk and what is not? It is risk. It is risk management. So long as you are organised to manage those risks, does it really matter what the definition is?

CHUCK TEIXEIRA: What makes operational risk unique compared to some of the other categories is that operational risk is the one that does slice across market credit, IT, HR, reputational. If you look at a pharmaceutical company, reputational risk is paramount to the effect on operational risk. That is what makes operational risk so unique to the other categories.

SIMON PERRY: I see reputational risk as an impact like financial risk. It is an interesting lens to understand how broadly you should be thinking in terms of risk and what is important and what isn't. I don't tend to advise

You have to tailor-make your definition to where you are, and driving a common definition, as Basel II has tried to do, may not be the right way
GEOFF TAYLOR

companies to develop a category called reputational risk, because by doing so you narrow your focus into thinking about reputational risk rather than perhaps thinking about financial risk, and quite often they have got very related pressure and impact. I like to think about reputation as a consequence, something that you protect, the same as you want to protect your finances.

HUGH PRICE: Depending on the nature of your business, you are going to prioritise risk in a completely different way. I am not too sure it matters whether you call it operational risk, strategic risk, health risk, whatever, as long as you recognise it and are doing something about it, trying to get best practice within your own business.

CHUCK TEIXEIRA: One of the important things, too, in that respect is being able to take those risk categories and look beyond the regulations that underpin them. If you are a bank, you have to deal with Basel and Sarbanes-Oxley. You look at it with those lenses, as opposed to stepping back and looking across the board to say, what is the real risk to my business, be it across market, credit, operational etc. That is difficult, especially in financial services.

GEOFF TAYLOR: Are you suggesting, perhaps, that regulation has a negative effect on risk?

CHUCK TEIXEIRA: It can have if people, if organisations, create everything in isolation, creating their own separate infrastructures as opposed to having enterprise-wide or much more clear, centralised risk management practice and setting up those definitions for the organisation, as opposed to necessarily on regulatory lines.

LEE NEEDHAM: There can be a clear temptation to align your whole risk management approach simply to comply with regulation as a kind of a ceiling, whereas I think regulation has to be seen as a minimum standard, and the controls and risk management strategies you use should actually exceed that and are far broader than simply the requirements of regulation. Clearly for banks, if you think of the three, market, credit and operational risk, operational risk is their smallest risk. The biggest risks for most banks are clearly on the credit and market side.

GEOFF TAYLOR: Can I challenge that? Sometimes I think the banks are very well managed in their financial risk area, because that is their business and they have been doing it for so long. They have a lot of modelling and other techniques available to limit their risks, so they know what their exposures are. What they don't model is an outbreak of food poisoning in their trading floor and all the traders don't turn up for three days. It is an operational risk but how do you model that?

CHUCK TEIXEIRA: It is tough to model, but in terms of operational risk, when you try to start modelling and looking at the financial impact, a lot of times the actual impact on a bank is quite minimal compared to if we change a credit risk curve on a trillion pounds portfolio. A slight adjustment can have a drastic financial effect.

LEE NEEDHAM: That's really my point. The financial impact of an operational risk occurring for a lot of banks is tiny compared to a shift in interest rates.

TERRY CUNNINGTON: In reality, there are a lot of risks that are very difficult to quantify for many businesses, banks probably less so, but where you get more strategic type risks, one-off events rather than a recurring risk, invariably a lot of subjective judgement comes in. If you come up with a number that has no credibility, what is the point in quantifying it? There is a number of that type of risk where you actually have to use subjective judgement, not just your own but those closer to the risk as well.

GEOFF TAYLOR: I tend to agree that people try and model risks that are, what I consider, unmodellable, like some of the reputational type impacts or political risks even. History doesn't tell you what is going to happen or what the next government will be, but those things are very interesting, particularly when you go into new markets. So the question is, should we worry about them, particularly on the financial institutions' side. If the impact is so insignificant, why are we spending so much time worrying about it? Why are the regulators spending so much time worrying about it, when fundamentally it is still the market credit risk that will bring the banking system down or the bank down, not the operational risk. Is that incorrect?

LEE NEEDHAM: I think the regulators' concerns stems from events such as Barings. They don't want to see another Barings.

CHUCK TEIXEIRA: You see more pressure as banks, hedge funds and other financial institutions are trying to get into more high margin activities. They are going into emerging markets and trying to expand their businesses as much as possible. Sometimes the appropriate governance risks and controls aren't necessarily in place. If in your mind it is not a material part of your business, you are not necessarily monitoring all the locations that you are involved in, and that increases the risk that the same thing could happen again

If you come up with a number that has no credibility, what is the point in quantifying it?
TERRY CUNNINGTON

MILAN MILOVANOVIC: As I see it, operational risk is something that drives and manages the other risk aspects, strategic risk for instance, reputational risk. Operational risk to me is something of a management risk. It is the glue that holds all the other key exposures together, strategic, reputational and what-have-you.

GEOFF TAYLOR: I am interested as well in the cultural aspect of the risk, because we see a different attitude across countries even in Europe, let alone when we start going into the emerging markets. The culture is different and how people operate is different. Perhaps they don't question superiors or there is a different business culture in the way the society works.

MILAN MILOVANOVIC: That's why it is so much more difficult to measure the effect of operational risk and more importantly when it fails. A lot of people forget that there are fundamental cultural differences even between the two main English speaking countries of the United States and the United Kingdom. That has an enormous effect on how a company operates on a global or even a transatlantic basis.

TERRY CUNNINGTON: I think that just goes to what Simon Perry was saying earlier about the need to customise your approach depending on the circumstances you are in, the type of the company, the countries in which you operate and, therefore, the cultures you are operating in. I don't think there are any merits in saying, this is the approach and you should comply. It should be – here are some good principles, elements of best practice, but you have got different circumstances, so you need to tailor it to your own organisation.

SIMON PERRY: At the moment, we are doing a lot of work around emerging markets, and often your rule book or what ever you call the norms go out the window there. Apparently, in China an internal auditor will be much more suspicious of a bank statement than he would be here, because it is not as uncommon as it would be here for your bank official to collude with the company to pretend there is more money in your bank statement than there actually is. You put less, much less trust in that than you would in the United Kingdom, where if you see a bank statement you tend to believe it.

TERRY CUNNINGTON: Two other aspects of culture differences are the level of transparency that people will use or tolerate in different companies, in different organisations and, in particular, in different countries. Transparency to me is absolutely key to good risk management, but if you have one of these countries where that value is not in the culture and people are not going to admit to having any risks, that makes life very, very difficult. The other one is communication, which goes with transparency. You need to have that cross-organisation communication so that the impact of an action on one part of the business is known in the other areas where they are actually affected by it and vice versa.

One of the problems that I have when defining operational risk is that operational risk tends in some organisations to promote silos, where you closely define the risks that you can do. They tend to be pretty well managed on a day to day basis, but if you do something that could affect another silo, that may not come out in the open. The first they know is when they get the effect in another silo. By having ERM where you are encouraging transparency and communication, then those things are known up front. You get a lot of benefit from that sort of approach, rather than just doing it from a bottom up and silo basis.

GEOFF TAYLOR: Unfortunately, traditional companies operate the silos. Forget about risk – they operate in silos

You see more pressure as banks, hedge funds and other financial institutions are trying to get into more high margin activities

CHUCK TEIXEIRA

Just because you have issued a policy and a procedure doesn't mean it is actually happening in the real world
SIMON PERRY

of business units, of geographical areas. They are in competition as to who is selling the most of this or whatever. Because they tend to operate in silos and risks can be hidden within a business unit, there's a tendency to say, look at that business unit. Isn't it doing well or not doing so well? Perhaps we need to re-educate managers with thinking about business in a non-silo way. But then how do you satisfy performance?

MILAN MILOVANOVIC: Where corporations have different divisions, different disciplines and different sectors, the role of a chief risk officer (CRO) on the board comes into play. That is the only way that you drive risk management right from the top downwards, and it becomes a true corporate-driven issue, whereas currently most companies look at it in their own entities, in their own little silos. If you have a global company crossing different industries, that can be dangerous, because at the end of the day the decision makers haven't got the full control, haven't got the knowledge.

SIMON PERRY: Is the only way to do it to create a board level risk role? Another way, perhaps harder, is to enthuse the CEOs, the CFOs, the operations directors, also at the apex of the organisation, to be absolutely zealous about risk as well and challenge reports about risk and what they are doing on risk.

MILAN MILOVANOVIC: But that should be one of the roles of the CRO, being in partnership with the chairman, the CEO and the main board directors. If you have one individual that has got the over-riding responsibility to drive the message of risk management down, with the support and the ownership of the chief executive or chairman, that is a classic and relatively simple way of monitoring and driving risk management through a corporate entity.

CHUCK TEIXEIRA: The really critical thing is defining who has got accountability and responsibility. I can't tell you in the last six months the number of large multinational corporations that I have been into where we started to do a mapping of who has what roles and responsibilities for risk, all aspects of it. It is not just the CROs. Some of it can be an operational risk management team separate from the CRO, internal audit, financial control that can control SOX and financial reporting, a whole variety of departments. When you start mapping it out, there is always overlap, and it is not very clear as to who actually monitors this, who actually takes accountability and who ensures there aren't things that are bubbling under the surface that should be taken care of.

TERRY CUNNINGTON: I think it is important to have a risk management strategy, part of which actually defines responsibilities for risk management at a line management basis, at board level, audit committee, risk committee, risk function, whatever and internal audit. You need to define where the borders of responsibility are, because otherwise you get gaps and duplication. That to me is a very, very important part upfront of having a board approved document that says, this is what we are trying to achieve, these are the responsibilities for it. Going with that, you need a culture of risk management. We all know cultural change takes time, but I think there are two good ways to address that with a people perspective. Firstly, we are in discussion with our HR department about making risk management a core competency with management down the organisation, and we would provide training to support that. The other element is if you incentivise performance to include good risk management, then it is going to happen. It is human nature.

HUGH PRICE: It seems to me, we need to prioritise risk management, and when it comes to silos, you should never have any no go areas where you have someone saying, 'this is our patch, this is how we do it, and we don't want you meddling'. That culture can be very, very dangerous if you let it grow within any business. Do you find these problems in different departments, different offices, different branches?

CHUCK TEIXEIRA: I think it is almost symptomatic of the size of the company. If you look at the FTSE50 or FTSE20 and Fortune 50 companies, those are the ones where almost every division and every business unit in the country has its own infrastructure, so none of it aggregates up to the top clearly, be it responsibility or seeing what is actually happening in all of the divisions, because it just becomes so complex and bureaucratic.

HUGH PRICE: So there is no over-arching management of risk?

CHUCK TEIXEIRA: There are principles at the very top, and there is a collection of some of the information but then it doesn't necessarily really flow all the way up and down. I think that is one of the biggest challenges.

GEOFF TAYLOR: There is a very clear point, depending on what kind of business you have and what geographic spread, where you have built-in entities and different profit centres, like a conglomeration of loose states in a federation, and each has a different approach. This is where you do need a definition of operational risk. How do you aggregate risks up so that the responsible directors at the top really know which risks they have got in which businesses. If you are each running different models of how you see operational risk, that aggregation

process is going to fail.

CHUCK TEIXEIRA: Building that coherent, clear culture is absolutely critical. I am working with one client right now where we did the mapping, and you could see the overlapping where all these different divisions had some risk management responsibility. The second part was they had over 600 risk management policies, and you can imagine the overlap. It has been an effort for my team to go through 600 policies and try to say, ok, what categories do these fit in, do we need all of these, how do we streamline it so that this company, from top to bottom, can have very consistent risk management policies. Then how we put it in place so that everybody has access, and we can build that culture and people know what they are supposed to be doing and deal with the responsibilities.

SIMON PERRY: Paradoxically, sometimes the bit of the business that knows the least about their group policies on risk is the group itself and some of the corporate functions.

MILAN MILOVANOVIC: Isn't there one core division that is solely responsible for driving policy and procedure?

CHUCK TEIXEIRA: In this case, because the business units have so much autonomy, what happens is the situation Simon describes where the group issues policies, and they have quality assurance type groups and operational risk management monitoring type functions, but power or responsibility is still distributed among many different divisions and many different departments. They issue their own separate interpretation of policies. Ideally, it would be all centralised.

SIMON PERRY: One of the greatest management tricks that global corporates could pull off would be if a business could acknowledge that many parts of it might not be in compliance with a policy and not require some sort of internal audit for that to be apparent. When you get into things like foreign corrupt practices laws, it is very easy for a business to say yes, we are fully compliance with this in Nigeria, but do they know that is just not possible or this is the way that business is done there? Transparency has to go side by side with policies. Just because you have issued a policy and a procedure doesn't mean it is actually happening in the real world.

CHUCK TEIXEIRA: A lot of institutions are trying to wrestle with how to monitor what is happening in all these different divisions in these countries on an ongoing basis. There needs to be something that alerts me to the fact that there may be problems bubbling under the surface that I must start investigating right away. Audit can help, certainly

HUGH PRICE: But it can get over bureaucratic.

CHUCK TEIXEIRA: It depends. In a lot of companies' internal audit, the programmes are defined on a rotational basis and set a year in advance. If you start having a problem in Nigeria, for example, and management doesn't tell you, how do you start understanding that there were factors that could have been highlighted to show you that further investigation needed to occur.

TERRY CUNNINGTON: I am talking as an ex-president of the Institute of Internal Auditors, a few years back. If you have a modern approach, then accepted best practice is that the organisation's view of risks should drive the internal audit plan. Internal audit should then give independent assurance or otherwise, and the results of their independent audit then underpins the organisation's view of risk. It is circular.

That is the approach we have adopted in Euronext, and I think it is a very successful one. In some organisations, there tends to be more focus on the financial side, but modern internal audit should be looking at a range similar to risk managers, but they are independent and they can give independent assurance. They shouldn't be doing their own models to define what audits they do; they should use the organisation's view of risk.

GEOFF TAYLOR: It is a risk in itself, that disconnect between risk management and audit, because there is a battle over who is running risk management. There are two discrete areas that should be working together. One is helping the business to define its policy and approach, and the other one is giving the verification about that.

TERRY CUNNINGTON: One is hands on and a management tool to help provide assurance to the board that the risks have been properly identified, analysed and matched, whereas internal audit is an independent function which gives an independent view on whether or not the risks are being properly managed in the areas they cover, and, very importantly, at an overall level is the risk management framework effective in the organisation?

SIMON PERRY: How well do you think internal audit

You should never have any no go areas where you have someone saying, 'this is our patch, this is how we do it, and we don't want you meddling'
HUGH PRICE

I think ultimately risk management is about driving down the deficiencies and increasing efficiencies, as simple as that
MILAN MILOVANOVIC

functions are measuring up to that challenge, linking their work to the risks of the organisation?

TERRY CUNNINGTON: It is getting there, but varies, in my experience as president. There are huge differences in practice and what people call a risk-based approach to internal audit varies from someone having a little risk model on an Excel spreadsheet and deciding how they are going to do audits with that, right to the other end of the spectrum where they have ERM in place, the risk profile of the company is driving their plans and they have a risk-based approach to how they do it.

SIMON PERRY: I see right the way up to the top of the FTSE 100 far too many internal audit departments trying to own risk management, because they see it as an opportunity to expand their role and influence and it is exciting work. Also, far too many of the departments audit to their own skill-set. Having seen that there are organisational risks which are in quite tricky areas, they fall back on auditing to within their own skill-set which tends to be around financial and IT.

CHUCK TEIXEIRA: There are some good examples where internal audit and risk management and operational risk management work hand in hand. With one of my clients, operational risk management produces a dashboard on a monthly basis and they analyse and see where things go from green to amber to red. Operational risk does the first analysis of something that turns red and identifies the issue. Is it a one-off thing or does this indicate that there might be a more systemic problem?

Internal audit has a policy of continuous audit so they have their pre-planned activities that they would normally do, but they also have what they call a 'continuous audit team'. If operational risk identifies something that might be an indication of a more significant problem, then internal audit goes in and investigates. Not only do you have a clear definition of what roles and responsibilities are between the two departments, you have clear definitions and they share the same definitions of what operational risk is. They are working together to contain any problems happening within the organisation.

GEOFF TAYLOR: That is a very good story to hear, because we talk a lot about risk management and why we do it. I think if you can see it as spreading best practice or bringing issues through transparency up and being able to deal with them and use that across the organisation, then you can talk about adding value.

That is probably the next sort of question in my mind. We have talked about operational risk – what is it, what isn't it. We are not going to come to a definitive answer on that. Then how do we add value with it? That is the other challenge. The board of directors don't really want to talk about something that isn't really going to add any value to their organisation.

TERRY CUNNINGTON: Risk management is all about improving the bottom line and in making the business case. Governance and regulation should be part of it, but they should not be the things that drive it, because otherwise you will have totally the wrong attitude by management in your company to what risk management is about.

MILAN MILOVANOVIC: I think ultimately risk management is about driving down the deficiencies and increasing efficiencies, as simple as that.

SIMON PERRY: It would be interesting to see what CEOs of the FTSE 250 said if you canvassed them and asked, is risk management (a) a necessary evil, or (b) there to protect the bottom line?

CHUCK TEIXEIRA: It is also creating a platform for growth. If you are growing actively into the new markets, new products etc. you want to make sure that you are not fighting fires at home. You also want to know that when you are going into these products or into these markets that you have the right infrastructure, the right mindset and the right skills to be able to deal with them effectively.

LEE COPPACK: If something isn't going to make a material impact on the bottom line or on shareholder value, however you define it, should you devote much in the way of resources to it?

TERRY CUNNINGTON: The question is toleration of risk or what your risk appetite is. It might be in this branch office out in the middle of nowhere which only has a £2m turnover that someone says this really important, but in terms of the overall picture in the group, then it is of next to no relevance. You have to gear up your risk management to cover both aspects. At a local level it is important. Often from a group perspective, it would get lost in the rounding. It doesn't mean you don't encourage good practices locally, however small the unit is.

LEE NEEDHAM: If you don't understand the size of the risk to start with, it is very difficult to determine how much resource you need to put in to managing that particular risk. You have to go through the whole identification, assessment and quantification before you can then make the decision whether this is something we are actually concerned about.

TERRY CUNNINGTON: You need a filtering mechanism.

We use the 5 by 5 probability matrix. Wherever you appear on that matrix determines whether you go up to board level, it is dealt with at business unit level or the level below that, or it is just something you live with. We find that a pretty effective way of filtering what risks need to be talked about at what level.

GEOFF TAYLOR: Often there is focus on the economic value added or however you define success in share price, but the broader stakeholders sometimes can influence your business more. Bad publicity may turn consumers away from you. It is hard to put that risk into a matrix somewhere, because you don't really know where that might be. You could say employee productivity when things are going well and you have got nice facilities and everything then, compared to not. I haven't seen those put into risk maps in a way that is very explicit. Partly, perhaps, we are avoiding difficult subjects.

TERRY CUNNINGTON: You are never going to get away from that. In defining our different levels and the impact part of that nature, we have financial amounts, but we also define it in terms of impact on the group objectives, on business objectives, shareholder value and reputational risk. If you can quantify it, great. It goes in that box. If you can't, then here are the equivalent assessments so you can try and compare very unalike risks, subjective and quantifiable risks, in a reasonable manner.

GEOFF TAYLOR: When it starts moving up to the senior managers, they always like to see a number somewhere. That is traditionally how businesses are run, particularly in the United States – quarterly results for everything – so your behaviour is all about driving the numbers to meet the analysts' expectations.

TERRY CUNNINGTON: Which encourages short-term risk.

GEOFF TAYLOR: Absolutely.

MILAN MILOVANOVIC: You are influenced by stakeholders, shareholders or directors, all looking at short term goals, whereas risk management itself is a long term issue and a long term management tool. Productivity levels can only be measured through several life cycles. Generally, management styles these days don't allow you to do that. You are reporting on a quarterly, even a monthly basis in some cases, which doesn't allow you to implement and give good risk management feedback to the board.

HUGH PRICE: Is it possible to give risk management feedback on a monthly basis?

MILAN MILOVANOVIC: No, not really, not to give a clear vision. All you are doing there is basically snapshots, and that it a dangerous way of going about measuring your risk exposure.

HUGH PRICE: It seems to me that the culture of the business is part of the risk. Isn't it?

CHUCK TEIXEIRA: It doesn't always have to be quantification. Let's take HR – what is the environment in terms of the mood, people's happiness and that type of stuff? Another thing could be employee turnover. Each department has a different threshold for turnover.

Departments with lower skilled workers expect a higher turnover rate. Let's say you expect 25% and when it exceeds 30%, you start to get worried. Other areas have very skilled, specialised and highly paid people, and it's an issue when even one walks out of the door.

GEOFF TAYLOR: You can't really report on risk on a monthly basis, but what we can look at is a kind of dashboard or radar screen of things that are changing. Maybe it is market risk where you know there is an event coming, and you can plan for it. There are other things that you can guess might turn up at some point, like a flu pandemic. They can be on the radar screen. Then there are the things that we know will happen at some point. If you are in San Francisco, you know there is going to be an earthquake of a significant magnitude at some point, but you don't need to discuss that every month because hopefully you have planned for it.

You can start to categorise risks in terms of emerging risks, risks that are always there, static but we don't know when they are going to happen, like a natural hazard, and then other risks which we just have to keep to ourselves, things which we might not perceive as a risk now but maybe become one. Building a risk radar screen would be adding value, I think, to that senior level so that we are not rushing up and saying, pandemic flu is coming and everything is terrible. We are just saying there is an issue and we are thinking about it, so that they can focus on driving the business and not worry about who is in charge of this risk.

TERRY CUNNINGTON: This leads me to go back to the point about a CRO. There needs to be someone pretty senior who is a champion for risk management and who co-ordinates risk management across the group. Boards absolutely hate receiving lots of different papers on risk management from different parts of the business, in different formats. They can't see what the overall risk portfolio is. One of the advantages of the ERM approach is having somebody as the champion. It means you pull this information together in a fairly concise way, looking at different types of risk on a portfolio basis, so that the board, or a risk committee

When it starts moving up to the senior managers, they always like to see a number somewhere
GEOFF TAYLOR

My impression is that one of the problems that have happened to many companies is a lack of imagination to see where things are going to blow up
LEE COPPACK

on its behalf, is aware of what is happening.

MILAN MILOVANOVIC: The champion must have the ability to make decisions and implement, not just to influence.

TERRY CUNNINGTON: Yes, but you have got to take account of the concept of risk ownership, because with the vast majority of risk, it is line management that manages the risk. You can provide all the assistance and whatever is necessary, but that is where the decisions have got to be made, be it board level or down at the core.

MILAN MILOVANOVIC: But that is the question of leadership.

HUGH PRICE: Isn't it also a question of authority? If the risk manager or whoever it might be doesn't have that authority at board level, it isn't going to work.

TERRY CUNNINGTON: It may work but it makes it more difficult. You do need the authority.

CHUCK TEIXEIRA: How do you make the business case for risk being essential to growth?

GEOFF TAYLOR: The only way to do that is by changing the risk definition and most risk definitions focus on the downside of risk. If we start to focus more on upside risk, and say, I am here to maximise sales in the country because I am going to look at all sorts of different levers that you can pull to make the decisions, then you are getting onto the turf of the business manager. They will say, hey, I am already pulling those levers about making more sales. How do we make the case that we can assist in that process?

TERRY CUNNINGTON: Opportunity risk is another word for upside risk. Selling – you can add value by looking at the individual opportunity, working with the people who are doing the project and helping them to identify, analyse and manage the risks to increase the likelihood of success. You can also do it within the context of your overall risk portfolio. If you can do it better than the competition, you have more chance than they have of succeeding. As a result, a lot of my team's time is spent working with the business on projects, business change, activities, opportunities, product launches, doing exactly that.

GEOFF TAYLOR: Lee, from the banking sector, do they see operational risk as an opportunity?

LEE NEEDHAM; I think they do. The problem with the regulations is that they only really concentrate on the downside. If your motivation as a bank is to deal with regulatory requirements, then you are going to concentrate entirely on the downside.

CHUCK TEIXEIRA: Part of the challenge for European banks, is that at the moment they are trying just to get through Sarbanes-Oxley and Basel II limitations. That's all they can see. If we look at the US companies who have already had to implement them and are now into years two and three, they are able to take a step back and say, I built all these huge infrastructures and what am I getting out of it? What is my strategy? What is the vision I have to take forward over the next three years and how do I get some value out of it?

GEOFF TAYLOR: My personal view is that SOX is a colossal waste of money. We have ticked a lot of boxes, we have viewed a lot of weaknesses, we have employed a lot of consultants and have we materially changed our risk profile? I don't think so. Have we significantly reduced the potential for a fraud? Not necessarily. That is the negative view, but there is a positive side that says, yes, perhaps we could take it as an opportunity to make sure we have got best practices across the company, but it is an expensive way of doing so. We could have done it without SOX.

LEE NEEDHAM: Is there an incentive without it though? The discipline that regulation encourages, is it not in itself a good thing? It does encourage organisations to look much more carefully at their risks and to understand them properly.

CHUCK TEIXEIRA: Would you have done this if it wasn't for Sarbanes-Oxley? Could we have done it in a cheaper way? Absolutely, but would you have done it if it wasn't in place? Then, what has it actually brought you in terms of the transparency and accountability? Sarbanes-Oxley attestations are cascaded through every organisation, so people actually have to sign off that they knew what controls were in place, that they were operated and there was nothing in their area except for this and having to caveat it. The moment they have to put their name and sign these things, all of a sudden it creates this whole change in their attitude. People are much more careful.

HUGH PRICE: The judge who dealt with the Enron case made the point that over-regulation can be damaging to business, because it makes businesses overly risk averse. I thought it was very interesting. He got right to the entrails of the Enron collapse and knew exactly what happened, and he said you can over-regulate and that can stifle businesses, because business is all about taking risk.

SIMON PERRY: If one looks at market research on risk events leading to the destruction of shareholder value,

financial risk is one of the smallest categories, together with catastrophe risk, although that has probably gone up in the light of Hurricane Katrina. It is not even financial risk in Sarbanes; it is financial reporting risk. It doesn't actually mind if none of your debtors pay you at all. As long as you report that correctly, that's fine. That's a good control.

I think a finance director of one of my clients put it best, and he is obsessed with strategic risk and what could ultimately destroy the value of his company. He described SOX as a sledgehammer to crack the wrong nut, the right nut being strategic risk, and I agree with that. Having said that, I think there has been value in Sarbanes-Oxley, not at the price, but it has been quite eye-opening for people with a background in internal controls to see just what levels of non-compliance with controls were out there. There are a lot of lessons for corporates that haven't been through SOX to try and get a handle in some more cost effective way.

GEOFF TAYLOR: One of the things that worries me with driving risk management into regulation, into standardisation, is that where then does the risk premium come when you are investing? Surely, as the investor, it is about taking risk. Should there not be some element of mystery about risk in order to say, this company is producing higher returns and this one is lower returns in the same industry and why is that?

CHUCK TEIXEIRA: There is a difference between my risk appetite and the risk strategy of a company versus my risk management activities to make sure that I am in line with that risk appetite and risk strategy. Even within financial institutions, there are some who have a much higher risk appetite, who are willing to be aggressive. What you want to ensure is that they have the infrastructure in place to make sure they are not doing things that out of line with what they set out to do. As an investor, you don't want to find out that you think you have a good corporate that has been there for 150 years which is typically conservative, when in fact they have gone out and done crazy types of investment and created structures that you had no awareness of and that do not match with the risk appetite and risk profile that you thought that company had.

HUGH PRICE: Recently, we had the very unpleasant situation of what is loosely described as the Nat West Three, the guys who have been extradited to the United States. More recently, the guy who is running some sort of gambling on the internet has been arrested, and I think he still is in America. Two days ago, I was reading that the plan in America is to outlaw the use of credit cards for gambling on the internet. Is it conceivable that if Barclaycard permitted the use of credit cards for on-line gambling in America, that your company director could be arrested on holiday in Florida?

LEE NEEDHAM: I think the regulation being framed that I have read about in the paper in the last few days is along those lines. Yes, the banks themselves could be culpable if they take orders from cardholders for online gaming in territories where they know it is not a permitted activity.

HUGH PRICE: How do you police that?

TERRY CUNNINGTON: That is a prime example of one-off risks of a strategic nature that come along and bite you. There are others – changes in the political make-up

of some of the countries you are operating in. It puts the emphasis on looking forward, looking at what could come up and hit you, and how likely it is. Then are you being proactive in the way that you assess how you would manage the impact it has and how to put yourself in the position to either reduce the likelihood or get some opportunities out of it? That is probably not in the definition of what people call operational risk. It certainly is within the definition of ERM.

SIMON PERRY: I know a US based technology company, a household name, huge, and they go through an interesting exercise as a board about every six months. They construct their doomsday list, which is the 10 risks that they would least like to happen, just terrible things, and think outside the box but look very much at their market. Over the last five years since they have been doing this, three of them have actually occurred.

LEE COPPACK: When people are talking about a doomsday scenario, do they take in outside thoughts from consumer organisations, from journalists or from non-government organisations? My impression is that one of the problems that has happened to many companies is a lack of imagination to see where things are going to blow up.

SIMON PERRY: I think they rely on the people in that boardroom to have links with those sorts of organisations or people to speak up. But I think you are right. A lot of organisations could do a better job about identifying those sorts of scenarios.

GEOFF TAYLOR: I think the rise of corporate responsibility to very senior levels is partly because they employ people who know Greenpeace, who know the Red Cross, the International Labour Organisation or whatever it is, so they can come to the board meeting and tell them about what these people are thinking.

CHUCK TEIXEIRA: And it does differ by industry as well. If I look at insurance or even banking, where it's a requirement to model catastrophic disaster scenarios and

The banks themselves could be culpable if they take orders from cardholders for online gaming in territories where they know it is not a permitted activity
LEE NEEDHAM

what the probability is, a lot of that information comes from different forms of research. You just have to go to analysts on a trading floor and they can tell you a whole bunch of different disaster scenarios and probabilities as to what can happen.

In my experience of talking to financial institutions, not a single one has told me, absolutely everything is under control, Everybody recognises, more so with internal than external fraud, that if there is collusion, it is very difficult to catch and address no matter what controls and monitoring you have in place.

GEOFF TAYLOR: Perhaps we have eradicated the single operator being able to do so much damage on their own, but if someone in treasury is setting up the orders and the other one is approving them or running the IT system and can circumvent the passwords, then it doesn't matter what systems you have got in place, you're in trouble. A single operator can't do so much damage depending on what level the person is.

CHUCK TEIXEIRA: You still have situations. The situation is that with a trader at their desk, you can tape their phone calls, you can see what orders they have put in, but if they just put that ticket in their drawer, there is no way that you really have to detect that activity.

GEOFF TAYLOR: I think I read somewhere as well that all the most profitable trades usually fall outside the risk management policy of the bank!

TERRY CUNNINGTON: One of the key things – and this applied to Barings as well – is not just having controls, but having somebody on the board who understands what is happening. In that particular case, they had a board who hadn't got a clue about derivatives and what was going on. The money was coming in, so great.

GEOFF TAYLOR: Someone once told me that traders lose almost as much as they make over a time, and if somebody is consistently getting better returns, that is an alarm bell to go and investigate.

TERRY CUNNINGTON: Only if you understand it. You can draw a parallel with IT. A little while ago on boards there was nobody that understood what IT was about. You got IT people coming along and saying, we could have a tremendous disaster. We must invest £x million in this system otherwise we've got big problems. Nobody on the board was qualified to question it, therefore, they said, oh, that sounds difficult. Yes, have the money and go off and do it.

GEOFF TAYLOR: That's why we have chief information officers.

MILAN MILOVANOVIC: Perhaps non-executive directors who come from certain disciplines can add value to the board in those sorts of scenarios.

TERRY CUNNINGTON: Yes. Following what it said in the Higgs Report, there is too much emphasis on ex-executive directors becoming non-executive directors in other companies. They have boardroom experience but they are not necessarily bringing anything to the party. You need accountants, you need lawyers, in some cases, you need people who understand the industry and you need people who understand IT. That's the sort of person you need to bring the necessary skills to the board.

CHUCK TEIXEIRA: When it comes to creativity and people thinking outside of the box in terms of what is risk management and what are the possible risks, it is not just financial services. I was looking at a healthcare company, and I found out because they sell supplies for operations, some of the reps actually participate in the surgeries on occasion. I just couldn't imagine that. The same thing as a trader – how do you deal with things where there are no means of having a control within your own company, because only this guy as a representative of the company is there. There is no means to observe him. How do you address these types of risk?

SIMON PERRY: Whistle blowing is a response, together with others, including training and strong disciplinary procedures.

CHUCK TEIXEIRA: Especially in a sales environment, there is so much pressure. There are such high targets to sell, sell, sell and by whatever means necessary.

GEOFF TAYLOR: We talk about corporate culture and whistle blowing, but I don't think corporate culture thinks that behaviour is acceptable. For companies that have whistleblower lines – how many calls do they actually get?

CHUCK TEIXEIRA: Some.

TERRY CUNNINGTON: When you have cases like that lady at the European Commission that was blowing the whistle, what happened to her? There are other examples around of whistle blowing, and they end up with no job so, it is very difficult for that to work.

CHUCK TEIXEIRA: Yes, but if you look at the big frauds and how they have been caught, a lot of them have been through whistleblowing. In one case, it was a note slipped under the door, an anonymous note saying, go look at this mysterious room. Sure enough, that was where all the real files were. That happens time and time again.

GEOFF TAYLOR: The difference with risk management is that it is not about whistle blowing. It is about helping the business to understand why some of things they are doing may not be in the best interest of the organisation. Our job is not to be police but to help them to understand, you're doing it this way and that may not be the best way of doing it, either because you will be out of compliance or because it is not acceptable culturally. In my experience, people are more prepared to break health and safety rules than financial rules. I wonder why?

LEE COPPACK: Geoff, as chairman would you like to sum up?

GEOFF TAYLOR: We have heard a lot of things. We have danced around the subject of operational risk, the broader risk picture, and we started out with a definition. Does it really matter what the definition is? Possibly not, unless you are a regulated industry. If you're not, then you can do whatever you like as long as you are consistent in your organisation. Terry Cunnington's point, which was an excellent one, is that if you use ERM you don't need to worry about the definition of operational or other risks. You can just build whatever risk picture works for your organisation, and think about all of the risks, including strategic ones. I think those are the things that I will carry out from this discussion.

There is too much emphasis on ex-executive directors becoming non-executive directors
Terry Cunnington

DEADLINE FOR ENTRIES
12 JANUARY 2007
JUDGING DAYS
8 FEBRUARY & 15 FEBRUARY 2007
AWARD PRESENTATIONS
WEDNESDAY 18 APRIL 2007, THE BREWERY, LONDON

CALL FOR ENTRIES

2007 EUROPEAN Strategic RISK RISK MANAGEMENT AWARDS

IN SEARCH OF RISK MANAGEMENT EXCELLENCE

HUGH JAMES · Endurance · ZURICH · ROYAL & SUNALLIANCE · Garwyn GROUP

Full details and an entry form are enclosed with your October issue of Strategic RISK
For further entry forms or details on how to enter
call Nas Smith on +44 (0)20 7618 3418
or visit www.strategicrisk.co.uk/awards