StrategicRISK

Nov 05

ROUNDTABLE 2005

CORPORATE GOVERNANCE

Sponsored by:

AON

ifs institute of financial services
School of Finance


ifs institute of financial services
School of Finance
Natural Selection
Focus your career in
Risk and Insurance Management
◆ Professional Diploma in Financial Services Management (Professional DFSM®)
◆ Applied Diploma in Financial Services Management (Applied DFSM®)
◆ Advanced Diploma in Risk and Insurance Management (AdvDipRIM)
◆ BSc (Hons) in Financial Services and Associateship (Risk and Insurance Management)
For more information please call the ifs on 01227 818609
www.ifslearning.com
The ifs is the official brand of The Chartered Institute of Bankers, a registered charity.

Corporate Governance

An introduction to the StrategicRISK roundtable discussion by **Sue Copeman**

In the last 10 years we have seen a plethora of corporate governance regulations and legislation, both nationally and globally. The growing focus on risk controls and reporting may be increasing the importance of the risk manager's role, but it also poses some challenges. For example, just how easy is it to turn risk into opportunity when the risk is a particularly prescriptive piece of legislation like the Sarbanes-Oxley Act (SOX)? And should such a law even concern risk managers, as it mainly revolves around the area of accurate financial reporting?

Our roundtable participants were divided on the subject of SOX. Some felt that the procedures necessary for compliance could provide a risk management spin off, for example in granting risk managers easier access to, and the ability to ask searching questions of, some areas of senior management. Others did not consider SOX particularly relevant for risk managers. There was, however, a general feeling that the UK non-prescriptive approach to corporate governance offered more potential for gaining a competitive edge.

The discussion also highlighted the sensitive relationship between risk management and internal audit. While a collaborative partnership is clearly the ideal, it was acknowledged that some rivalries do exist and could act to the detriment of those areas where both functions overlap.

Prescriptive legislation like SOX is rarely welcomed by companies. However, most participants agreed that regulation generally has been one of the key drivers for corporate governance.

Sue Copeman
Editor

Roundtable participants

Paul Hopkin, director of risk management, Rank Group, chaired the discussion

Mark Butterworth, chief operating officer, Liberty Syndicate Management

Cary Depel, compliance and legal director, IFX Markets

Patrick Devine, partner, Reynolds Porter Chamberlain, solicitors

Marc DonFrancesco, consultant, Institute of Financial Services

Corey Gooch, associate director enterprise risk management, Aon

Sheryl Lawrence, risk director, Barclaycard

Mick Michael, Sarbanes-Oxley project team, National Grid

Corporate Governance

How do all these developments actually affect our activities as risk managers?

Paul Hopkin

PAUL HOPKIN: We have a range of expertise and experience round the table so I look forward to a lively and informative discussion. Just to set the context, national and international corporate governance regulations are increasing disclosure requirements for companies and, in some cases, the personal accountability of directors. For example, the UK Government now requires directors of quoted companies to prepare an operating and financial review, and that OFR must include a description of the principal risks and uncertainties facing the business. And non-US companies with listings in the US – and the Rank Group is such a company – will soon need to comply with the Sarbanes-Oxley Act.

Before we begin, I would like to briefly give you a little more background. I recently looked at the information I have on the OFR, and perhaps it is worth reflecting on it in some detail. In the paper on guidance on the OFR and changes to the directors' report, the OFR schedule specifies matters that need to be included. It says that directors are required to provide a balanced and comprehensive analysis, consistent with the size and complexity of the business, of the company's development and performance during the financial year, the company's (or group's) position at the end of the year, and the main trends and factors underlying the development, performance and position of the company (or group), and which ones are likely to affect it in the future.

So the OFR is forward-looking, and that is perhaps the key development that has come out of it. As far as the Sarbanes-Oxley Act is concerned, we are familiar with it – indeed some of us are probably more familiar with it than we might want to be. On the broader corporate governance issue, I see that the London Stock Exchange printed a booklet on corporate governance during the course of last year, which was a very useful summary. It talks about the responsibilities of boards, including the membership, the accountability of boards, delegation of authority, remuneration of board members – in other words the inputs into the board – and then the outputs from the board in terms of strategy, corporate social responsibility, risk, audit and disclosure. It is a good publication, I would recommend it, and it is available free from the LSE's website.

Having made these comments by way of background and context, perhaps we should look at the first of the discussion points – key issues for risk managers. How do all these developments actually affect our businesses and our activities as risk managers? Why are they relevant?

COREY GOOCH: I think they provide opportunities for risk managers to become more involved in managing much of the material risk outside their traditional function. They provide an opportunity to establish relationships with other people in the business. To be effective at implementing enterprise risk management (ERM) in corporate governance within a business, you have to build and develop those relationships over time. Cross functional representation is a key part of that. This also helps to enhance your role as a value protector and a value creator also. We talked about this at the recent IRM forum.

MICK MICHAEL: We see a lot of debate in precisely that area. I think is an area for risk managers to excel in, because there is so much discussion going on about the cost benefits of the increasing corporate governance. Whatever it is that you do, you always have to come back to those two points. Certainly, with Sarbanes-Oxley we are seeing lots of companies, initially because of what appeared to be coming out as the drivers in America, diving into the detail and just as a matter of course then spending a lot of money. What appears to be happening now is that people are beginning to step back from that and adopt a more risk based approach. We are now seeing a lot more pragmatism being applied. This is enabling us all to hone down the scope of the work we are looking at, and perhaps focus on more of the entity controls and the umbrella controls in an organisation to help in that. For me, one of the issues is making sure you get the balance right between risk, reward, cost and benefit.

SHERYL LAWRENCE: I see it as part of what I would call topping and tailing. In terms of topping, it is creating the environment within which effective risk management happens and in terms of tailing, it creates positive feedback, so that you can have the learning circle completed. I think previously we had risk managers who could be ignored or who did not have any real importance attached to them. In the current environment, risk management has now become a key control mechanism among a series of controls, which together give you effective governance.

PAUL HOPKIN: That is interesting. Perhaps in a Sarbanes-Oxley context, it is accepted that it is the results, the certification that comes out of the organisation, that are important. When you talk about the feedback loop, your comments suggest that it is somewhat more internal

MARC DONFRANCESCO: There is probably still some more work to be done. People see risk management and Sarbanes-Oxley as a box ticking exercise. Really you have to have a systematic approach throughout the organisation. It is not just about the risk manager, it is not

just about the FD – everyone has got a part to play.

PAUL HOPKIN: The point about the box ticking exercise is well made; we surely all want to avoid that.

MARK BUTTERWORTH: The key issue now for risk managers is that over the last decade there has been a growing awareness within the board about risk management practices. It used to be rather a cloudy issue, kind of belonging to that guy in the corner – the specialist they had. But now it is such an important part of the delivery of corporate governance – how are we going to deliver it? Around the boardroom table they are now asking, "Are we good at corporate governance? What makes us better at corporate governance than XYZ company?" And that is the contribution that risk management makes, by saying whether it is really effective, well-regarded and well-respected, embedded and communicated across the whole of the company – all those sorts of things. So the key point for risk managers is that they are now well placed. It is now the time to deliver on the promises that have been around for the last decade. Directors have got some of the issues of governance at the top of the agenda, and they are looking to the corporate players around them to deliver and make life easier for them.

CARY DEPEL: Following on from what Mark was saying, I think it is a brilliant opportunity for the risk management profession. We have seen it over the last 10 years. Occasionally you will find an organisation has appointed a chief risk officer (CRO), which is a board level position. People are much better placed to make that next step up to board level and be both the technical person and the effective communicator and integrator of the strategy and vision of the company.

MARC DONFRANCESCO: Rising to the top table, so to speak, you have got to take everyone up with you. That needs communication and also a degree of education as well. The really good guys that operate on that level will be the people that can actually impart that message throughout the organisation and have it as part of their culture. That will separate the great from the good risk managers.

COREY GOOCH: Communication is a huge part of making this process effective. You have to have it. If you are going to get buy-in and get people in the business to help implement the process for good corporate governance, you must be able to communicate in an efficient time line. You have to do the process and build the buy-in to implement it in the background. The communication aspect is critical. You also have the board members and, to a degree the senior management, who are the channel to the external investors, and they have to be able to communicate the plan and the strategy effectively too.

SHERYL LAWRENCE: I think it is also worth highlighting the integrator role or the integrator aspect of the role. It is not that the risk manager does everything; it is that the risk manager must be the focal point through which all of the other disciplines are integrated. Otherwise you may have different bursts of activity all running in parallel. The danger of Sarbanes-Oxley is that it is seen as a financial reporting risk screen that is going to drive our legal compliance, HR, health and safety, and everything else. The important thing for the risk manager now is to really bring all these together so that we can see what the aggregate picture looks like and be able to see how one aspect overlies another.

PATRICK DEVINE: It is interesting for me to see how the role of the risk manager has developed over the last 10 or 15 years. Some 15 or so years ago, risk managers were largely responsible for insurance buying within their organisation. Risk was something that was insured and nothing else really. There was not this broad scope that we are now familiar with because of developments over the past decade and which has been gathering in pace. It is quite interesting to me to see how quickly it has become a main board issue. And the point you make about integration is actually critical, because risk is a common factor throughout every operating system in any organisation. It is the one word that everyone actually now understands. In a sense, the risk manager is almost acting as the chief information officer. I think a lot of information comes to a very good risk manager in a very good risk management environment that a lot of other people do not see.

MARK BUTTERWORTH: Can I just add a footnote about the changing issues? I think that risk managers in the last 10–15 years have had to do a certain amount of self-promotion. They have had to communicate; they have had to gain the attention of the board or the senior people.

But now, as corporate governance is developing through things like the role of non-executive directors, audit committees and so on, non-executive directors are becoming much more powerful, influential, well-informed people. So if they are directors in company A and they see very good risk management, they will look for it and demand it in other companies too. If there is no chief risk officer or the equivalent on the board of the company where they are a non-executive director, they will ask, "what are we doing about risk management? Who is our head of risk?" You can expect some demand, and it is going to be high level demand. I heard the expression this week, step up to that demand. So there are going to be some issues for risk managers. It is a good thing, I am promoting it. This is all to do with the opportunity we have been talking about. We have an excellent opening for risk management.

You must be able to communicate in an efficient time line.

Corey Gooch

The big area of risk is strategy formulation

Paul Hopkin

PAUL HOPKIN: Everyone round the table has made the point that risk management is a much higher profile issue than ever before. Two somewhat provocative questions come to mind. Has risk management as we understood it 10 or 15 years ago, and our ability to push it forward, passed by a generation of risk managers? And while risk management is the high profile issue of the board, what has it done for the risk manager? Is the risk manager actually called to the board table? Risk is shown by the London Stock Exchange as a box, you must 'do' risk. But in the areas the LSE talks about – strategy, corporate social responsibility, risk, audit and disclosure – surely the biggest risk is getting your strategy wrong. Does risk management belong alongside strategy? Does the risk manager get into strategic decision-making?

MARK BUTTERWORTH: I think the point about missing a generation is really important. A lot of risk management development and promotion has come from what you might call the event risk people. Whether they are involved in insurance buying or on the audit side, if something goes wrong they are preventing or dealing with it.

One of the other things that has developed in the last 10 or 15 years is risk management education. Ten years ago there was probably only one university in the UK offering risk management education. Now there are MSCs, BA degrees, MBAs in insurance, risk governance, etc; there is a whole cadre of people coming into industry and commerce who have not seen any pigeon-holing of risk management, and in one particular moment or another, they will talk about strategic risk management, corporate risk management and corporate governance. So this idea about having missed a generation, I think you have really put your finger on it, Paul

PAUL HOPKIN: I will ask the question again just to reinforce the point. Has the risk management initiative by-passed risk managers?

COREY GOOCH: I am one of those insurance geeks if you will. I have a degree in risk management and insurance and also in finance from an American university. That kind of ties in with another one of our points about tying risk management into audit. There is a big danger. Maybe it is not in terms of the risk management initiative passing risk managers by, but I do feel that risk managers needs to be more proactive in getting themselves a seat at the table. If you look at Sarbanes-Oxley, specifically in the US, it really flows into the audit committee. The director of internal audit usually does the reporting. So in certain companies the risk manager is being forced ever more into the box of being told to document the rest, deal with the insurance, tell audit the results, and they will test them and report to the board. In certain instances they are getting pushed out. Risk managers need to be more proactive and try to get into that. There is also a lot of complicity now. When you are dealing with the insurance markets, the D&O carriers and things like that, you do need to be well aware of what is going on, because if you are trying to sell your business to the markets you do have to play a role in that.

PAUL HOPKIN: Perhaps the harsh analysis of what you have just said is that the risk management initiative has passed risk managers by.

SHERYL LAWRENCE: I want to add something to that. There is an interesting dynamic within our business where I think the risk manager did become more prominent, but, as we move into an environment where risk is embedded and there are new business areas that are accountable for managing their own risk, then they bring their risks to the table. It is not the risk manager any longer that brings the risk to the table, business executives are bringing their own risks to the table. The risk management role then in fact becomes almost a first layer pre-audit of challenge in terms of oversight. Do you have a risk manager at the board table, or is everyone around the board table a risk manager who carries out other functions as well? I think that is where we are beginning to move to within our business.

MICK MICHAEL: I support that view. Risk managers as individuals have matured because of what they have had to go through. If you go back over the years, probably before Turnbull, but maybe as a result of Turnbull, there was a lot of emphasis on putting a process in place. Initially when risk managers came in, their job at that time was very much to focus on what the process was, and that process led to reporting up to the board. What we are now seeing is a change, almost like a morphing away from that role, towards one where the approach is more, 'yes, the process tends to work well, we now need to focus much more on the environment within which that process operates.' When you look at it in this way, you come back to the risk manager being an integrator, a facilitator, and actually having a far broader role involving a whole host of different things which in many cases are very soft in nature. Many of us are at this point now in terms of being able to have an opportunity to influence decisions and strategies, which would not have happened in the past.

PAUL HOPKIN: Control and environment are the first component of COSO, and increasingly it is becoming an area that companies realise they have neglected. The question asked at audit committee is what is the control environment in this department or this area? It is an easy question to ask, you need a structure to answer it.

CARY DEPEL: My experience, both direct and indirect, supports a lot of what Sheryl and Mick have said. In my view it is the holy grail of risk management if everybody in the business manages the risks in the first instance. That is to say they identify them, attempt to measure them, apply risk control techniques and have some

influence in how residual risk exposures are dealt with. All the people that I have worked for in the last five years have felt acutely that they are risk managers.

SHERYL LAWRENCE: If you ask us all what is the risk process I think we would all do quite well, but when it comes to the control environment, what is it? How do you measure it? What does it contain? And for us certainly, what has been really helpful over the last 12 or 18 months, is to be quite clear as to what we mean by it. It is quite challenging because it makes it much more of a conscious activity than many would prefer to have; they would rather it just remained nebulous.

PAUL HOPKIN: This is one of the dilemmas I am interested in and that we are starting to explore. You can talk about risk management in the way we all do, but the big area of risk is strategy formulation. We as risk managers, I suspect, do not get behind closed doors with the CEO and CFO as they talk about what they are going to do, and say to them, 'don't forget about risk.'

PATRICK DEVINE: We started by talking about what has happened over the last 10 or 15 years, which is a valuable thing to do. As I see it, speaking as a lawyer, part of the way that the role has developed is that there are certain industries where risk management is more important and other industries where it is less important.You can make a brutal distinction if you will. Those in which it is perceived as being more important and where it has a greater resonance at board level are the regulating industries – banking, investment and insurance – where you have now got the Financial Services and Markets Act. There is no debate: this is a risk management system, this is a corporate governance system, etc. And you have personal liability at board level and approved person level. You have got to have systems and controls in place.

You would expect the result in Liberty Syndicates, which is an international insurance company, to be that everyone around the board table understands risk. That is how they got to be in that industry. It is easier in some respects where you have a legal imperative and where everyone understands what a risk means, because that is what they do for a living: they take other people's risk. So you can see that in certain industries risk management assumes a greater profile compared, say, to a small or medium sized manufacturer or service provider, where it assumes a lower responsibility. So we have seen over the last 10 or 15 years that some industries have perforce been pushed into it more quickly than others. Others might be acting under a code, Turnbull or whatever it might be, where you can comply or explain, which is taking a somewhat à la carte attitude towards corporate governance. There are some quite famous remarks made in annual reports by certain people who are not very keen on some of these codes, so it is going to be patchy, whatever happens.

CARY DEPEL: Logically I would agree with everything you said but historically and practically speaking I haven't seen the insurance industry be very intelligent in their risk taking!

MARK BUTTERWORTH: I agree with the concept that regulated industries seem to be a little bit ahead of the field. But I think you can also look at many inherently risky businesses – licensed businesses, or those required to demonstrate a positive and effective good track record and success in delivering things in order to secure future funding. If you take, for example, a large international construction company building big bridges in Hong Kong, you have to deliver them safely and on time. And they do do good risk analysis for good commercial reasons. So the welcoming of risk management into the board room can be driven by a number of things. I am coming back to the point that the door is now open for a time; how are risk managers actually going to make the most of the opportunity?

It was recently asked whether a functional manager, whether involved in production, procurement, marketing or whatever, should be given responsibility for risk management at board level. I think that would be a mistake. The seat is there and is valid for a risk officer, a risk director, around any company table. He or she then has to deliver the role alongside the finance director, the marketing director and those other professionals. Following on from another point that was made, you may have a marketing director, for example, but if I was the

Historically and practically speaking I have not seen the insurance industry be very intelligent in their risk taking

Cary Depel

It is a growing pain for the corporate culture

Patrick Devine

risk manager in that company I would feel I had something to contribute to his role. I would always want to be promoting my company. The same applies with the finance director; I would always want to understand what we were doing in terms of our financial management and to support what he was doing. Therefore the others around the table should be educated, and I think do now see it as their role, in assisting with the technical risk management and governance functions that the specialist brings to the table.

PAUL HOPKIN: To what extent do we see internal audit as rivals in this beauty parade, or are we all singing from the same hymn sheet? We as risk managers will often look at the identification of controls and what we're going to do about it as somehow the end of the process, but that is where audit interfaces. Internal audit will ask what are the controls and then go out and test those controls and get to certification through that sort of process. To what extent do we work with them? Do we see them as rivals? Do we each understand what the other one is talking about in terminology and language?

MICK MICHAEL: I do not see it at all as rivalry but as a relationship, a partnership. There is so much benefit that can be gained from audit picking up on the good work that risk management does, which then goes on and helps them in their planning. I see risk managers having to work with as many different people as possible and one of the key partnerships is with audit.

MARC DONFRANCESCO: There is a disconnect though, isn't there? You mention words like 'internal audit' or 'compliance' back in the office, and you can hear the collective groan around the department. Everything should be geared up and this relates directly to Sarbanes-Oxley. This should be about business improvement, about improving efficiency and effectiveness as much as just surviving and complying with the right regulations. There is a real disconnect I think between compliance, the way internal audit is run and the way business is run. By having lots of different functions all doing their own thing, you do maintain objectivity, but maybe they are missing a trick, maybe there is more they could contribute to the business up front, which I think is the point you were making, Paul. They come in at the end and may say that you have done something in the wrong manner, ask you to sort these things out and then leave you alone to do this. It might be helpful to have had this conversation earlier. Your assets are your people, your reputation and the knowledge management side of things. And you can destroy reputation very easily. I think there is more that can be done up front.

COREY GOOCH: I agree that internal audit has to be brought in from the beginning, because when you are setting the strategy everybody needs to know all the different parts of the strategy. The risk management and risk control side of the process have to work together. You have to avoid conflict of interest. I am sure some of you have seen that when the COSO ERM framework came out last year, the Institute of Internal Auditors published their White Paper on the same day. It talks about what roles that they can, cannot and could play with some oversight in the ERM process. They are an integral part of the process, but internal audit should not set the strategy to avoid conflict of interest and I am concerned that to a degree that is where it could very well be going. A Conference Board report which came out recently talks about how ERM is seen increasingly as important in responsibility, and that responsibility goes in order of the board, the CEO, the CFO and then internal audit. It does not say risk manager, it says internal audit, and that is a concern. In theory it should play out as a partnership; we should all work together to try and make it better for the organisation, but I think there is some rivalry. I was at an internal audit conference a couple of weeks ago in San Francisco, and they think they should be leading us.

SHERYL LAWRENCE: Certainly I think the roles are complementary. There is an assurance requirement within a risk manager's role. If somebody has put in some litigation which is not worth the paper it is written on, you need to know that now, not when an audit comes along some time later. So I think it is important to have some assurance. Equally it is important within the risk management framework that processes are tested by audit for their effectiveness and efficiency. So certainly I think the risk manager's role is there to ensure that ERM is effectively implemented, and that is cradle to grave, but internal audit is another line of defence.

PATRICK DEVINE: I would like to go back to the original point about whether the risk management profession has missed an opportunity in the past couple of years. I think this is now the modern era of risk management. We have not seen this level of importance before.

Internally, within organisations, the codes of governance that we have seen are quite up to speed with this modern era where you can have internal audit with the traditional checking function. But there is now a different checking function which will become the traditional checking function. I do not think we have quite got the corporate culture yet where internal audit actually sees itself necessarily as a partner or supporting the risk management process, although that is the ideal. So you are getting a clash of cultures. It is not just that this legislation is very painful or these rules are very painful, it is actually a growing pain for the corporate culture as well. It is not just the individual risk manager; it is how we interrelate with the other groups because they are all quite territorial.

SHERYL LAWRENCE: I think also the audit function is a little bit more mature in terms of its processes and therefore it has moved into the space that should have been there for risk management, so risk management has a job to do, to get them out of that space and into the space that they should occupy. They have been moving into risk-based auditing now for at least eight to ten years. They have their risk profiles, they do their risk assessments and that drives their audit programme. Well you might say are we speaking a common language? Is there a common assessment of risk? They have got their assessment of risk and they are now arguing that actually it needs to be objective, it needs to be independent. We have got to get them out of that space and into the right space they need to be in, and that will be a journey and that might take a tug of war.

PAUL HOPKIN: That's fighting talk!

CARY DEPEL: Looking at the difference between internal audit and risk management, I would view internal audit as a function which I would not want to have involved in the strategy formulation of the business, or for that matter in the day-to-day operations of the business. I would see that more as the role of the risk management function. Internal audit, in my view, ought to be independent and should come in, look at the strategy, look at the tactical or operating plans, look at the risk management plans and ask 'Are there controls in place? Do they make sense? Are they intelligent? Are they being used? Are they robust? Is information coming out that is useful and used? That is maybe what you are saying, Sheryl. If they think they should be into the operational parts of the business... well, there is a strong argument that they should not and they probably ought to be pulled away from that.

PAUL HOPKIN: To some extent if I take your argument to the extreme, you are seeing internal audit not as partners with risk managers but as a distinct and different function that checks afterwards.

CARY DEPEL: Well, yes. The follow on to this was acutely made aware to us during our last FSA risk assessment visit. We are a small company of about 104 employees, but we are a plc, and they were very keen to ask us why, although we have a person at board level responsible for internal audit, there is no real internal audit committee or internal audit function within the business. Our response to them was that we were a small business. We really cannot afford to have that much, and what we try to do is hire the right kind of people with the right kind of multi-disciplinary approach, so that in fact, to the extent that you believe people have integrity and intelligence, they can actually do what the risk management and internal audit do in one fell swoop.

PAUL HOPKIN: Certainly within my own organisation we have an audit committee which comprises non-executive directors only. There is also a group management risk committee which is an executive committee.

MARK BUTTERWORTH: Essentially it is the ambition that the non-execs come to the audit committee. The audit committee end of spectrum would be financial audit, we have the relationship with the external and statutory audit; it is the control measuring, time-kicking environment. The other end of the risk management is looking towards efficient operations: training of people, giving them freedom to work within certain constraints, and so on. It is a bit more flexible. Having said that, when you get towards the middle, sometimes I am not sure whether we are doing risk management at any particular day of the week, or whether we are doing audit work. We have a system where there are a number of risks, an electronic mapping system and a certain number of controls. Our risk manager audits the controls and I use that word deliberately. He audits the effectiveness and the operation of the controls but he is a risk manager. So there comes a point in the middle where we all work together even though we have different inherent characteristics.

SHERYL LAWRENCE: Likewise we have a risk committee and an audit committee, and it has taken a little time to ensure that the right things go to the right one. The audit committee is really about control effectiveness; the risk committee is about exposures, so it is more about the uncertainty and severity of the risk; what could go wrong in terms of the worst-case scenarios. So whether a particular risk is well controlled or not could be covered at the audit committee

MICK MICHAEL: We have a different take on that. We have an audit committee which is assurance driven; we have something known as a risk and responsibility committee, which has its agenda driven very much by the softer risks that come out from the risk register, such as reputation and integrity, the ethical side of things, health and safety, environmental and HR type-issues. Interestingly, we do not have a risk committee. The way that we have chosen to deal with things is to have risk flow through the executive directors. So the executives see their role very much on the management side and dealing with performance, and the audit committee and the risk and responsibility committee are there much more for assurance and are looking for independent assurance. However, the risk professionals will present reports to different committees. When I had that role, I would go to both the audit committee and the risk and

Sometimes I am not sure whether we are doing risk management or audit work

Mark Butterworth

What everyone wants to achieve at the end of the day with Sarbanes-Oxley, is a clean bill of health

Mick Michael

responsibility committee with different agendas. It does depend on the nature of your organisation. It is ultimately driven by the executives seeing their role as more performance-orientated, with the non-execs looking more for assurance and looking for that assurance to come both from management and also from more independent routes like internal audit.

PAUL HOPKIN: Are we saying therefore that's there an area in the middle of common interest, an area of overlap, and that we as risk managers or as internal audit have distinct areas of responsibility and influence?

MARK BUTTERWORTH: There is symbiosis. We both feed off each other

MICK MICHAEL: You definitely have to come together, and that is why I see this as a working partnership. If there is antagonism and rivalry then you are going to be at both extremes and what is going to happen to those bits in the middle that do cross over and need both of you to get together?

PATRICK DEVINE: Can I ask just for my own clarification, internal audit is not a forward-looking role, is it? It is a checking role, is that correct?

SHERYL LAWRENCE: I think it is more of a testing role, and that test can be applied to forward-looking things as much as learning from things that have happened.

MICK MICHAEL: If they are risk-based, their plan should enable them to look at the frequency of things, the severity of things. If something just never goes wrong then why would you necessarily want to look at it? But if risk information is telling you that you have got the potential for a particular problem to happen, then surely you would want that to flow through to audit so that they can create a plan around it.

PATRICK DEVINE: We always have the business plan looking forward over the next three to five years, and they will be doing their spot check today to see if it is en route.

PAUL HOPKIN: It depends so much on the role the organisation has carved out for internal audit. Just as we as risk managers talk about the upside of risk, isn't their catchphrase 'the added value of internal audit'? So they believe they make their positive contribution, albeit in a somewhat different area in a somewhat different way.

SHERYL LAWRENCE: It also depends on whether their work is focused on design or operating effectiveness. Perhaps before the last two to three years, it was primarily around design, and was concerned with evidence as to whether a control was working well in practice. Today, particularly with Sarbanes-Oxley, the audit resourcing profile has shifted. Perhaps 10 years ago there were more junior people; then they went to more senior people; now they may be going back to more junior people as they are focusing more on evidence.

PAUL HOPKIN: On the subject of Sarbanes-Oxley and the audit certification area, I see Sarbanes-Oxley as certification, especially section 404. You may consider that I am viewing it too narrowly, but if Sarbanes-Oxley is substantially a certification piece of legislation, doesn't it affect internal/external audit and really not affect risk managers? Or should I not be so dismissive?

SHERYL LAWRENCE: Across our business, organisation-wide, Sarbanes-Oxley is variously managed. Each sector has chosen where to position it, in some cases tied in with operational risk, and in some cases with finance.

CARY DEPEL: I am not sure I understand the question. Are you are asking whether the certification requirements are eventually going to filter down to the risk management level?

PAUL HOPKIN: I am seeking to be somewhat provocative perhaps, in saying that one interpretation of Sarbanes-Oxley, especially Section 404, is that it is a certification exercise, making sure that organisations tell the truth. It does not matter how bad their results are, they must tell the truth, and Section 404 is about ensuring that the truth is told. In which case it ceases to be a risk management function per se – it is not about managing risk, it is about telling the truth about how well or badly you have performed, your certification of performance. And that is why I ask the question: is all this Sarbanes-Oxley stuff over the horizon somewhere as far as we as risk managers are concerned, so we needn't worry too much about it?

MICK MICHAEL: I don't agree with that all. Risk managers should be worrying about it. There is a lot they can do to contribute to it. For instance, in respect of one aspect of Sarbanes-Oxley, the testing side, what should our testing strategy be? There is a lot of work that we are currently going through at the moment, pulling together a whole host of different strands that would influence that testing strategy. One aspect will be, what has come out from audit, what concerns are there? Another aspect is what the directors are actually thinking. Another aspect would be looking at the risk information – is that pointing us in the direction of having to go and perhaps look at a particular business more than another business – that is one aspect in terms of using outputs. The other side, which I think is totally in the realms of a good risk

manager, is the point that was raised earlier about this opportunity that risk managers have now of being proactive. What everyone wants to achieve at the end of the day with 404 and Sarbanes-Oxley generally is a clean bill of health. To have that clean bill of health you want an organisation that is well controlled, taking us back to the control environment again. We require a risk- and compliance-aware organisation. And that is where the risk manager comes in again, in terms of going around speaking to people, making sure they are aware. When you are talking about the control framework, they are there to offer advice on what that control framework might look like. It is not just audit that could do that. Indeed audit might actually be concerned about doing it to any great extent because then their impartiality and independence might be called into question.

CARY DEPEL: More cynically, the certification is just a way of imposing a strict liability regime on the CEO and FD which means to say you take intention out of the equation altogether. It does not matter that they did not intend to mislead anybody. The fact is that once they have signed their name on the dotted line, if somebody has been misled in a material way they go to gaol.

MARK BUTTERWORTH: Is hanging a sword over someone always effective? I do not think it always is. But I do fully support Mick's point about getting the benefits out of Sarbanes-Oxley. We have lived with it for a while now and it has been a chore. We have said that a number of times. It is time now to say, where is our payback? You have to analyse your systems and processes linked to your financial statements. While you are doing that, why not look and see if they are efficient, if they are effective, if they have over-engineered themselves, do we need to make any changes? This is part of the risk manager's toolbox; let us see where we can actually capitalise on it.

MICK MICHAEL: When I first moved into dealing with Sarbanes-Oxley, I was rather reluctant, but people told me I would do a good job. Before I knew that much about it, my fear was that I would be going into the detail, focusing right at the lower end where I do not believe the benefit lies. For me the benefit is looking strategically at a high level across the control framework. If we do this in a clever way, can we actually reduce the amount of work because we are placing emphasis on the fact that we are a well controlled company at a high level? The City agrees with this perception. We have a very good safety record, we score highly in corporate responsibility, etc. All these things paint the picture of a very well controlled company. Why therefore have we used that as a justification or an argument for us to approach Sarbanes-Oxley in a more sensible pragmatic way? It is because people are using that type of language now. More and more people will eventually warm to Sarbanes-Oxley – as much as they possibly can – because they are not going to see it as organisations responding to something purely for compliance. We are doing it much more to try and get the business benefit out of it. That is why I think we get the benefit of the Turnbull code of governance. Turnbull was not prescriptive, and the companies that have done well through Turnbull have done so because they applied pragmatism to it and did it in a way that was right for their own organisation and directors.

COREY GOOCH: It is about operational performance, isn't it? You do not want to over-control yourself. You want to make sure you are taking the right amount of risk so that you perform to the optimum. Your shareholders demand that you reward them as investors in the organisation. If you have a good process – it is not too much or too little – then it gives you the safety to really perform better than your competition.

CARY DEPEL: This will be rewarded in the financial services industry for those that want to take up the challenge with the Basel II capital requirements. These have now built in an operational risk manager to sit alongside market and credit risk. And if you choose the super-special approach, which is completely bespoke, you can reduce your capital requirements even more considerably than if you take one of the standardised approaches. So there is hopefully some payback.

PATRICK DEVINE: Which you do not get with Sarbanes-Oxley. There is a point of distinction between Turnbull in the UK and the US approach that we are all familiar with. The US approach is very restrictive, but in the UK it is not one size fits all. As Paul mentioned, the OFR guidance talks about the nature, size and complexity of the business. You are allowed to cherry-pick, as it were, to suit your own business. And if you are really good at it, you can score a competitive advantage. The prescriptive approach of Sarbanes-Oxley means that everybody has to do it; it is compulsory, and that certificate has to be issued at the end of the year. The only comfort that you get as a business is that the cost of complying with Sarbanes-Oxley Act is similar for your competitors. I suspect that if anyone had gone to their board proposing voluntarily the kind of measures required to comply with Sarbanes-Oxley before the act came in, they would be looking at a new career.

PAUL HOPKIN: I think there's also a danger that if you do Sarbanes-Oxley section 404 your own way, you could have your external auditors saying, well and good, you've gone down that path, but when we come to attestation we are going to do it our way, and if your way did not help us very much it will cost you more money.

You want to make sure you are taking the right amount of risk so that you perform to the optimum

Corey Gooch

To have a principle in a piece of legislation is almost like the US approach – you breach a principle and you get a penalty

Patrick Devine

MICK MICHAEL: The key is to bring your external auditors along with you right from the start.

MARC DONFRANCESCO: On the subject of using it almost as a promotional tool, the environment now has probably never been better. This applies particularly in professional services, insurance for example, anything where you are playing with numbers, people want to know you are not exaggerating the picture. The investors definitely want to know, but your clients also want to know that you are still going to be around. Being able to say that you do things very well is part of the promotional message.

PAUL HOPKIN: So I think we have a mixed message as far as Sarbanes-Oxley is concerned. There is my view that it is over the top and over the hill and your view, Mark, that there are some benefits.

MARK BUTTERWORTH: Whether it is over the top, over the hill, there is nothing you can do about it. It is a requirement. You have got to make the best of what you have got, so let's try to get some benefit out of it.

SHERYL LAWRENCE: When you said about Sarbanes-Oxley providing a case for reviewing processes and efficiency, do you think there is a case for extending that approach to other risks, not just financial reporting risks?

MARK BUTTERWORTH: I think the approach is a positive affirmation of real risk controls. I like the testing side of things. Risk managers have been somewhat stuck in a corner. I think we have shied away from approaching particular managers in the business and asking some specific questions. For example, do we approach the procurement director and say, "we know you have these controls over procurement and you have been charged to get the best price for your raw materials. You have got one supplier at the moment, have you got risk associated with that? Let's look at the credentials of that supplier, what reserves do you have in your stock, do you do a risk analysis? I will come and have a look." Now, that procurement director will be used to people coming and having a look, because Sarbanes-Oxley positively requires it. You have got to get out and get into the businesses and talk to the managers and ask them, would you mind, tell me how it works please, show me, and they are getting used to hearing that.

PAUL HOPKIN: What, in terms of recent and current corporate governance developments, is actually helping us as risk managers – the revision to Turnbull, the ERM COSO model, Sarbanes-Oxley itself, the OFR – what things are happening out there that we as a risk management community and in the name of risk management can put our hands up and say, yes, this is really helping?

SHERYL LAWRENCE: Within banking it is easy to point to Basel II as being a definitive requirement. The business use tests are quite searching.

PAUL HOPKIN: That is a business specialist area. What about more generically?

MICK MICHAEL: For me, what comes out of Sarbanes-Oxley is the part of it that not many have focused much on – the part that touches on COSO or another control framework, and that focuses on the entity-level controls. It is those cross-organisational controls, your policies, procedures, delegations, code of conduct, all those sorts of things, which touch the whole organisation but which nonetheless are very important in the context of financial reporting and disclosure. There you have an opportunity to look across the piece, to ask the question across the piece. What we are thinking of doing is utilising responses from employees' surveys and more general things like that to help in our response, but maybe also to do more of the detailed specific testing in the finance community. It is Mark's point, looking at things in a way to try to get business benefit where possible

PAUL HOPKIN: Are you embracing the AIRMIC/ALARM/IRM standard or the revised Australian standard? Do you feel they help?

MICK MICHAEL: They are helpful. I was looking at the annual report of an international company with an Australian background, which states that they based their risk management on the Australian standard. All the directors would have approved that. It is like a format to which the work that is done in risk management, that has international approval. I point to the UK risk management standard as a format. We do not follow it to the letter, but, as I mentioned, we have a separate risk management committee, and I have told the board that our framework is based on a recognised standard. Having standards does give assurance to other colleagues around the board table.

CARY DEPEL: We all need to speak a common language. I have noticed in the past when talking about risk management, people often at times end up talking at cross purposes; sometimes they use the very same words to mean substantially very different things. I do not know whether we will ever get to a point where all of the language used is common to all, but I think it is important to move along that continuum.

PAUL HOPKIN: I would reinforce that by saying we have used the phrase in our discussion, 'control environment'. Maybe before COSO became more high profile, we would

not have used that phrase. And each of us understands what it is we are talking about.

PATRICK DEVINE: I find it interesting that no one has mentioned the Financial Services and Markets Act, where you have to have systems and controls; you must have reporting; you do an external audit and have visits from the FSA where you are checked. If you look at the 11 principles that preface the Act itself as to the general conduct of business rules and the penalties for breaching them, it is a very non UK approach. To have a principle in a piece of legislation is almost like the US approach – you breach a principle and you get a penalty. You have got the real detail of what is a system and control.

MARK BUTTERWORTH: They are high level principles, but when you go into the handbook they are rules, so they do have teeth within the way they operate. But in the environment of corporate governance generally in the UK, as I said earlier, there are many other businesses, such as licensed businesses, that are required to meet rigorous standards.

PAUL HOPKIN: I am sure you are not going so far as to say that regulation is the driver of the corporate governance, to the benefit of risk management. I would love a simple answer to the question of what is the driver?

MARK BUTTERWORTH: Unfortunately, regulation has been for a lot of businesses.

PAUL HOPKIN: In certain industries undoubtedly regulation is a key driver, but that does not necessarily embed the mentality into the company.

MARK BUTTERWORTH: I think that you have got to be able to demonstrate and measure the hard successes in risk management. Many of them are intangible. But if you take, for example, a particular initiative such as driver training and demonstrate that it has reduced accidents, or that installing intruder alarms in branches of a national retailer has reduced theft, you are showing that there is a pay off. And that is when you start to get buy in – hearts and minds support – as opposed to mere compliance with regulatory requirements.

CARY DEPEL: I actually think that being forced to do something does eventually alter your behaviour in the direction of what you are being forced to do. Whatever you have to practise, whether you like it or not, eventually ends up being what you are good at.

COREY GOOCH: It may not be the best driver, but it does help get us there. You have all these different requirements, especially for global corporations around the world, that you have to comply with – stock exchange listing requirements, regulatory requirements, etc. So you try to create the best framework that you can to comply with them. As we said earlier, it is a matter of: let's do the best we can with it and eventually it will become the practice. And as we get better at it – hopefully better than our competitors – so we will thaw to the idea of it.

PATRICK DEVINE: What regulation does is give you is automatic buy-in.

SHERYL LAWRENCE: I think it is also rather a chicken and egg situation. What caused the regulation? It is the complexity of businesses; it is the growth of globalisation. Maybe we were too slow in responding to these changes, and this is what drove regulation. We kind of turned a blind eye to it; now we are being forced to put our house in order.

CARY DEPEL: In the risk management technique, after you have identified and measured your risks in terms of severity, frequency, aggregation, correlation and all these things, you try to apply metrics, then you control risks. You apply risk control techniques, which are basically changes in people, behaviours and systems. We tend to do that on a cost-benefit basis, but we may be looking at the cost in a different way to the regulator. The thing about regulation sometimes is that it just takes out the whole cost benefit equation as far as we have historically seen it. Or the regulators may have a different perspective where they are factoring in costs that we have never even considered. In that way it takes away the typical business tool – will I make some money out of this or will it give me more revenue benefit than it costs me to do? That is just not an option with regulation.

PAUL HOPKIN: It does seem that regulation and the regulatory expectations of framework are a stronger driver than most in terms of lifting risk management. Maybe the OFR, which has just become a requirement for companies, will be the next step upwards.

MARC DONFRANCESCO: British Standards have announced that they are going to develop a standard for risk management as well as business continuity. Obviously it will embrace all the best of what is out there already and, knowing the groups involved, I am sure they will make it as practical as possible. But 10 years ago no one would have thought there was a need for it; they would probably have considered it too obscure.

SHERYL LAWRENCE: Going back to the OFR, I think it has certainly driven our approach to corporate governance and risk. You may have a different driver each

Maybe we were too slow in responding to these changes, and this is what drove regulation

Sheryl Lawrence

10 years ago no one would have thought there was a need for it; they would have considered it too obscure

Marc DonFrancesco

time. Does that mean that there is a whole new set of activity? Let us implement it properly once and for all. And then they can bring in whatever regulation they like.

PAUL HOPKIN: Just to round off the discussion, I would like to look at the issue of directors' and officers' liability (D&O). Is the enhancement of corporate governance standards and risk management helping D&O insurance placements, or are the effects of hard and soft market cycles so overwhelming that it does not make a great deal of difference?

COREY GOOCH: I am not a D&O expert in our organisation, but we do have people who are and I specifically asked them that. They said that Sarbanes-Oxley and a lot of the corporate governance requirements actually give D&O underwriters more assurance that the control environment is in place. The other side of the coin is that, now that we know you have this control environment, what do you do when your risk profile changes? You add a new business; you get into a new market; you go into India and China and places like that. You have it for your current operations, but the risk profile could change dramatically over a short period of time. Will you be able to roll out that control environment on an ongoing basis and have the resources to deal with those new risks?

PATRICK DEVINE: On the one hand the insurance industry must be pleased that there are now rigid controls in place, that are perhaps just implicit in a lot of companies. But the downside of course is that there is now extra reporting. There is now data being tracked that was not tracked before. There is now a lot more transparency. And when you come to do your renewal for your D&O insurance, you have to declare whether any of the directors are aware of anything that has arisen in the past year which might give rise to a claim. There is now so much more public information available that not to disclose is actually quite a tricky thing to do. If you are operating in an environment with more and more rules which demand that you are more and more open about what you do, and then they start making investigations into it, that transparency could actually become a rod for a company's back.

SHERYL LAWRENCE: Also do these regimes increase the size of the potential claim?

PATRICK DEVINE: They can create a whole new area of liability.

PAUL HOPKIN: Does D&O become more difficult as corporate governance standards improve? Is there a significant downside?

MARC DONFRANCESCO: It depends. If you are looking at the insurance market, a lot of it is capacity driven. And there is still some new money, some new capacity, coming in. But one insurer which has D&O as one of its core products said recently that it was going to take a very cautious approach to it. A few years ago you could not give D&O cover away, then no one could afford it, now we have got a situation where there is a bit of a mixture going on in the market.

MARK BUTTERWORTH: I would hope that the legislators around the world would give safe harbour to directors who were able to demonstrate to any observer the process they have gone through to establish a review process. Regulation is not going to totally stop things going wrong somewhere, and that should not automatically mean that those directors are at fault and are personally liable. We need more time to see what happens. It is too early to judge at this stage, particularly in the US. In the UK, we have had around 13 to 15 years of development of corporate governance standards and I would hope that therefore there is a lower risk of error.

PAUL HOPKIN: What you say is true, but the reality is, as Marc said earlier, that two or three years ago D&O insurance was impossibly expensive and before that stupidly cheap. Now maybe it has reached some kind of balance.

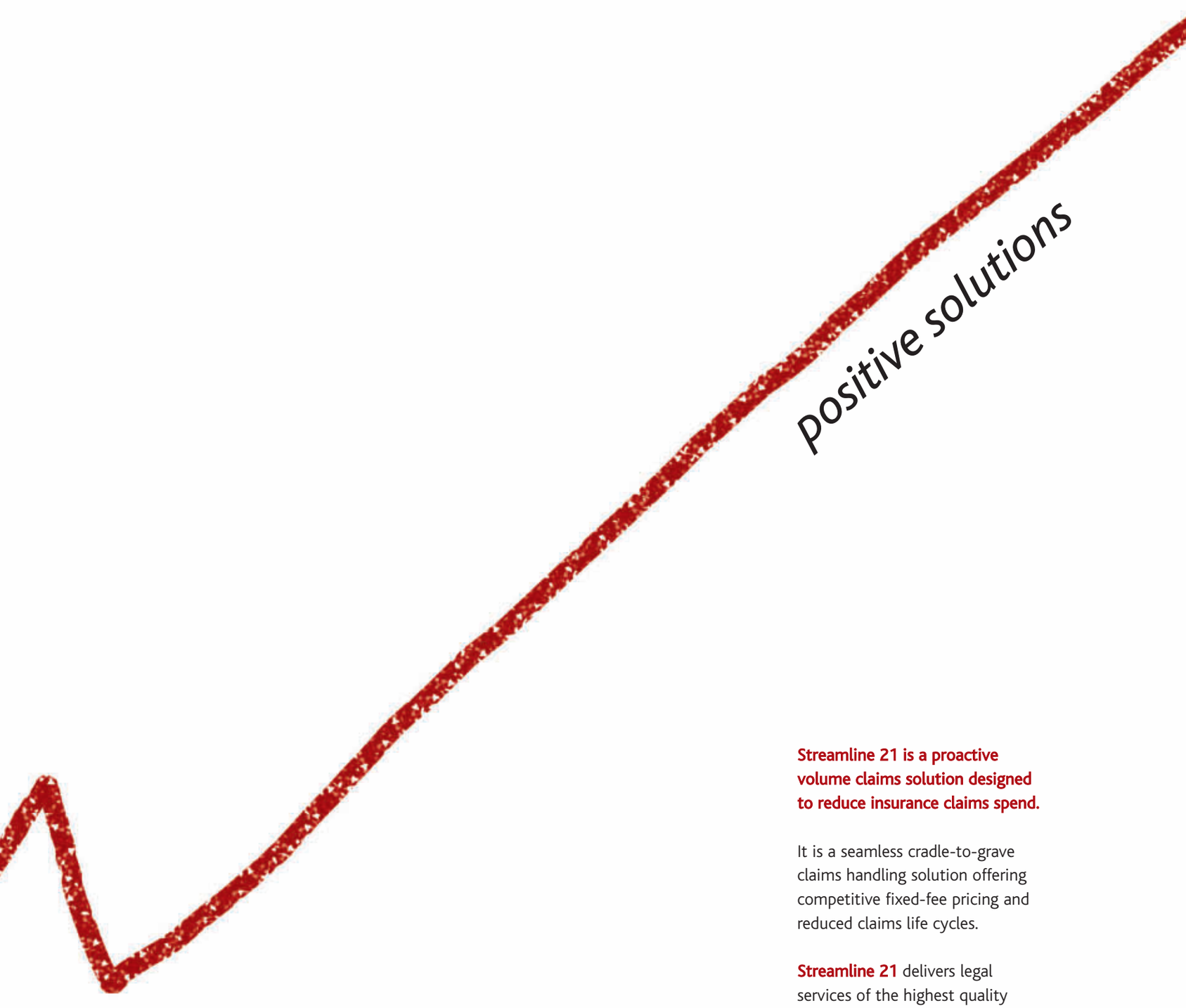
PATRICK DEVINE: Didn't the high cost relate to risk perception because it was coincident with Tyco, WorldCom, Enron or whatever?

CARY DEPEL: Price goes up in relation to the claim experience.

MARC DONFRANCESCO: There is a perception by some underwriters that there are some time bombs already written. There is an unknown factor. It is a question of how much risk the underwriter is prepared to take. It is the perception of risk, not generally, but more specifically by the guys that control the capacity. And there will always be some people with a more cavalier attitude to risk. For some it will pay off, for others it won't.

COREY GOOCH: Will Sarbanes-Oxley and other corporate governance prevent scandals? I think it will, but it will not be immediate, it will happen over time. There will be more scandals to come; the time bombs are still out there, but over time, as we get more data on best practices and bring them in, it should reduce the scandals. I think it is going to take a couple more years.

MARC DONFRANCESCO: Regarding the powerful executives who have been untouchable in the past, I think there is increasing evidence in the last few years, even in this last year, that that is no longer the case.



Streamline 21 is a proactive volume claims solution designed to reduce insurance claims spend.

It is a seamless cradle-to-grave claims handling solution offering competitive fixed-fee pricing and reduced claims life cycles.

Streamline 21 delivers legal services of the highest quality throughout the UK.

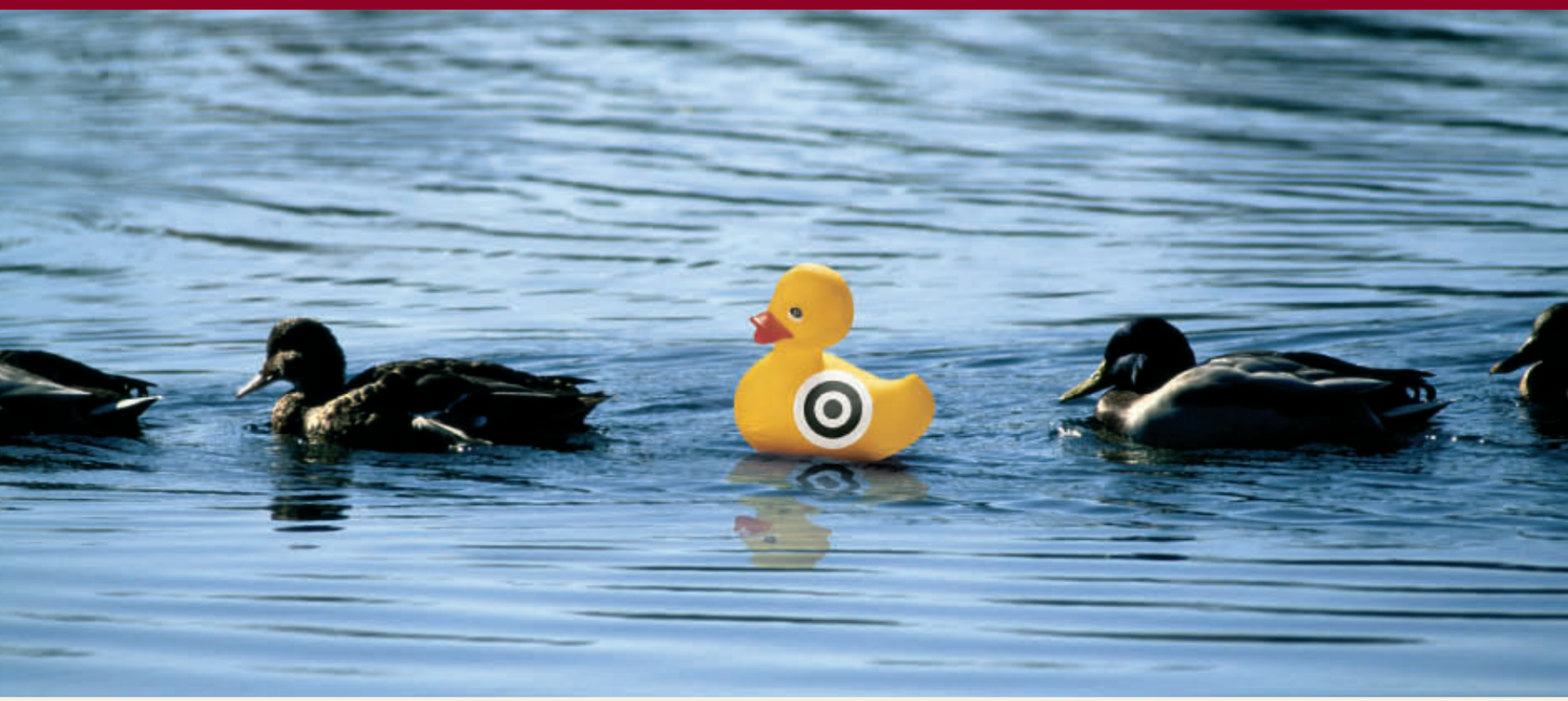
Streamline 21 consistently ensures the best commercial outcome, in the shortest possible time.

For a demonstration, please email:
philip.dicken@hughjames.com
or call: 029 2039 1071

www.hughjames.com

streamline 21

Don't be left vulnerable by poor risk management.



As a leading risk management consultancy and insurance broker, Aon has the global network and hundreds of sector specialists to meet your risk management needs in a rapidly changing world.

With outstanding expertise in risk management, risk transfer, insurance broking, actuarial and analytical services, we can create and implement a comprehensive risk infrastructure to safeguard your company's prospects.

We can also help you go forward with solutions that could actually enable your organisation to take on additional risk, while growing more securely. And Aon puts the client first, with flexibility lying at the heart of everything we do.

For further information, please contact Catherine McMenamin on 020 8612 5754, email: catherine.mcmenamin@ars.aon.co.uk

www.aon.co.uk

AON

Risk Management • Insurance & Reinsurance Brokerage • Human Capital & Management Consultancy • Outsourcing