

RISK ADVISORY

Issue 1 February 2003

Chief Executive's Note

Five years ago, together with a number of fellow directors, I helped establish The Risk Advisory Group. Our objective in doing so was to build Europe's largest privately owned independent consultancy to help companies, financial institutions and multilaterals evaluate, manage and mitigate business risk – whether it be associated with business opportunities or critical business problems, anywhere in the world.

In the ensuing period the business has substantially expanded from its initial core offerings of business intelligence and corporate investigations. Within The Risk Advisory Group we now have a specialist emerging markets practice with an office in Moscow, a digital investigations practice, and a team of highly qualified forensic accountants. Our staff speak 25 languages fluently. We support our human resources with access to a huge array of information resources and the latest investigative hardware and software.

Three years ago, as a result of a client request, we started Zephon, an employee screening business, and last year launched Janusian, a political risk and security consultancy.

The world has moved on considerably since the business was started. Never have the risks faced by our clients been more diverse, with the results of getting things wrong more dramatic and costly than ever imagined. This is reflected in the recent survey we conducted in association with the Institute of Chartered Accountants, which showed that all companies are more concerned about the areas we cover than ever before.

Through **Risk Advisory** we hope to help our clients evaluate, manage and mitigate the risks that their businesses inevitably face in an increasingly hostile economic, regulatory and geo-political environment.

I hope you find this newsletter useful. Finally, I would like to take this opportunity of thanking all our clients for the support they have provided us over the first five years. We very much look forward to working with you to achieve your business objectives in the future.



Bill Waite
Chief Executive



CONTENTS

Security Consultancy

- [Exploring the Iraq-Al Qaeda nexus – Dr David Claridge](#)

Guest article

- [Criminalising the cartels – Joanne Rickards, Partner, Peters & Peters](#)

Emerging Markets

- [Doing business in Russia: myths and reality – Christopher Peters](#)

Employee Screening

- [Criminal records – Alan Beazley](#)

Digital Investigations

- [Gone, but not forgotten... – Bob Fletcher](#)

Corporate Investigations

- [Restoring investor confidence: failure to comply will damage your health – Hitesh Patel](#)

Business Intelligence

- [Importance of background checks – Henry Pugh](#)



Exploring the Iraq-Al Qaeda nexus

Although Hans Blix has been unable to provide the US with the smoking gun it has been seeking, it is evident that we are on the brink of war with Iraq. With substantial US and British military resources already in – or committed to – the Gulf region, there are few opportunities for turning back. There is little desire on the part of the Bush administration to seek alternatives to toppling Saddam Hussein by force.

The weapons inspectors' report, delivered on 27 January, was sufficiently damning of Iraq for the US to engage a Catch-22 to justify its determination for war. If the inspectors discover concealed weapons of mass destruction, it's war; if no weapons of mass destruction are uncovered, then it's war anyway, on the basis that we know Iraq has them and is concealing them in violation of UN Security Council Resolution 1441.

As a back-up to the 'failure to disclose' argument President Bush's State of the Union address re-introduced the question of collaboration between Iraq and Al-Qaeda (AQ). Since 11 September 2001 there have been repeated attempts by the administration to demonstrate a concrete connection between the two, first around Mohammed Atta, the senior member of the 9/11 hijackers, and subsequently in accusations that Baghdad had developed a relationship with AQ operatives. On no occasion has convincing evidence of this connection been made available in open source, raising questions about the true quality of the intelligence the US possesses.

Atta was reported to have met Iraqi intelligence officer Ahmed Khalil Ibrahim Samir al-Ani in Prague in April 2001, but Czech and US intelligence officials later revealed that the meeting had almost certainly never taken place. In September last year, Condoleezza Rice and Donald Rumsfeld claimed to have intelligence primarily derived from interrogations of

suspects in custody – referred to by the Defense Secretary as 'bullet-proof' – of a connection between AQ and Iraq. It was claimed that AQ had received 'unspecified' training in the use of chemical and biological weapons from Iraq, and that AQ had sounded out the Iraqi regime as a possible opportunity for safe haven. It was further suggested that senior AQ figures had been in Iraq – including Baghdad – during the 1990s and that some may have remained there. No specific evidence was offered and the claims were met with scepticism from most quarters. At the time even Mr Rumsfeld cast doubt on the information relating to chem-bio training by asking reporters not to print it. It is probable that when Secretary of State Colin Powell elaborates on President Bush's claimed connection it will build upon this baseline of intelligence.

The President's words may also be interpreted as a reference to alleged support from Baghdad's intelligence services for Ansar al-Islam, the Islamist group based in Northern Iraq, which has undisputed ties with Al-Qaeda. Ansar was formed by Kurdish Islamists in August 2001, with funding and support from Al-Qaeda. It has since swollen from only around 30 founding members to an estimated 600, as multi-national 'Afghan Arabs' fleeing US military operations in Eastern Afghanistan have sought sanctuary among its ranks. Ansar is well armed, experienced in guerrilla warfare, and controls territory close to the Iranian border, near Halabjah. Ansar guerrillas have clashed repeatedly with Patriotic Union of Kurdistan (PUK) *peshmerga*, with both sides suffering heavy losses in a sustained engagement in December last year.

Saddam has a history of playing Kurdish factions off against one another, and there have been several reports that Iraqi Mukhabarat intelligence officers have made contact with Ansar. They are rumoured to provide weapons and money in return for a continuation of the campaign against the PUK. An Al-Qaeda operative and Mukhabarat agent named Abu Wa'il is considered to be the linkman



between Iraqi intelligence and Ansar. As a means of undermining what they believe is PUK rhetoric intended to garner US support, other Kurdish factions play down the significance of the reputed AQ-Baghdad connection. However, there can be no doubt that Ansar has become a significant potential channel for AQ resources in the region.

A recent article in the *Washington Post* suggested that credible intelligence had been received by the US that Ansar handled a chemical agent, possibly VX nerve gas, in Northern Iraq, which was reported to have arrived via Turkey. If Saddam has the quantities of nerve agent at his disposal that the US believes, he would surely have passed a haul directly from his own territory but, despite the geographical discrepancy, the *Post* suggests Saddam may have been behind the weapons transfer. However, it now appears more likely that if VX or another agent did fall into the hands of Ansar it was through AQ's own channels, passing from the Caucasus through Georgia and Turkey to northern Iraq.

It is possible that any such acquisition is part of a concerted shift in Al Qaeda's global strategy towards the use of weapons of mass destruction in Europe and North America. According to US intelligence officials there is evidence to link the Algerians involved in the British ricin plot to middle-ranking Al Qaeda operative Abu Massan al Zarqawi, who Jordanian intelligence claim has sought sanctuary with Ansar in northern Iraq.¹ These relationships may suggest a westward-facing logistics network linking AQ bases in the Caucasus with the outside world.

Alternatively, the end destination may have been Iraq, as Ansar seeks to prepare for retaliation against US forces who are likely to be nearby in considerable strength in the not too distant future. At the time of the nerve agent plot the US military threat assessment raised the

prospect of a chemical attack at the Incirlik airbase in Southern Turkey. Perhaps the intention is to disrupt the activities of US forces prior to, and during, the inevitable military campaign. Could Iraq be behind a terrorist project of this sort?

But if the US could prove a substantive connection between Al Qaeda and Saddam it would likely have justifiable cause to launch an attack on Iraq irrespective of the conclusions of the UNMOVIC team. The fact that it has been unable to do so strongly suggests that there is no such connection. The 'axis of evil' concept can only be stretched so far: in this case it is a potentiality not an actuality. Iraq almost certainly does have contact with Ansar, but that does not mean it directs its actions. In racing to prove a case against Iraq the US is overlooking the role of Iran's much more substantial support for Ansar, and Al Qaeda.

Disrupting the prospect of a Kurdish state on its borders is as much in the interests of Tehran as it is Baghdad. An American presence is even less welcome. Ansar are likely to be the basis for efforts by AQ and Iranian hard-liners to challenge the forthcoming American military effort in Iraq, and to undermine the reconstruction process that will inevitably follow. The Iraqi people are likely to welcome liberation from Saddam. Others will use it as an opportunity for further confrontation. Western companies seeking future opportunities in sanction-free Iraq would do well to recognise that removing Saddam is only half the battle.

Dr David Claridge

David Claridge is Managing Director of Janusian Security Risk Management. If you would like to know any more about security threats consultancy, please contact him at

Claridge@janusian.com

[Back to contents](#)

¹ Zarqawi is wanted in connection with the assassination of the American official Laurence Foley in Amman in October.



Criminalising the Cartels

By the summer of 2003 the Enterprise Act is expected to come into force. The legislation criminalises hardcore cartel activity, with those who engage in it facing up to five years in prison. With implementation only months away, the OFT and SFO are busy recruiting lawyers and investigators in order to hit the ground running: the OFT already claims to be uncovering cartels at a rate of one a month and the Enterprise Act is pretty much guaranteed to increase that statistic given the mixture of 'stick and carrot' reforms it contains.

Under the Enterprise Act, individuals can be prosecuted if they have dishonestly agreed with at least one other person to engage in one of the prohibited cartel activities. The Act lists them: they are, typically, price fixing, bid rigging, market-sharing or limiting production. The fixing, rigging or sharing needs to be agreed between individuals who are at the same level of supply or production (termed horizontal agreements) and those in a vertical relationship will not be caught by the Act. The aim is to protect the consumer from unfair, anti-competitive practices and to ensure the market within which consumers transact is a fair one. Interestingly, an offence will have been committed irrespective of whether the agreement is actually implemented.

Hardcore cartel offences are notoriously difficult to uncover – so will this Act make any real difference? Yes, because the OFT have not only been given hefty new sticks in the form of powers of investigation, but also a carrot to dangle in front of potential whistleblowers: an immunity regime, based on the successful US model. In fact, the carrot may ultimately prove more powerful than the stick in generating lines of enquiry for the OFT and SFO.

The OFT will have new powers, modelled on those of the SFO. They will be able to compel the production of documents and information as well as compel individuals to answer questions. The penalties for non-co-operation or providing misleading

information are fines and/or imprisonment. There is no privilege against self incrimination (you can't 'take the fifth') and only material that is the subject of legal professional privilege is exempt from production. Everything else must be made available, subject only to relevance. Search warrants may be obtained instead (or as well, if the OFT believe you have failed to comply with a request for information) and material can be seized from the office, factory or an individual's home.

The Act also allows the OFT to use intrusive surveillance techniques against cartel suspects. Bugs in the boardroom, a car or an individual's home could be authorised, and it is likely that the Act will be amended between now and implementation to allow the OFT to use intelligence gathered from those acting under cover. So will future board meetings take place in lead-lined rooms? Will pinstriped suits be abandoned in favour of figure hugging Lycra from now on? Only time will tell, but the fear of who is listening in or taping the conversation is likely to be a real one, as information provided in this way may well give the OFT the ability to prove who was the cartel leader. This is an important matter when the issue of leniency comes to be considered.

Under the Enterprise Act, therefore, the OFT will have formidable powers to gather information in support of their inquiry. In practice, however, much of their intelligence is likely to be derived from information provided to them by a whistleblower – which is where the significance of the Act's immunity regime comes in.



Immunity can be granted to one or more offenders if they come forward and co-operate with the investigators. They can receive their very own 'get out of jail free card' if they admit their participation in the cartel offence, provide the OFT with all information, documents and other evidence available to them and maintain continuous and complete co-operation throughout the investigation. They must refrain from further cartel activity, except as directed by the OFT (conceivably this could mean them going back into the boardroom under cover) and, most importantly, they must not have compelled others to take part or have been the lead instigator of the cartel agreement. The role of the whistleblower or the individual prepared to act under cover cannot be underestimated, as this is one simple and unambiguous way for the OFT to identify the cartel leaders and gather evidence.

Cynics suggest that the minute a board meeting is over there will be a rush for the door by several directors keen to be first to get into the OFT and secure their own individual immunity. Of course, only dishonest participators need make the dash, as those who have acted honestly have no need of the 'no-action letter'.

The Competition Act 1998 – which covers much the same ground as the Enterprise Act –has been in force since 2000, but affects *businesses* that have been involved in cartels, not individuals. Significant fines can be imposed for businesses that have engaged in anti-competitive practises at both a UK and EU level. With the advent of personal criminal liability under the Enterprise Act, cartelists will find that they are wearing their own as well as their corporate hat – and it seems only human nature for them to consider their own position first, which is likely to crystallise the conflict of interests between themselves and their business.

Another major change brought in by the Enterprise Act is new disqualification powers. Competition Disqualification Orders (CDOs) against directors can be applied for in the civil courts by OFT or other regulators. All that is required for a

CDO to be imposed against the director is for his company to have breached competition law and the court to consider that his conduct makes him unfit to be involved in the management of a company. The period of disqualification will vary depending upon the facts of each case, but the maximum term is 15 years. It is widely believed that CDOs will be frequently sought, as the civil standard of proof is low: proof of conduct giving rise to a disqualification order needs only to be on the balance of probabilities, no dishonesty is required and in certain circumstances whole boards could be subject to disqualification proceedings. Such proof could, of course, emanate from a variety of sources, including a whistleblowing director seeking immunity from prosecution, or from boardroom surveillance. From this summer, board meetings may never be the same again.

Joanne Rickards

Joanne Rickards is a Partner in Peters & Peters' Fraud and Regulatory Unit and has been listed as one of the Hot 100 Lawyers in 'The Lawyer' magazine, January 2003.

jrickards@petersandpeters.co.uk

[Back to contents](#)



General perceptions and pre-conceptions of doing business in Russia

More than most other countries, Russia suffers from a plethora of perceptions and misperceptions in the eyes of Westerners – some justified, but many based on no more than Hollywood stereotyping. For a businessman contemplating entry into the Russian market, the conflicting stories - many presented as reliable 'fact' - make it difficult to reach a sound decision as to the costs and benefits of doing business there. In this article we seek to present some of the most frequent claims about the Russian business scene, to explain their origin and to what extent they may once have been justified, and to discuss whether they are still justified today.



All Russian businessmen are criminals.

This claim dates to the very end of the Soviet era and the immediately succeeding period. The Soviet state was collapsing, with no stable and viable entity apparently capable of replacing it. Almost inevitably, an asset grab, particularly of natural resources, ensued. In particular, ranking members in the central and regional communist party hierarchies assumed control of many state enterprises. In too many cases they also took over the finances of these enterprises, leaving employees, contractors and creditors unpaid. This asset grab was characterised by a high level of brutality: the early to mid-1990s witnessed a high number of contract killings and other criminal activity, as those who had seized assets sought to

consolidate and expand their positions. These criminals were frequently associated with figures who were connected to government circles, and it is fair to say that a significant number of Russia's current leading businessmen would not be comfortable with too close an examination of their activities in that period, however irreproachable their conduct has since been. Equally, however, many of today's Russian businessmen and businesswomen have reached their positions through a mixture of hard work, good fortune and good contacts, and have no active contact with organised crime (although whether they have ever had to pay protection money is a different question). It would be a mistake to assume that the business atmosphere and practices of the early and mid-1990s are still the norm. While a cautious approach is always advisable, a Western businessman or businesswoman might risk losing the opportunity to do profitable business in Russia by relying too heavily on such generalised and uninformed judgements.

Surely the communist era mentality still prevails in Russia?

The experience of many visitors to Russia, both businessmen and tourists, leaves many with the impression of an overbearing state staffed by obstructive officials with little sense of the need to be helpful, courteous or efficient. This may range from dealings with customs and passport staff upon first arrival at the airport, to encounters with police demanding production of a passport for no apparent reason. Further contact with staff in many Russian shops, who appear to resent the very presence of customers willing to spend money, confirm, for many, the impression that an anti-business communist-era mindset still prevails. This would, however, be inaccurate, especially when applied to the growing private business sector, particularly among small and medium enterprises. While many of today's business managers may indeed be former members of the Communist Party, this should not be taken as evidence of any particular mindset. For many, membership



of the party was simply a part of life, and a means of getting ahead: it implied no particular ideological devotion to the party's tenets. Furthermore, it should be remembered that change was brought to the USSR largely by reformist members of the party. Nevertheless, it is certainly useful to know of individuals' activities in the past, particularly if they are currently in senior positions, and therefore likely to have been professionally active in the communist period. Such knowledge can give an idea of their past and present associations and therefore of their loyalties and intentions.

Russia is an inherently unstable and risky place in which to do business – the risks always outweigh the benefits.

While this charge could certainly have been made with some – although not complete – justification ten years ago, it is certainly no longer axiomatic. The job of The Risk Advisory Group in Russia is not to deter clients from doing business in Russia simply by telling them that Russia is generally too risky, but rather to identify, present and explain to them the specific risks which they may face in their line of business and thus to assist them in mitigating that risk. Since the partial default and rouble devaluation of August 1998 (which historians may come to judge as a 'good thing' for the Russian economy, painful though it was for many ordinary citizens and businesses at the time), inflation has remained steady, the local stockmarket has seen impressive growth, and business and tax law is gradually becoming more coherent and consistent – for example, personal income tax is now set at a flat rate of 13 percent. However, much remains to be done: large parts of the business code remain incomprehensible, self-contradictory and inimical to outside investment, particularly with regard to taxation; much legal process remains inefficient, slow, and vulnerable to external pressure; and inflation, though steady, still needs to fall further.

Nevertheless, the charge that Russia is inherently unstable and excessively risky is neither fair nor true. The dramatic turnaround in the Russian economy in the last ten years, brutally volatile though it has at times been, is sufficient proof of that. As outside investment rises, and as Russian businesses seek to expand into the West, where rules and conventions regarding transparency and past behaviour are more concrete (though still far from perfect), we expect the Russian market to continue its process of normalisation.

Christopher Peters

Christopher Peters is a Senior Associate with The Risk Advisory Group. If you would like to know more about any issues related to emerging markets, please contact him at

Christopher.peters@riskadvisory.net

[Back to contents](#)



Employee Screening – Criminal Records



The Criminal Records Bureau (CRB) became operational in March 2002 and has been dogged by poor publicity ever since. What went wrong and when will the service improve?

By any criteria, setting up the CRB was an ambitious project. Established under Part V of the 1997 Police Act, the CRB is an executive agency of the Home Office run under a public/private partnership with the outsourcing specialist Capita. Conceived in response to growing public pressure to reduce the risk of inappropriate persons working with children and other vulnerable groups, its scope has broadened into a one-stop shop for those seeking access to criminal record information to make informed decisions in relation to employment and licensing. This has involved centralising data from various sources including the Police National Computer system, for which data input responsibility was devolved to police forces in 1995. With over six million names recorded, the PNC is the only database to which all police forces have access and as such should play a central role in operational policing: many forces, however, saw maintaining accurate and timely PNC data merely as low priority administration, and built their own local systems instead.

By March 2001 the situation was so critical that not one police force was meeting the PNC compliance strategy targets adopted by the chief constables the previous year. It was taking an average of 55 days to

input 90 percent of arrest/summons data (the original target set by the Home Office being 100 percent in 24 hours) and the results of 450,000 court cases were waiting to be input, with nearly half being over nine months late.

By the time the CRB became operational the backlog had been reduced to around 25,000, and concerns about data integrity were overshadowed by public concern about the time taken by the CRB to produce its disclosure certificates. By the summer the media were in full pursuit of any and every story about schools waiting months for checks on teachers to be returned.. Though the situation has since improved, Enhanced Disclosures (which relate to those working with children and other vulnerable groups) are still taking between five and six weeks to come through, while the CRB claims that Standard Disclosures (which apply to any other role excepted from the Rehabilitation of Offenders Act) are now coming within the three week target turnaround. The Basic Disclosure service is unlikely to be available until early 2003 (there is an increasing likelihood that it may be postponed indefinitely), and the requirement for Disclosures for care workers and agency nurses has been put back a year until 2004.

Questions about the reasons for the delays are many and the answers are not entirely clear. Did Capita build its operation on a poor specification? Was demand for the service underestimated? Why was the service originally designed as a telephone based operation only? The fact is that all of these and other factors have probably played their part: when it launched, the CRB was not planning to operate a paper-based application system alongside a phone-based system and many delays are caused by incorrect completion of the paper form by applicants or inadequate verification of identity by the employer or other registered body. In addition, demand for disclosures may have exceeded expectations, although the CRB business plan's volume assumptions tie back to the ultimate demand estimate of 8.9 million



applications (of which 50 percent for basic disclosures) published by the Home Office in January 2002. And it is worth remembering that in handling a current volume of 60,000 disclosures a week, the CRB is providing responses to more than treble the number of enquiries made of all the police forces under the old system.

Turning to the future, it seems likely that the CRB will shortly meet its targets for turnaround times on higher level disclosures, and extending the timescales when new categories (care workers, nursing agency workers, school governors) require checks will help. But the CRB will also have to handle an increasing number of applications from employers in financial services concerning FSA approved persons, and those licensed in due course by the Security Industry Authority will also require CRB checks. And although we are normally sceptical about the implementation of large scale government technology projects (PPP or otherwise), perhaps the real turning point in making the CRB a success will be the development of alternative internet-based systems. That will involve consideration of electronic signatures, security, processing sensitive personal data.....sounds almost enough for another article.

Alan Beazley

Alan Beazley is a Director of Zephon Employee Screening. If you would like to know more about employee screening related issues, please contact him at alan.beazley@zephon.com

[Back to contents](#)

Gone, but not forgotten...

When the first reports of Enron's problems hit the press, no-one could have imagined just how severe would be the impact on the businesses of those involved. The effect on Andersen in particular gave us all a salutary reminder that Othello's words – *'O! I have lost my reputation. I have lost the immortal part of myself, and what remains is bestial'* - apply as much in the 21st century global marketplace as they did in early 17th century Venice.

Andersen's reputation was severely damaged, and the firm subsequently destroyed, by reports of documents being shredded in a few of their offices around the world. These reports caused some wry smiles here at The Risk Advisory Group, particularly among our corporate investigations and computer security teams: because hidden in these reports was a 'triple-whammy' that illustrated perfectly the way in which individuals – and corporations – forget just how pervasive is the role of the computer in today's business world.

Andersen was first 'whammied' by the shredding stories themselves. Nothing acts as quite such a potent symbol of 'something to hide' as the corporate shredder.

The 'double' came from the fact that the shredders' actions were almost certainly a complete waste of time. Destroying paper copies of any documents – unless they are handwritten letters, sent only by 'snail mail' – is useless in an age where almost every business document resides on a computer system somewhere.

And the 'triple-whammy'? The Andersen audit team would have known that, in common with many other large accountancy practices, the firm had its own forensic computing unit dedicated to recovering lost or deleted data from computer systems. These same people would also be very well qualified to make sure that Enron's computer systems were well purged of any incriminating data and put beyond recovery – even by experts.



This could be thought of as electronic shredding, to complement the physical stuff, which would effectively be turning the gamekeepers back into poachers. If Andersen failed to spot this tactic they could rightly be accused of incompetence on top of the other charges now working their way through the US judicial process. If they did spot the problem, and deployed their in-house electronic team on Enron's computers, then the offences would seem to have been compounded.

As a morality tale of business in the 21st century, the Enron/Andersen saga still has plenty of life in it – and I am sure that it will be picked over by commentators for some time to come. But the accountancy profession should not ignore the forensic computing elements of the story. For they provide some useful lessons for us all.

Lessons:

1. **Even experienced professionals forget how much data is stored in IT systems in business today.**

- Almost every business document and every transaction starts or ends up on a computer system at some point.
- People sometimes commit intensely personal information to media such as email. There is a common view that e-mail is the electronic equivalent of the Registered Letter. It is not; it is the equivalent of the postcard. We have experienced many examples in which an image of a desktop computer's hard disc has revealed disloyalty, financial distress, and fraud.
- The memory in many of today's desktop computers is gigantic. 40 Giga Bytes is not unusual. That is the information equivalent to a pile of A4 sheets of paper as high as Ben Nevis!
- The data is also held in more locations than is often realised. The desktop is only the start of a long chain of servers, routers, contingency sites, and back-up tapes – all of which would hold copies of a message for varying periods. Because of this, our

investigators are almost always able to recover data that's been lost or deliberately deleted.

2. **Although Andersen's actions do not so far seem to have been fraudulent, fraud is now one of the biggest issues facing business today.**

- Fraud costs UK businesses tens of billions of pounds a year, depending on which survey you believe.
- It is often not prosecuted because companies do not want the publicity OR they cannot find the evidence.



Forensic computing is often the answer. It is generally clear to expert investigators when attempts have been made to delete data – and we can generally find it and re-assemble it. Inevitably, the large potential criminal gains from fraud have resulted in a technological 'arms race' in which the forensic systems compete with new products aimed at permanently eradicating data from computers.

3. **Companies can protect themselves and their clients.**

- Get your policies, systems, staff awareness, and monitoring in place before you have a problem;
- When you do suspect you have a problem follow the Golden Rules:
 - Don't panic but move fast
 - Don't touch anything
 - Get independent professional help



Conclusion

Enron / Andersen was a corporate tragedy of immense proportions. And although the shredding was probably only a symptom of wider problems, it does give us a good opportunity to look at issues around information protection and electronic document discovery. This has implications for a large cross section of all litigation in Europe and the USA. Fraud is a growing issue for businesses in many sectors – and one in which accountants have clear roles to play in prevention and/or discovery. But just as people forget how much data they commit to IT systems, accountants may sometimes forget how much they can recover through the use of expert, independent investigators.

Bob Fletcher

Bob Fletcher is a Director of The Risk Advisory Group. If you would like to know more about digital investigations, please contact him at

Bob.fletcher@riskadvisory.net

[Back to contents](#)

Restoring investor confidence – failure to comply will damage your health

Signs of trouble ahead

2002 was in many respects a veritable *annus horribilis* for the corporate world and the general investor community. The fall of global giants, such as Enron and Andersen, thrust business onto the front page, while companies such as WorldCom, Tyco, Xerox and Qwest Communications added to the growing list of alleged fraud, false accounting, insider trading and corporate excess. In many cases there had been suggestions for some time that all was not well. Despite this, however, regulators appeared to have done little to quell the enthusiasm with which the US public flocked to take part in the false goldrush: it has been established, for example, that directors of some US companies had cashed in \$64bn worth of shares before those companies collapsed, and that Enron had not only parked its substantial mountain of debt off its balance sheet in Special Purpose Vehicles but had also consistently altered its reported figures, showing \$1bn net income in mid-2001 while simultaneously having a cash outflow of \$1bn.

Separate investigations were launched by Eliot Spitzer to look into the role in the scandals of some of the biggest banks on Wall Street. It was alleged that some investment bankers had encouraged research analysts to issue 'buy' notices on the very same stock that they privately derided, so that lucrative banking fees from the big corporate clients would not be put at risk. Although not proven, an immediate impact of these enquiries has been for the banks to agree to restructure their functions to avoid internal conflicts of interest as well as incurring fines totalling \$1.4bn.

Effects and responsibility

As the impact of these scandals spread across the globe, with job losses and



shattered investor confidence leading to substantial falls in stock market values both in the US and other mature economies, it became apparent that an underlying problem was the ease with which the general investor had been deceived by statements that were at best non-transparent and at worst false and misleading. US politicians laid the blame for this at the door of executive directors, auditors, analysts and investment bankers. These professionals, it was argued, had been charged with managing the interests of shareholders and investors but had lost sight of their role by putting profits and personal gain before the interests of the general investing public. In order to strengthen commitment to ethical conduct, improve corporate governance and increase the quality and timeliness of public company disclosure, President Bush signed the Sarbanes-Oxley Act of 2002 with the aim of restoring investor confidence.

Sarbanes-Oxley Act 2002 - Courtroom against Boardroom

a. Who it affects

Although the Act's primary impact is in the US, it nevertheless has an extra-territorial reach. The Act applies to all 'issuers' (including 'foreign private issuers') that have securities registered under s12 of the Securities Exchange Act. This captures all non-US corporates that have American Depository Receipts (ADRs) listed on the NYSE or Nasdaq or that have sold or will be selling securities in the USA under a registration statement falling within the Securities Act 1933. The Act, however, does not apply to foreign private issuers whose securities or ADRs are traded only



on the OTC Bulletin Board or 'Pink Sheets' market.

b. What executives should know

- Each periodic report filed with the SEC by the issuer must be accompanied by written statements from the CEO and the CFO certifying that the report 'fully complies' with the relevant sections of the Exchange Act and that the information 'fairly presents' in all material respects the financial condition and results of its operations. It is a federal crime, punishable by imprisonment and/or fine, to make a false certification.
- Each periodic report filed with the SEC by the issuer must include other certifications by the CEO and the CFO with reference to, *inter alia*:
 - having reviewed the report;
 - making an untrue statement or omitting to state a material fact;
 - being responsible for designing, evaluating and reporting on the system of internal controls;
 - having disclosed to the auditors and the audit committee any significant deficiencies in internal controls or frauds, whether or not material, involving management or employees who have significant role in the internal controls;
 - A violation of these certifications carries civil penalties.
- CEOs and CFOs will forfeit all incentive- and equity-based compensation for a 12 month period following publication of any financial statement that is later restated as a result of misconduct.
- A registered accounting firm may not perform any audit service for the issuer if the CEO, CFO or its equivalent was previously employed by the auditor in the last 12 months and had worked on the issuer's audit.
- Loans or extensions to existing credit arrangements by the issuer to its directors or executive officers are prohibited.



- Any changes in the ownership of the issuer's equity held by directors, officers or ten percent shareholders need to be disclosed within two days of such transactions instead of the ten days previously allowed.
- The issuer must disclose whether or not it has adopted a 'code of ethics' applicable to the principal financial officers.
- Each annual set of financial statements must contain an 'internal control report' stating the responsibility of management for establishing and maintaining internal control structures and an assessment of the effectiveness of the same.
- Any *pro forma* figures issued to the SEC or other public disclosures must be reconciled to GAAP and must not be misleading.
- All material off-balance sheet transactions, arrangements, obligations and other relationships with unconsolidated entities or other persons must be disclosed in each annual and quarterly report filed with the SEC.
- Financial statements must reflect all 'material correcting adjustments' that have been identified by a registered public accounting firm in accordance with GAAP and SEC rules.
- It will be an offence for any officer or director to fraudulently influence or deceive the auditor for the purpose of rendering the financial statements materially misleading.
- Whistleblowing employees who have been dismissed or discriminated against for assisting an investigation into breaches of SEC rules or fraud against shareholders will be protected by rights to a civil action. Any person knowingly taking harmful action, including interfering with lawful employment, against a whistleblower will be subject to a criminal offence

punishable by fine and/or imprisonment.

- The SEC has the responsibility of reviewing the disclosures made by an issuer 'on a regular and systematic basis' and which will be undertaken at least once every three years.

c. ***What boards should know***

- Boards must disclose to the public 'on a rapid and current basis' such additional information concerning material changes in its financial condition or operations.
- All audit committee members must be independent, should have the responsibility instead of management for the appointment, compensation and oversight of the auditor and must have the authority to hire independent counsel and other advisers. It must be disclosed whether or not the committee includes at least one member who is a 'financial expert' and to state why, if not. The SEC has the power to direct the national securities exchanges (NYSE, etc) to prohibit the listing of securities of any company that does not have an audit committee which complies with the foregoing.
- Lawyers representing issuers before the SEC must report evidence of material violation of securities law or breach of fiduciary duty by the company to the chief legal counsel or the CEO and on failing to get an appropriate response to the audit committee.
- The Public Company Accounting Oversight Board, comprised of five members, will be created and managed under the supervision of the SEC, to register public accounting firms, including non-US firms, to establish auditing, quality control, ethics and other standards relating to audit reports and inspect, investigate and discipline, as appropriate, registered accounting firms.



- Every public accounting firm engaged in the preparation or issue of any audit report with respect to any US issuer must be registered with the Board.
- Registered public accounting firms are prohibited from providing non-audit services contemporaneously with an audit.
- The SEC has to adopt within one year of the Act rules reasonably designed to address conflicts of interest between research analysts, investment banking divisions and issuers as well as rules governing disclosures to be made by research analysts.
- The Act also creates new criminal actions which are applicable to multiple constituencies, including destruction, alteration or falsification of records in federal investigations, criminal proceedings and bankruptcy and securities fraud involving a public company.

d. When is the Act effective?

Owing to the complex and extensive nature of the legislation, certain provisions of the Act are effective immediately, such as the requirement that CEOs and CFOs certify periodic reports, or the ban on new loans to directors and officers of the company. Other aspects of the Sarbanes-Oxley Act will largely come into force when the appropriate implementation regulations have been adopted by the SEC, primarily within 180 or 270 days defined by the Act.

This period prior to full implementation has given rise to an element of uncertainty and confusion, accompanied by intense lobbying on behalf of parties affected by the legislation. This has been seen recently by Abbey National stopping loans to directors while companies such as Lloyds TSB, Barclays and the Royal Bank of Scotland are still seeking advice on how to comply with the legislation. The

onerous and wide ranging requirements of the Act seem already to have deterred some foreign issuers from listing on US exchanges. Notable examples are German carmaker Porsche, which recently abandoned its plans for a listing on the NYSE, and Benfield, the UK insurance company.

What are the implications for you?

The primary focus of the Act is with financial risk management, an emphasis which places it at odds with corporate governance principles laid down by many European countries, including the UK. While intense lobbying to the SEC is currently under way, there are concerns that the SEC does not have enough exemptive authority to resolve the issues raised by non-US issuers, and it remains to be seen whether a mutually satisfactory resolution can be achieved.

The cost-benefit fallout from the Act will start to affect the strategies of some leading non-US corporations as they ponder on how effectively and at minimal cost to comply with the Act, not be at the mercy of regulators, shareholders and prosecutors, but still deliver on long-term plans. To mitigate the risks involved in charting these waters, certain commentators – including Harvey Pitt, outgoing chairman of the SEC – have stressed the importance to actual or potential foreign issuers of engaging specialist financial investigators as a ‘second line of defence’ against possible future regulatory intervention.

A recent risk survey of the FTSE 500 by The Risk Advisory Group in conjunction with the Institute of Chartered Accountants, for example, revealed that an increased awareness of risks among senior directors is not reflected in the attention given to these risks by boards in general. Despite financial scandals in the UK such as My Travel, HP Bulmer, Amey and Marconi, non-compliance with regulation, accounting and criminal risks was lowest rated among risks considered by boards. Evidence of this neglect is



further borne out by the increasing number of fraud investigations undertaken by the Group in the last year.

The Sarbanes-Oxley Act raises the standard of corporate governance to a new level, with severe penalties – both criminal and civil – for non-compliance. Those who can meet the challenge will be able to participate in the largest capital and consumer market in the world. Those who fail will face an increased cost of capital as they are forced to access financing through other routes with fewer strictures but higher premiums, and it appears now to be merely a matter of time before a foreign issuer falls foul of the directives of the Sarbanes-Oxley Act.

Hitesh N Patel

Hitesh is the Head of Financial & Special Investigations. If you would like to know more about corporate investigations and fraud related issues please contact him at hitesh.patel@riskadvisory.net

[Back to contents](#)

Importance of background checks



Financial institutions pull out of one in ten deals (10.1 percent) as a result of information uncovered during background checks on the other party, according to research carried out by The Risk Advisory Group in 2002. In a further one in eight cases (13.4 per cent), significant modifications to the deal are made as a result of the investigation.

These figures were derived from a review of the 132 deals on which The Risk Advisory Group conducted investigations during the first six months of 2002. Of the 119 for which decisions had been taken by the client at the time that the survey was released in September, two-thirds (65.5 percent) went ahead with no significant modifications and there were a further one in ten (10.9 percent) in which the institution pulled out for other reasons.

All of the due diligence assignments conducted by The Risk Advisory Group's Business Intelligence and Emerging Markets practices for financial institutions in the first half of 2002 were included in the survey. The core client groups involved were investment banks, private equity houses, private banks and multilateral lending institutions. On most occasions, The Risk Advisory Group was asked to carry out its research as the client came close to finalising an investment with the subject of an enquiry, but cases also covered acquisitions, IPOs, new client acceptance and correspondent banking relationships.



The cases examined touched on most of the world's leading economies but were concentrated in The Risk Advisory Group's core areas of Europe, the Middle East and Africa.

The findings which led clients to pull out of or modify deals included poor references from former business partners, non-transparent sources of wealth and even suspected links with criminal or terrorist groups. For example, one client asked us to conduct routine background checks on the management team of a property investment fund which it was considering backing. Research uncovered evidence that one of the fund's partners had spent much of the early 1990s under investigation by his country's regulatory authorities who were looking into the collapse of a property company of which he was a director. While the individual in question was never tried, several of his colleagues were convicted of wrong-doing in connection with the episode. The subject had failed to disclose any of this in the relevant section of his disclosure questionnaire and, when confronted with our findings by our client, voluntarily withdrew from the venture.

On another occasion our research found that our client was on the point of accepting a mandate to act as corporate finance adviser to a business which had been accused of human rights violations in connection with its mining activities in a west African country.

Overall, about half of the terminated or substantially modified deals were changed because of integrity-related issues, and half because of concerns about qualitative factors.

In integrity due diligence assignments, research teams consult a range of public record and other data sources, nominated referees and a network of informal contacts, in order to provide clients with an independent assessment of the suitability of potential business partners. Investigations focus on the qualitative factors not covered by traditional financial and legal due diligence, such as

managerial competence, verification of career histories, involvement in controversial episodes or undisclosed business interests

Henry Pugh

Henry Pugh is a Director of The Risk Advisory Group. If you would like to know more about due diligence, please contact him at

Henry.pugh@riskadvisory.net

[Back to contents](#)

