

Coping with Compliance



A white paper exploring the ramifications of legislation
and industry regulations on the financial services sector

Introduction

Perhaps the greatest challenge to hit the Financial Services Industry in recent years is the need to prove that everything it does complies with the raft of regulations and legislation that range from the everyday requirements of Customs and Excise for VAT returns through to the need to satisfy aggrieved customers that every possible step has been taken to protect and enhance their investments.

The operating climate is getting steadily tougher as new burdens are imposed, although regulatory control has always been a part of the financial services landscape, in recent years the legislation and regulations impacting the sector have increased dramatically.

Compliance is not just about FSA or BASEL II. In addition to these, the Data Protection Act, the USA PATRIOT Act, anti-terrorism and anti money laundering legislation are combining to put financial services organisations under extraordinary pressures to generate and deliver information that can prove they are not just well-governed, but squeaky-clean!



Audit trail

In addition the increasing volume of data that is generated by trading must not only be stored safely and protected, it must also be available for immediate access upon demand by the appropriate authorities. Not only can they demand the data, unless you can also deliver a complete audit trail of the events from its origination to its ultimate destruction of required, there is a growing tendency to suspect its probity.

As a result the financial services industry is now facing one of its greatest challenges – the ability to prove compliance. Trading contracts, financial management and risk are all key factors in proving compliance, and companies need not only to follow best practice, but also be able to prove they are doing so.

This White Paper, put together by three of the UK's leading experts in compliance requirements and methodologies sets out the background, identifies the areas where businesses can trip up, and suggests a range of practical policies and operations to ensure that when the regulators call, all will be in order.

The authors' names, plus their contact information is at the back of the paper.

Your legal obligations

In the UK many laws demand access to information about the interactions of businesses with their suppliers and customers. These include the Data Protection Act (DPA), the Anti-Terrorism, Crime and Security Act 2001, the Proceeds of Crime Act 2002, together with various Statutory Instruments driven from the EU and UN, the Companies Act 1985, the Insolvency Act 1986 and the Taxes Management Act 1970.

Additionally, the FSA imposes a raft of demands for auditability on the Financial Services sector, including the ability to show details of all and any transactions with each and every customer. Banks face the strictures imposed by the BASEL II accord that demand three year's worth of accurate record keeping so that by the end of 2006 financial institutions will be able to forecast accurately their liquidity and credit risks and be able to demonstrate their ability to survive a major business outage or terrorist attack.

For companies regulated overseas or with a US or foreign parent or correspondent company, the burden is even greater. SEC Regulations, Sarbanes-Oxley and a raft of legislation emanating from Europe and the US governing the auditability of research and manufacturing information, are adding to the daily demand for timely and accurate information.

But perhaps the most dramatic piece of legislation, in many ways the world's first globally enforceable law comes from the other side of the Atlantic in the form of the USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001). This all-embracing legislation, rushed through Congress in the immediate aftermath of September 11, demands that any bank or financial services company that has a correspondent account in the US, must hand over to the US treasury any customer records from any geography within seven days of the request, or face termination of the correspondent relationship. Failure to comply results in a fines of up to \$10,000 per day.

Although this somewhat draconian imposition of the Pax Americana, was introduced to have a serious impact on money laundering, thought to be a major source of funds for terrorist groups, but is also causing a lot of lost sleep among many citizens with interests in the established offshore havens!



Access to information

In addition to the legislative burden imposed by these various acts, organisations are also required to be able to instantly lay their hands upon a wealth of information to satisfy other bodies. This affects information ranging from the quarterly submission of VAT returns, through the way organisations conduct their personnel management, to complying with health and safety, disability discrimination and equal opportunity laws, as well as self-regulation.

Each of these acts or bodies imposes its own requirements for the retention periods of data, but compliance with one does not mean compliance with all. While common business practice may be that e-mails are held for one year, taxation authorities can demand data going back six.

From a litigation perspective, the general rule should be that any information that could be pertinent should be retained for as long as the possibility of litigation exists. For example, the right to bring a civil action based on breach of contract will lapse five years after the date of the relevant breach, unless court proceedings are commenced within that period. To be safe, a company should retain both the contract and ancillary documents for the period of the contract plus six years, or twelve years if the document is executed as a deed.

There are similar prescription and limitation rules in relation to claims for personal injury caused by negligence, which must be entered within three years, and product liability for which the period is ten years.

However, a company being investigated for a potential tax fraud by the Inland Revenue may be requested to produce documents going back as far as 21 years. Whilst the company may only be under an obligation to retain tax papers for six years, not being able to produce relevant documentation may prejudice its ability to defend itself during such an investigation.

Penalties for failing to comply

Many of the different statutes and regulations referred to in this briefing paper include sanctions for non-compliance, which may include fines and/or imprisonment, and may extend to the personal liability of directors, managers or other responsible officers of an organisation.

Failure to retain appropriate documentation may also lead to uncertainty regarding agreed contractual terms, or difficulties with responding to information requests under the DPA, or orders for discovery in court. Above all, organisations will be concerned with the risk to their reputations and commercial standing of any publicised failure to comply.

The basic premise behind BASEL II was to provide a safe indication of corporate security in the financial sector. The costs of failing to meet its requirements will be stringent, both financially, and in terms of the headlong rush by investors to move their equities away from any company found wanting!

The penalties for those organisations that fall foul of the US legislation are more severe and much more rapid. With the US feeling increasingly powerful on the world stage, any argument against its laws, is likely to be seen as unpatriotic and result in swift and summary justice – to the point of closure of the business!

Although the suggestion of corporate fraud does not occur widely, the risks to an executive of being brought to account for his or her company's behaviour are very real, particularly under legislation covering the way a business conducts its relationships with its employees and those about whom it holds data.

For example, Section 61 of the DPA provides that where an offence is committed by a body corporate and is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, any director, manager, secretary or officer, or any person who was purporting to act in any such capacity, that person as well as the body corporate shall be guilty of that offence.

Cutting through the legalese, this arguably means that anyone can be held personally to account for their organisation's actions if the buck stops on their shoulders!

No defence

The DPA creates a number of offences for which certain defences may be available, however, the defences vary according to the particular offence.

For example, it is an offence to fail to notify the Information Commissioner of changes to a register entry, unless it can be shown that all due diligence to comply with the duty was exercised. In contrast, the offences of processing without notification and enforced subject access are strict liability offences for which there are no defences.

Organisations are facing a massive growth in claims from dissatisfied personnel or customers. Hardly a day passes without headlines describing massive damages won by employees suing their former employers for some form of negligence or discriminatory

behaviour. In addition the Financial Services Ombudsman while currently unable to meet its own targets for delivering opinions on cases, estimates that to date less than 5% of those who could claim for damages as a result of pensions or endowment mis-selling have so far claimed. This suggests a veritable mountain of imminent claims.

These cases are won or lost on the weight of evidence. In this respect the organisation that can readily access all documents that are relevant to an action, and prove their validity, stands to be able to see an action dismissed or settled at a far earlier stage of what are inevitably costly proceedings. The means to be able to access company documents is the subject of much of the rest of this paper.

To delete or not to delete...

Is indeed an extremely cogent question. When is a document old and when is it still current? There is no easy answer to this dilemma, because the criteria vary substantially with the nature and content of each document. For example, an e-mail confirming a meeting will become history as soon as the meeting is past, but assuming the premiums continue to be paid, the original terms and conditions of a life insurance policy will remain valid until it pays out. If taken out early enough on the life insured, this could be several decades after they were issued. Traditionally, the storage of documents has been treated largely in terms of data rather than being driven by the content. However, the exponential growth in the volume of information now stored – analyst estimates range from 50% to 200%+ per annum – means that the practice of storing everything forever would place an intolerable demand on IT hardware budgets.



Policy-based retention

A more sustainable approach is to introduce policy-based retention. This calls for the setting of rules about how long a document should be stored and how accessible it needs to be. Such a policy will in turn help define the best place to store it. In many ways good retention policies reflect the best practices that used to be applied to the storage and archiving of paper documents, with the added advantage that the process can be automated.

In order to introduce policy-based data retention, organisations need to set up not just the appropriate hardware and management applications, but also management policies that can be laid down and followed throughout the organisation.

Even before the discussions around technology commence, the organisation needs to identify its business needs and how it uses documents. The expertise to conduct such an exercise rarely exists in-house, so a specialist market is developing with the arrival of experts who will advise organisations and work with them to help develop appropriate policies.

A word of caution – although there are many companies that offer to assist organisations with the development of storage policies to ensure compliance, it is a very complex process that requires an understanding not just of the infrastructure and application capabilities offered by the technology vendors, but also the way that the organisation works. As with so many good new ideas, there is a significant risk that ill-informed choices can end up becoming little more than expensive shelfware.

When developing a retention policy, there are a number of key considerations that must be borne in mind. Not least of these is the need for compliance with the various acts, statutes and industry regulators as already described.



Whose data is it?

One of the most complex issues faced by organisations setting out to manage data effectively is 'who owns the data?' This is always a tricky one – while individuals within an organisation will expect to be able to access any documents they have created or used, they will rarely be prepared to accept responsibility for their care and accessibility. Historically, an employee who finds a document missing would simply have turned to the IT manager and lambasted him about its loss!

Now, however, the various acts and regulations have given enforcement officers the ability to drill down to an individual level within an organisation, and take action against those who consented to, or connived in the commission of, an offence, or whose negligence caused the offence.

This gives rise to a potential minefield- while the law states that individuals must take care of the data they process, the employer should ensure that it does not place its staff in a position where they could be forced to break the law. A test case has yet to be heard, but any organisation storing documents electronically needs to take this issue very seriously.

To protect itself against legislative action, an organisation needs to have not just a nominated compliance officer, but also needs to ensure that he or she has the relevant authority and technical knowledge to be able to make sure that the needs of compliance are met. In much the same way as the last decade has seen the growth of Health & Safety Officers as a key aspect of risk management, so too will the importance of compliance grow in the next ten years.

The compliance officer's role is to ensure that the organisation enables the technology and processes to deliver auditable proof of compliance as a cornerstone of its defence in any action, whether criminal or civil.

Existing guidelines, such as ISO/IEC 17799 – an international standard on information security management, share many points of reference with compliance legislation. As an example, many of Basel II's operational risk principles can be met by having an ISO 17799 security policy.

If only we knew what it is we know...

Computer systems have no intelligence; to them there is no discernible difference between an e-mail about a meeting and a life policy – they are all simply data files. A solution needs to be introduced that can identify the type of data each file contains and the business rules that should attach to it covering ownership, retention, access rights and deletion.

There are many technology solutions that help to identify the content of a data file and describe it either by the file type, e.g. e-mail, graphic or text. There are also a number of more sophisticated applications that can also describe its content.

This latter approach, which uses a system of 'meta-tagging', is the technology that drives the Internet. It works by having a number of keywords that describe the content of each document in a hidden 'metadata' file that is part of the document, even though you would not normally see it. Internet search engines find documents by reading the metadata attached to them.

Metadata tagging is an effective system, because in addition to describing the document and its content, it can also be used to track the history of its creation, and any changes that have been made to it. To get an idea of how it works, call up an email on your PC and click "View Internet headers" under the 'Edit' tab. Although what now appears at the top of your email looks like something from Star Trek, it is in fact a step-by-step description of the route taken by that email on its journey around the Internet from the sender to you.

Classifying data

Fortunately there are now applications available that can help automate the whole process of identifying metatags and classifying documents by them, even allowing you to drill down and find out if their content has been altered without authority. This is particularly useful for legacy data that has never been near a website, so it is now possible to implement solutions that allow individual files to be identified by both structured and unstructured content.

This information is then used to support the organisation's storage management policy and can handle dramatic amounts of data – one of these systems is used by the New York Stock Exchange to track and record all share trades, and one credit card operator has logged and archived over 200 million transaction records in a single day using this type of application.

Unfortunately, although the implementation of these systems sounds like a miracle panacea to proving compliance, in reality there is a lot more detail that needs to be covered. Before being able to even answer a regulator's request for information, it is vital that an organisation can understand the nature and type of data that is being stored, and indeed how and when it is used.

A highly effective approach to identifying the data held by an organisation and establishing what it is and how to use it, is to extract a copy of the information held in the company's operational IT systems and pool it into a data warehouse. Once the data warehouse has been created, all the different types of information are held in a common format, regardless of their source. This common bank of data can then be used to supply any business intelligence or analytic application, and allows the company to achieve the holy grail of business intelligence – otherwise known as a 'single view of the truth'.

Efficiency gains

While building a data warehouse is an extremely detailed process, and can be equally laborious, recent innovations in ETL (Extract, Transform & Load) technology mean that once the process has been set up for one data source, such as sales records from IFAs, then as much as 80% of the donkey work of setting up a similar system for another part of the business can be saved by re-using the same methodology.

This represents a massive leap in efficiency and is achieved using a process known as CDC (Changed Data Capture), which extracts only the information that has changed in the source. To illustrate the effect of this, imagine your last credit card statement and how this would be used in a data warehouse. Using traditional ETL, every character on the statement would be captured by the application, making a bulky record. Using CDC, only the details of this month's transactions would be noted – potentially reducing the data extraction process by up to 90%.

Not only does this make for a very much faster operation that can reduce the need for batch data processing – one of the industry's biggest IT headaches, it also very effectively leverages the investment in the solution by applying it right across the business for a single licence fee, it also makes a significant contribution to reducing the need to store many multiple copies of similar data, in different forms for different applications.

This type of application also helps overcome one of the biggest challenges facing financial services organisations, that of being able to develop a single, and accurate picture, of all its dealings. It also delivers the ability to answer immediately any regulator's request for information. One company interviewed in the research for this paper pointed out that under FSA requirements they could be asked to produce information from 26 different IT systems in their organisation in order to be able to give a complete picture of their dealings with just one customer.

Given that each system, not only has its own unique way of identifying and describing its records, but is also held in a different vendor's database application, achieving this could be a task that would tie up an entire IT department for weeks – just to answer a single request!

However, while the data warehouse route offers one fast, clean and effective weapon in a company's compliance armoury, it also adds another overhead by creating a pool of data that needs to be stored electronically. This brings us on to the next question – where and how to hold data?

I know we've got that information somewhere

By far the greatest volumes of data are actually stored on individual machines, and often these are distributed around the organisation. This sort of widely distributed Directly Attached Storage (DAS) is extremely hard to manage, and most storage administrators dream of the day when they can finally wrest back all the hard disks used by the business and place them in a single, manageable environment!

Although any organisation talking to a storage vendor about putting in a two terabyte storage solution would be taken as a serious player, that is exactly the volume of storage available to an IT manager with 1,000 desktops or laptops on his network, boasting an average 20Gb disk on each one!

For policy-based retention to work, the storage solution has to ensure that distributed data is managed as efficiently as that on a centralised store, such as a Storage Area Network (SAN). The law is not mindful of the complexities of IT, it simply requires compliance, and woe betide those who don't achieve it.



SAN or NAS, Tape or Optical?

Many organisations now look at storage infrastructures in three sections. The first is the production environment, where speed of access and return of documents is business-critical. Storage technologies here are typically a combination of Direct Attached, SAN and Network Attached.

The second environment is the archive, where copies of all documents are kept, often in tape libraries or on optical disks, and from which data recovery is managed. Data recovery, by virtue of the technology, is invariably a much less rapid process than production, but the cost per gigabyte of tape is a fraction of that of hard disk, so it achieves a balance of cost and efficiency.


A third storage environment is the 'near store'. This is normally provided by lower cost hard disk arrays that do not offer the ultra-fast performance of a production system, but are blisteringly fast in comparison to restoration from tape. They are pitched midway between tape and production solutions in price.

They offer an ideal storage medium for large and infrequently accessed documents, or as a half-way house between production and archive, for example, storing e-mails in the three to six months after they have been sent, in case they become needed as part of an ongoing discussion.

Policy-based storage management allows an organisation to deploy all three storage environments in the most appropriate and cost-effective way.



Resilience – the key to compliance



Building resilience into your storage architecture is an essential consideration for meeting compliance requirements.

In hardware terms resilience can be achieved relatively easily through the mirroring of data between sites, and the use of best practices in keeping backup and disaster recovery processes up-to-date. A properly integrated storage environment, running policy-based retention, will give an organisation not just a trouble-free and sound platform to underpin its business, it will also give its IT manager the ability to sleep soundly at night!


Although total outages are a rare occurrence, data does get lost during routine operations and the challenge of maintaining business continuity now has the added complication of having to demonstrate compliance by ensuring that data is recovered and not corrupted.

There was much publicity around the shredding of documents during the Enron debacle. Although those brought to trial claimed they were simply shredding old documents, the prosecution was able to claim that the documents were cogent to the proceedings. In the absence of a complete set of corporate documents, the presumption of guilt rather than innocence became a lot easier to suggest, with the consequence that Enron immediately lost credibility in the eyes of the court.

Faced with a similar electronic situation an IT manager who has the ability to demonstrate recovery and security practices, and provide an audit trail that proves them, could find it prevents a minor event turning into the loss of a major litigation.



Standardising best practice



Much of the background to compliance legislation and regulation lies in the desire to standardise best practice and eliminate sharp practice. Although the US leads the way with Sarbanes-Oxley, SEC regulations and Food & Drug Administration (FDA) requirements, similar strictures, such as BASEL II, are being introduced continually in Europe.

In order to demonstrate compliance, an organisation may have to go to extraordinary lengths. For example, it may be required to not just produce a final version of a document, but also to show the stages and iterations it went through before it was completed. E-mail strings are now admissible evidence in support of contracts, as is tracking data drawn from website visits. Not only does this data have to be available it has to be capable of being demonstrated as valid, and not having been interfered with or amended in any way.

Our data is secure, so where's the risk?

In reality the risk is all around. While it is simple to look at the physical aspects of data security as a key to compliance, in reality one of the biggest issues facing the industry today is that of the risks associated with sharing data with other parties, and in particular with outsourced suppliers.

While the FSA has been extremely busy with its risk assessment programme, designed to reduce the risk faced by organisations that outsource business to other suppliers, particularly those offshore, now that much of this work is completed, the onus falls on the industry to ensure that the high standards demanded initially by the FSA are maintained.

Although in part this will be a matter of the enforceability of contracts, which can be difficult in overseas jurisdictions, it is also vital to remember that any outsourced service provider is subject to the same strictures for data management and security as a domestic operator. If the company outsourcing the work does not ensure that these are maintained, then they will be held just as liable as if they committed the breach themselves.



Managing offshore compliance

When services are transferred offshore, the importance of some typical outsourcing contractual terms increases. Ensuring quality through a proper service level regime almost goes without saying, however, it is important to translate the promises made by local suppliers when bidding for the contract into meaningful service levels focussing on performance in the areas important to the outsourcer's business objectives. This could be reinforced by a requirement for a parental guarantee or the posting of a performance bond with an English bank.

A comprehensive dispute resolution process provides an important alternative to slow external legal apparatus. Even force majeure clauses will need to take into account the reality of the situation within the offshore location where for example power outages may be commonplace. Offshore service providers can and often do allow the contract to be governed by English law with English courts having jurisdiction although such clauses may be subject to overriding local law.

A clear exit plan is important in all outsourcing relationships but of critical importance in an offshore outsourcing. It is unusual for the outsourcer to bring in-house services that have been outsourced offshore but the exit plan will need to provide for the appointment of an alternative service provider and the seamless transfer of the provision of the services to the alternative service provider (including the transfer of information and know-how), who will in most cases be a competitor of the outgoing service provider.

Business continuity and disaster recovery plans are another way in which the outsourcer can mitigate the risks of having his business operations performed in a country which is likely to be more prone to disaster than the outsourcer's home country so that, in the event of a disaster interrupting the services, they can be provided from a secondary location almost immediately with a minimal loss to service provision and standards..

A recent case of call centre operatives, apparently working for a credit card company, calling customers from its 'Delhi' call centre and asking for security sensitive information, highlights a major security risk. Apparently the company concerned does not have any outsourced operations in Delhi, but key customer details have made their

way into the hands of unscrupulous operators, with potentially serious consequences as trusting customers reveal their most secret security details.

Identity fraud is a major concern among the Metropolitan Police's Computer Crime Unit, in the words of their commander. "Once you have enough information to pass yourself off as a credit card holder, it is a very simple matter to obtain birth certificates, copies of utility bill statements, and even a passport, with very little chance of being caught." The current concern about terrorist attacks highlights the importance of effective data control.



Preventing security breaches

There are a number of ways an organisation can identify, track and prevent the unauthorised exchange of data. Technology that can monitor the content of e-mail and web transactions has been available for several years. These solutions search for certain words, sentences or phrases either in the subject, body or an attachment of an email and then follow an appropriate course of action depending on company policies. This may be simply to record the exchange or to hold the e-mail until it has been reviewed, or in some cases delete it. In this way, an organisation can see where confidential reports and data are being sent – and by whom.

The removal of confidential data on media, such as floppy disks, CDs and USB-based memory sticks, can also be tracked and monitored by specialist applications. These solutions sit on the desktop or laptop PC and can either prevent copying, or will log and encrypt data being transferred. The data can then only be read by another device with the same encryption software. Different levels of encryption can be set to allow different levels of authority.

Even the modification of files can be monitored, thanks to software that looks for changes in files, and then sends an alert to a security administrator. Being able to identify and record these security breaches is a key component in compliance.



Maintaining confidentiality

Because an organisation's data is the foundation of its intellectual property it is only natural that it be closely guarded using both physical security and encryption systems. However, the arrival of legislation such as the DPA places a further onus upon organisations by setting an obligation to destroy or anonymise any personal data, after the purposes for which it was originally stored have been satisfied.

Not only does this mean that security practices must be to a high level and auditable, both in terms of physical and digital security, but also that potentially confidential data is not accidentally exported.

The most frequent cause of this occurs when IT equipment is disposed of, either at the end of its life or when passed on. This could be to an employee or deserving cause supported by the organisation. Press reports of secret documents found in an old laptop usually follow a poorly managed disposal procedure.

This is another area where legislation is set to bite – in August 2004 an EU Directive covering the disposal of Waste Electrical and Electronic Equipment (WEEE) moves the onus to individual companies to ensure that their end-of-life equipment is recycled in an environmentally-friendly manner.

This will involve engaging a reliable, and also auditable, third party specialist contractor, part of whose service will be to prove that any data on hard disks has been completely erased with no possibility of recovery, even with the most efficient forensic tools.

Summary

Benefits of compliance

By implementing appropriate legal solutions, including a document retention policy, data security policy, information request policy, and IT hardware disposal policy, organisations can ensure that they are taking the necessary steps to address the legal, technical and commercial issues.

However, legal policies are only effective if combined with appropriate technical solutions, which manage electronic document retention to enable efficient storage, retrieval and destruction of data, and can also prove the authenticity and integrity of electronic documents.

This makes a strong case for organisations, both in the public and private sectors, to consider policy-based data management solutions. Appropriate solutions will not only achieve legal and regulatory compliance but also business benefits in the form of improved operational efficiency and reduced costs.

Questions to consider

There are some key points to consider when devising and implementing document retention policies:

- Does the compliance officer in your organisation have full executive authority to ensure that all necessary compliance measures have been implemented?
- How much does storage of electronic documents cost your organisation? What proportion of the documents stored is actually required to be retained for legal or commercial reasons? What proportion of the documents is actually unnecessary duplication? Do you have an appropriate document retention policy in place?
- Could your organisation respond to an information request from an individual for all documents including e-mails that you hold about them, as required under the DPA?
- Could your organisation be able to prove its risk position as required under BASEL II? Could you answer a request from the US treasury for a full breakdown of all activity on all the accounts worldwide held with you by a single customer within 7 days as required by the USA PATRIOT Act?
- Would your organisation be able to respond properly to a discovery request for documents to be submitted to a court in relation to a dispute, ensuring that only the required documents are disclosed and no others? What would be the cost to your business of processing such a request?
- Does your organisation have an appropriate Information Request Policy in place?
- Would your organisation be able to prove the authenticity and integrity of a retained e-mail vital to proof of contractual terms entered into? Are your IT systems able to provide this vital evidential weight?
- How does your organisation ensure data is destroyed? Is the data overwritten adequately? Are hard-drives cleaned upon return to a vendor, or physically destroyed? Does your organisation have an appropriate IT Hardware Disposal Policy in place?
- How resilient are your organisation's IT systems? Are there appropriate back-up and disaster recovery systems in place? How secure are they?

About the authors

Robert Courtneidge Partner, Osborne Clarke

Robert is a specialist IT partner, who has worked in the cards and payments systems arena since 1989, covering all aspects of consumer finance and the technology behind it. In particular, he focuses on areas such as bank cards, payment systems, consumer protection, data protection and information technology.

He has particular knowledge of recent data protection laws and data privacy forms an integral part of the advice he gives all his clients, whether they are UK based or multi-national.

He has worked in house for much of his career, initially for part of Lloyds TSB Group, then for Citibank in the UK. Since moving back to private practice, his client list ranges from major banks and card organisations to internet start-ups, call centres and ISP's. Robert joined Osborne Clarke as a Partner in July 2001.

Robert can be contacted by email: robert.courtneidge@osborneclarke.com

Simon Gay Information Infrastructure Practice Leader, Computacenter PLC

Simon Gay leads the storage practice of Computacenter, a specialist unit that advises organisations on the development of effective document retention policies and supplies infrastructure implementation and management services. As Europe's leading independent provider of IT infrastructure services, Computacenter has an unrivalled breadth and depth of knowledge which is used to help its customers maximise the value of IT to their businesses.

Computacenter's services cover every stage of infrastructure investment. The company can advise customers on their IT strategy, implement the most appropriate technology, from a wide range of leading vendors, and manage elements of their technology infrastructures on their behalf. At every stage Computacenter helps its customers minimise the cost and maximise the business value of their IT expenditure.

Simon's email is Simon_gay@computacenter.com

Phil Kane Senior Director, Field Services Europe, Informatica

Phil Kane has experience of integrating data warehousing solutions from both the vendor and user sides of the fence including working on a number of MIS projects for various council groups and charities in Greater London.

He moved to set up his own company offering training in both management information systems and data warehousing, serving multinational organisations, including Shell and other petrochemical giants.

After 14 years success in this enterprise Phil became one of Informatica's first senior consultants and has been the technical architect on many data warehouse and integration projects before going on to lead Field Services for the company throughout EMEA.

Phil can be contacted on 01628 511367, or by email at pkane@informatica.com

