

FEBRUARY 2008

Information Risk Management

---

Legal Compliance within  
the Financial Services Industry

CONFIDENTIAL

# Contents

---

<b>1.</b>	<b>Executive Summary</b>	<b>1</b>
1.1	Overview	1
1.2	Why is Information Risk Management important?	2
1.3	A holistic approach to information management	2
<b>2.</b>	<b>European laws for information handling in the financial services sector</b>	<b>4</b>
2.1	Overview	4
2.2	The legal framework for the financial services sector	6
2.3	The identity of the regulated entities	7
2.4	Table of core laws	7
2.5	The most important laws for the financial services sector	9
2.6	The Data Protection Directive	10
2.7	The Capital Requirements Directive (Basel II)	13
2.8	The Lamfalussy Directives	15
2.9	MiFID	16
2.10	The Market Abuse Directive	21
2.11	The Prospectus Directive	22
2.12	The Transparency Directive	23
2.13	The Anti Money Laundering Directive	23
<b>3.</b>	<b>Key IT projects for the Financial Services Industry</b>	<b>25</b>
3.1	Overview	25
3.2	Act in accordance with international standards	26
3.3	Implement Privacy Enhancing Technologies (“PETs”)	28
3.4	Protect the network perimeter	28
3.5	Protect records and data in storage	28
3.6	Protection of data in transit and in communications	30
3.7	Monitor and log all events	31
3.8	Identity management	31
3.9	Table showing IT projects by reference to core laws	31
<b>4.</b>	<b>Our Technology Law Group</b>	<b>34</b>
<b>5.</b>	<b>Contacts</b>	<b>35</b>

---

# Executive Summary

## 1.1 Overview

“Information Risk Management” follows the information’s path as it is created, distributed, stored, copied, transformed and interacted with throughout its lifecycle. This path provides a holistic view that enables organisations to develop a comprehensive risk mitigation strategy. This strategy ensures that information is an asset, not a liability, and it allows organisations to accelerate their business initiatives.

In others words Information Risk Management is a methodology that helps organisations to

- ▶ Secure business continuity.
- ▶ Meet regulatory and governance challenges.
- ▶ Expand into new markets.
- ▶ Improve customer confidence.
- ▶ Reduce the cost of doing business.

Information Risk Management encourages organisations to take a holistic approach to the management of information in which (1) the information lifecycle, (2) the risks threatening information and (3) the laws affecting information are all identified before strategic business decisions are taken. Critically, Information Risk Management enables organisations to understand and predict the impact and consequence of potential decisions: foresight facilitates better decision taking.

In this White Paper we address one of the key components of good information management, namely legal compliance as it affects the financial services sector within Europe. We will identify core laws of the European Union that affect the handling of information within this sector, where these laws require IT solutions. We will also identify core IT projects that are central to legal compliance.

## 1.2 Why is Information Risk Management important?

Nowadays it is hard to open a newspaper, turn on the television or radio or log-on to the WWW without hearing about yet another case of information mishandling, such as a data security breach or loss of data. Information mishandling is a very big news and governments all across the world have cottoned-on. In the United States, for example, the majority of States have introduced reporting of security breaches legislation<sup>1</sup>, a trend that is being picked-up in Europe<sup>2</sup>. Within the UK the pace of change is incredibly fast and it is now accepted across government that new criminal laws will be required to punish information mishandling<sup>3</sup>.

Of course, the financial services sector is not immune to cases of information mishandling, quite the contrary. The news of fraudulent trading at Société Générale is a story of global significance and it stands as yet another example of the fact that when information risk is ignored the consequences can be disastrous. Inevitably, Société Générale will lead to a further wave of legislation to improve information handling in the financial services sector.

There is another picture than can be painted to show why Information Risk Management is important: basically, there is substantial evidence to show that people, businesses and markets react favourably to good information handling. Organisations can turn a negative into a positive, in the same way that the motor industry now makes a virtue of safety features such as airbags, side impact bars, anti-lock brakes and high intensity braking lights; yes, cars do crash, so now marketers draw attention to the devices that have been implemented to reduce the risks! In the same way a point will soon be reached whereby organisations will make a substantial play of their Information Risk Management procedures.

## 1.3 A holistic approach to information management

A holistic approach to information management requires the enterprise to consider its information processes as a whole and to identify the risks existing throughout the information lifecycle. This marks a significant departure from the traditional “silo approach”, where information management is handled on a piecemeal basis.

---

<sup>1</sup> In January 2008 there were at least 13 reported security breach cases in the United States, all of which came to light as a result of the security breach legislation. See “Data Security: 13 Breaches Reported So Far This Month”, David Nagel, 25th January 2008.

[http://campustechnology.com/articles/57790\\_3/](http://campustechnology.com/articles/57790_3/)

<sup>2</sup> For example, in November 2007 the European Commission of the European Union adopted a proposal for a new Directive that will see the introduction of reporting of security breach obligations within the legal framework for publicly available communications networks and services.

[http://ec.europa.eu/information\\_society/policy/ecomms/doc/library/proposals/697/com\\_2007\\_0697\\_en.pdf](http://ec.europa.eu/information_society/policy/ecomms/doc/library/proposals/697/com_2007_0697_en.pdf)

<sup>3</sup> See “The Protection of Private Data”, the first report of the House of Commons Justice Committee for session 2007-08, 3rd January 2008.

<http://www.publications.parliament.uk/pa/cm200708/cmselect/cmjust/154/154.pdf>

A holistic approach to information management recognises that information is central to the enterprise and that its handling encompasses many different purposes, requirements and uses throughout its lifecycle. A holistic approach also recognises that the value of information to the enterprise changes over the course of the information lifecycle; the value of information is never static.

In distinction, the silo approach to information management focuses on small components of the information lifecycle in isolation, perhaps information handling to satisfy the needs of one particular business unit, or one geographical area of business, or one specific business development strategy.

The holistic approach recognises - and helps to eliminate - the considerable disadvantages within the silo approach; the holistic approach recognises that very often there are downstream consequences of information handling for any given purpose. For example, the holistic approach will recognise that information handling for direct marketing purposes may carry with it wider consequences in terms of compliance with European data protection laws, which, in turn, imposes obligations concerning information security, storage and retention. Or, for example, the holistic approach will recognise that information handling within the foreign subsidiaries of a US company may result in legal obligations in the US under the Sarbanes-Oxley Act, which, in turn, imposes obligations concerning the quality of records-keeping for auditing and financial reporting purposes. Or, for example, the holistic approach will recognise the ever-present risk of litigation within commercial activity, which, in turn, imposes disclosure and discovery obligations in respect of documents.

Organisations that continue with the traditional silo approach to information management – particularly those operating in the financial services sector and on the international stage – run the risk of being found non-compliant with the multitude of laws that impose obligations in respect of security and management of information. The silo approach also involves a “risk of ignorance”; if the organisation is unable to see past the silo it can never know if its information lifecycle is fully compliant in other areas.

Unfortunately, there is considerable evidence that the silo approach is still the norm in the financial services sector, which, in these days of global tightening of credit, increased regulation and increased political and public concern, cannot be acceptable.

# 2

---

## European laws for information handling in the financial services sector

### 2.1 Overview

The European Union has long been engaged on a process of harmonisation of national laws concerning the financial services sector. These laws impose concrete information handling obligations upon regulated entities. They also impose obligations on how regulated entities run their operations. The core objectives of these laws are:

- ▶ Furtherance of the Internal Market in Europe for financial services.
- ▶ Enhancing the stability of the financial services sector.
- ▶ Protecting the interests of investors and customers and promoting confidence.

Without doubt, these laws implicitly require regulated entities to adopt a holistic approach to their information handling.

Naturally, many of these harmonising laws impact on IT. However, there is a distinct reluctance within Europe to the setting of detailed rules for IT. For example, in 2002 the European Commission issued a series of very detailed harmonising Directives in order to further the Internal Market in electronic communications networks and services. These laws are obviously “IT-centric” and yet they preferred to remain neutral on technological issues. Indeed, the “Framework Directive”<sup>4</sup> emphasised that EU Member States should:

*“ensure that national regulatory authorities take the utmost account of the desirability of making regulation technologically neutral, that is to say that it neither imposes nor discriminates in favour of the use of a particular type of technology”.*

---

<sup>4</sup> Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services.  
[http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l\\_108/l\\_10820020424en00330050.pdf](http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_108/l_10820020424en00330050.pdf)

The main ways in which European Union laws for the financial services sector affect IT use are shown in the table below:

How EU laws for the financial service sector affect IT use	
Effect	Commentary
Robust systems	Financial Services Institutions must have robust systems for doing business, which can withstand disaster, criminal activity and negligent and accidental negative effects. As business relies upon IT, the requirement for robust systems means that regulated entities must implement an appropriate level of security to protect their IT networks and data.
Records keeping	Financial Services Institutions are required to keep full and proper records of their activities. As the majority of records are nowadays held electronically, this requires regulated entities to implement data storage solutions with appropriate security features.
Transparency	Financial Services Institutions are required to deliver-up information about their activities to their regulatory bodies, to the markets, to their shareholders and to their customers. This requires the implementation of systems that will deliver the required information within the required timeframes. Again, due to the predominance of electronic data, appropriate implementing IT is required.
Privacy and data protection	Financial Institutions are required to comply with data protection laws, which protect the privacy of personal information undergoing processing. These laws mainly concern electronic data about individuals and they impose specific obligations that impact upon IT, for instance a requirement for an appropriate level of security to keep data safe from unlawful access and loss and damage.

Thus, it can be authoritatively stated that the European Union has legislated for informational security in the financial services sector. However, compliance with these laws cannot be achieved without a holistic approach to information management, one that puts the information lifecycle at the heart of the enterprise's concerns.

## 2.2 The legal framework for the financial services sector

The European Union promotes “an overarching policy and strategy in financial services and financial markets” that “ensures coherence and consistency between the various policy areas, such as banking, insurance, securities and investment funds, financial markets infrastructure, retail financial services and payment systems.”<sup>5</sup> It does this through long term policy frameworks; the “Financial Services Action Plan” set the agenda for 1999 to 2005. The current agenda is contained in the “White Paper on Financial Services Policy”, which covers the period 2005 to 2010. The current agenda continues the previous one.

Regulated entities need to familiarise themselves with both documents to fully understand the nature of the obligations they face now and in the future. The core strategic objectives of the Financial Services Action Plan and the White Paper are shown in the table below.

Core objectives of EU Action Plan and White Paper for financial services policy, 1999-2010	
Action Plan 1999-2005	White Paper 2005-2010
Ensuring a wholesale Internal Market within Europe for financial services.	Dynamically consolidating progress already made and ensuring sound implementation of existing rules.
Open and secure retail markets.	Driving through better regulation principles into all policy making.
State of the art prudential rules and supervision.	Enhanced supervisory convergence.
	Creating more competition between service providers, especially those operating in retail markets.
	Expanding the EU's external influence in globalizing capital markets.

<sup>5</sup> [http://ec.europa.eu/internal\\_market/finances/index\\_en.htm](http://ec.europa.eu/internal_market/finances/index_en.htm)

## 2.3 The identity of the regulated entities

The EU's regulatory framework applies to three core areas, (1) banking, (2) insurance and (3) securities. The framework extends to retail financial services, occupational pensions and payment services. It also addresses financial markets infrastructure, financial conglomerates and financial malpractice.

## 2.4 Table of core laws

The table below identifies the core EU laws applicable to the financial services sector within Europe (excluding insurance<sup>6</sup>) that are considered in this White Paper. It should be immediately apparent from the length of this table that the financial services sector is very highly regulated.

All of these laws impact upon the handling of information to a greater or lesser extent. As such, where they concern electronically held information they will require considered strategies for IT which, of course, should take account of informational security at all times.

This in itself justifies the adoption of a holistic approach to information management within this sector.

Core EU laws for the financial services sector (excluding insurance)	
Banking laws	Concerning
Directive 2000/46/EC of the European Parliament and of the Council of 18.9.2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions	Capital Requirements etc
Directive 2002/87/EC of the European Parliament and of the Council of 16.12.2002 on the supplementary supervision of credit institutions, insurance undertakings and investment firms in a financial conglomerate	Capital Requirements etc
Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions	Capital Requirements etc
Directive 2006/49/EC of the European Parliament and of the Council of 14 June 2006 on the capital adequacy of investment firms and credit institutions	Capital Requirements etc

<sup>6</sup> The numbers of insurance laws are such that they will require consideration in a separate White Paper.

### Securities and investment funds laws

Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation (market abuse)	Market Abuse
Directive 2003/71/EC of the European Parliament and of the Council of 4 November 2003 on the prospectus to be published when securities are offered to the public or admitted to trading and amending Directive 2001/34/EC	Prospectuses
Commission Directive 2003/124/EC of 22 December 2003 implementing Directive 2003/6/EC of the European Parliament and of the Council as regards the definition and public disclosure of inside information and the definition of market manipulation	Market Abuse
Commission Directive 2003/125/EC of 22 December 2003 implementing Directive 2003/6/EC of the European Parliament and of the Council as regards the fair presentation of investment recommendations and the disclosure of conflicts of interest	Market Abuse
Commission Regulation (EC) No 2273/2003 of 22 December 2003 implementing Directive 2003/6/EC of the European Parliament and of the Council as regards exemptions for buy-back programmes and stabilisation of financial instruments	Market Abuse
Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC	MiFID
Commission Directive 2004/72/EC of 29 April 2004 implementing Directive 2003/6/EC of the European Parliament and of the Council as regards accepted market practices	Market Abuse
Commission Regulation (EC) No 809/2004 of 29 April 2004 implementing Directive 2003/71/EC of the European Parliament and of the Council as regards information contained in prospectuses as well as the format, incorporation by reference and publication of such prospectuses and dissemination of advertisements	Prospectuses
Directive 2004/109/EC of the European Parliament and of the Council of 15 December 2004 on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and amending Directive 2001/34/EC	Transparency
Directive 2006/31/EC of the European Parliament and of the Council of 5 April	MiFID

2006 amending directive 2004/39/EC on markets in financial instruments, as regards certain deadlines	
Commission Decision of 4 December 2006 on the use by third country issuers of securities of information prepared under internationally accepted accounting standards	Transparency
Commission Regulation (EC) No 1787/2006 of 4 December 2006 amending Commission Regulation (EC) 809/2004 implementing Directive 2003/71/EC of the European Parliament and of the Council as regards information contained in prospectuses as well as the format, incorporation by reference and publication of such prospectuses and dissemination of advertisements	Prospectuses
Commission Directive 2007/14/EC of 8 March 2007 laying down detailed rules for the implementation of certain provisions of Directive 2004/109/EC on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market	Transparency
Commission Recommendation of 11 October 2007 on the electronic network of officially appointed mechanisms for the central storage of regulated information referred to in Directive 2004/109/EC of the European Parliament and of the Council	Transparency
Commission Regulation (EC) No 1569/2007 of 21 December 2007 establishing a mechanism for the determination of equivalence of accounting standards applied by third country issuers of securities pursuant to Directives 2003/71/EC and 2004/109/EC of the European Parliament and of the Council	Transparency
<b>Financial crime laws</b>	
Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing	Money Laundering
Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis	Money Laundering

The effect of some of these laws is discussed below.

## 2.5 The most important laws for the financial services sector

The most important laws for the financial services sector which impact upon information security are:

- ▶ The Data Protection Directive.
- ▶ The Capital Requirements Directive.
- ▶ The Lamfalussy Directives.
- ▶ The Anti-Money Laundering Directive.

## 2.6 The Data Protection Directive

The principal EU law impacting upon information handling is the Data Protection Directive of 1995<sup>7</sup>. This Directive contains an express security dimension.

### (a) Aims and objectives

The Data Protection Directive regulates the “processing” of “personal data” by “controllers”, in order to achieve two objectives, namely (1) the protection of fundamental rights and freedoms, particularly privacy and (2) to maintain the free flow of personal data around Europe. The core focus of the Directive is the processing of electronic personal data by computers and computer-controlled equipment.

### (b) Application and reach

The Data Protection Directive’s application extends much further than the financial services sector; basically every company, public body and third sector organisation is regulated by the Data Protection Directive as a “controller”, making it one of the most important laws in the entire history of European law. However, the processing of personal data within the financial services sector is of enhanced concern within Europe, due to the importance of the financial services sector to the European economy and the fact that failure of data protection in this sector carries with it the potential for significant harm to be caused to the individuals concerned and wider public confidence.

### (c) The role of regulators

Furthermore, it is important to recognise that the regulation of data processing within the financial services sector is significantly enhanced when compared to the state of regulation in many other sectors. To explain, under the Data Protection Directive EU Member States are obliged to appoint independent data protection regulators; in the UK the independent regulator is called the Information Commissioner. However, EU financial services legislation also requires its own national regulators; in the UK the independent regulator is called the Financial Services Authority. Due to the connection between failure of data protection and financial crimes, such as “identity theft”, financial services

---

<sup>7</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

institutions face dual regulation of data protection. To illustrate, in the UK in 2007 two very well known financial services institutions were fined considerable sums of money by the Financial Services Authority for failure of data protection on the ground that this gave rise to a risk of financial crime; in February 2007 the Nationwide Building Society was fined £980,000<sup>8</sup> and in December 2007 Norwich Union Life was fined £1.26m<sup>9</sup>.

#### **(d) Principles of data protection**

At the heart of the Data Protection Directive are a series of principles which, when taken collectively, point firmly to the need for a holistic Information Risk Management strategy. These principles say that personal data must be:

- ▶ Processed fairly and lawfully.
- ▶ Processed for a specified purpose.
- ▶ Adequate, relevant and not excessive.
- ▶ Accurate and, where necessary, kept up to date.
- ▶ Retained only for as long as is necessary.
- ▶ Processed in accordance with the rights of the individual concerned.
- ▶ Kept safe and secure.
- ▶ Not be transferred to countries outside of Europe that do not provide adequate protection.

#### **(e) Data security**

Article 17 of the Directive deals with security saying:

*“1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.*

*Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.*

---

<sup>8</sup> <http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/021.shtml>

<sup>9</sup> <http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/130.shtml>

2. *The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.*

3. *The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:*

*- the processor shall act only on instructions from the controller,*

*- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.*

4. *For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.”*

There are two operative elements within Article 17 that are worth drawing out:

- ▶ The technical security measures must be “appropriate”. This requires the controller to have regard to the nature of the personal data, the harm that could result from a security breach and whether the data are transmitted through a network.
- ▶ The controller must have regard to the “state of the art”. This means that the controller must keep up to date with advances in technology.

It clearly follows that controllers must constantly keep their networks and systems safe from internal and external threats to data. The Directive also recognises that the security of data is affected by the users of networks and systems. Thus, for example, the seventh data protection principle within the UK’s Data Protection Act 1998 (which transposes the Directive into UK law) is accompanied by an interpretation section that obliges controllers to check the reliability of their employees:

*“The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.”<sup>10</sup>*

Checking the reliability of employees may often require ongoing monitoring of their activities and the law has made provision for this fact. For example, UK Regulations<sup>11</sup> permit employers to monitor their workers’ communications in defined circumstances. Similarly, the UK’s Information Commissioner has

---

<sup>10</sup> Data Protection Act 1998, Schedule 1 Part II para. 10.

<sup>11</sup> The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. <http://www.opsi.gov.uk/si/si2000/20002699.htm>

recognised the validity of workplace monitoring in his Employment Practices Code<sup>12</sup>. Very often a vital component of effective workplace monitoring will be the monitoring of the network activity and behaviour of employees, which will require specific IT solutions.

#### **(f) Data protection and the information lifecycle**

At the very heart of compliance with the Data Protection Directive is an understanding of the information lifecycle. If the enterprise does not understand the information lifecycle then it cannot hope to be confident that its processing activities satisfy the principles identified above. To repeat, data protection requires a holistic strategy that places an understanding of the information lifecycle at the very top of the corporate agenda.

## **2.7 The Capital Requirements Directive (Basel II)**

### **(a) Overview – relationship with Basel II**

In 1988 the Basel Committee on Banking Supervision adopted the Basel Capital Accord (Basel I), which was aimed at strengthening the international banking system through higher capital requirements. Basel II<sup>13</sup>, adopted in 2004, continues this agenda with the introduction of a more detailed focus on risk and a widening of disclosure rules.

### **(b) Transposition of Basel II into EU law**

Within the European Union Basel II has been implemented by the “Capital Requirements Directive” (“the CRD” for short). However, it is important to note that when people speak about the Capital Requirements Directive they are actually referring to two EU legal instruments:

- ▶ 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions. In the UK this is often called “The Banking Consolidation Directive”.
- ▶ Directive 2006/49/EC of the European Parliament and of the Council of 14 June 2006 on the capital adequacy of investment firms and credit institutions. In the UK this is referred to as “The Capital Adequacy Directive”.

It should also be noted that the CRD extends further than Basel II, covering investment firms as well as credit institutions (banks are considered to be credit institutions for these purposes).

---

<sup>12</sup>

[http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/employment\\_practices\\_code.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/employment_practices_code.pdf)

<sup>13</sup> <http://www.bis.org/publ/bcbs128.pdf>

### (c) Aims and objectives

The CRD's overriding priorities are the stability of the banking and financial system and the furtherance of the Internal Market for banking and investment services. Key components include:

- ▶ Home country regulation and mutual recognition.
- ▶ The implementation of new rules for taking up and pursuing banking services.
- ▶ The implementation of new procedures for the regulation of credit institutions and investment firms, called prudential supervision.
- ▶ The introduction of new methods for calculating risk. The level of risk faced by an organisation will determine the size of its capital reserves.
- ▶ The CRD identifies three kinds of risk (i) credit risk, (ii) market risk and (iii) operational risk.

### (d) Operational risk

"Operational risk" is defined in Directive 2006/48/EC as "the risk of loss resulting from inadequate or failed processes, people and systems or from external events, and includes legal risk". Recital 45 to Directive 2006/48/EC identifies the connection between risk and capital reserves, saying that "operational risk is a significant risk faced by credit institutions requiring coverage by own funds". Article 102 of Directive 2006/48/EC explains how operational risk will be regulated, stating that national regulators "shall require credit institutions to hold own funds against operational risk".

It will be obvious that the definition of operational risk extends to IT systems. From this it is easy to deduce that poor IT systems can increase risk and that good systems can reduce risk. Thus, good IT systems can minimise the capital requirements for banks and investment firms, increasing their liquidity<sup>14</sup>.

Similarly, it will be appreciated that IT has a very important role to play in the assessment and calculation of credit risk and market risk. IT also has a significant role to play in records management, with records management playing a key role in prudential supervision.

The following matters should be noted:

- ▶ Directive 2006/48/EC requires national regulators to ensure that "every credit institution have robust governance arrangements, which include a clear

---

<sup>14</sup> For the calculation of funds that must be held against operational risk, see Annex X of Directive 2006/48/EC. This gives organisations three choices for calculating own funds, the "basic indicator approach", the "standardised approach" and the "advanced measurement approach". The organisation will select the approach that is financially in its interests.

organisational structure with well defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks it is or might be exposed to, and adequate internal control mechanisms, including sound administrative and accounting procedures.”

- ▶ Directive 2006/48/EC provides banks with three choices for calculating operational risk, (i) the basic indicator approach, (ii) the standardised approach and (iii) the advanced measurement approach. The first two approaches result in a capital requirement based on a percentage of business turnover. The advanced measurement approach allows banks to use their own risk models.
- ▶ The advanced measurement approach may be preferred by a bank as it can result in a lower capital requirement than the other approaches. However, before a bank can take advantage of the advanced measurement approach it must be able to satisfy the standards in Annex X Part 3. These include an ability to capture all loss data. Loss data for these purposes extends to business disruption and systems failure “event-types”.
- ▶ Annex V to Directive 2006/48/EC, paragraph 13 says that “contingency and business continuity plans shall be in place to ensure a credit institution’s ability to operate on an ongoing basis and limit losses in the event of severe business disruption”.

The rewards for banks that reduce risk are significant; in simplistic terms they are required to hold less capital, meaning they can lend more money and thereby earn greater profits. Similarly, investment firms’ liquidity is increased through the control of risk

Banks and investment firms have reviewed their IT strategies as a result of the CRD and they will continue to do so. Indeed, in light of the recent international stock market turmoil which stems at least in part from a failure of risk assessment within the US sub-prime mortgage market, banks and investment firms will be further incentivised to review their IT strategies. During their review they should adopt a holistic approach, taking full account of the information lifecycle.

## **2.8 The Lamfalussy Directives**

The Lamfalussy Directives are at the heart of the EU Financial Services Action Plan for 1999 to 2005. They are:

- ▶ MiFID.
- ▶ The Market Abuse Directive.
- ▶ The Prospectus Directive.
- ▶ The Transparency Directive.

The European Commission summary of the effect of these Directives is as follows:

*“All four are crucial pieces of legislation, which form an essential part of the Commission’s Financial Services Action Plan.*

*The Directive on Markets in Financial Instruments, for example, creates an effective “single passport”, which will allow investment firms to operate across the EU whilst ensuring a high level of protection for investors. The Market Abuse Directive aims to prevent insider dealing and market manipulation. This is essential, if investor confidence is to be maintained.*

*The Transparency Directive is also important for investor confidence. It sets out uniform rules for the disclosure of accurate, comprehensive and timely information by issuers throughout the EU. The Prospectus Directive, meanwhile, provides issuers (including SMEs) with a “single passport”, which will allow them to raise investment capital on a pan-European basis. This will allow them to “shop around” seeking out the cheapest capital available to them.”*

## **2.9 MiFID**

### **(a) Overview**

MiFID stands for the “Market in Financial Instruments Directive”. However it is important to note that when people speak about MiFID they will be referring to three EU legal instruments, namely:

- ▶ Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC.
- ▶ Commission Directive 2006/73/EC of 10 August 2006 implementing Directive 2004/39/EC of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive.
- ▶ Commission Regulation (EC) No 1287/2006 of 10 August 2006 implementing Directive 2004/39/EC of the European Parliament and of the Council as regards recordkeeping obligations for investment firms, transaction reporting, market transparency, admission of financial instruments to trading, and defined terms for the purposes of that Directive.

Directive 2004/39/EC is sometimes called the “Level 1 Directive”. Directive 2006/73/EC is sometimes called the “Level 2 Directive”. Regulation 1287/2006 is sometimes called the “Level 2 Regulation”.

## (b) Scope

Directive 2004/39/EC applies to (i) investment firms, (ii) regulated markets and, to a limited extent, (ii) authorised credit institutions providing one or more investment services and/or performing investment activities.

Insurance undertakings, collective investment undertakings and pension funds are excluded from regulation.

The financial instruments that are regulated are listed in Annex I Section C of Directive 2004/39/EC. These include:

- ▶ Transferable securities.
- ▶ Money-market instruments.
- ▶ Units in collective investment undertakings.
- ▶ Various options, futures, swaps, forward rate agreements and other derivative contracts.
- ▶ Derivative instruments for the transfer of credit risk.
- ▶ Financial contracts for differences.

The investment services and activities that are regulated in respect of these instruments are listed in Annex I Section A to Directive 2004/39/EC, which are:

- ▶ Reception and transmission of orders in relation to one or more financial instruments.
- ▶ Execution of orders on behalf of clients.
- ▶ Dealing on own account.
- ▶ Portfolio management.
- ▶ Investment advice.
- ▶ Underwriting of financial instruments and/or placing of financial instruments on a firm commitment basis.
- ▶ Placing of financial instruments without a firm commitment basis
- ▶ Operation of Multilateral Trading Facilities.

Additionally, certain “ancillary services” are regulated as listed in Annex I Section B to Directive 2004/39/EC:

- ▶ Safekeeping and administration of financial instruments for the account of clients, including custodianship and related services such as cash/collateral management.

- ▶ Granting credits or loans to an investor to allow them to carry out a transaction in one or more financial instruments, where the firm granting the credit or loan is involved in the transaction.
- ▶ Advice to undertakings on capital structure, industrial strategy and related matters and advice and services relating to mergers and the purchase of undertakings.
- ▶ Foreign exchange services where these are connected to the provision of investment services.
- ▶ Investment research and financial analysis or other forms of general recommendations relating to transactions in financial instruments.
- ▶ Services related to underwriting.
- ▶ Investment services and activities as well as ancillary services of the type included under Section A or B of Annex I related to certain underlying derivatives where these are connected to the provision of investment or ancillary services.

**(c) Aims and objectives**

MiFID's overriding priorities are the protection of the investor and the upholding of the integrity and overall efficiency of the financial system.

Key components include:

- ▶ Home country regulation – This principle means that those engaged in the supply and servicing of financial instruments and related advice will be able to trade on a pan-European basis if their activities are lawful in their home countries.
- ▶ The implementation of new best execution rules – These obligations are designed to ensure that investment firms execute client orders on terms that are most favourable to the client.
- ▶ The implementation of new pre and post-trade transparency rules – These obligations are designed to further the overriding priorities.
- ▶ The implementation of new client reporting rules – Again, these obligations are designed to further the overriding priorities.

**(d) Key provisions impacting upon information handling and IT**

Directive 2004/39/EC contains many obligations that impact upon information handling and IT:

- ▶ Recitals 43, 46 and 62 require regulated parties and national regulators to comply with the Data Protection Directive. The Data Protection Directive is analysed above.

- ▶ Recital 63 refers to a professional secrecy rule, to be complied with during data transmissions between national regulators.
- ▶ Article 12.6 requires investment firms to “arrange for records to be kept of all services and transactions undertaken by it which shall be sufficient to enable the competent authority to monitor compliance with the requirements under this Directive, and in particular to ascertain that the investment firm has complied with all obligations with respect to clients or potential clients.”
- ▶ Article 13.5 requires investment firms to “have sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for information processing systems.”
- ▶ Article 13.6. requires investment firms to “arrange for records to be kept of all services and transactions undertaken by it which shall be sufficient to enable the competent authority to monitor compliance with the requirements under this Directive”.
- ▶ Article 25.2. requires “investment firms to keep at the disposal of the competent authority, for at least five years, the relevant data relating to all transactions in financial instruments which they have carried out”. These records must comply with anti money laundering rules also.
- ▶ Article 50 gives national regulators a right of access to records, including telephone and data traffic records.
- ▶ Article 55.1.(c) obliges auditors to report any failures of records keeping.

The Level 2 Directive (Directive 2006/73/EC) includes the following records keeping obligations:

- ▶ Article 5.1.(f) requires investment firms to “maintain adequate and orderly records of their business and internal organisation”.
- ▶ Article 5.2 requires investment firms to “establish, implement and maintain systems and procedures that are adequate to safeguard the security, integrity and confidentiality of information, taking into account the nature of the information in question.”
- ▶ Article 6.3.(a), which deals with compliance functions, requires compliance to have access to all relevant information.
- ▶ Article 10 requires investment firms to “establish, implement and maintain effective and transparent procedures for the reasonable and prompt handling of complaints received from retail clients or potential retail clients, and to keep a record of each complaint and the measures taken for its resolution.”
- ▶ In order to prevent conflicts of interest, Article 12.2.(b) requires investment firms using outsourcing services to ensure that the outsourcing provider

keeps records of all personal transactions entered into by certain relevant persons.

- ▶ For the purposes of safeguarding client assets Article 16.1.(a) requires investment firms to “keep such records and accounts as are necessary to enable them at any time and without delay to distinguish assets held for one client from assets held for any other client, and from their own assets”. Article 16.1.(f) says that “they must introduce adequate organisational arrangements to minimise the risk of the loss or diminution of client assets, or of rights in connection with those assets, as a result of misuse of the assets, fraud, poor administration, inadequate record-keeping or negligence.”
- ▶ Article 19.2. says that “the records of the investment firm shall include details of the client on whose instructions the use of the financial instruments has been effected, as well as the number of financial instruments used belonging to each client who has given his consent, so as to enable the correct allocation of any loss.”
- ▶ Article 23 says that investment firms must “keep and regularly to update a record of the kinds of investment or ancillary service or investment activity carried out by or on behalf of the firm in which a conflict of interest entailing a material risk of damage to the interests of one or more clients has arisen or, in the case of an ongoing service or activity, may arise.”
- ▶ Article 47.1.(b) says that client orders must be executed promptly and “accurately recorded and allocated”.
- ▶ Article 51 sets a minimum five year retention period, but those records which set out the rights and obligations of the investment firm must be kept for the length of the client relationship, if longer.
- ▶ Article 51.2 prescribes the records managements standards which are (1) the competent authority must be able to access them readily and be able to reconstitute each key stage of the processing of each transaction, (2) it must be possible for any corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained and (3) it must not be possible for the records otherwise to be manipulated or altered.

The Level 2 Regulation (Regulation 1287/2006) provides even more detail about the records keeping obligations facing investment firms. Notable obligations include:

- ▶ Recital 4 addresses the systems for the reporting of transactions to national regulators. The objective is to “ensure that a single data set is collected from all investment firms with a minimum of variation between Member States, so as to minimise the extent to which businesses operating across borders are subject to different reporting obligations, and so as to maximise the proportion of data held by a competent authority that can be shared with other competent authorities.”

- ▶ Article 7 prescribes the information that should be recorded in respect of “every order received from a client, and in relation to every decision to deal taken in providing the service of portfolio management”.
- ▶ Article 8 prescribes the information that should be recorded after the execution of a transaction.
- ▶ In respect of reporting of transactions to national regulators, Article 12 says that these reports shall be made electronically. The systems for reporting must ensure the security and confidentiality of the data reported, incorporate mechanisms for identifying and correcting errors in a transaction report, incorporate mechanisms for authenticating the source of the transaction report and include appropriate precautionary measures to enable the timely resumption of reporting in the case of system failure.
- ▶ Article 24 requires investment firms to keep records of their quoted prices for no less than 12 months.

#### **(e) Summary of impact**

In summary MiFID contains the following key obligations which impact upon information handling and IT:

- ▶ Trading systems are electronic and they need to be protected from threats to them. These systems should be capable of delivering information on events that occur within the network.
- ▶ The obligation to keep records requires the implementation of an IT strategy that preserves the integrity of data.
- ▶ The obligation to report transactions to national regulators in an electronic format needs safe and secure communications systems.
- ▶ Investment firms must comply with the Data Protection Directive, which contains specific security provisions and many indirect security and records keeping provisions.

In conclusion, it is inevitable that as a result of MiFID regulated persons will have to review their IT strategies, adopting a holistic approach.

## **2.10 The Market Abuse Directive**

The Market Abuse Directive consists of four Directives<sup>15</sup> and one Regulation<sup>16</sup>. The 2003 Framework Directive observes that:

---

<sup>15</sup> Directives 2003/6/EC, Directive 2003/124/EC, Directive 2003/125/EC and Directive 2004/72/EC.

<sup>16</sup> Regulation (EC)2273/2003.

*“An integrated and efficient financial market requires market integrity. The smooth functioning of securities markets and public confidence in markets are prerequisites for economic growth and wealth. Market abuse harms the integrity of financial markets and public confidence in securities and derivatives.”*

The Framework Directive goes on to identify market abuse as consisting of insider dealing and market manipulation. It also identifies the role of technology within market abuse:

*“New financial and technical developments enhance the incentives, means and opportunities for market abuse: through new products, new technologies, increasing cross-border activities and the Internet.”*

Insider dealing results from having insider information, which is defined as “information of a precise nature which has not been made public, relating, directly or indirectly, to one or more issuers of financial instruments or to one or more financial instruments and which, if it were made public, would be likely to have a significant effect on the prices of those financial instruments or on the price of related derivative financial instruments”. The Framework Directive prohibits the use of insider information and in order to be able to “police” the prohibition it requires regulated entities to (1) disclose insider information in their possession to the public as soon as possible and (2) supply their national regulators within a list of all those people within their organisations who have access to insider information.

Directive 2003/124/EC expands upon the Framework Directive with the primary purpose of clarifying the information that must be released to the general public; if a “reasonable investor” would be likely to use the information as part of their investment decision taking then the information must be disclosed “in a manner which enables fast access and complete, correct and timely assessment of the information by the public”, unless the information falls within one of the narrow categories of that which can be withheld.

Naturally, before a regulated entity can form a conclusion about insider information it needs to understand the entirety of the information it possesses and how it is used and accessed, which requires the entity to adopt a holistic approach to its analysis with the information lifecycle at its heart.

## **2.11 The Prospectus Directive**

The framework Directive for prospectuses is Directive 2003/71/EC. It harmonises the requirements “for the drawing up, approval and distribution of the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market situated or operating within a Member State”.

Directive 2003/71/EC requires the issuing of a prospectus when an offer of securities is made to the public and when securities are to be admitted to a regulated market for trading. Article 5 says that:

*“the prospectus shall contain all information which, according to the particular nature of the issuer and of the securities offered to the public or admitted to trading on a regulated market, is necessary to enable investors to make an informed assessment of the assets and liabilities, financial position, profit and losses, and prospects of the issuer and of any guarantor, and of the rights attaching to such securities. This information shall be presented in an easily analysable and comprehensible form.”*

Directive 2003/71/EC is supplemented by Regulation (EC)809/2004, which contains detailed rules about the information to be contained in prospectuses. Regarding prospectuses issued electronically it says:

*“Where a prospectus is published in electronic form, additional safety measures compared to traditional means of publication, using best practices available, are necessary in order to maintain the integrity of the information, to avoid manipulation or modification from unauthorised persons, to avoid altering its comprehensibility and to escape from possible adverse consequences from different approaches on offer of securities to the public in third countries.”*

## **2.12 The Transparency Directive**

The Transparency Directive 2004/109/EC is designed to enhance transparency on EU capital markets. It “establishes requirements in relation to the disclosure of periodic and ongoing information about issuers whose securities are already admitted to trading on a regulated market situated or operating within a Member State.” In summary, issuers must disclose annual and half-yearly financial reports and, where they are issuers of shares, interim financial statements.

## **2.13 The Anti Money Laundering Directive**

EU anti-money laundering rules contained in the Third Money Laundering Directive<sup>17</sup> impact upon a very wide cross section of economic life. They apply to credit institutions, financial institutions, auditors, insolvency practitioners, external accountants and tax advisers, independent legal professionals, trust or company service providers, estate agents, high value dealers and even casinos.

These relevant persons are obliged to carry out “customer due diligence” checks, which means properly identifying the customer by reference to reliable information obtained from independent sources. These customer due diligence procedures must be carried out whenever the relevant person establishes a business relationship, carries out an occasional transaction, suspects money laundering or terrorist financing or doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification. Additionally, the relevant person must carry out ongoing monitoring of the customer and keep associated records.

---

<sup>17</sup> Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

Article 30 sets the records keeping obligations. Customer due diligence records must be retained for five years, commencing from the date the business relationship ends or the occasional transaction is completed. The relevant person is therefore required to establish appropriate procedures for the records keeping purposes.

Failure to comply with these records keeping obligations is a criminal offence. Thus, regulated entities will wish to take steps to ensure that the security of their networks is adequately protected.

# 3

## Key IT projects for the Financial Services Industry

### 3.1 Overview

Compliance with the laws identified and discussed in the previous section of this White Paper necessarily involve IT projects. Core IT projects are identified later, but in summary Financial Services Institutions should consider the range of IT issues identified in the table below.

Core IT projects for Financial Services Institutions		
Business consideration	IT consideration	Risk consideration
The endpoint	User terminal equipment such as desktops and laptops, mobile computing devices, portable storage media and computing peripherals.	The core areas of risk include the loss of the equipment, unauthorised access and use and loss of, or damage to, stored data.
The network	WANs/LANs/VPNs, mobile networks, Internet, data centres and branches of the organisation.	The core areas of risk include eavesdropping through monitoring, surveillance and interception and network downtime and unavailability.
The applications	The range of applications is very wide, covering enterprise applications, custom and bespoke applications, email applications, web applications and other third party applications.	The core areas of risk encompass all those mentioned above. The use of applications for crime and the potential for unauthorised distribution of data is included.
The databases and servers	All types of servers, including	The core areas of risk

	application servers, database servers, print servers, file servers and replicated servers.	encompass all of those mentioned above.
The storage	In addition to portable and mobile storage devices, considerations include production systems, back-up systems, disaster recovery systems and archives.	See section 3.5 below for a detailed analysis of the risk issues. In summary, these include media loss, unauthorised access and use, data loss or corruption, downtime and unavailability.

### 3.2 Act in accordance with international standards

Finance Services Institutions cannot avoid dealing with informational security, which extends to (1) security of the network, (2) security of the information processed within the network and (3) securing of information leaving the network.

Thus, regulated entities are advised to consider established international standards for informational security as a matter of best practice.

BS ISO/IEC 27001:2005 is an international standard that has “been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining an Information Security Management System (ISMS)”. An ISMS is “designed to ensure the selection of adequate and proportionate security controls that protection information assets and give confidence to interested parties”. The standard contains a table of “control objectives and controls” that are to be achieved within an ISMS meeting the international standard. Key elements within the control objectives and controls matters are network security management, monitoring and access controls. Compliance with 27001:2005 cannot be achieved without a holistic approach like Information Risk Management.

In addition to international standards there are developing industry standards for the financial services sector, which need to be considered as appropriate. For example, the PCI Security Standards Council has set the pace for the payment cards industry, through its Data Security Standard (PCI DSS)<sup>18</sup>. The standard consists of twelve primary requirements for the security of payment card data, details of which are contained in the table below.

<sup>18</sup> [https://www.pcisecuritystandards.org/pdfs/pci\\_dss\\_v1-1.pdf](https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf)

**The Payment Card Industry's "Data Security Standard" (PCI DSS)**

Obligation	Requirement
Build and Maintain a Secure Network	1: Install and maintain a firewall configuration to protect cardholder data.  2: Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3: Protect stored cardholder data.  4: Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	5: Use and regularly update anti-virus software.  6: Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7: Restrict access to cardholder data by business need-to-know.  8: Assign a unique ID to each person with computer access.  9: Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10: Track and monitor all access to network resources and cardholder data.  11: Regularly test security systems and processes.
Maintain an Information Security Policy	12: Maintain a policy that addresses information security.

Similarly, the Single European Payment Area (SEPA) for credit transfers and direct debits requires adherence to technical standards that guarantee the security of payment card data during its transmission and in storage<sup>19</sup>.

<sup>19</sup> For further details see the European Payments Council.  
<http://www.europeanpaymentscouncil.eu/index.cfm>

### **3.3 Implement Privacy Enhancing Technologies (“PETs”)**

When focusing on compliance with the Data Protection Directive Financial Services Institutions should always try to implement technologies that will protect privacy.

In May 2007 the European Commission addressed a very important communication<sup>20</sup> to the European Parliament and the European Council, calling for the promotion of Privacy Enhancing Technologies (“PETs”). The Commission’s communication observes that despite Article 17 of the Data Protection Directive, the current legal framework concerning technological measures might not be sufficient to protect privacy. Therefore, the Commission recommends the promotion of Privacy Enhancing Technologies:

*“The Commission considers that PETs should be developed and more widely used, in particular where personal data is processed through ICT<sup>21</sup> networks. The Commission considers that wider use of PETs would improve the protection of privacy as well as help fulfil data protection rules. The use of PETs would be complementary to the existing legal framework and enforcement mechanisms.”*

As regards the meaning of PETs the communication points to a number of definitions, but prefers “a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system”.

### **3.4 Protect the network perimeter**

The Financial Services Institution should ensure that sufficiently strong technologies are implemented in order to protect the network from external attack. Intrusion prevention and intrusion detection technologies are critical. Firewalls, anti-virus software and similar technologies etc. are all essential.

### **3.5 Protect records and data in storage**

As regards records, these should be stored in robust technologies that enable (1) classification of records, (2) which preserve the integrity of the data, (3) which give ready access to the data and (4) which enable comprehensive auditing of events.

Again, there are a plethora of international standards that can act as useful benchmarks, such as ISO 15489-1:2001 “Information and Documentation –

---

<sup>20</sup> A “communication” is generally considered to be the first step along the path to new EU legislation. Thus, the PETs communication stands as a clear statement of intent. In any event, national regulators regularly cite PETs as a solution to the technological obligations within data protection law. It is the writer’s opinion that the adoption of PETs is a core component of good information handling.

<sup>21</sup> ICT stands for information and communications technologies.

Records Management". While they are couched in different shades of language they all point to the same consideration for the management of data as records. When considered collectively the following amalgam of standards can be created:

**(a) The nature of the technology**

- (i) Robustness – The technology must display a low susceptibility to physical damage.
- (ii) Longevity – The technology must prevent records degradation during the information lifecycle.
- (iii) Obsolescence – The technology must be based on established, proven platforms.
- (iv) Scalability – The technology must scale to meet the organisation's requirements.
- (v) Open standards – The technology must take advantage of as many open standards as possible.
- (vi) Cost – The technology must reduce the cost of records keeping by as much as possible.
- (vii) Security – The technology must provide robust security.

**(b) Records capture**

- (i) Wide capture – The technology must capture as many different file types as possible.
- (ii) Complete capture – The technology must capture every new record.
- (iii) Classification – The technology must allow records to be classified.
- (iv) Metadata – The technology must create or support metadata.
- (v) Unique identifiers – The technology must allocate unique identifiers to each unique record.

**(c) Content protection**

- (i) Protection against data loss or damage due to system failure - The technology must display features that go to protect the data from corruption caused by software/ hardware failure.

- (ii) Protection against overwrite - The technology must display features that prevent the accidental or deliberate overwriting of records.
- (iii) Protection against delete - The technology must display features that prevent the accidental or deliberate deletion of records otherwise than in accordance with a predefined schedule.
- (iv) Safe delete - The technology must enable the complete and irreversible deletion of records.

**(d) Access and retrieval**

- (i) Complete access and retrieval – The technology must allow access and retrieval of all records.
- (ii) Speed of retrieval – The technology must facilitate quick access and retrieval of records.
- (iii) Protection against unauthorised access and retrieval – The technology must facilitate controls and limitations over access and retrieval.
- (iv) Search – The technology must facilitate search.

**(e) Monitoring and audit**

- (i) Complete monitoring and audit – The technology must facilitate the monitoring and auditing of all events.

### **3.6 Protection of data in transit and in communications**

A core consideration will always be encryption of data on portable storage devices and on laptops. For instance, the UK Information Commissioner, who is responsible for data protection, recently issued a press release setting out his views on encryption of laptops<sup>22</sup>:

*“There have been a number of reports recently of laptop computers, containing personal information which have been stolen from vehicles, dwellings or left in inappropriate places without being protected adequately. The Information Commissioner has formed the view that in future, where such losses occur and where encryption software has not been used to protect the data, enforcement action will be pursued.*

*The ICO recommends that portable and mobile devices including magnetic media, used to store and transmit personal information, the loss of which could*

---

<sup>22</sup> [http://www.ico.gov.uk/about\\_us/news\\_and\\_views/current\\_topics/Our%20approach%20to%20encryption.aspx](http://www.ico.gov.uk/about_us/news_and_views/current_topics/Our%20approach%20to%20encryption.aspx)

cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information.

Personal information, which is stored, transmitted or processed in information, communication and technical infrastructures, should also be managed and protected in accordance with the organisation's security policy and using best practice methodologies such as using the International Standard 27001."

Financial Services Institutions can be confident that these views are shared by regulators all across Europe.

It is imperative that Financial Services Institutions implement technology in order to ensure the privacy and confidentiality of communications.

### 3.7 Monitor and log all events

Every event that occurs in respect of the network and in respect of data should be monitored so as to ensure that the network functions properly and in order to ensure that access is restricted as appropriate. Where necessary telephone and other electronic communications made by workers should be monitored to ensure appropriate behaviours.

### 3.8 Identity management

Ensuring that access to the network and data is restricted to those who are entitled to have access, Financial Services Institutions should investigate and implement identity management technologies.

### 3.9 Table showing IT projects by reference to core laws

The table below identifies the types of IT projects that are required in order to achieve compliance with the core laws discussed in this White Paper

IT projects required to achieve compliance with core laws	
Law	Project
Data Protection Directive	In order to ensure compliance with the data protection principles controllers must understand the information lifecycle. Technologies are required that enable classification of data, in order to ensure processing to purpose and satisfactory retention. Technologies are also required to enable inaccurate data to be corrected as appropriate.

	<p>Data storage technologies are significant considerations. Storage must keep data safe while at the same time making it readily accessible, correctable and erasable when required.</p> <p>As the Data Protection Directive contains a specific security provision the entire network and all of the data within it must be protected. Access control technologies, personnel identification technologies (identity management), event management technologies, perimeter security technologies, encryption technologies and communications monitoring technologies are all required.</p> <p>Appropriate back-up and disaster recovery technologies are required also.</p>
Capital Requirements Directive	<p>The core focus is operational risk, which includes the risks associated with failed processes, systems etc.</p> <p>The range of technologies required to achieve compliance with the CRD mirrors those required for achieving compliance with the Data Protection Directive.</p>
MiFID	<p>There are two key areas of focus requiring IT solutions. The first is the keeping of proper records. As with the Data Protection Directive this requires appropriate data storage which preserves the integrity of the data while at all times keeping it accessible. The second is effective safeguards and arrangements for the protection of information processing systems. Again, the range of technologies required for achieving compliance mirrors those required for compliance with the Data Protection Directive.</p>
Market Abuse Directive	<p>The focus of the Market Abuse Directive is disclosure of information to investors and the identification of those persons who have access to relevant information.</p> <p>Technologies are required that enable information to be classified and delivered-up as necessary. Again, records storage and records management technologies are required.</p> <p>Access control and identity management technologies are also required, to ensure that access to sensitive data is limited and monitored at all times.</p>
Prospectus Directive and Transparency Directives	<p>The focus of these Directives is disclosure of information. As with the Market Abuse Directive, technologies are required that</p>

	enable information to be classified and delivered-up as necessary.
Money Laundering Directive	The focus of the Money Laundering Directive is the long term storage of records, which should be capable of easy access and retrieval. A definite five year retention period should be set.

# 4

---

## Our Technology Law Group

“...excellent and expanding practice...wins promotion to the top tier of our ranking this year off the back of major hires and sterling work.” *Chambers UK, 2007*

We have one of the UK's largest teams of technology law specialists comprising 10 partners and 19 assistant solicitors. Our expertise is recognised by the leading UK legal guides *The Legal 500*, and *Chambers UK*. They are further supported by other specialist groups within the firm – competition, procurement, employment, property and tax – all of whom are also very experienced in advising companies on technology projects and the related issues.

Our technology law group is dedicated to commercial technology and outsourcing matters. We advise on a vast array of matters including technology licensing, outsourcing projects, procurement, systems development, distribution arrangements and consulting agreements. We have extensive experience of advising on related legal and regulatory issues such as e-commerce, telecommunications and freedom of information. Indeed, our practitioners write some of the leading text books in these areas.

We have a dedicated privacy and information law group which is recognised as being one of the most highly regarded in the country. The group has specialist knowledge across all areas of data protection, freedom of information, information sharing, confidentiality and human rights law. Our experience embraces all aspects of data protection law including protection audits, devising e-privacy strategies, drafting privacy policies, rules and guidelines, advice on dealings with data owners, processors, data protection authorities and other regulatory agencies and advice on all aspects of international data transfer. We believe that our technical expertise in privacy law and our understanding of the value of employee and customer data can be of great value to our clients.

---

## Contacts

**Stewart Room**

Partner, Technology Law Group

t: (0)20 7861 4850

e: [stewart.room@ffw.com](mailto:stewart.room@ffw.com)

Stewart is a partner in our technology law group, within the privacy and information law group. He is dual qualified as a barrister and a solicitor holding full Higher Court Rights of Audience, with over 16 years experience as a litigator and advocate. He has considerable expertise and reputation in data protection and privacy law matters, contentious and non-contentious. His non-contentious experience covers auditing, consulting, advice on the exercise of data subject rights, compensation claims, direct marketing, data security, data retention, data access and trans-border data flows, drafting of documents (company rules and procedures, controller-processor contracts, employment contracts, privacy statements) and management and worker training. His contentious experience covers both civil and criminal data protection and privacy cases and he is heavily involved in defending data controllers and individuals in prosecutions brought by the Information Commissioner.

His clients include EMC, Computer Associates, Hitachi Data Systems, RSA, Symantec, Marks and Spencer, APACS, Unicef and many other household names.

He is a regular contributor to legal and academic journals. He has also written a book on the subject, "Data Protection and Compliance in Context" (November 2006) as well as the data protection chapter in "Goode: Consumer Credit Law and Practice" (2005). He undertakes media work, appearing as the UK legal expert in the Channel 4 Dispatches documentary "The Data Theft Scandal", which exposed security failings in the Indian Call Centre industry (2006). He is currently writing a book on e-mail law, to be published by the Law Society in 2008. Stewart sits on the British Computer Society's Information Privacy Expert Panel, has participated as a member of The Sedona Conference expert working group on electronically stored information and he is the elected President of the National Association of Data Protection and Freedom of Information Officers. He is a visiting lecturer on computer law at Queen Mary, University of London.