Regulatory Compliance

Business Opportunity/Technical Challenge

Author: Peter Abrahams
Published: April 2005

a White Paper by

Introduction

Good corporate governance has always been an essential part of running a successful enterprise. However in the last few years new regulations have put the spotlight on this area and especially the ability to prove compliance with the regulations to external auditors.

The ability to comply raises questions about the adequacy of information technology used within the enterprise and poses technical challenges as to how to fully meet the regulations.

Companies that can rise to these challenges will find that they have built an infrastructure that will:

- Improve their internal controls.
- Improve the visibility and understanding of the business.
- Create greater business agility.

Altogether these will provide substantial competitive advantage.

This paper briefly describes regulatory compliance and who it will affect. It then looks in more detail at some of the technology issues, specifically around information flow. Finally it looks at the business benefits of compliance.

What is Regulatory Compliance?

There have always been regulations relating to how companies carry out their business and report on it. These were designed to ensure that they paid relevant taxes, treated customers and suppliers fairly, did not adversely impact the environment or the community, and provided reliable information for investors and creditors.

In spite of these controls the business world has been rocked by high profile corporate disasters; Enron, Barings, WorldCom, Equitable Life to name some of the worst examples.

In response various authorities have developed new regulations and the most noticeable include:

- Sarbanes Oxley Act in the United States.
- Basel II for international financial services.
- New reporting requirements from the Financial Services Authority (FSA) in the UK.

All of these are designed to improve the quality and completeness of the reporting of information by enterprises. Essential prerequisites to such reporting are well

defined, documented and controlled processes running the organisation. The new regulations therefore concern themselves both with the quality of the processes as well as the content of the resulting reports.

The intent of the regulations is:

- To protect the public interest by reducing the possibility of sudden corporate collapse with the impact that has on employees, local communities and pension provision.
- To build confidence with investors so that they can make informed decisions based on reliable, accurate information.
- To create global standardization to simplify international business and investment.
- To help ensure economic stability which is always adversely affected by financial scandals and collapse.

So, who will it effect?

The regulations tend to be targeted at specific sectors—Basel II with financial services, and Sarbanes Oxley with listed US companies—but it is clear that the impact will be far wider.

For example, the geographic spread of Sarbanes Oxley includes any subsidiary of a US listed company, any non-US company with a listing on a US stock exchange, or any company with significant numbers of shares held by US citizens.

If we look at companies that provide services, especially outsourcing, to regulated companies it appears that they will have to abide by the spirit, if not the letter, of the law. If they do not then it is difficult to see how the requesting company can fully compliant.

It must be assumed that companies that do not meet the standards of the regulation will gradually find it more difficult to work with regulated companies or organisations for one or more of the following reasons:

- During a merger or acquisition, the cost and complexity of complying before the merger can complete may be prohibitive and make the deal less attractive.
- When attracting new investment, because the lack of formal controls will make the investment more risky and either unacceptable or expensive.
- When providing goods or services, when the client may be concerned about the quality of information they will receive.

It should also be noted that any public body will wish to comply with the spirit to avoid any possible public scandal.

In practice this means that every company and organisation is impacted, from the largest international businesses to the Mom and Pop store, across all types of institutions: government, commercial, NGO, charities etc.

Some organisations have to comply within a strict timetable whereas others have the luxury of being able to make changes at an easier pace. At the end of the day, however, every organisation should look at improving their internal processes and reporting regime in line with the regulations.

So what are the technology challenges?

The challenge is to provide the CEO and the CFO with the information they need to be able to sign off the reporting and the processes within the business. The CEO and CFO are responsible for the information in the reports and the processes that help to create that information. The Sarbanes Oxley Act, for example, makes them personally responsible with the possibility of fines or jail sentences if they do not comply.

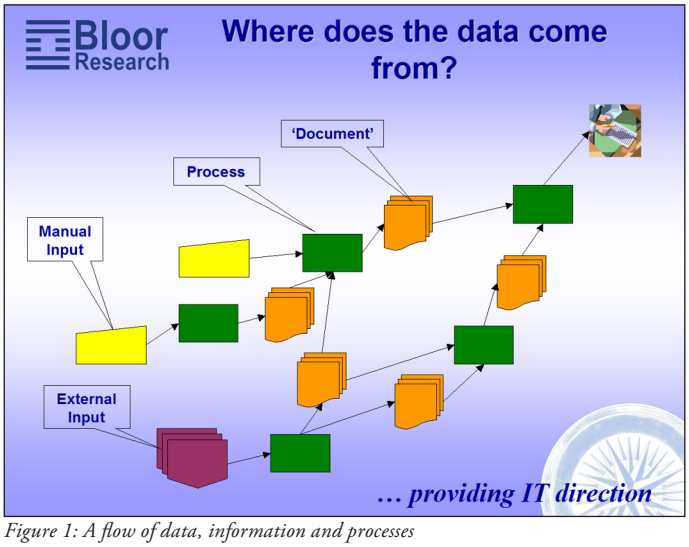

Figure 1: A flow of data, information and processes

Most of the processes and reports will be created with the aid of IT. This means that the CIO has to provide a set of solutions that can enable the CEO to see that the processes have been properly carried out and the information obtained is accurate. It would appear that the CIO attesting to the CEO that everything is in order will not be sufficient.

Figure 1 shows a simplified flow of data, information and processes that contribute to reports presented by the CEO. The final report is seen in the top right of the picture.

As can be seen the information comes from a variety of sources including:

- Information from external sources (suppliers, customers, markets etc.), which might come in electronically or in human readable form.
- Information from internal sources that, again, might be inputted manually or from automated devices or sensors such as RFID.

-Once in the enterprise this information will be processed, both automatically and by humans, to produce new information and trigger new events.

The information will flow between processes as a 'document'. Document is in quotes here to imply a variety of different formats; paper, email, electronic messages, computer files, database records etc.

How can the CIO show to the CEO that:

- The inputs are accurate.
- The processes accurately reflect the requirements defined by the management.
- The document flows are safe, accurate and consistent.
- The whole is transparent and auditable.
- That the inherent risks are understood, monitored and controlled.

Technology can help in all these areas, but this report is going to concentrate on the movement of documents between the processes.

Document movement

The technology involved in document movement can be anything from purely manual, with physical documents being shipped around, to full straight through processing (STP) where the document is moved electronically without any human intervention from entry into the system to final report creation.

This report looks at various options and analyses their benefits, drawbacks and risks, specifically as they relate to regulatory compliance.

Swivel chair technology

This is a technology we might have expected to have disappeared by the beginning of the 21st century; however it is still quite common.

Figure 2: Swivel-chair technology

A clerk reads information from one document, paper or on a screen, extracts the relevant information, potentially does some simple calculations or transforms, and keys it into a new document.

Although crude it has some nice features. It is very easy to set up the initial implementation; the clerk is told what is required and their intelligence can be used to implement the process and also to recognise out-of-line situations and resolve them. It is very flexible so that new requirements can be added at will.

Very obviously in terms of regulator compliance it has several major issues:

- Often the clerk will be told verbally rather than have a formal document defining the data movement requirements.
- Changes to the process may be made without any documentation and these could be initiated by the clerk, producing the right results but with out any audit trail of the change.
- Humans are not good at doing this type of repetitive job; errors of transcription will creep in. This kind of error can be reduced by having a second clerk validate the input but this is both costly and requires a set of well defined procedures.

- There are dangers of the document being moved repeated times or a document not being moved at all; this is more likely if the job is shared amongst several clerks. Again procedures can be built to reduce this problem but at a cost.

- If there is inadequate documentation there will be real problems if the clerk falls under the proverbial bus, passing the task on to a new clerk will be error prone, time consuming and costly.

File transfer

As Figure 3 implies, file transfer technology originated with physical magnetic tapes being moved from one process to the next. Nowadays the actual move is done electronically using one of the many file transfer protocol (FTP) packages available. In this way a file of data from one process is made available as input to subsequent processes.

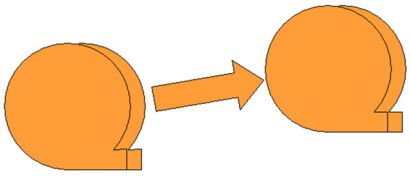

Figure 3: File transfer technology

The big advantage is that there should not be any transcription errors. Also, within a file, each of the records in the input should be transmitted once and only once to the target.

There are still major issues with this protocol:

- The receiving system has to be able to read the output from the transmitting system. In the initial implementation that may not be a problem; but as new versions of the source process are developed that produce new types of information a serious synchronisation problem emerges. This problem is even worse if the source file is used by more than one target system. If any, or all, of the end points are packaged applications the situation may become intractable.

- There is no external definition of the format of the file being transferred. The file is defined internally in both sending and receiving processes but this is not in a format that is accessible to the CEO or the auditors.

- Ensuring that the file is transferred once and only once requires some external procedure. The procedure must be able to deal with in-flight failures such as the file being only partially sent. Often this procedure is manual or semi-automated and therefore error prone and difficult to monitor.

- Security of the file needs careful monitoring to ensure that it is not read, copied or modified during transfer. This monitoring is not an inherent part of FTP and needs to be built on top of the application but this does not always happen.

- The data can only be transferred when a file is complete; this means that individual documents may be delayed for a considerable time. This time delay could have implications for the agility of the systems, the controls of the total business process or the ability to gain business advantage from real time processing.

FTP is a step forward from the swivel chair in terms of speed and accuracy, but at a cost of flexibility and transparency.

Simple messaging

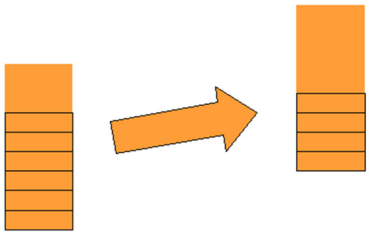

Figure 4: Messaging technology

Simple messaging, such as IBM basic MQSeries, is designed to assure the delivery of messages, or 'documents', from one system to another in a timely and controlled fashion.

Messages are input by the source system and then it is the message oriented middleware (MOM) that takes responsibility for the delivery to the target. The MOM concept provides a rudimentary level of documentation, monitoring and system management. Information is available about the end points and the volume and reliability of the traffic. Security and encryption can be included to avoid the messages being tampered with on route.

Originally the protocols and interfaces to support MOM were proprietary but in the last few years there has been a move to create standards, including JMS and JCA, so that different systems can communicate more easily.

Simple messaging is the necessary basis for providing an environment that can support regulatory compliance. However, there are several missing elements including:

- External documentation of the format of the messages, including a record of the changes over time.
- Ability to route messages
- Ability to transform messages in flight so that source and target(s) do not have to have the same structure or exactly the same content.
- Auditing and logging of the messages that have been transferred. This enables the auditors and business management to analyse and understand out-of-line situations and test conformance.
- Ability to define business processes externally to the individual processes.

All this definition and monitoring must be implemented so that they can be inspected directly by the business managers (including the CEO) and the auditors. Only under these circumstances can the CEO legitimately sign off the reports and processes as being correct.

The outline of a solution for regulatory compliance

In parallel with the increased demand for regulatory compliance there has been development of several interrelated technologies that will aid the provision of compliant IT systems. These include: Event Driven Architecture (EDA), Service

Orientated Architecture (SOA), Business Process Management, Human Workflow Management, Extended mark-up language (XML) and its various derivatives, Web services, Business activity monitoring (BAM) and Composite Applications.

All of these are designed to enable solutions to be developed more quickly and more flexibly. The principle concept behind all of them is that more of the implementation should be held in a declarative format rather than in code. XML is declarative because the definitions of the message formats are held externally in a Document Type Definition (DTD). The benefit is that the DTD can be viewed and understood by business analysts, and the DTD is used directly in the processing of the message. There is therefore no translation process between the definition understood by the user and the processing in production. The DTD can be accessed by editors to simplify the viewing and creation; in this way the information will be available and understandable by business managers, including the CEO.

Similar declarative methods are available for transforming messages, routing messages, creating business processes, event processing and interaction between automated and human processing.

To implement these solutions requires more intelligence in the messaging infrastructure. This extra intelligence means that auditing and logging can be included. These facilities can be used to aid regulatory compliance by enabling business managers and auditors to review past transactions to ensure that they have been processed correctly.

The combination of declarative methods and intelligence in the messaging infrastructure will allow the CEO to verify that there are well defined business processes in place and that they are being faithfully implemented. The auditors will then find it much easier to confirm compliance, thus these technologies are an essential part of fully meeting regulatory compliance legislation.

The business opportunity

Companies that have to comply with existing regulations, especially Sarbanes Oxley, are spending large amounts of money and time to ensure compliance. Partly this is due to the speed of the implementation of the new laws and partly the comprehensive coverage required.

In the short term, for these businesses, compliance is a major drain on resources but in the long term the better controls will provide considerable business benefits:

- The improved business controls will reduce risk of significant failures. Risk reduction has a multitude of benefits such as:
    - » Reduction in time and effort expended by senior management fire fighting.

  - » Reduction in capital that has to be laid aside for such eventualities.
  - » The improved ability to attract investors.
- The greater automation will reduce the cost of processing leading directly to a benefit on the bottom line.
- The new infrastructure will increase the flexibility of IT and therefore the agility of the business. Being able to respond more quickly to new opportunities, new threats and new market requirements will bring new business and increase profits.
- Finally, non-compliance is just not an option.

Businesses that are not immediately impacted by the regulations should be looking to implement similar solutions, as they should be able to gain the same business benefits. They will benefit from not having the pace forced on them and this should reduce the implementation cost. If they implement now they should benefit further in the future:

- They will be prepared when regulation does start affecting them directly, this may occur because of extensions in the regulations or because their business changes in size or nature.
- If they want to merge with a regulated company the lack of compliance will be a hindrance.
- They will find that regulated companies will prefer to be supplied by them.

Business and IT management should both see compliance as a positive move giving them the incentive to develop better systems and controls for their companies.

Modern integration software will significantly reduce the cost of compliance.

Copyright & Disclaimer

Suite 4, Town Hall, 86 Watling Street East
TOWCESTER, Northamptonshire, NN12 6BS, United Kingdom

Tel: +44 (0)870 345 9911 – Fax: +44 (0)870 345 9922
Web: www.bloor-research.com – email: info@bloor-research.com