lustratus

Research

Upgrading Risk and Compliance Management on System z

Delivering enhanced business transparency for mainframe workloads

Author: *Steve Craggs*

December 2008
Version 1.00

Table of Contents

Executive Summary

Company executives around the world are drastically increasing their focus on properly governing their businesses as they step through increasingly complex minefields of fiscal integrity, government regulation, stakeholder concerns and a dramatically shifting market landscape. It has never been so important for companies to be able to clearly demonstrate the appropriate level of control and management, ensuring all parts of the business without exception are operating within corporate policy and externally imposed demands. Given this increased focus on corporate governance, managing business risk and regulatory compliance can be a matter of survival, and there is perhaps no market segment where this is more true than the financial services industry. Financial institutions are under the public spotlight as never before, making shareholders, media and government bodies focus with laser-beam intensity on day-to-day company health and the performance of the senior management team, and spawning more and more regulatory activity.

But this increased focus on the minutae of business operations causes problems for many large corporations. IT systems that have grown up over thirty or forty years, often based on IBM mainframes and the ubiquitous CICS transaction processing software, are the backbone of operational processing across the world, but they were never designed with this level of internal visibility in mind – the focus was always to have an application that delivered the right results, without a particular focus on *how* those results were delivered. In short, it was results that mattered. Of course, the same is still true today, but the added need to demonstrate the appropriate level of corporate governance, for example by ensuring that regulations and policies are followed or that risk is properly managed, requires a greater degree of transparency in IT-driven business operations.

So, technology is required that allows companies to pay closer attention to the details of business operations, looking inside the mainframe applications that previously remained stubbornly opaque. But care must be taken to deliver this increased transparency in a practical fashion – requiring a compliance officer to watch every transaction in order to ensure regulations are faithfully being met is clearly not the answer. What is actually needed is the ability to 'manage by exception', leaving the vast majority of transactions that are operating within required limits alone and only flagging ones that seem to be out of line.

Fortunately, the IT industry has come up with business events technology, where certain business conditions can be pre-defined as being noteworthy in some way and then detected and resolved as prescribed. Not only does this provide a way of increasing the transparency of IT-based business operations, but it also provides more or less real-time notification, allowing a much greater degree of timeliness and responsiveness than offered today by the typical weekly or monthly compliance reports. The final piece of the puzzle is that a method of upgrading existing mainframe applications is required to generate the information on how transaction execution is progressing, to provide the necessary input to determine if a particular event has occurred. IBM has recently announced just such support for CICS, enabling all System z CICS workloads to be instrumented in order to provide business transparency, which in turn leads to better corporate governance through more effective risk and compliance management.

Risk and compliance are not optional – managing them effectively is of paramount importance, and often nothing short of a survival issue. But the corollary is that effectively managing risk and compliance delivers greater confidence and increased operational freedom, resulting in greater competitiveness and improved returns to the business and all its stakeholders.

The growing importance of managing risk

In today's climate of increasingly tight market conditions, driven by the difficulties of raising credit and the corresponding fears over the health and security of businesses across the world, one word has risen to the top of mind for many executives – risk. While strategic and operational risk are obviously part of the concern, for example in terms of the ability to switch rapidly between partners and service providers, for many the immediate concerns lie in managing financial and compliance risk. As far as financial risk is concerned, this is obviously a high priority in a world where financial flexibility has been so seriously restricted, both internally and in partner companies. It is becoming more and more critical that companies have an accurate and up-to-date assessment of their consolidated business performance and financial commitments for example. However, compliance risk is also likely to become a growing challenge as governments across the globe take actions to try to protect the worldwide economy from suffering from the current wave of problems again.

This compliance challenge is going to be particularly hard for companies operating in the financial services sector, where many politicians are directing their fire. The industry is expecting to see waves of additional regulations pouring forth from the various government-backed regulatory authorities as discussions continue over how to prevent the perceived inadequacies of the current financial model. However, financial risk is perhaps an even more serious issue for financial institutions, since they are one of the most heavily exposed sectors in the current downturn and in many cases have ended up with governments becoming large and potentially demanding shareholders.

On top of this, in today's tense business climate this issue of risk management is much more personal than perhaps it was before. Responsible corporate governance has become even more of a focus in recent times due to stakeholder concerns over company performance and survival. Executives are expected to be whiter than white in the way corporate policy is defined, laid out, enacted and evaluated on an ongoing basis. Risk and compliance management is seen as an absolutely key element of governance, since if a company suffers badly, there will be no shortage of people wanting to find executive scapegoats. It is vital that executives can point to a clean sheet in complying with industry rules and taking a sensible attitude to risk if their jobs are to be preserved.

So managing risk and compliance is going to be a major focus for executives in the next few years. Already in the financial market, for example, reports prepared to satisfy national regulators, such as those stemming from the Basel Accords covering capital and risk, are being requested with ever greater frequency. Where companies used to produce these reports monthly, management is now demanding the same reports weekly, daily or even on an intra-day basis. Even outside the finance industry, executive management teams are constantly asking for up-to-date information regarding cashflow, exposures and business performance, in order to be able to respond to developing risks quickly enough to avoid disaster.

There is another side to the risk coin, however, and it is a major driver behind the desire to get a much more real-time picture of risk. In the past, risk management has typically been handled in 'batch' mode - that is through reports produced on a monthly or weekly basis. The reason why this has normally proved sufficient is that companies have been running their day-to-day operations within wide safety margins, so there has been less need for constant, by the minute risk management. However, the current economic climate tends to make companies cautious and is certainly squeezing margins to the bone, causing competition to intensify. Often the difference between winning and losing business can be remarkably slim. In this environment, companies can gain an edge by sailing closer to the wind, making aggressive and hence risky deals with their clients. In other words, companies gain by operating closer to the safety margin. However current economic conditions mean the penalties for over-reaching are extremely severe, and therefore the only way to take this route to competitive advantage is to keep a much closer eye on risk in real-time, or as near to real time as possible. Waiting for a weekly report could result in a company becoming critically exposed in the intervening period.

Of course, most companies drive their day-to-day operations with IT systems, and therefore the pressure to support the risk and compliance management needs and initiatives of the business quickly becomes focused on the IT department. It is here that many companies find themselves struggling due to the lack of business transparency in the operational IT systems.

IT and business transparency

The business transparency issue

The problem stems to a large extent from the way IT systems have developed over the years. For most of the IT industry's lifetime, business applications have been developed by programmers based on a set of business requirements. That is, the business department specifies what the application is to do, and the programmers design and build the applications to fulfil these stated needs. Today, on the IBM mainframe platform alone, trillions of dollars have been invested in these business applications. But the problem is that when these applications were written, they were written to fulfil the business needs at the time, and unfortunately in the majority of cases the business logic controlling the application operation ended up being embedded in the program design and implementation. The consequence is that, while the application may function correctly and deliver the required results, it is often extremely difficult to determine from a business perspective exactly what the application is doing inside. A technical monitoring tool can measure how IT resources are being utilized based on disk usage or program execution times, for example, but it cannot say how many times a purchase order has had to be referred to a supervisor for special approval. Admittedly, many mainframe companies have addressed this problem up to a point, but this has involved writing lots of software to translate technical resource activities into business-related reports, and in a dynamic business world this software needs frequent maintenance and introduces considerable latency in the provision of this crucial business performance information. In summary, the real problem is there is insufficient business transparency in operational execution.

The implications of this lack of business transparency in many IT workloads today is that when business executives ask for more information about business factors such as the level of exposure to a particular client, or how close the current liquidity position is to the boundary of compliance, IT often cannot answer because the current applications were not designed to provide this information. Even if the application was designed to provide at least some of the business related performance data required, this will usually be in the form of offline reports that typically run in the mainframe system's batch window.

In most cases it will be possible for IT to eventually change the necessary applications to deliver what is needed, but this can be extremely costly and time consuming, often requiring the development team to unpick design decisions made years ago in order to get at the embedded business logic. In addition, because of the speed and extent of change in these difficult economic conditions, by the time the requested functionality is deployed into production operations the requirements may well have changed again.

This transparency problem is often particularly prevalent in IBM mainframe workloads, largely due to the massive deployment of applications over the last forty years in environments such as IBM's ubiquitous CICS transaction processing environment. Lots of major companies rely on their CICS application investments, but many of these applications were developed before the current fashion for software architecture methodologies such as service-oriented architecture (SOA). Therefore these applications typically hide business logic within the technical application implementation, with all the transparency implications discussed earlier.

Look at the way mainframe CICS applications are structured, for example. A CICS application is usually made up of a whole selection of programs, all linked together as required at execution time when the required CICS transaction is requested. To be fair to the programming profession, few CICS programmers would write a new application in a single program, which would represent the ultimate in lack of transparency. Often there will be a program to handle the user interface, and separate programs to cope with different user menu choices or user

requests. However, although these programs have a structure in the eyes of the programmer, they rarely relate to specific business steps. Even the internal comments are likely to refer to the way the program works rather than the business actions it is taking.

This leaves many IT organizations in a real bind. On the one hand the business is desperately demanding more business-oriented information, perhaps even in real-time, to ensure the necessary level of risk and compliance management, but on the other the changes needed are expensive and complex. The problem is exacerbated by the additional factor that current economic conditions typically result in IT being asked to do more with less, making available resource desperately hard to find.

The IT response to the lack of business transparency

In simple terms, there is an answer – if the business logic can be made more accessible while continuing to exert its control over operational execution, then when business needs change the business logic can be altered accordingly. Perhaps more importantly, it suddenly becomes possible to follow what is happening in terms of business process execution in the operational IT systems. So, when a business executive asks for a real-time measure of what percentage of loan applications for more than $1M are being approved without reference to a supervisor, it is now much easier to put the mechanism in place to supply the desired information.

This may seem like an idle dream, but over the past few years a number of technologies have emerged in the IT space to support this end. For example, business process management (BPM) software is designed to allow the business process flow embodying the implemented business logic to be extracted from application implementation, so that business logic can be manipulated directly to change application execution. This automatically gives greater control over business process implementation, but has the important added benefit of providing improved business transparency as mentioned above, particularly when coupled with business activity monitoring (BAM). BAM technology keys off the different steps in the process being defined by the BPM process flow to enable monitoring to be done at the level of individual business process steps. So, if the BPM-specified business logic includes a test to determine whether an insurance claim needs to be routed to the exceptions department for special handling, then the BAM tool can measure how often the exceptions step is executed and therefore can display the percentage of claims resulting in special handling on a real-time basis.

However, there is a problem with the BPM / BAM approach. While there is no question that implementing a full BPM / BAM solution will provide the sort of business transparency required to handle the rapidly changing and evolving risk and compliance management needs, it can be a massive undertaking. In order to implement BPM, it is necessary to understand how each process currently works, how it should work, how to structure IT implementation to fulfil BPM process execution and how to migrate to this new world from today's implementation without disrupting service levels. Of these steps, the first deserves special mention. It may seem ridiculous to focus on the need to understand how processes are currently implemented – after all, these implementations have probably been service the company well for many years. But unfortunately due to the historic evolution of a lot of mainframe software and the embedding of business logic into programs, it is often the case that discovering how a process is currently implemented is a major issue, particularly since the skills that were involved in the original implementation may well not be available any more, for instance because of retirement or attrition.

So, for many companies, while BPM is definitely a strategic target over time, the business need for immediate support of constantly evolving risk and compliance measures demands a more rapid solution to the business transparency problem.

Introducing the concept of business events

Stepping back from the technical issues for a moment, the need for business transparency can be encapsulated in the types of questions business executives are asking. Examples might include

- Are we in danger of exceeding our exposure limit to an individual business partner?
- Are any suspicious patterns of money transfers taking place?
- Are there any real-time corporate actions we need to be aware of?
- Is current business activity within acceptable trading boundaries?

These questions may be driven from a general concern over financial risk, or specific concerns about remaining within compliance guidelines. But they all require a level of visibility of current business operations, quite possibly in real time. In other words, they require a degree of business transparency which is probably more than that exhibited by the average CICS workload on System z, because these are not questions that were expected when the original CICS applications were developed and because of the way CICS applications tend to be designed, as mentioned earlier, where business logic is hidden.

In fact, all these questions relate to particular business events. A business event is defined as a pre-defined set of business conditions being met. So, for example, in answer to the first question a business event could be defined as the exposure to a single business partner reaching 80% of the acceptable limit. The second question could involve a business event defined as multiple transfers over a particular size occurring to and from the same pattern of accounts, and similarly for the other sample questions.

Business event processing software has emerged as the way to manage business events and their handling. Using business event processing software, the user can define the conditions to be met for a particular business event to have occurred, and also the corresponding set of actions to be taken. The runtime part of the business event processing software now monitors the specified conditions in real time to see if they are met, and if an event does occur then it invokes the specified actions, such as raising an alert to the compliance officer or automatically starting an audit trail for operations to or from a specified account. Detecting the event might involve detecting multiple business conditions across a range of systems, correlating them, and even looking for patterns that might either confirm an event or predict an event that is about to occur.

In risk and compliance terms, the occurrence of the event is often equivalent to a warning light flashing or even a full scale fire alarm sounding. In summary, the components of a business processing software solution are

- Event definition interface – a business-oriented interface to define the event business conditions
- Event detection software – detecting that an event may have occurred
- Correlation – events might involve multiple business conditions across different systems
- Pattern matching – events may involve recognizable patterns developing, which can lead to prediction
- Action execution – triggering the necessary actions to respond to the detected event

The importance of events to business transparency

Closer examination quickly shows that business events support can provide an attractive way of gaining some level of business transparency, particularly as it relates to real time operations. Admittedly it does not go nearly as far as a full BPM/BAM solution, where the whole business process becomes much more visible, but on the other hand it involves a lot less work. Instead of having to gather the knowledge together of exactly how processes are currently defined and implemented, it is only necessary to understand the subset of execution corresponding to the desired business events. This makes a huge difference to the effort required to implement events-based transparency as opposed to BPM, and it is much less invasive too. It is like putting a sensor into the system, just as technical monitoring tools do today, but instead of the sensor being attuned to IT-related information such as the depth of a disk-based message queue, it is a business execution-related sensor checking things like the number of purchase orders still waiting to be processed.

There is still technical work required, obviously. IT specialists will need to translate the business event definition into what this means in terms of IT execution. However, the other big advantage of business events as a route to greater business transparency is that the event definitions and associated actions to be taken are typically decoupled from the technical implementation. So, while the translation of a sensor point from business to technical implementation terms has to be handled within the IT execution environment, the business event definition and actions can remain in a separate repository, referred to by the events handling software at run-time. This means it remains easily accessible for future changes. In fact, the best business events-handling products provide an interface to these definitions that is non-technical and therefore easily understood by the business users involved. The screen-shot below is an example of the accessibility of this type of approach for business users, taken from the IBM WebSphere Business Events product.

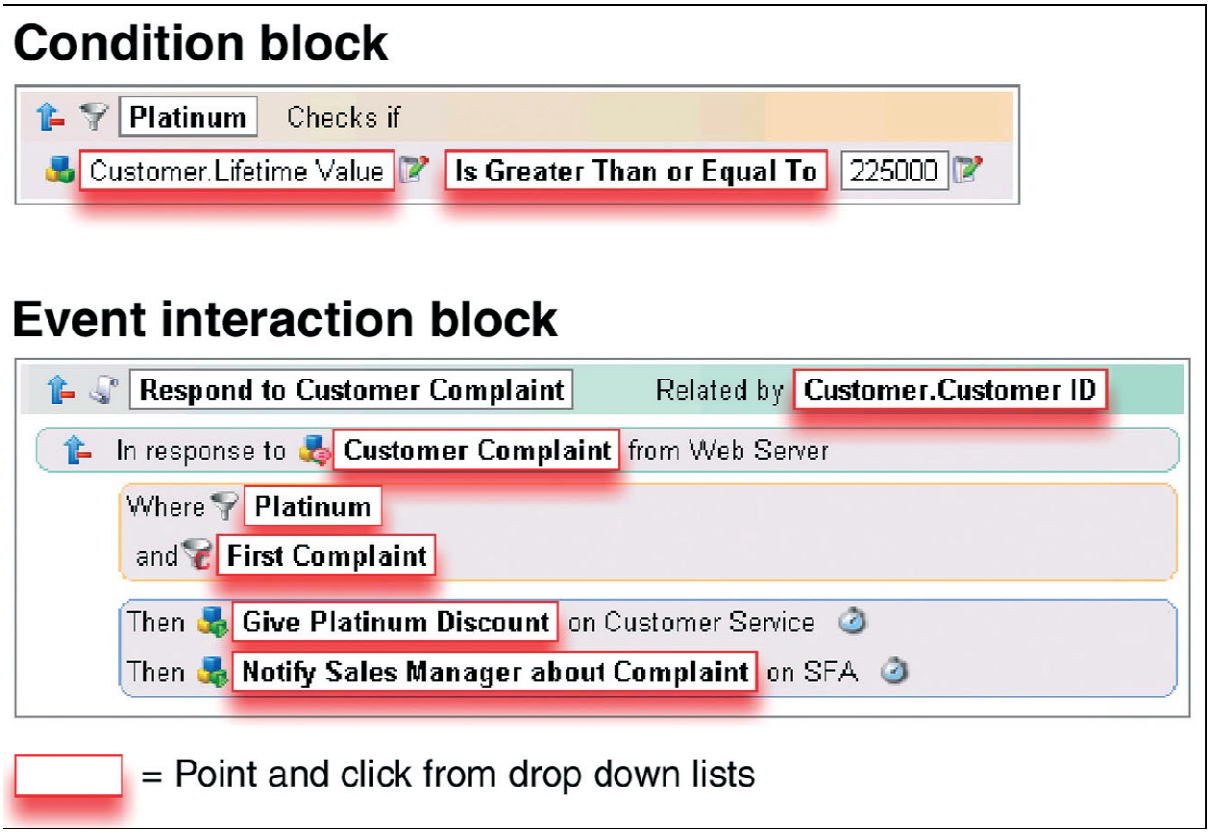

Figure 1:- Defining events with IBM WebSphere Business Events

In this example, a Platinum rated customer is defined to be a customer whose lifetime value is at least $225,000. Although not shown, there would also have been definitions of First Complaint as being a complaint from a customer that has never complained before, and the two actions in the event specification which are to be taken if the event occurs. One action sets an automatic discount for the customer, and the other notifies the local sales manager of the complaint. Different conditions and actions are accessible through pull-down lists. The whole point is to have an interface that is simple for a business specialist to use, both for defining events and inspecting current event specifications.

Exception management through the use of events

One key aspect of events handling that is particularly relevant when looking to deliver improved risk and compliance management is that events can be used to support exception management. Consider a company that has gone a long way in adopting BPM, and can now see day-to-day operations in terms of business process flows and actions. Trying to keep track of every single operation within every single process instance quickly becomes unmanageable as loads grow. This is a common problem in the world of IT, where for 99.99% of the time everything is probably working fine – the trick is to concentrate attention on the exceptions.

Events processing is ideally suited to the concept of exception management. In other words, while business operations are proceeding within defined limits, everything is allowed to continue freely. It is only when a defined business condition occurs that the business events processing software jumps awake. In reality, the software never really sleeps since it is probably monitoring a whole lot of sensors to check if any of the defined events have occurred, but this is a very passive sort of activity. However, the effect is that handling business events is a great way to manage operations based on business exceptions, which is the most efficient and sometimes only way for real-time operational systems to be sensibly controlled and monitored.

So business events handling and the associated products can provide an efficient, cost-efficient way to quickly leverage improved business transparency, which in turn provides an effective way to address the needs for more accurate, efficient, flexible and even real-time risk mitigation. But the missing piece is how to place the business sensors within the existing IT workload, and as discussed previously this is a particular challenge for mainframe workloads like CICS applications.

IBM's CICS joins the event fold

For those thousands of major corporations running the majority of their day-to-day operational systems under IBM's CICS transaction processing system on System z, while the CICS / System z combination has proved remarkably effective and resilient over the years its one drawback has been that of business visibility. This has not been a pressing issue until recently – after all, these mission-critical systems work well and have done for a long time, so where is the problem?

In essence, as highlighted earlier, the problem is that CICS applications have usually been designed to be driven through a user interface, executing whatever service is requested efficiently, reliably and effectively. An analogy might be a mathematician answering all the questions in an exam with the right answers, but without showing the working out that got to those answers. Good governance is not just about getting the right results, but also about being able to validate that these results have been obtained in the right way and within the bounds of defined business practices or adhering to external regulations.

IBM has already delivered new business events processing capability in the shape of the WebSphere Business Events product, based largely on its acquisition of AppSoft. However, while this software is adept at processing events from multiple sources, correlating them and executing the desired responses to the detected events, its effectiveness is limited almost entirely by the extent of its sources of events. In some newly developed service-oriented architecture (SOA) environments, this is not too difficult a challenge to meet because the design of SOA applications is to have multiple linked business services that each relate to a particular business activity. This makes it relatively easy to hook the events monitoring software into the relevant business events. However, CICS does not have the same sort of externally visible business-function bounded architecture. From the business operations point of view, while the results can be checked the 'working out' is not visible.

IBM's answer is to deliver new CICS functionality, initially as an IBM SupportPac and presumably to be incorporated into the product at a later date. The new support enables event information to be generated and emitted from CICS applications and passed on to WebSphere Business Events for processing. Basically, the CICS programmer finds the relevant points in the application and makes a CICS call to generate the event information at that time and pass it to the events processor. So, for example, at the point a CICS application implements a transfer of funds, a piece of logic could be inserted to check if the transfer was in excess of $100M and if so to generate event information and send it to the events processor, which will in turn determine if this might be part of a set of business conditions that it has been told to detect.

The details of this support and how to use it are available from IBM, bust as far as this paper is concerned the key point here is that IBM has now provided a way to 'get under the covers' of CICS applications. It now

becomes possible to instrument the applications so that events can be used to provide the upgraded risk and compliance management that current business circumstances demand.

Using events to manage compliance and risk

The following scenarios are hypothetical, and are intended to demonstrate some example of how business events support can help users upgrade their compliance and risk management, particularly with CICS workloads on System z, based on the latest IBM events support. For the sake of this discussion, attention will be focused on the finance industry since this market sector is finding itself very hard pressed in terms of risk and compliance management, as discussed earlier.

One of the common themes is the fact that financial services companies have frequently been in business a long time, and have developed a wide array of application systems for different business disciplines. One system might deal with corporate actions, another with trading needs and a third with account handling, for example. Frequently, a big challenge on the risk and compliance management front is getting a consolidated assessment across all the different operational systems, and of course events handling helps address this issue.

Scenario 1 – Corporate Actions

A particularly topical scenario might be related to Corporate Actions. The story of the European bankers and Lehmann Brothers is well-known to many, and forms a useful basis for a hypothetical scenario for the use of business events. For those who may be unaware of the details, essentially a European bank transferred a sum in the order of €500M to Lehmann Brothers after it had gone bankrupt. Of course, the money cannot be recovered, and so the bank is significantly out of pocket. The problem here is one of accurately assessing counterparty risk, and more importantly in a timely manner. Before the recent global economic difficulties, banks could afford to apply a lot more leeway to this issue – it would be reasonable to assume that if the counterparty is another major financial institution, then risk is minimal. However, in the rapidly shifting new world these same assurances do not hold nearly the same weight. So instead, banks need to watch developments around counterparties much more carefully.

Corporate Actions systems are designed to receive relevant company information in this area, such as Lehmann Brothers going bust. But if that information is not adequately linked in real time to the payments system, then this is of little value. If, instead, a set of business events were defined that reflected increased counterparty risk based on activity within the corporate actions application suite, then other operational systems such as payments could be made aware if a significant event has occurred. In simple terms, the action resulting from the event of a counterparty going bust should be to immediately suspend all transfers to that counterparty.

Scenario 2 – Money Laundering

While a particular corporate actions-related event might be a straightforward example of event handling, at the other extreme is money laundering. Financial institutions are required to report suspicious activities in terms of money transfers, where money laundering might be taking place. Unfortunately the criminals engaged in money laundering often make use of large numbers of accounts, trying to make their activities as difficult to read as possible. However, there are a number of complex activity patterns that at least raise a flag to the possibility of money laundering. In order to accurately assess and detect these patterns, it is often necessary to be aware of large transfers of funds across the bank's systems and the parties on whose behalf the transfers are being made.

This is an immensely complex scenario, but taking a highly simplistic view a bank might define an event to represent the transfer of more than a specified limit of funds. On occurrence of the event, the involved parties are recorded. Now, advanced analytical software can analyse the detected events, correlate them and look for

the suspect patterns. If such a pattern is detected, then the necessary parties can be informed and actions taken.

Scenario 3 – Best Execution Trading

There are numerous regulations in different countries and trading areas across the world governing securities trading, and one area that is the subject of much regulation is 'best execution' trading. Best execution is all about executing orders while taking into account not just the price but also the cost, speed, certainty of execution and various other factors. In Europe, for example, MiFID (the Markets in Financial Instruments Directive) requires investment companies to publish their policies on best execution, and it is then up to the corporate compliance department to monitor execution of that policy and log any exceptions for further investigation.

Events technology allows the situation where a client is offered a trade that is not at the best price to be detected and the compliance officer informed. Wider information gathered at the same time might point to the same trader being involved each time, perhaps indicating a suspicious pattern. Of course there may be a valid reason for the trader overriding the best execution offer – perhaps the client has specified special conditions on the trade that restrict the way the order is to be filled, for instance. But at least if the compliance officer is made aware of the situation and it is logged, then management can demonstrate that it is exerting the correct level of governance, being aware of the situation and prepared to act if appropriate. This is one of those strange situations where compliance management is not about showing whether the best result was delivered, but proving that the correct procedures were followed regardless of the final outcome.

Summary

IT must continue to deliver the support to handle the day-to-day operations of the business, as it does today, but at the same time it must open itself up more widely to closer inspection, particularly from a business perspective. Today's systems monitoring software may shine a light on the minute-by-minute technical performance of IT, but it is little use to a business executive struggling to ensure operations remain within corporate policy and externally regulated guidelines because it is based on an IT perspective of operations rather than one that relates more closely to the execution of the business transaction.

Events processing technology provides exactly the sort of IT capability needed to address the lack of transparency displayed by many applications in the IBM mainframe environment, and thereby to provide business-oriented insight into operational performance and execution. The events-based solution involves a way to define particular business conditions or occurrences of interest, the means to gather information to determine if any of the conditions have been met and a facility to take a pre-defined action if an event is detected. As such, compliance and risk can be managed on an exception basis, raising a flag to compliance officers only when specified boundaries have been crossed.

Judicious use of the new technology helps companies to clearly demonstrate adherence to regulations throughout operations, and can provide a much clearer and more up-to-date assessment of risk, allowing companies to compete more effectively by delivering a higher level of confidence that corporate activities remain within acceptable operating criteria, and therefore enabling greater freedom in trading activities.

About Lustratus Research

Lustratus Research Limited, founded in 2006, aims to deliver independent and unbiased analysis of global software technology trends for senior IT and business unit management, shedding light on the latest developments and best practices and interpreting them into business value and impact. Lustratus analysts include some of the top thought leaders worldwide in infrastructure software.

Lustratus offers a unique structure of materials, consisting of three categories—Insights, Reports and Research. The Insight offers concise analysis and opinion, while the Report offers more comprehensive breadth and depth. Research documents provide the results of practical investigations and experiences. Lustratus prides itself on bringing the technical and business aspects of technology and best practices together, in order to clearly address the business impacts. Each Lustratus document is graded based on its technical or business orientation, as a guide to readers.

Terms and Conditions

Lustratus Research Limited
St. David's, 5 Elsfield Way, Oxford OX2 8EW, UK
Tel: +44 (0)1865 559040

www.lustratus.com

Ref STC/LR/43680422/V1.0