Cost-Effective Compliance

What it Consists of
and
How to Achieve It

By
Don Farber
Co-Founder, Vineyardsoft Corporation

Vineyardsoft Corporation
www.vineyardsoft.com
800-850-8055

Sarbanes-Oxley™. Also known as “SOX”. Two names that appeared within the last decade and now typically evoke a reaction amongst executives and IT professionals alike that usually includes much head-shaking and eye-rolling.

Why such a negative reaction?

In a word, overhead. The amount of time and money required for an organization to become “compliant” – whether with the Sarbanes-Oxley rules, or a different set of guidelines – is considerable. In fact, a 2007 report on the cost of implementing SOX among 168 companies showed an average cost of almost two million dollars. (Yes – “million”.)

So is it a surprise that any company outside of the Fortune 500 runs for cover whenever the subject of “compliancy” is raised? Hardly.

So why should an organization strive to become compliant, just how do you go about doing so, and is it possible to implement a set of compliancy rules without breaking the bank, and without causing a mass mutiny of your IT staff?

What is “Compliancy”

In its most fundamental form, an organization that agrees to be “compliant” is in essence agreeing to conduct their business according to a set of widely-known and widely-acceptable rules. One such set is Sarbanes-Oxley, but other such sets with different rules also exist.

The concept of compliancy initially reached the forefront of business initiatives back in 2002 when the “Sarbanes–Oxley Act of 2002” was passed in the U.S. congress. The need for companies to follow certain business guidelines was precipitated by questionable events surrounding major U.S. corporations such as Enron, Tyco International, Adelphia, Peregrine Systems and WorldCom. These events (a kind word for “scandals”) cost investors of these businesses billions of dollars.

So it was decided that publicly-held companies needed to operate their businesses according to certain guidelines; these guidelines, to a large extent, require organizations to do four things:

- Audit the history of critical activities
- Monitor their business data
- Communicate / Report on business activities
- Define specific actions in response to various business conditions

Now most businesses today would probably assert that they do these four things “to some degree” – and even the organizations mentioned previously could have asserted that prior to 2002. But unfortunately, prior to 2002, no one had yet defined what an acceptable “degree” was.

And, as history has demonstrated, far too many organizations – when left to determine this for themselves – will often do the least possible amount of compliancy-checking, and this leaves open too great a potential for organizations to hide critical information from their investors and from the public at large.

Why Be Compliant? (Because You ***Have*** to)

For some organizations (such as the ones mentioned in the preceding section), becoming compliant isn't a choice. If an organization is publicly-held, they need to be accountable to their investors. And, defined according to the best interests of investors, compliance rules such as Sarbanes-Oxley were created to give investors a sense of security and to force companies to be more diligent in their everyday practices.

And it's worked. Compliant companies are less-able to conduct nefarious business transactions and public investors are correspondingly less concerned about the stability or practices of the institutions they invest in.

But compliance has come to such organizations at a cost – often a great cost in terms of compliancy infrastructure and staff resources. So -- if you were to ask many of these compliant organizations whether they would *willfully* have chosen to become compliant, the unfortunate answer is often "no".

Why Be Compliant? (Because You ***Want*** to)

However . . .

Organizations are beginning to realize that there are some significant benefits to becoming compliant, if only the cost to do so were not so overwhelming (or as overwhelming as many organizations think it is).

There are two reasons why compliancy initiatives are becoming more common among those organizations that are not legally-bound to become compliant:

1) **Better decision-making & improved efficiency**. In learning about compliancy rules, organizations are realizing that these rules (to a great degree) reflect "best business practices", such as auditing, exception management, pre-emptive alerts about activities *before* they become problems, and so on.

   As it turns out, the kind of compliance information that a public corporation is required to divulge to their investors is the same kind of information that managers or executives within a company would be interested in. In a nutshell, it's this kind of business activity and transactional information that helps executives make better decisions, and helps departmental staff make better use of their time.

2) **Improved customer service & customer relations**. So much of compliance rules are about communications – whether to investors, customers, prospects, suppliers, etc. – that businesses today realize that with compliance comes improved customer satisfaction.

   Customers are kept better informed (about such things as expiring contracts, expiring leases, the status of deliveries, and so on), organizations are more able to anticipate and predict client needs, and the response time to client requests is significantly shortened.

   But most importantly from a customer service perspective is the fact that with compliance comes a corresponding set of "managed expectations". More and more organizations are realizing that without "set expectations", they can never hope to meet or exceed the expectations that their clients bring to every encounter. Compliance is all about commitments, and once an organization commits to meeting those things that are

expected of them, they now have a clear path to both meeting and exceeding those expectations.

So – that being the case, why isn't every company clamoring to claim the "compliant" label? The answer is that for many years now the prospect of becoming "compliant" has simply been a prospect that most organizations find too expensive, too complex, and too time-consuming to implement.

And that fact demands that we take a look at how most organizations go about trying to achieve some degree of compliancy.

How Organizations Try to be Compliant

Organizations today often rely on some combination of the following three tools to monitor their business' daily activities and keep their organizations running according to their own set of acceptable business practices:

- Internal audit reports
- Managerial exception reports
- Interactive analytics

Audit reports have existed almost as long as the financial departments that rely on them; reports on "cash in & cash out", "check reconciliations", and other such information have long been relied on by CFOs and CEOs alike. And although showing valuable information, audit reports suffer from one major issue – timeliness.

By their very nature, audit reports show what "had happened" – and they are typically run on infrequent periodic intervals such as weekly, monthly, or quarterly. The information within them is often out-of-date and if it did reveal lapses or problems, the response was typically "oh well – we'll try to do better next time".

And – when "next time" arrived . . . and passed, those same reports were reviewed again to see how an organization performed. Hopefully, better – but if not, there was always another "next time" to look forward to.

So, audit reports were useful in showing an organization when, where, and why they were (and were not) compliant, but the information in them was so old – and so rarely reviewed – that they seldom helped an organization improve on their compliancy.

Managerial exception reports are a newer concept – and a good one. Exception reports were bred out of the understanding that in order to run most efficiently, an organization needs to perform their daily activities within an acceptable range of values. Invoices need to be paid within an acceptable timeframe, stock needs to be re-ordered when it drops below a certain percentage, and so on.

Thus managers quickly realized that they needed to know when their business' activities fell outside of those acceptable values.

Those occasions – referred to as "exceptions" – became as invaluable to managers and executives as any analytical tool in their arsenal. Unfortunately, the value of exception reports is too often reliant on too many manual processes – the process of running the reports, the process of delivering those reports to the appropriate recipients, the availability of those recipients to review those reports, and (ultimately) the ability for those recipients to take some kind of meaningful action in response to the data shown.

Too many opportunities for meaningful data to go unseen and un-acted upon. And so, in an effort to cut out the steps of running reports and delivering reports, we see tool # 3, or . . .

Interactive analytics, also known as "slice and dice" solutions. The edge that interactive analytics have is that the data is "right there" – right in front of the person who (hopefully) is empowered to do something about it.

And interactive analytics are great tools, but not ideal for compliancy purposes for two simple reasons. First, they are – by nature – interactive. Someone has to stop what they're doing, run them, and review them. Who's going to do that – and how often is *often enough*?

Secondly, interactive analytics are ideal for managers, but compliancy affects all members of an organization. Do you really want your folks in sales, shipping, or HR to be playing with an interactive analytical tool, checking to see if they are "in compliance" rather than doing their regularly scheduled jobs?

And thereby lie the top three challenges of compliance – the inability to monitor and respond to business activities in a timely manner, an overly high reliance on manual processes, and the need for human intervention to perform the appropriate monitoring and/or response.

How Organizations Can be Compliant

Compliancy – regardless of whose rules you play by, typically involves the following four items:

1) Automated documenting (auditing) of specific business activities (e.g., financial transactions)
2) Automated monitoring of acceptable operational parameters
3) Automated delivery of required information
4) Automated actions in response to certain business activities

You'll notice a bit of a "theme" in the preceding four items – the word "automated". And that's what's key to an organization's ability to adhere to a set of compliancy rules; by automating the various aspects of the compliancy process, the challenges of timeliness, manual labor, and human intervention all go away.

But let's explore each of these 4 aspects of compliancy a bit more closely.

Automated Documenting of Specific Business Activities

Call it "automated documenting" or call it "auditing", they both speak to the same fundamental need of any system of compliancy – the need to track when certain business activities occur and when changes happen within those activities. Transactions over a certain dollar amount, adjustments made to inventory based on physical counts, and writing off uncollectable receivables balances are all good examples of business activities or transactions that often require auditing in order for an organization to comply with specified guidelines.

So too is the ability to audit changes to key information within an organization or within an organization's business activities. Tracking when a client's credit status or credit limit was changed, when a supplier has changed the cost of an item, or when a job's budget is altered are all very typical examples of the need to audit.

But most critical of all is the need for these audits to occur automatically and dynamically. Auditing often needs to occur multiple times during the day; even if nothing of importance happens during 95% of those audits, the remaining 5% -- which catch critical activities **when** they happen – are what makes this whole process work.

Automated Monitoring of Acceptable Operational Parameters

This is truly at the heart of any compliance system; by its very definition the word "compliance" implies a sense of boundaries between which an organization is expected to operate. "Out of compliance" means that something has occurred that has fallen outside of those predefined boundaries.

And if that concept sounds familiar to you, that's because we've mentioned it earlier in this document – only that time it was referred to by its more familiar title of "exception management". Anything that falls outside of an organization's acceptable operational parameters is considered an "exception" to normal processing and thus worthy of attention, response, and – hopefully – prevention.

The key to making exception management succeed is the ability to automate the "three R's" that constitute exception management – **run**, **review**, and **respond**. Exception management is useful only if all three of these happen – and happen without human intervention. Exception monitoring must occur automatically and periodically, exception details must be automatically delivered to the appropriate people, and – wherever possible – automated responses to pre-defined exception conditions must occur.

Automated Delivery of Required Information

The scandals that hit the market prior to 2002 were primarily due to one major failing within organizations – their inability (either intentional or unintentional) – to keep people informed about what was happening within their businesses. And that's why one of the key components of any compliancy system is the automated delivery of relevant data to the appropriate parties.

Now this might not seem like such a big deal – but it is in fact one of the most difficult aspects of compliancy to implement due to three specific criteria:

- The delivery must be automated (not dependent on human intervention)
- The delivered information must be "relevant" – i.e., include only those details that are related to the business condition that occurred
- The information must reach the most appropriate recipients

And this is precisely where traditional reporting or analytical tools fail to meet the requirements of compliancy systems. Reports too often deliver too much information, leaving the reader to hunt down the specific details they require. Interactive analytical tools rely too much on human initiative, and typically are restricted to access by a select group of managers, due to their cost and demands on time.

Automated Actions in Response to Certain Business Conditions

The last major component for an organization to achieve compliancy is the definition of logical actions that automatically execute in response to pre-defined business conditions. In many organizations these actions are referred to as "workflow".

Now the automatic creation of audit trails as well as the communication of key business data can also be considered kinds of "workflow actions". But in terms of software applications, "workflow" is more specifically thought of as business processes that get triggered within an application as a result of specific business conditions occurring.

For example, you might have a compliancy rule that states if a client is over 30 days past due, you should not process any additional orders for them. Thus the "workflow" for this rule would be to put such a client on credit hold within your accounting system.

Automated actions are what makes compliance really pay off, because what good is it to identify when you go out of compliance, to document and communicate it, if you're not able to respond intelligently to the out-of-compliance situation when it occurs?

When "stuff" happens, an organization bound by compliancy rules does not leave the appropriate responses to chance. And that's the final link in the chain that makes compliancy systems work.

Cost-Effective Compliance

So – is there a cost-effective way to implement a system of compliancy guidelines without breaking the bank and without requiring hundreds of staff-hours to implement and maintain it?

Fortunately, yes.

Right around the time that Sarbanes-Oxley came to light, a type of software solution called "Business Activity Monitoring" entered the marketplace. With its own irresistible acronym ("BAM"), Business Activity Monitoring technologies arose out of the direct need for organizations to automate the four processes that embody the drive for compliance.

BAM solutions automate the monitoring of business data; exactly what conditions are monitored are determined by each company and are based on their business, their industry, and any compliance regulations that exist there. And of course with monitoring comes auditing and the ability to detect whenever key business data has been changed.

But the monitoring performed by BAM solutions go far beyond traditional auditing or even standard reporting. BAM's analytical capabilities often approach those of interactive "slice and dice" solutions, so that trends, exceptions, and even cross-departmental analyses are possible. And because compliance applies to an entire organization (and not just to individual departments), most BAM solutions complement that by monitoring all business data, including email activity and operating system conditions.

From an "automated response" perspective, Business Activity Monitoring solutions fulfill all the needs of your typical compliance solutions. Those include the real-time delivery of relevant data, whether those communications are as simple as a short text message saying "we just processed the following transaction" or as sophisticated as a proposed purchase order backed up by historical sales analysis.

And those automated responses extend beyond *communications* to the actual *automation* of pro-active business processes – much as in the example discussed earlier of automating the process whereby an overdue client is automatically placed on credit hold to prevent future orders from being placed for them.

But what really sets BAM solutions apart from other compliancy-support systems is their low price point and exceptionally low total cost of ownership. BAM solutions can be adopted for less than $2,000 per organization – and rarely exceed a maximum cost of $10,000. (Prices are typically

based on the number of front-office and back-office software applications that an organization wishes to monitor for compliancy.)

In fact, the most expensive part of a BAM solution for compliancy purposes typically occurs before the BAM solution even arrives. That's the time when you need to define what compliancy rules your organization needs to operate by. In some cases, such as Sarbanes-Oxley, those rules are presented to you – but you still need to determine how to apply them to your own business model. And don't be surprised if that process takes more than a few hours to complete.

But once you have defined the compliancy rules as they pertain to your organization, your industry, and your data, the configuration of a BAM system to support those rules is typically a rather straightforward one – often just a series of "if – then" business scenarios. After that, BAM becomes a "set it and forget it" solution in which compliancy checking is automated and the rest of your staff can get back to business as usual.

To Be or Not To Be . . . Compliant:

Compliancy regulations such as Sarbanes-Oxley came to the forefront of the business world because a select few companies – albeit exceedingly visible ones – decided to take advantage of the fact that they didn't have to be accountable to their shareholders. And so, not only was the concept of compliancy thrust upon us, but so too was the notion that compliancy was necessary to "keep bad things from happening" in our business world.

That's an unfair label to give compliancy, because a system of compliancy is just as capable of promoting beneficial behavior within a company as it is of preventing bad behavior from occurring.

And it's unfortunate because too many organizations still view compliancy as a kind of punishment imposed on them, their staff, and their pocketbooks. And of course this perspective wasn't helped by the fact that early compliancy initiatives often cost companies in the millions of dollars and – due to their reliance on extensive manual processes – were an absolute horror to implement.

To be sure, one of the benefits of compliancy is that it gives shareholders a greater sense of security in terms of how the organizations they invest in conduct themselves. But more and more organizations today – even those not in the public eye – are beginning to see the value of conducting business according to a set of compliance rules.

Compliance gives organizations greater visibility into their everyday business activities. It gives them faster recognition of – and an ability to respond to – exceptions in daily business transactions. And compliance pushes organizations to define "standards of operation" that yield the best possible business results – greater productivity, greater profitability, and superior customer relationships.

And so, given the choice between adopting a compliancy system and not adopting one, the potential business benefits to adopting compliance make that an easy decision. And with the advent of Business Activity Monitoring solutions, organizations can now make the choice to become compliant in a manageable, cost-effective manner.