EXECUTIVE BRIEF

Changing the Compliance Formula
– *and Improving Competitiveness*

A STEP-BY-STEP APPROACH TO COMPLIANCE

SIX SIGMA **QUALTEC**

Executive Brief

A STEP-BY-STEP APPROACH TO COMPLIANCE

Changing the Compliance Formula – and Improving Competitiveness

This is the first of two Executive Briefings designed to provide a step-by-step approach to compliance that can improve your competitiveness. This paper is designed to help you rethink the nature of compliance and your response to it. Briefing two will address strategies for deploying process excellence tools in your organization to achieve optimum compliance.

If your company is like most, you face growing regulatory and compliance demands that sap your competitiveness, absorb time, money, and other valuable resources. Yet despite your best efforts, these resources do not sufficiently reduce your risk of violations. Perhaps you console yourself with the thought that your competitors face the same burdens. Like thoroughbreds in a stakes race, all competitors have to carry the same weight, so that at the end of the day compliance isn't a factor in the outcome.

But all compliance programs aren't created equal. When you're facing tough questions with SOX, the EPA, OSHA, FERC, the FDA, the SEC or other agencies, how you approach the issues can make an enormous difference in the performance of your compliance process and thus your degree of risk and the costs you are incurring. If you can improve process performance, mitigate risks, and cut costs you gain tangible advantages over your competition – including the luxury of being able to devote more time and money to your core business. We believe that an appreciation of process fundamentals, the application of process excellence tools, and the strategic deployment of your compliance program can take you beyond compliance to greater competitiveness. It begins with a rethinking of the nature of regulation and compliance.

Understanding the Regulatory Arena and Compliance

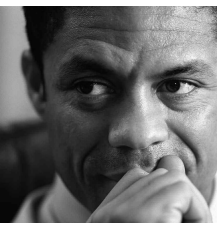
A clear-eyed view of the realities of the regulatory environment and your company's place in it is essential for dealing rationally with compliance. Make no mistake about it; many regulatory frameworks were earned by the companies they govern – and it was not for good behavior. The regulations are designed to prevent unfair advantage, misleading financial reporting, fraud, dangerous practices and products, and other forms of abuse.

Such rules and laws are a constraint on what you can do, not a guide. Too often organizations look to the regulations for guidance on how to how to execute the company's processes to bring them into compliance – in effect, deferring to someone who knows less about the processes than the company does. It is far more effective and efficient to use regulation for specification – that is, to define what must be achieved and how high the bar is set. Remember, too, that regulations specify the minimum standard that you must meet – and there is no extra credit for going above and beyond it.

Given the interests of various players, enforcement of those minimum standards can be exacting and unforgiving. Your auditor, for example, does not want to miss something that your regulator subsequently catches. Regulators, fearing that the General Accountability Office (GAO) might accuse them of doing a poor job, do not want to be blamed for your non-compliance. Above all, regulators do not care about you; they are there to protect others from you.

Faced with these realities, you must find a way to meet regulatory requirements that is measurable, reliable, and efficient. Merely managing the issue by opinion can be very expensive – interpretation by a lawyer that you are in compliance is simply insufficient. You must be able to drive compliance to a measurable specification. Management by fear can be even more expensive, inducing you to greatly overspend on compliance and to shy away from reasonably acceptable risks that could mean far better business results.

Amid the fear and confusion that often surrounds compliance, this much we do know: it costs companies much more money than their accounting systems say; many of their compliance efforts don't work very well; and their procedures, approvals, and inspections often



fail to satisfy regulators. The accounting system may track, say, expenditures in Quality Assurance or Legal but, from the boardroom to the back office to the shop floor or the branch office, many uncounted hours are devoted both to achieving compliance and to demonstrating that it has been achieved. Despite this enormous expenditure of time and money, many companies are still regularly found to be at fault. They may then redouble their efforts; but because their compliance processes are premised on the concept of inspections after the fact, they are managing only to constrain non-compliance, not to prevent it. As a result, the organization continues to hemorrhage resources.

In rethinking compliance, it is crucial to distinguish between a regulatory requirement and how it is satisfied. A regulatory requirement is a rule that must be observed or a standard to be met. Often, organizations take a broad-brush approach and simply establish a policy that says, in effect, to meet a rule in precisely the same way each time the rule applies.

For example, when changing a process or developing a new one an organization operating a government facility was required to submit proposed changes to regulators for review and approval before work could commence. The company's review policy required that a large number of individuals review and comment on the proposed changes before submitting them to the regulators. Although it was often unnecessary for everyone to comment, they did so anyway because it was expected of them. However, in most cases, a subset of the reviewers could have easily met the regulatory rule, depending on the type of process and issues being reviewed. But because of the company's rigid and far too broad policy, the review process was lengthy, fraught with re-work, and painful.

Further, policies and procedures are not controls. A policy merely states an intention to do something; a control ensures that it is done, done repeatedly, and done up to standard. Moreover, policies have to be read, understood, and remembered, all of which opens many possible routes to failure.

As the quality pioneers of the twentieth century taught us, work is accomplished through processes – and in no other way – whether they are manufacturing processes or business processes. To achieve compliance you must be able to improve those work processes or design new ones. In other words, the way in which you meet a requirement must be embedded in the work itself, not merely displayed on a policy document. In order to sustain compliance, you must be able to establish controls within those processes. Certainly, you may have policies that apply, but the way in which we build, operate, and control work processes constitutes how we meet a requirement.

Weighing Risks, Consequences, and Costs

The struggle to achieve compliance entails different types of risks, different consequences of different magnitudes, and different kinds of costs. As we improve processes or create new ones, we therefore must make choices that balance those elements against the level of effectiveness of the controls we establish. Controls should be commensurate with risks, consequences, and costs – neither overcompensating nor undercompensating for them.

Understanding Process Risks

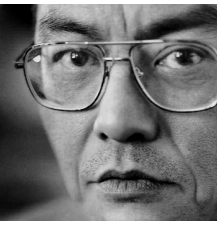
The risks in processes are generally of three kinds:

DETECTION: How likely is your process to detect a defect or an infraction or to confirm success? In a football game, for example, are all infractions detected? When the referee spots the ball after a play can there be any assurance that he is spotting it correctly? When the referee is some distance away, is that pile-up at the goal line a touchdown or a successful goal line stand? Instant replay, of course, was instituted to improve detection, but the results are often ambiguous and still depend on human judgment.

Many business and manufacturing processes rely on human inspections to detect defects. Do all inspectors detect equally? Are any distracted? In manufacturing facilities, many of these inspections are in a noisy, fast-moving environment. In services settings, such as checking mortgage applications for completeness and accuracy, "inspections" often take place in similarly distracting circumstances.

Executive Brief

A STEP-BY-STEP APPROACH TO COMPLIANCE



An electric utility was working diligently to repair an accounting process found non-compliant for SOX. When the fixes were in place a Measurement System Analysis (MSA) revealed that the process captured only 80% of the defects. The process was then able to deal with the defects it was detecting but because a significant number of defects still passed undetected the company was in a far more dangerous situation than they perceived.

DECISION OR EVALUATION: Even if you do catch an anomaly, are you able to label or judge it correctly? For example, in our football game, when a receiver and a defender become entangled is the interference defensive or offensive? Was that ball bouncing around loose in the backfield a forward pass or a fumble? Or consider election officials in Florida poring over defective ballots in the 2000 presidential race with magnifying glasses – often hopelessly trying to judge correctly the voter's intent.

When you review a document, how do you decide if it is acceptable or unacceptable? Should it be reviewed, for example, by in-house legal staff or by far more expensive outside counsel? Does a procedure meet the regulatory standard or not? When you review the evidence in a filing how do you determine whether it is complete and correct?

EXECUTION EFFECTIVENESS: How well or often does the process meet the requirement? What is the probability of meeting the requirement each time? This involves the actual process capability. (Six Sigma methodology calls this the Sigma level – the defects per unit.) If a process has a failure rate of 2%, we are likely to have a risk of non-compliance two out every hundred events.

Understanding Consequences of Failure

The consequences of failing to mitigate such risks can range from a nuisance to a catastrophe and many points in between. For example, defense contractors must comply with stringent government regulations in, among many other areas, the use of IT and software. Employees are forbidden, for example, to surf the internet on government time. If detected, such a violation is likely to result in a relatively trivial consequence – a reprimand or the like. Consider, however, the more serious example of a defense contractor who, because certification of the software it employed was nearing expiration, faced the prospect of recertifying every piece of software on every PC – at a potential cost of several million dollars.

Potential nuisances should not receive the same attention as potential catastrophes. Moreover, when establishing controls that are commensurate with the risk, the probability that a particular consequence will occur, as well as its magnitude, must be taken into account.

Understanding Costs

There are three major categories of costs:

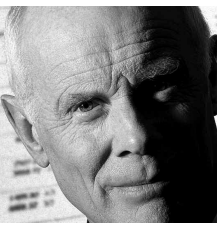
COMPLIANCE: These costs encompass the systems, resources, spend, and investments associated with compliance. These familiar expenditures could range from technology used to monitor processes to Quality Assurance personnel to legal resources to the hours each person spends dealing with compliance development and execution, including:

- ❏ Reports
- ❏ Evaluations
- ❏ Meetings
- ❏ Software and monitoring systems
- ❏ Regulatory filings
- ❏ Audits and auditors
- ❏ Lawyers
- ❏ Conferences
- ❏ Lobbying
- ❏ Dedicated departments and executives (CCOs)
- ❏ Mandatory training
- ❏ Approvals reviews
- ❏ Documentation and records
- ❏ Environmental cleanliness technology
- ❏ Vendor processes
- ❏ Security clearances, processes, resources, technology
- ❏ Software qualifications and testing

But compliance can also create opportunity costs – the most frequently overlooked costs when assessing the impact of compliance. For example, SOX has made many foreign investors leery of investing in American jurisdictions and risking exposure to the penalties for non-compliance with the law.

Executive Brief

A STEP-BY-STEP APPROACH TO COMPLIANCE



But the most fundamental opportunity cost, however, is that the time spent on compliance is time not spent on the company's core business.

NON-COMPLIANCE: These costs include the penalties, recovery activities, loss of business, loss of investment, and damage to reputation that result from non-compliance. For example, in the pharmaceutical industry, the failure of a product batch to meet specifications results in costly internal investigation of the source of the failure, rework, time-consuming reporting and record-keeping, suspension of manufacturing, and missed market opportunities due to lack of product to meet demand. Repeated failures of this kind can lead to FDA investigations and, in some cases, the shuttering of plants that fail to meet the agency's good manufacturing practices (cGMP) requirements.

Non-compliance can also result in long-term costs. The more frequently companies fail to comply with regulatory requirements, the more regulation is created to bring them into line. Prior to SOX, there were numerous SEC rules about acceptable accounting practices, but spectacular and widespread accounting scandals made those rules appear to be inadequate. As a result, Congress imposed the far more comprehensive, stringent, and costly financial controls of Sarbanes-Oxley. AMR Research estimates that companies will spend $6 billion in 2006 complying with SOX, roughly equal to the $6.1 billion they spent in 2005.

FEAR OF NON-COMPLIANCE: Inordinate management fears of falling into non-compliance can unnecessarily burden and constrain business strategies, operations, and processes through additional conservatism, over-investment in compliance resources, legal influence, and the promulgation of disproportionate controls. In the initial rush to comply with SOX, for example, many companies simply threw vast amounts of money and resources at it without regard to value. Because SOX violations can mean harsh penalties both for the corporation and its officers, including fines and jail time, many fearful CEOs and directors have no difficulty justifying what, in many cases, are wasteful expenditures.

Consider also the case of a leading operator of government facilities. At one facility, the company's processes dealt with materials that could contaminate groundwater and a large number of wells at the site, requiring the company to meet environmental and customer regulations regarding the potential pollution. As part of the operating contract, the operator developed and filed a procedure that required that 100% of the wells be tested with the same frequency for intrusion of contaminants. Because the company so feared EPA sanctions, they unnecessarily sampled all of the wells with the same frequency, although a large percentage of the wells had been inactive for 20 years. As a result, the company was oversampling a huge percentage of wells that didn't require it and undersampling the 5% of active wells that did. This overzealous approach was not only costly but, ironically, the company was still not in compliance.

Once we fully understand all three of these factors – the risks, consequences, and costs – we can then being to determine what controls are appropriate. As previously noted, the nature and comprehensiveness of the controls will vary with the magnitude and probability of the risks and consequences. However, there is one principle that has been proven through experience to apply to almost all cases of assuring process compliance: it is more effective and less costly in the long run to predict and prevent failure rather than to detect and correct for it. As the great quality pioneers also taught us, quality should be designed in at the outset, not inspected in later.

Detecting and correcting for failure after the fact is not only expensive, it doesn't always work. With detect-and-correct, you may find that you're dead before you realize you're sick – some infractions cannot be corrected before catastrophe ensues. For example, if you fail to comply with a SOX requirement for a material disclosure that was not detected until the financial documents were submitted, someone could go to jail.

Predicting and preventing failure is less expensive than detect-and-correct, but it requires a different way of managing. Instead of inspecting in compliance after the fact, you can deploy proven process excellence tools that identify root causes of non-compliance problems in processes as far upstream in the causal chain as possible. You can then manage those variables within the specifications for compliance, which may differ for different regulations, risks, consequences, and costs. If you cannot fix a process once and for all, then you must redesign it. Addressing compliance in this far more effective fashion requires the integration and deployment of a management system and a technical toolkit – the subject of the second installment in this series.

Six Sigma **Qualtec**

Your Strategic Partner

Six Sigma Qualtec is a premier provider of process management and performance improvement consulting, training, and technology solutions that drive breakthrough growth, productivity and value for our clients.

We are unique in our ability to customize the integration of management disciplines to meet the industry-specific requirements of global leaders in financial services, natural resources, manufacturing, process and service industries.

Princeton Office

Six Sigma Qualtec
821 Alexander Road
Suite 130
Princeton, NJ 08540 • USA

toll free (800) 247-9871
phone (609) 925-9458
fax (609) 419-9855
email info@ssqi.com
website www.ssqi.com

Tempe Office

Six Sigma Qualtec
1295 W. Washington Street
Suite 208
Tempe, AZ 85281 • USA

toll free (800) 247-9871
phone (480) 586-2600
fax (480) 586-2586
email info@ssqi.com
website www.ssqi.com

European Office

Six Sigma Qualtec
P.O. Box 2959
Kenilworth
CV8 1XR
United Kingdom

tel +44 (0) 1926 859555
fax +44 (0) 8701 400023
email info@ssqi.co.uk
website www.ssqi.co.uk