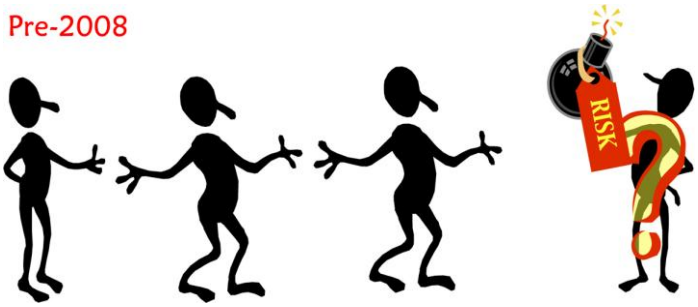
QA as a Risk Management Methodology

I've said that QA is a risk management methodology, a business strategy, and a profit driver. Let's look at the first of these. Risk to business takes many forms, but is always measured in potential lost profit. Risk is generally managed by identifying and assessing potential risks, then prioritizing the allocation of resources to minimize, monitor, and/or control them. Prioritization evaluates the probability of each potential negative event, its financial impact, and the cost of mitigating it: if it has a low probability and mitigation costs exceed estimated event costs, a management decision may be made not to mitigate.

Until about 2008, it was relatively easy to obtain good insurance. This meant that the core of a risk management plan could often simply be described as "quantify the risk and insure to that amount." With insurance as an easily erected safety net, few perceived a need to ***qualify*** the risk and adjust internal processes and procedures to actually prevent the potential event. The cost of covering the risk with an insurance policy would likely be lower than the cost of prevention, so why expend resources on process analysis and redesign? But in 2008, this scenario changed.

Insurance and Risk: Pre 2008 and Post 2008

Every company that carries insurance has a risk analysis profile. Often that profile is supported by the declared presence of QA programs, generally attested to by voluminous submissions of documentation. The risk analysis profile enables the company to obtain General Liability, Product Liability, and Errors and Omissions insurance coverage—without which it could not operate.



Instead of validating the risk analysis profiles of individual companies and industries, verifying that the calculated risk assessments were accurate, insurance companies aggregated their risks and offset them by bundling them up and reinsuring them. In theory, in a bundled package of policies, there would be a statistically even distribution of good and bad risks that reinsurers could average and value. Business insurance was offered and priced based on the actuarial risk of claims occurring and reinsured in packages.

In essence, prior to 2008 risk management was accomplished by handing off the risk: businesses passed their risk on to insurers and insurers passed their risk on to reinsurers. Neither businesses nor insurers performed real risk assessment—why should they bother, since they were passing it on? In fact, since no profiles were being validated, there was no sound basis for any risk valuation. These bundles were risk bombs waiting to go off, and they were simply passed along ever higher up the food chain, all the way to the top of the industry—the master reinsurers.

In 2008, a series of events completely changed the way in which master reinsurance companies looked at risk analysis profiles supported by documentation. As with every good game of pass the hand-

grenade or Russian Roulette, eventually there was a loser. The unvalidated risk analysis profiles of industries and companies proved to be totally inaccurate and claims escalated to stratospheric proportions. The master reinsurers started to reject claims, on the quite correct assumption that many of the risk analysis profiles on which risk assessments had been based and coverage granted were bogus, thus invalidating coverage.

Senior executives are well aware of what it will do to their bottom line if they cannot count on claims against standard General Liability and Errors and Omissions policies being paid. Either the company will end up self-insuring against whole categories of claims, or insurance premiums will skyrocket. Either way, cost and risk could reach levels that jeopardize the operation of any company.

QA and Regulatory Risk

One specific risk that cannot be insured against is the risk that the company will violate a regulation and be forced to pay fines or penalties. Indeed, there is usually a check box somewhere on an insurance application form that requires a company officer or designee to attest to the fact that the company adheres to regulations that govern its industry. While different industries are governed by different regulations with respect to their product (tangible or intangible), all companies are governed by financial regulations. The Sarbanes–Oxley Act of 2002 (commonly referred to as SOx) produced a whole slew of new financial regulations for public companies, to be phased in over a specified period of time. Almost 10 years later, the implications of some of these are just beginning to be fully understood. In particular, the impact of the requirement that management and the external auditor report annually on the adequacy of the company's internal control over financial reporting (§ 404) continues to be debated.

The Dodd–Frank Act of 2010 required the Securities and Exchange Commission to study whether the burden of complying with SOx internal control reporting requirements could be reduced for mid-sized companies while still maintaining investor protections. The April 2011 report of this SEC study recommended that compliance requirements remain unchanged. It also recommended that the Public Company Accounting Oversight Board (PCAOB—created by SOx to oversee public company auditors) continue to document its experiences through what amounts to collection of best practices. The report expressed strong support for continued development of guidance on enterprise risk management, internal control and fraud deterrence by the Committee of Sponsoring Organizations of the Treadway Commission (COSO—a joint initiative of five professional associations). COSO publishes a common internal control model against which systems can be assessed. "The [SEC] Staff believes that this project can contribute to effective and efficient audits by providing management and auditors with improved internal control guidance that reflects today's operating and regulatory environment and by allowing constituent groups to share information on improvements that can be made that enhance the ability to design, implement, and assess internal controls."[1]

So while regulators and legislators do not always name QA as an outright requirement, QA programs—where they exist—play a significant role in demonstrating to regulators and auditors that a company is adhering to regulations or accepted best practices. Indeed, in addition to the common requirements for public companies to demonstrate effective internal controls of financial systems, in many industries

[1] "Study and Recommendations on Section 404(b) of the Sarbanes-Oxley Act of 2002 For Issuers With Public Float Between $75 and $250 Million," U.S. Securities and Exchange Commission, April 2011, p. 9.

license to operate depends on attestation that there is a QA program in place governing operations as well. And then, of course, regulations mandate that any company that sells to government at any level adhere to specific quality practices whose stringency increases with the risk inherent in the product being acquired. These may range from simply requiring that sellers of office supplies have records of inspection of goods to requiring that any company that sells into a nuclear facility demonstrate by audit adherence to the NQA-1 quality standard as defined by Federal regulation.

QA and Risk Management

A true risk management profile is a total reflection of the risk potential of the company as a whole. It must be based not on paper declarations, but on the actual operations of the company. Deming's original work made two simple points that are still valid today:

1. The greater the influence of Quality Assurance programs on the operations of the company as a whole, the lower the potential risk, the lower the cost to offset that risk, and therefore the lower the insurance premium.
2. The smaller the influence of Quality Assurance programs on the operations of the company as a whole, the higher the potential risk, the greater the cost to offset that risk, and therefore the higher the insurance premium.

Look at this photograph of a small corner store in Asia and ask yourself if the sign that declares it an ISO 9001:2000 Certified Company can really be a true reflection of the way the store operates.

Photograph courtesy of Michael Bolton, DevelopSense.

Unfortunately in many overseas countries language and cultural differences have created an environment where you can literally buy a complete QA/QC package, including signs and certificates, without any adherence to QA best practices or activities of any sort. This is especially problematic for western companies who attempt to offshore work and services without doing credible due diligence on

their prospective partners. Though the impetus for offshoring is an attempt to cut costs, offshoring may actually increase costs by opening up huge liability for the western company.

So What Is Real QA?

Real Quality Assurance is a systematic methodology for doing things right. In many ways, QA is a state of mind. We say that "Quality Assurance is the assurance of quality—all encompassing, never ceasing." Let's break that down: the Merriam-Webster dictionary defines assurance first as an "act or action." To assure is to make a positive promise that others can have confidence will be fulfilled.

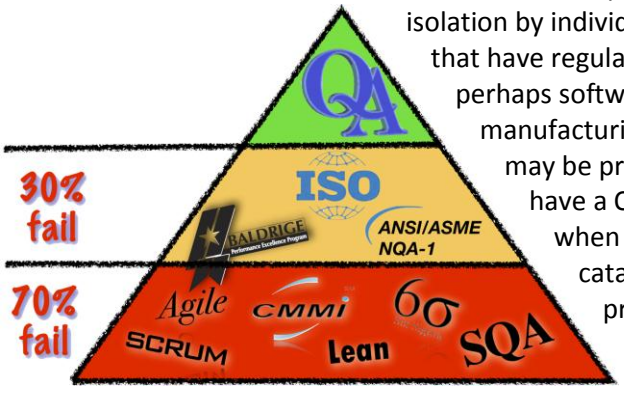
Real Quality Assurance Is …

- A systematic methodology for doing things right
- A state of mind
- A reflection of the total operations of the company as a whole
- The assurance of quality—all encompassing, never ceasing

"All encompassing" emphasizes that a promise of quality must be a reflection of the total operations of the company as a whole. We have all heard it said in jest that "the operation was a success, but the patient died." If QA is implemented piecemeal, with some departments adhering to a specific quality control protocol and others to a different one or even to none, it might be said that one aspect of the total effort was executed with excellent quality—but the customer was not satisfied with the product. Finally, "never ceasing" emphasizes that QA is a continuous and active process.

QA is a Program, Not a Manual

Quality certification programs like ISO and Baldrige for a long time relied on documentation to demonstrate that a company was applying QA in its operations. Unfortunately, this fueled a focus on documentation to the detriment of action. Most QA programs that exist today are really manuals of documented policies and procedures. Often, the entire manual simply sits on a shelf and is dusted off when the auditor comes. In other cases, individual policies or procedures are faithfully carried out in isolation by individual departments. These may be the departments that have regulatory or contractual compliance requirements. Or perhaps software developers operate under Agile and hardware manufacturing operates under Six Sigma. These departments may be practicing Quality Control, but the company does not have a Quality Assurance program! We see proof of this when we are called in to do root cause analysis on a catastrophic project failure. We ask: "What was the primary controlling quality assurance program that you were using during this failed project?" The most frequent answer is some sort of specific QC protocol—a good indicator that there really was no company-wide QA program in place. Companies that adhere to a QA program as described in this article rarely have to analyze failed programs.



Quality Assurance is Not Quality Control

Quality Assurance is a radically different approach from enforced Quality Control. At a psychological level, QC attempts to enforce seemingly arbitrary rules for human behavior—which we know is not

often a successful approach. QA, on the other hand, as exemplified in the works of Deming, promotes organizational structures that encourage employees to act in certain ways. I will point you back to Deming's 14 Points for Management, often cited as the source for a QA program, but less frequently read. Point 8 begins "Drive out fear"; Point 12 talks about a worker's "right to pride of workmanship"; the last point ends with "The transformation is everybody's job." When one reads these points, it is clear that Deming is speaking of creating a culture of quality in which companies can "cease dependence on inspection to achieve quality" because quality is built into the product in the first place.

QA	versus	QC
methodology	drives	paperwork
people	not	statistics
continuous cycle	produces	individual outputs
	≠	

Quality Assurance is about delivering customer and employee satisfaction, whereas Quality Control is often about complying with an external mandate such as regulatory compliance requirements. You could argue that QA is driven by internal culture of collaboration whereas QC is dictated by outside sources. In a true QA program, the methodology for doing things right is developed from the shop floor up, and it always drives the paperwork rather than being altered to accommodate the paperwork. People and their actions always are the focus of the program; the statistics are a byproduct that is a useful tool and not the measure of success. A true QA program is never "completed" because it is about continuous improvement, not about inspecting individual outputs.

We represent the Plan–Do–Check–Act cycle as a spiral, because we believe that real QA is a repetitive process that is always looking for further improvement by a continuous re-examination of the complete activity. Tremendous problems are caused by QC systems such as Baldrige that take the opposite viewpoint and mandate that what is happening in the real world is irrelevant, the written record is all that counts. Many importers are now supporting the legal claim that if the product is defective but the paperwork is correct, then the product is correct—and this is a large issue for the QA/QC industry

Consistency

Consistency of practices is one of the most important indicators that a company is practicing real Quality Assurance. This is a fundamental but simple principle. At the very beginning of this article, I said that true QA is both systemic and systematic. If this is so, then the evidence that QA is being practiced will be pervasive throughout an organization. Any manager or administrator can check this by simply looking at

any practice or problem and checking four aspects of any activity. When we do a process audit, the first thing we do for any process is ask four questions:

1. You **say** you are running a Quality Assurance program: describe it to us.
2. Show us the **written** documentation that supports your statement.
3. Show us your **MIS/IT** system and allow us to verify that, at all stages the programmed workflow, activity logs, and web records support your original statement
4. Allow us to visually observe as you **do** the work you have described.

We call this the Say–Write–IT–Do cycle. Very simply, if the answer to any one of those four questions is consistent with the answers to the other three, it gets a green light; if not, it gets a red or amber light.

You can perform this check on any activity, it's a very simple check that takes little time, and anyone can ask the questions (it doesn't have to be an expert in the field). Companies that practice real QA will have lots of green lights, whereas companies that don't will have lots of red lights. Paradoxically, this simple test is at the same time much easier to perform, far more detailed and generally more actionable than an ISO floor audit.

Why Should You Care?

It's true that at the beginning of this article, I talked about "religiously" practicing Quality Assurance, and QA may be my personal religion, but the practical reason that companies who have real QA programs practice it is because, when practiced correctly, Quality Assurance improves the bottom line.

Deming's Point 5 is: "Improve constantly and forever the system of production and service, to improve quality and productivity, and thus constantly decrease costs." Both Shewhart and Deming, although they were trained as scientists and statisticians, were pragmatists who focused on the practical and the operational. Deming's work in Japan in the 1950s and onward was about rebuilding the Japanese economy. His Japanese students recognized this and developed a formula that demonstrates in stark terms the connection between quality and profits. They determined that:

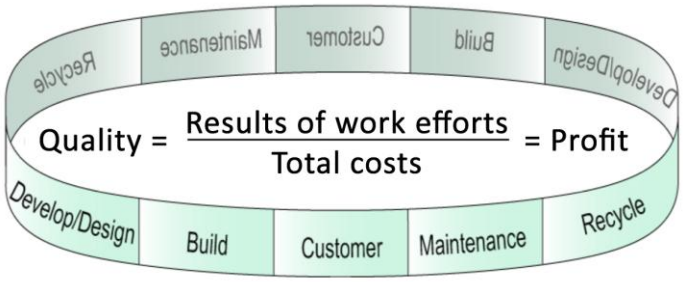
a) When people and organizations focus primarily on quality, quality tends to increase and costs fall over time. This was represented formulaically as:

$$\text{Quality} = \frac{\text{Results of work efforts}}{\text{Total Costs}}$$

b) When people and organizations focus primarily on costs, costs tend to rise and quality declines over time.

Let's expand a little bit on those two premises. First, we look at the right side of the equation and determine that it is also one definition of profit. Then, we have said that QA must be applied

consistently across all departments. But it also must be applied consistently across all phases of a product life cycle. So if we add these two factors to the original formula, we end up with:



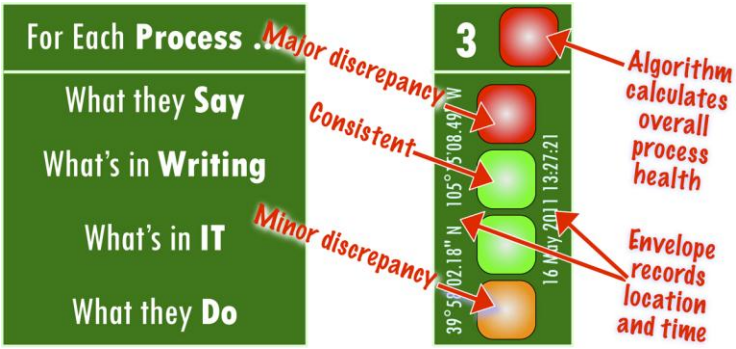
An Example

How do I know this is so? Let me cite an example from my own experience. Many years ago Fluor-Daniel became involved with Nation's Bank to develop a Best Practices/Quality Assurance system for its loan portfolio group. Initially, the QA system started in the construction loan division, but it soon spread across the entire bank. Simply, Nation's found it in their best interest to develop real best practice procedures to support their clients' utilization of the loans they were receiving. An independent review of the activities of the best practice quality assurance initiative inside the bank, supported by Fluor, found that these efforts accounted for a steady 14–20% increase in the group's profit margins.

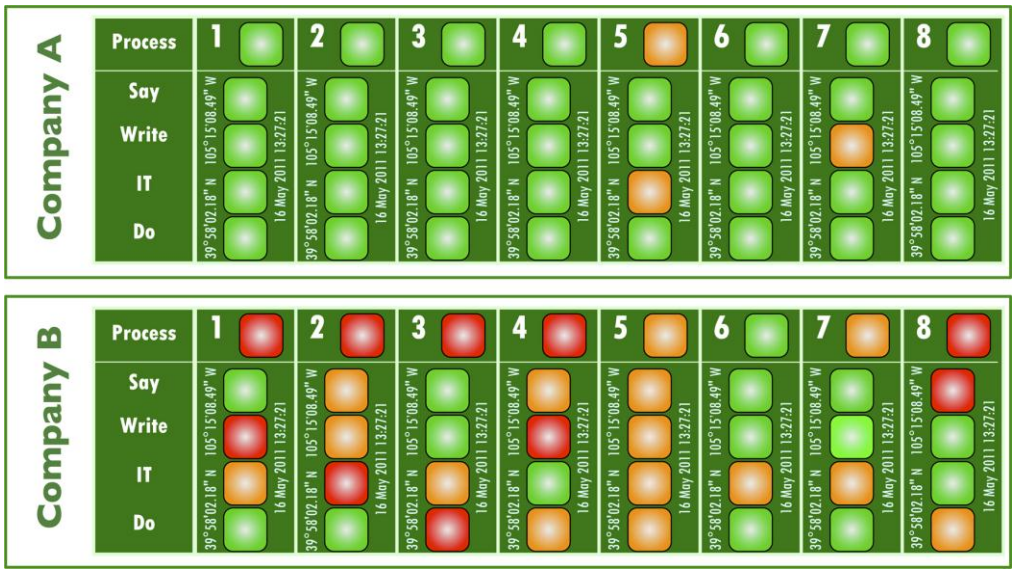
The positive impact of real Quality Assurance can be measured against the corporate bottom line, and the formula is still relevant today in all industries.

Assessing a Company's QA Program

Previously, we described a simple four-step process analysis that we use during process audits. We called it the Say–Write–IT–Do cycle. Performing this kind of analysis is a quick and easy way to tell if a company is adhering to best practices of any kind, or practicing QA. To analyze processes in this way, you do not have to know the jargon, understand highly technical issues, or have had extensive training at the highest level of any specific QA or QC program.



We use a simple web-based system to collect the results of individual process analyses, which can be logged on a mobile device. When a log entry is created, the entry envelope automatically associates each record with a location and a time. Coupled with a model of the workflow, the system uses an algorithm to calculate the overall process health based on the Say–Write–IT–Do scores.



The results of the analysis of individual processes are aggregated at any desired level (department, division, etc.) Above is a comparison of the display of results from two different companies. You can see at a glance which company is on relatively sound footing and which one is in trouble. Would it surprise you to know that Company B entered bankruptcy shortly after this snapshot was taken?

Integrated Quality Assurance

I'm going to recap what I've said:

- QA is a state of mind
- QA is a system that embraces the entire operations of a company
- QA is a business strategy
- QA is a risk management methodology
- QA is a profit driver.

With the technologies available today, Quality Assurance can easily be integrated into the information systems of any company. A simple dashboard like the one illustrated above can become a continuous monitoring system that not only alerts management when a process is veering off track, but also reassures funding sources and insurers that a company is actively practicing QA, and that its QA system is in good health.

Ultimately, however, it's the first bullet that counts. When QA is integrated into the culture of a company, waste is radically reduced and profits increase. It's that simple.