



Internal Control ~ Grasping At Straws?



For years, managers and executives in the private and public sectors have sought foolproof ways to improve their bottom line, be it enhanced profits or improved services. Those of us in government service may recall past and current attempts by New York State to improve its operations. We have seen a wave of centralizing and decentralizing services, be it computer support, fleet management, telecommunications – each change an attempt to enhance performance beyond mediocrity.

Back in the 1960’s, the State of New York employed a variety of **management improvement tools** and techniques; PPBS (Program-Planning - Budgeting – Systems), followed a few years later by PAR (Program Analysis & Review). The next wave of experimentation included MBO (Management by Objective), TQM (Total Quality Management) and HPO (High Performance Organization) as mechanisms for improving productivity, accountability and ultimately the bottom line.

A recent Dilbert cartoon featured our hero of the cubicle interviewing a prospective employee. We have a slogan: “All our employees are empowered”, to which the would-be recruit parries with “If all your employees are empowered, why do the need a slogan?”

All these past and current management trends have many things in common, so let us focus on the logic of what it takes to run a smooth operation – especially one with changing mandates, shrinking workforce and tight budget.

For starters, everything you do in government should relate back to legislation, be it your agency’s enabling statute, or a patchwork quilt of laws and regulations added through the years. If

you cannot point back to such a mandate, then it’s time to ask some questions.

In each of your operations/pro-grams/functions, you are trying to achieve one thing, while avoiding another. Public assistance programs aim to provide an economic safety net to those in need, while ferreting out fraudulent activity that scams the system. Health agencies are concerned about affordable and professional medical services, but need to be alert to unethical practices amongst pharmacies, doctors and business offices alike. Nuclear regulatory agencies are caught in a Catch-22, with citizens nervous about radioactive waste and reactor accidents, while at the same time our dependence on foreign oil has far-reaching consequences.

This may seem an awfully Big Picture to those of you with more mundane concerns, like licensing day care centers, giving eye tests to drivers, or dissecting crows and bats to monitor environmental health. But civilization as we know it depends on all its complex parts working efficiently, effectively, and honestly.



Efficiency vs. Effectiveness

Jargon and buzz-phrases do not improve communication for the uninitiated. And pet phrases from various management theories can age out rapidly. But there is more than a semantic distinction between certain pairs of similarly sounding words.

Efficiency – you may be able to process the paperwork from applicants in record time, at a rock-bottom price, with every entry scrutinized for completeness, *but*

Effectiveness – depends on the front-end of the process being tied into other activities, to ensure program goals are met. For example, does anyone double-check the veracity of the information contained in the application? Is the information collected relevant to the program function, be it licensing, small business loans, employability, or eligibility for public assistance?



What is Internal Control?

Internal control is NOT a collection of disconnected processes and procedures. Internal control IS an integrated approach to sound management. It may involve specialized equipment (combination locks, computer passwords, refrigerator thermometers, smoke detectors, fire extinguishers, etc.) but most of all it depends on PEOPLE. People who understand the why’s and how’s of the program, the significance of information generated, the purpose behind all that specialized equipment – and when to ignore it.

Internal control certainly involves PROCEDURES – be it OSC payroll requirements, OGS purchasing, OFT computer security, EZ-Pass scanners or State Police radar – but each of these procedures depends on people, people talking to other people, people entering accurate/timely data into computer systems, people following up on problems and exceptions to the rule.

Know Your People

There are people who are clearly uncomfortable when we bring up this topic. They think that there is an ironclad rule of privacy that prohibits them from learning anything personal about co-workers.

True, when hiring new workers, there are certain questions that are rightfully prohibited during the interview process. Your race, ethnicity, religion, marital status, political affiliation and sexual orientation have no part in the recruitment/selection process, be it for initial employment or promotion. But this does not prohibit you from learning a little bit about your staff once they are on board.

For example, does someone belong to an organization that is antithetical to the vision and mission of your agency? Are they working a second job somewhere that constitutes a conflict of interest, or interferes with their productivity and attendance at their government job? You

know what grade level they are – are they living beyond their means?

Of course, getting to know your people also can be a positive experience. Your file clerk by day may be a web designer at night. Your senior accountant may be a wiz at restoring old Jaguars. The shop teacher in your facility may be bilingual. Your youth counselor may be a talented musician.

Just as government is the sum of its parts, we as individuals are the sum of our parts – our unique background, education, talents, passions, biases, ambitions, and even our clinical depressions.

Part of getting to know your people involves getting to know what they are good at. Micromanagers plague those who are quite capable of working without supervision. Laissez-faire managers are the bane of those who require constant attention to stay focused on tasks. And most of your people will be somewhere in between – excelling at the things they enjoy, and avoiding the onerous.

Some Definitions

We cannot totally escape some “boilerplate” definitions of internal control, though we can discuss them logically.

In New York State government, Internal control is a process, designed to implement a legislative mandate, executed by executive, management, supervisory and line staff, to provide **reasonable assurance** that objectives will be achieved effectively and efficiently, in compliance with applicable laws and regulations, supported by reliable financial and program reporting.

Reasonable assurance – takes into consideration the significance of the program or activity (e.g. its cost, impact on people, effect on agency reputation), likelihood of error (some risks go with the territory), and relevance and affordability of controls to those risks.



Five Components of Internal Control

Currently there are five major components of a good internal control system (equally applicable to large or small organizations):

1. Control Environment

Do you deal directly with the public? In an office or residential setting? Do you handle large volumes of transactions, with or without a monetary component? Does your executive set an example for ethical values and integrity? Does your agency seek, train and retain competent employees? What is your management’s philosophy and operating style? Are you highly centralized, or are offices/facilities/decisions decentralized? Is there an independent oversight body that reviews and evaluates your successes, and your failures?

Is your workforce stable? Does your agency have a long-standing, positive reputation in its field? Are the resources provided commensurate with your responsibilities? Are your computer networks secure, your data stable, your offices safe and environmentally healthy?

If you can answer YES to each of these questions, we would then ask you if there are any job openings within your organization. But, seriously, you get the picture – all these things affect your work, your agency’s mission, and how you feel about your job.

2. Risk Assessment

Every operation faces internal and external risks – be it employee pilferage, contractor kickbacks, applicant fraud, bogus credentials, communicable diseases or computer network failure. Something as simple as a faulty smoke detector can interfere with success. Handling hard currency requires special procedures. Agencies that serve residential populations in a 24/7 setting must focus on the special risks not inherent in a 9 to 5 office operation. Blacktopping your driveway is not as risky as bridge and tunnel construction, though you won’t want to track anything indoors.

Risk assessment is an ongoing process that identifies the likelihood of a risk, the potential magnitude of a risk, and the degree to which such risk could interfere with your agency’s mission and program success. Has it happened before? Then it will happen again, unless you establish procedures to control such risk.

3. Control Activities

Policies and procedures can help ensure success, by controlling significant risks. They include activities such as approvals, authorizations, verifications, account reconciliations, operating reviews, protection of assets and segregation (or separation) of duties.

The challenge for government workers here is to avoid over-control of insignificant risks, while avoiding under-control of significant risks. For example, drivers must have their vehicles inspected annually by a professional, licensed third party. Getting that sticker from your brother-in-law who never looks under the hood may keep you from getting a traffic ticket, but won’t protect you from that icy hill in February. By the same token, checking your tire pressure and oil level periodically is wise, but if you start doing this twice a day, someone might think you have an Obsessive Compulsive Disorder.

Your main concern is getting the job done in a timely and accurate way. Accuracy also means honesty. Get those three bids in writing from reputable firms. Lock up valuables overnight. Have someone balance the checkbook who doesn’t write the checks. Call up past employers and schools/universities to verify an applicant’s work history and educational credentials. Have your fire extinguishers inspected annually, and recharged as necessary. Change those computer passwords when an employee leaves your agency, or your bureau.

We are all familiar with the logical procedures involved in purchasing – including physical count of the goods received examination of their quality, date-checking of dairy goods, etc. But did you know that the temperature at which crude oil is delivered can affect how many gallons are actually provided? Was that shipment of flu vaccine you just received part of a manufacturer’s recall?

4. Information and Communication

Certainly, those in the military know the value of good information and communication. Knowing where the enemy is, where your own troops are, and the location of innocent civilians are all important elements of war and peace. The Pentagon may term this military intelligence, or command & control, but it is what it is. Phrases like “friendly fire” and “collateral damage” pop up when communication fails.



Internal Control – More Than a Good Idea – It’s Also the Law!



All too often in a hierarchical system, information is “managed”, i.e. it is restricted to a limited few (under the theory that “knowledge is power”.) Some supervisors also embrace the Nike slogan “just do it” when an employee seeks a greater understanding of his/her role and responsibility.

With apologies to the State Police and Department of Correctional Services, most of you will never be instructed to storm a building or tackle a fugitive, so you should have time for the luxury of knowing why you do what you do. Knowing “why” may also improve your chances for finding a more efficient and more effective way to do your job.

Effective organizations are not afraid of information and communication. They look upon their employees as colleagues, are not afraid to answer questions, or even consider new ways of doing things. Transforming an ineffective organization involves more than taking a few HPO or TQM classes, giving speeches or cutting ribbons. It involves development of a corporate culture that encourages communication up and down the ladder, and sideways between divisions and bureaus. Yes, you should still read the manual, but comparing notes with your peers can be invaluable.

Much of what we do in government is repetitive by its very nature. Every year Taxation & Finance deals with the same eternal issues. Every year, thousands of citizens smile into the face of the DMV’s flattering camera. Every year, the courts deliver thousands of all ages to our facilities, for education, correction, rehabilitation, medical treatment and the like. With long-established processes in place to continue these activities, there should be time to talk about the job, compare notes, and envision alternatives.

A side issue for some, but it effects all – open communication between interested parties, be they regulators, “stakeholders”, families, advocacy groups, legislative bodies or advisory groups.

5. Monitoring

On an ongoing basis, managers need to monitor operations – to assess the quality of the system’s performance over time. This includes regular management and supervisory activities, and other actions personnel take in performing their duties. The focus should be on critical aspects of an operation to ensure that key elements are conducted properly. Where performance falls short of expectation, managers need to notify those responsible for taking

corrective action, and engages in follow-up activity to ensure their warning was heeded.

A supervisor “monitors” staff attendance via visual observation, phone calls, computer log-in and/or spot-checks on-site. A program manager “monitors” grant activity through conversations (phone or in-person) with service providers or clients, or on-site visits to local service providers. A grant administrator “monitors” expenditure activity on a periodic basis by reviewing expenditure reports or claims on a monthly or quarterly basis, comparing them to projections.

Within the broad category of “monitoring” we can also place “evaluation” and “auditing”. The distinction between these activities and managerial monitoring is primarily organizational.

To ensure independent, unbiased thinking, evaluators and auditors cannot be part of the operation being reviewed. Evaluators are frequently specialists in program areas, employing research methods to determine the effectiveness of program services. Auditors (in the past) focused on financial issues, employing accounting skills to review inventories, fiscal resources, integrity in payrolls, purchasing and grants. But more and more, auditors are becoming management generalists, with a growing understanding of agency goals, program specialties, and bottom-line criteria of success. And of course, auditors will tell you they are there to help you.

Tying It All Together

A good internal control **system** depends on “synergy”, i.e., the whole should be greater than the sum of its parts. The five components discussed above should form an integrated system that reacts dynamically to changing conditions. Internal controls are most effective when they are built-in to an operation, not added on by some external force. In other words, don’t do it because the law says you have to do it. Do it because it makes sense.

Be on the lookout for changing conditions. Staff turnover, new legislation, demographic changes in population served, unusual weather conditions, economic downturn, or even terrorist attack all require quick response to changing conditions. Youth facilities and adult correctional facilities must pay attention to judicial system flow-through, when constructing and staffing residential facilities. The Department of Transportation has its hands full monitoring traffic chokepoints throughout the state



Internal Control – More Than a Good Idea – It’s Also the Law!



(you may think the Northway is intolerable at rush hour, but we are a distant second place to other roadways to the south and west).

The **reasonable assurance** doctrine requires that all five components of your internal control system (a/k/a/ management control) work together. When they do, your job is easier. When they don't your job is virtually impossible.

What Internal Control Cannot Do

Internal control cannot change a poor manager into a good one. But it can change a good manager into a better one, and set the stage for the next generation of managers. This is an important consideration, given our rapidly aging work force.

Shifts in government policy or programs, competitors' actions or economic conditions can be beyond your control, but at least you will be the first one on your block to recognize this.

Internal controls cannot guarantee an ironclad defense against fraud, waste and mismanagement. Human nature is what it is, and there are those who are indolent, deceitful and imaginative just waiting to scam your system.

An internal control system, no matter how well conceived and operated, can provide only reasonable--not absolute--assurance that you will achieve your objectives. Judgments in decision-making can be faulty. Breakdowns can occur because of simple error or mistake. Controls can be circumvented by the collusion of two or more people, and management may choose to override the system. There are also resource constraints, and the benefits of controls must be considered relative to their costs.

Internal control is an essential tool in achieving your objectives, but it is not a silver bullet. When combined with well-trained, motivated staff working within an environment where the goals are clear, internal controls will enable a manager to successfully attain their organizational objectives both efficiently and effectively.

Case Studies

The following Case Studies depict a prototypical work process that would be influenced by the establishment and application (or absence) of internal controls.



Trainee(s) would be asked to:

1. Evaluate the control environment to determine the level of inherent risk,
2. Determine what controls would need to be imposed to provide 'absolute assurance',
3. Of those controls, which ones would provide a satisfactory level of 'reasonable assurance'?
4. How would reasonable assurance controls be implemented?
5. How might they be monitored?
6. How might communication flow support or stifle the success of the controls in minimizing risk/maximizing success?