CHAPTER ONE

1 Corporate Governance: A Gut Check

THE GREAT SOX FALLACY

One of the key corporate undertakings that undermined and will continue to undermine the success of enterprise risk management (ERM) is Sarbanes-Oxley (SOX). The most amazing thing about the SOX effort was how few of the so-called knowledgeable practitioners that were giving guidance on the subject matter actually understood the salient issues relative to why SOX evolved in the first place. I authored and taught an auditor training class entitled "Sarbanes-Oxley: A Road Map to Compliance." It was astounding to see how misguided the compliance efforts were that were being sold to these client companies as the panacea for all of their problems. It was even more astounding to hear how little people really understood about what the act was intended to do and how their whole focus in life was on Sections 302 and 404 of the act. Some of the key points I tried to explain to the seminar participants were the following:

- The problems that gave rise to SOX in the first place did not start nor would they end in finance.

- The real issues were centered on ineffective operations and the inability to generate a profit.
- When the risks that were present in operations that undermined their ability to operate effectively were not mitigated, then the risk of financial ineptness was imminent.
- This would leave the financial people with no other alternative but to manipulate the numbers to meet analysts' expectations.
- Implementing an overabundance of controls in finance for financial reporting would not solve the problem.
- There were many more sections to the act than just Sections 302 and 404, such as Section 409 on real-time disclosure.
- The gathering up of a bunch of control information and then trying to test them inadequately with archaic methods was going to be of little or no use.
- The preferred method of compliance (a top-down risk assessment approach that would be data driven and holistic to the enterprise) was the only effective way to deal with these problems.
- When the risks were identified, the root cause events had to be addressed, and that would be the first step for resolving these issues.
- I also informed them at that time that they had just seen the tip of the iceberg and that there was much more to follow.

The top-down risk-based approach was supported by the pronouncements from the Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB) in 2005 when they too observed that the ''check the box mentality'' of the compliance approach used by virtually all of the large consulting houses had missed the mark of satisfying the requirements of the act.

The subsequent gigantic meltdown of the banking industry brought on by significantly undermanaged risk in the real estate markets speaks volumes about the ineffectiveness of the act and gives us a glimpse of another piece of the iceberg starting to surface.

Sarbanes-Oxley was a noble effort in its intent to protect shareholders' interest; however, the message was lost on the practitioners in their zeal to generate quick profits in catastrophic conditions, which they had had a great hand in creating. The first catastrophic mistake was to embrace the Committee of Sponsoring Organizations (COSO) model as *the* framework for compliance—not because COSO is a bad framework; but since it is internal control-focused, it is clearly audit centric. What was required was a business model, not an audit model. Instead of performing a knee-jerk reaction to the circumstances, cooler

heads should have prevailed and waited for the COSO ERM model (completed approximately two years later), which would have yielded a much more beneficial governance structure.

Unfortunately, so much money, time, and effort was put into the Sarbanes-Oxley exercise, with mixed or less than satisfactory results, that it soured senior management in many organizations from taking on any other major corporate initiatives, which would have included ERM, of course. So now there is great resistance to adopting another environment that appears to be an add-on to the already fractionalized compliance efforts of the organization. Therein lies the tale of woe for ERM and the significant reluctance to embrace it.

THE VISION-CHALLENGED LEADING THE EVEN-MORE-VISION-CHALLENGED

Absent the few independent practitioners (like myself) who are crying out in the wilderness against the multiheaded monsters of the world who keep espousing the same old tune, you don't see many fresh ideas coming out of the large-scale consulting groups. It is the same old process for evaluating risks that has literally been around for years. The process is based upon scoring methodologies, such as one-through-five, or zero-through-three or some other convoluted number combination that is applied to risks, control effectiveness, impact, and other such subject matter.

At the end of these exercises, some type of generic ''risk-based'' conclusion is inevitably reached, which is normally comprised of a band of green, a massive band of yellow, and a band of red. This is normally followed by some other gyration for refining the process, which involves discarding the high and low scorers, tweaking this, and tweaking that in order to justify an already preordained conclusion. Worse yet, the whole exercise must be repeated every time risk needs to be evaluated on an enterprise basis. This will, of course, be necessary because unlike these static models, risk is not static at all. Talk about the application of AI (artificial intelligence)—these exercises are a classic example, in a very different sense of the phrase.

Why in the world do we have all of this massive computing power, generating terabytes of data that supposedly drives everything in our organization and yet not one of the supposed visionaries from these large consulting consortiums has ever thought, *You know what, maybe we should use data as the basis for risk assessment?* What are they thinking? Or even a more puzzling conundrum is that maybe they're not thinking, and therefore where is their vision?

I cannot possibly imagine a bigger risk than spending millions or billions of dollars being led by supposed visionaries who have no vision.

GOING BACK TO THE FUTURE? HOW *NOT* TO RUN IT

One of the greatest risks plaguing organizations in the past, today, and certainly into the future will be the inability to implement successfully progressive, highly advanced risk-centric systems. The following observations are meant to highlight some of the key areas of concern. I originally conceived ''The Dirty Dozen Critical Shortcomings of Application Systems Implementation'' as an article for publication. These observations came into existence after years of my own audit experience and reverification of its accuracy with thousands of my audit constituents.

I discussed it with Professor Larry Rittenberg, the current COSO Chairman Emeritus, and we tossed it back and forth with modifications. With all due respect to Larry, who is an extremely busy person, since the results of our discussions were never published, I have reverted back to my original content for the purposes of this book.

In the continuing environment of voracious systems implementation, it is perhaps time to step back and learn some lessons from history. Many of these are not new lessons, but neither have they been learned. In the following sections I will visit some critical shortcomings that continue to hinder our progress in real utilization of the vast systems capabilities that our organizations possess.

SYSTEMIC FAILURE: CRITICAL SHORTCOMINGS OF APPLICATION SYSTEMS IMPLEMENTATION

The ''dirty dozen'' shortcomings are listed and expanded upon in the following pages. They represent my views of significant risks and areas of failure that are all too prolific in this discipline.

1. Moving to a New Application Platform: What's the Business Reason?
2. Inaccuracy of the Financial Projections and Committed Costs of the System (OOPS!)
3. Failure to Establish a Realistic Timeline That Incorporates All Critical Aspects of Implementation

4. The Phase 2 Syndrome—Never Happens!
5. Failure to Do a Total Systems/Personnel Impact Analysis
6. Implementing a Platform Contrary to the Established Design Criteria
7. Back to the Future
8. ACE (The Awful Consultant Experience)
9. Data, Data Everywhere, but I Can't Answer Your Question
10. SCORE (System-Centric Oversight and Risk Evaluation) AWOL
11. The Dog and Pony Show
12. Getting Cooked by the Boilerplate Contract

Moving to a New Application Platform: What's the Business Reason?

One thing that will guarantee failure to achieve the original objective of a project is when no original objective was established. One of the key questions that the system sponsor should be able to address is the primary business reason for the change.

It is not appropriate to change system platforms just for the sake of change or because everybody's doing it. Each organization is unique in its needs and requirements. As a result, because our primary competitors are moving to a client/server platform does not necessarily mean that the client/server platform is appropriate for us. If a financially viable business reason that necessitates the change cannot be specifically identified and justified, there is no reason to change environments.

The business reason must be critical to the overall success of the organization. It must be clearly justified by returns on investment that warrant the capital expenditures, and it must be vital to meeting the needs of our customers, or carving out a larger share of the marketplace, to name only a few.

Migrating to new systems for no apparent reason is a consummate example of following the crowd no matter where the crowd is going. If the crowd is rushing into a burning building, should we all follow along? A new system is not the panacea for all business ills. In fact, it is probably dealing with a symptom instead of the real cause.

Inaccuracy of the Financial Projections and Committed Costs of the System

If you have ever seen the acquisition and implementation of a large-scale system from start to finish you have almost assuredly seen OOPS, the Overspending Our Project Scenario. This can occur in different forms, some of which

are detailed in the following list. The always popular ''let's soft sell the original financial estimates to justify the project to senior management or the board.'' Simply stated, all of the costs are not included that will be required to make the system a reality. Factors that will be ''overlooked'' include:

- Long-term technical support
- Specialized consultants or contractors required
- Ancillary hardware that becomes necessary due to primary platform inadequacies
- Additional software that will be purchased by the users to plug the ''gaps'' in the system (real or perceived)
- Future technological upgrades required, which are inherent to the software (turnkey environment—hardware and software)
- Moving beyond Vanilla when it really needs to be a 40 scoop 30 topping banana split to deliver the baseline requirements of the users
- The *real* life cycle of the system before it requires significant changes to keep pace with business changes
- The business interruption that occurs when new releases of the software are installed and the associated costs
- The hidden costs never accounted for when the users are so dissatisfied with the system that is delivered that they have to buy computers and software to build workarounds that have the desired functionality
- The cost of application support when the flood of user requests for modifications materializes because the system misses the mark so badly
- The cost estimate is simply wholly inadequate and poorly prepared, and fails miserably in contemplating all of the cost that will be necessary

Think about it. When was last time you saw a system of any magnitude come in under its original financial and time projections?

Failure to Establish a Realistic Timeline That Incorporates All Critical Aspects of a System

Where do these implementation dates come from, anyway? It appears that they are rarely in touch with reality and what is required for the system to be fully operational and functioning as originally envisioned. Every implementation date should be grounded in some legal or regulatory issue, or in a defined and justified business requirement.

If the required date is known and cannot be achieved—when exploding the timeline backwards given the resources available or essential lead times

required—another course of action should be explored. The common practice of pulling an implementation date ''out of the air'' and then tying the CIO's and other related party's bonus compensation package to it runs totally contrary to sound business logic.

The objective of the exercise is not to see how fast the system can be implemented, but how well it meets business needs. Half-baked implementations tied to timelines that have no basis in reason or logic always fail to achieve the key objectives: increased productivity, lower operating costs, better information, and ease of use. In fact, in most instances productivity takes giant strides backwards resulting in more hidden cost to the company or organization.

The Phase 2 Syndrome—Never Happens!

Doesn't it seem that the key features that the business requires or that were critical to the overall satisfaction of user community are never in Phase 1? Why is that? It doesn't really do any good to purchase the most powerful and feature-packed system available, and then fail to implement its primary functionality. The standard phrase that is normally heard when the users ask about the features is ''It will be implemented in Phase 2.''

Unfortunately, as many disgruntled users and overoptimistic senior executives have learned, Phase 2 is a figment of IT's imagination. By the time this event is raised as an issue, new releases of the base software are out, and the hamsters are trapped on the same hamster wheel for all eternity. If the original intent of purchasing the system was to implement minimal functionality, then save a lot of money, buy a cheaper system with far fewer features, or better yet do nothing—it will be a lot less risky.

Failure to Do a Total Systems/Personnel Impact Analysis

Prior to implementing any system, there should be a total inventory performed of all of the systems and personnel that will be impacted by the new environment. This says by definition that IS/IT is only part of the landscape. The users should, of course, be the primary drivers of the system, though IT normally dominates the project, even though it's a staff function and not a line function (another failure point), and as such the analysis should identify all affiliated and peripheral users of the system.

Failure to perform the appropriate impact analysis on both systems and personnel will virtually guarantee a technological or human rejection of the system once implemented. When the project is first anticipated, it should be mandatory that a thorough and complete impact analysis be performed.

Communication and feedback loops should be established to ensure that vital information is available as necessary to everyone who will experience the impact or, more likely than not, suffer the negative fallout of the project.

Implementing a Platform Contrary to the Established Design Criteria

As we have progressed across the spectrum of systems implementation theory, today we've achieved 180 degrees of separation from traditional viewpoints. The problem is that contemporary theory is rarely, if ever, followed in its purest state, therefore issues arise on a postimplementation basis.

The traditional theory of systems implementation was essentially that the organization would purchase a system that most closely approximated its operations and then modify the system to fit the business. As we know contemporary theory—as advanced by Systems, Applications & Products in Data Processing (SAP) and other similar platforms—is to reengineer the business to fit the software. The unfortunate reality is that most organizations want to embrace the new technology but not the new implementation theory.

As such, new platforms are implemented with old theory. Today's systems are self-contained, highly integrated information flow systems, and they are meant to be implemented in their entirety, a pure state of existence. However, in practice only portions of the new platforms are implemented, instead of in their entirety. And then these partial systems are interfaced to other existing systems in the business. Some of the negative results of mixing the two competing theories include the following:

- Potential loss of data integrity and mistrust of the resulting information that is generated by the system
- Excessive maintenance costs on interfacing
- Customization cost to the original software, assuming it can be performed
- The necessity to update the customized environment at great expense each time a new release of the software is brought out
- Potential need for conversion tables or other intermediate steps to convert the data for use, which are subject to error and extremely expensive to maintain

Back to the Future

How many people do you know who would acquire a brand-new $300,000 house with four bedrooms, three baths, and a two-car garage, and then rip

out one bedroom, two baths, and tear down one side of the garage? Perhaps they would do this so it looked like the house they grew up in as a kid—an example of the ''comfort zone theory.'' Obviously, no one in a sane state of mind would do this. However, how many times have you seen organizations buy brand-new systems and then modify the reporting, functionality, and overall design of the system to make it look like the system that was in existence before?

Why is this done—simply because it makes people feel more comfortable? Clearly what has occurred here is a horrendous waste of organizational resources, and instead of positioning ourselves for the future, we have slipped neatly and quietly into the past. When was the last time that someone actually reviewed the outcome of a system implementation to ensure that it met the fundamental criterion of financial return or efficiency gains relative to the original assumptions? Every system that is implemented should move the organization forward, not backwards. We have got to run the organizations that we have today and will have in the future—not the ones we had yesterday. No enlightened executives should be encouraging the ''chase yourself around the block theory'' because you always end up at the same old house, only unfortunately much poorer.

ACE (The Awful Consultant Experience)

Normally when you hear the expression ''ace in the hole'' it is a positive thing that creates a competitive advantage. A more accurate interpretation of ACE as it is used in the context here is that an awful consulting experience can put you far in the hole financially and technologically. The awful consulting experience can occur in a variety of ways:

- You pay a lot of money for highly skilled consultants but end up training a number of recent graduates to be better at their next job.
- There is a lack of stability in the consulting team, where the consultants are going out of your business as fast as the revolving door can turn and moving on for bigger and better money.
- The consultant tries to do too much and simply is not equipped to handle it and doesn't have other resources to draw on.
- The consultant holds you hostage and becomes such an integral part of your business that you can't live without him; therefore you hire him at exorbitant cost.

- No knowledge transfer takes place between the consultant and your personnel, and therefore you are never allowed to own your system (the ransom event).
- Numerous other instances that due to lack of time and space I will not mention.

Data, Data Everywhere, but I Can't Answer Your Question

Let's think back to what seems to be centuries-old logic. Recalling one of the fundamental principles of why databases were created in the first place would bring to mind the issue of data redundancy. One of the driving forces behind the creation of databases was to eliminate all of the extraneous data that seem to be in divergent locations around the organization. Well, looks like they have come full circle. Now in many major organizations there must be thousands of versions of relatively the same data in the form of spreadsheets, databases, and miscellaneous files to name a few.

We seem to have all types and kinds of data out there, but it does not appear to be structured in any logical fashion that makes it accessible. In literally thousands of situations where I have asked people (auditors primarily) how they would objectively assess risk in their respective organizations, the answer normally comes back as "I would love to do it" or "That would be great if the data was there."

It seems almost incomprehensible that in the twenty-first century, with computers having existed for decades, people would still advance that argument—except that it's true more often than not. We have had data scattered among several systems and databases for years, and now we want it to take up residence in data warehouses or data farms. That is a noble exercise that should yield tremendous benefits, assuming data integrity to the source system can be assured.

The issue of concern is this—is it data for data's sake or data for information's sake? The point being made is that in system development on very rare occasions is a targeted data analysis performed that will allow the organization to consistently oversee the critical aspects of its business with virtually little or no effort. In most organizations, we are nowhere near attaining that type of instantaneous feedback on the pulse of daily activities that drive our existence.

The fundamentals aren't even in place; an example would be a credit memorandum where the reason codes are not accurate. Therefore, the organization cannot even address the problem that caused the customer's dissatisfaction. There is an old axiom that still holds true: "You can't fix a problem you don't know you have." In this day and age, if you can't measure it, you don't know you

have it. Therefore, by definition you cannot solve it and make it go away. There are all kinds of data out there, but there is a real dearth of valuable information to run the business. This is commonly referred to as the DRIP theory (data rich, information poor).

SCORE (System-Centric Oversight and Risk Evaluation) AWOL

By this time in the systems evolutionary cycle it should be an accepted fact that every system has the ability to utilize tools and methodologies that provide for consistent and accurate oversight of the organization on a continuous basis. The fundamental problem is that although systems can perform these tasks, the systems implementers choose not to let them. System-centric tools should be standard in every system created and should utilize the data that runs the organization to provide a continuous feedback oversight mechanism.

Such tools and methodologies would allow management to have a continuous view of the world they are responsible for. They should be able to evaluate their risk on a daily or even hourly or minute-by-minute basis if they so desire, which would allow them to react to business hotspots as soon as they occur. These tools and techniques should be incorporated into the system and be keyed to the users, so that they will be able to fulfill their primary management responsibilities quickly and without having to go through significant data analysis.

As the title of this section implies, these types of tools are AWOL (absent without leave) or essentially nonexistent. The failure is that the data is for the most part there, the tools should be, and we are significantly underutilizing our IT resources, which we have spent billions of dollars to acquire. This is a classic case of mismanagement of resources. Unless systems implementation strategies change in the foreseeable future, this huge waste of organizational resources is destined to continue.

The Dog and Pony Show

Everyone that has been involved in a systems implementation has been to the dog and pony show. The dog and pony show comes in different varieties, two of which are:

1. The software demonstration
2. The visit to customers of the software vendor to see an actual installation

The software demonstration is a bit of the dog and pony show in that it normally occurs in the vendor evaluation and selection stage. By that time the

vendor has responded to the Request for Proposal (RFP) and stated with certainty that they can meet all of the requirements that your organization is looking for in a system. Conveniently when we see the demo, sure enough, all of the features are there.

At some point it would be prudent for the organization to verify that in fact they have seen a real-live system and not a vaporware version of how it would appear if the vendor got the job. Learning that the system is not all that it appeared to be in the demo is disastrous—especially if the problem isn't recognized before the postcontract phase.

The second show, the customer visit, should never be limited to the primary suggestions of the vendor. Clearly, vendors would select those successful implementations that would present their product in a favorable light. What needs to be determined is what is not so favorable. So the key is to determine how to get in contact with the primary regional and national user groups of the software you intend to buy, so that you can have in-depth discussions regarding the key issues they have with the software and vendor.

This is not to say that vendor-arranged site visits are worthless, but some very specific things need to be determined at the site visit. For instance, is this organization similar to ours; are they of comparable size; do they have the same business structure, same number of locations, and same transaction intensity—to name a few? Getting to the real gutsy issues with the system is the most critical thing that can be done prior to making any commitment with the vendor. Once you sign the contract, they have just become a partner in your business. For more on contracts, see the next section.

Getting Cooked by the Boilerplate Contract

Without a doubt one of the worst things an organization can do is sign a boilerplate contract with the software vendor. Prior to signing any contract, the organization should have a trusted and knowledgeable representative in-house—or hired—that will visit the vendor's site before the contractual commitments are signed. The representative has to check for a number of things that may negatively impact the organization, some of which are the following:

- The ability of the vendor to technically support the system
- The financial viability of the vendor and their likelihood to continue to support the product
- The necessity of software source code escrow to protect the organization in the event of vendor failure

- The depth of knowledge regarding the product throughout the vendor's staff
- The operations of the vendor (to develop a sense of their strengths and weaknesses)
- Any discrepancy between demonstrated software and existing code
- The potential existence of multiple software vendors who have written individual portions of the system being purchased

In addition to this list, this person should receive in-depth training on the system to enable him to understand all of its key attributes and nuances. Without any type of contract protection for the organization, which can only come about if the representative thoroughly understands the system, the organization will have no protection, or it will only be obtained by costly litigation. In that case there are only losers.

These dirty dozen failures in systems implementation have only scratched the surface of the significant amount of waste that goes on continually in systems implementation. This is a huge continuing risk to the organization. It is imperative that some significant changes be made in software implementation before we go through another round of predestined failures. The future depends on IT—the time for change is now!

WHAT IS GRC ANYWAY?

It always astounds me when I look at how certain terminology and/or "new" initiatives emerge. Take for instance Total Quality Management (TQM). That original science, fostered by such greats as Deming, Juran, and Crosby back in the 1940s, brought to business practice some extremely practical and useful tools for modifying and improving process. In addition, they championed the utilization of metrics and measurements to make a business better one process at a time. Most of their tools could be employed today in major corporations to solve many of the problems in their operating areas that have forced companies to seek the solution of outsourcing as their only way out.

Yet anyone who has read the "Ventoro Offshore 2005 Research Preliminary Findings and Conclusions," which can be located at Ventoro.com, will clearly see from the statistics presented that the largest cost savings coming out of outsourcing efforts by major corporations are from process improvements, not from salary and wages as is popularly believed. This subject is discussed in Chapter 9 in the context of risk.

All of that aside, TQM was not good enough. To give things just a little different twist, Reengineering was conceived, and Six Sigma made common ordinary individuals into black belts. (Karate anyone?)

Now we have people talking about GRC. So let's break it down and see what this means. G is obviously governance, which I believe everybody in this country would say we need a little more of. R stands for risk management, a nice concept but poorly done in many large, medium, and small organizations alike. And C is the dreaded compliance, which has been traditionally overseen by regulators of course, but some would ask how effectively.

The acronym implies that these are separate and distinct areas of concern, which they clearly are not. They are all interlocking and inseparable when viewed using any type of common sense. The key point being missed here is that all of these should be part of logical but interrelated subsets of ERM. That is, ERM should be the overarching umbrella under which each and every one of these fall. The classic mistake made by most corporations today is that they are treating these as separate and distinct areas of concern and in some cases like SOX compliance, creating a separate and distinct unit to oversee it.

There's no reason for any of this, as these areas should all be subsets of the larger ERM environment, which would unite them into one unified effort. Corporate governance will be fulfilled by a highly effective, well-structured, properly automated ERM environment.

Remember, the E stands for enterprise, which means that everything, by definition, would be governed highly effectively by a centralized methodology. R is the effective identification of and determination of risk and is inherent in ERM. Last, but not least, M stands for management of all risks. Compliance is just another subset that has to be effectively managed as a critical risk of the enterprise. My vote would be to get away from acronyms such as GRC that imply fractionalized corporate structures that are highly duplicative and cost-inefficient.

ARE YOU CUBIN'?

What I'm alluding to here is this: are you familiar with the two cubes brought to us by the good folks of COSO?

The cubes are, of course, the COSO framework and the COSO ERM framework. I think we are all painfully familiar with the origination of the COSO framework, which was brought about as a result of the savings and loan failures in this country. At that time COSO was working with the Treadway Commission in an attempt to keep the federal government from regulating the audit industry.

The audit industry was a subject of great scrutiny at that time as a result of the failure of approximately 600 different savings and loans scattered around this country. In essence, what we had was a total failure of the second tier of the banking system.

This was brought about by such inflated property values that everybody hung out a shingle in front of his house thinking he was a real estate appraiser. These ''appraisers'' supplied inflated values to the savings and loans, which then lent money on these inflated values to unsuspecting clients. Does this sound at all familiar? If you did nothing more than change the sign from property appraiser to mortgage broker out in front of the same quack's house, you would replicate a key factor in the massive financial meltdown we just went through. We just never learn, do we?

Yes, this has happened before, and it is actually what gave rise to COSO as an entity. COSO's goal was to keep the federal government out of the audit industry, which they successfully did. The argument was that they would create the COSO model or internal control framework, and this would fix everything.

The intention was to have all organizations embrace the model, and raise management awareness of the importance of internal control. The model and its framework were intended to lead to a higher degree of corporate governance and ethics resulting in the elimination of misstatement and malfeasance in the corporate boardrooms. Noble intent, that is for sure, but the question still remains: has the effort worked? I don't believe that you have to cogitate too hard to determine if it has or has not—clearly not.

Even more mystifying is that it became the standard of compliance for Sarbanes-Oxley when it was embraced in 2002. I will not speculate any further on this subject matter. I believe by applying a little common sense you can arrive at your own conclusions as to whether the outcome satisfied the mission.

All that discussion aside, in the fall of 2004 COSO created the COSO/ERM framework, and quite honestly I believe that COSO did an exceptional job in putting together guidance for embracing risk. As I mentioned before, Professor Larry Rittenberg attended a presentation I gave in 2001 on enterprise-wide risk assessment (EWRA), as I called it then, which addressed a lot of the subject matter that later came out in this framework. To his credit I feel that Professor Rittenberg has done an exceptional job in furthering risk as a key corporate initiative, which is personally very pleasing to me, and he should be commended for that work.

Figures 1.1 and 1.2 are the two cubes that are the products of COSO. They are presented here to make a comparison at least in the context of how I view them. I will not grind through each and every attribute of these models, but it is important to understand some of the key criteria that are being presented by them. It is

FIGURE 1.1 The COSO Cube

Source: COSO.

important that corporate executives and board members understand what is being exemplified by these models and the subtle, but very important, differences between the two. Shown in Figures 1.1, 1.2, and 1.3 are the COSO cubes.

Three key questions need to be asked in reviewing the cubes:

1. How do they differ?
2. Why do they differ?
3. What is the implication of this?

My take on these questions is as follows. In viewing the cubes side by side what you start to notice are some fundamental differences in the contents, but the implications of these may not be clear-cut. On both of the cubes across the top are areas of corporate strategic concern. The thought process is that the five bands or eight bands below those levels, if properly included in the corporate governance structure, will ensure the accomplishment of the strategic objectives. A noticeable difference between the two cubes when you look at the strategic objectives level is the presence of four objectives on the COSO/ERM cube versus three on the COSO cube.

On the COSO/ERM, cube you can see a category of Strategic has been added. That is a very important category in that it can take into account such critical

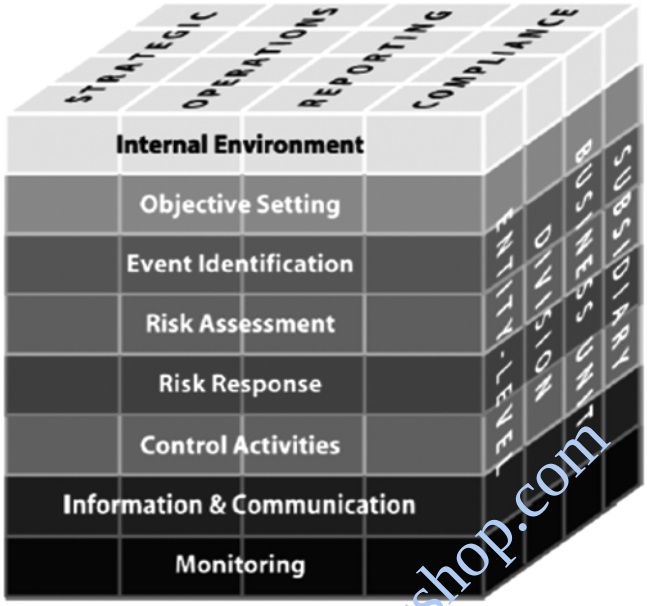

FIGURE 1.2 The COSO/ERM Cube

Source: COSO.

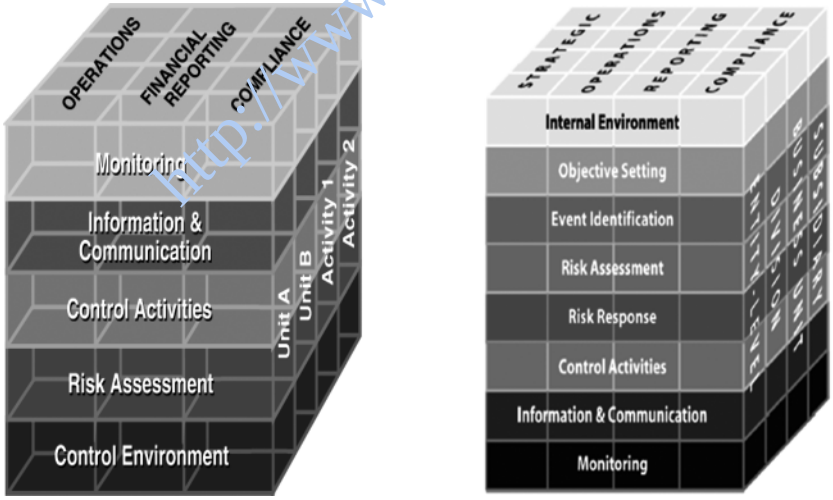

FIGURE 1.3 Side-by-Side Comparison of the Cubes

Source: COSO.

corporate initiatives as outsourcing and mergers and acquisitions. Both of these areas are, of course, fraught with risk, a subject matter that will be discussed in Chapter 9. The other notable difference at that level is that ''Reporting'' has replaced ''Financial Reporting,'' creating a much more business enterprise flavor as opposed to accounting flavor.

When you look at the COSO cube and its five original bands, it is clearly emphasized that controls are the main focus of that environment and that risk plays a very minor role. If you look deeper at the framework, you can see that control environment forms the foundation of the cube. Just as in a house, it is the supporting infrastructure that makes everything work.

You can also see that risk assessment is actually following, or appears to be an afterthought in relationship to control activities, as you come down from the top of the model. The implication is clear that controls precede risk assessment.

Think about that for a moment, and you'll probably start asking the same question that I did when I saw the model back when it was first issued. How can controls possibly precede risk in any type of thought process? That makes absolutely no sense from a logical perspective. If you don't know where your risk is or what it is, how do you know what to control and how to control it?

For example, what if I told you that one room on one floor of the 40-story hotel was filled with gold and all of the rest of the 600 rooms were standard hotel rooms. Then I said that I wanted you to design a control plan for the premises. You could do whatever you wanted in order to bring the hotel into an appropriate controlled state of existence.

What would you do first? Start running around and installing big steel doors on every room in the building, stationing armed guards at the front door of the hotel, screening all customers as they came in the door, and searching them? Clearly not. You would first take a tour of the hotel, locate the room where the gold is in fact located, the point of maximum risk, and secure that area appropriately.

That would be logical, that would be *common sense*! However, if you were to talk with any high-ranking auditor in most of the large auditing houses in 2010 they would tell you they are definitely looking at risk. In practice that is simply not true. They are only concerned about how many controls they should test and how big a sample they should take to justify their opinion. Risk assessment could not be any farther away from the process. They are still following the precedent expressed in the original COSO model, which is to put controls first, with risk assessment as an afterthought.

When you look at the COSO/ERM model, you start to see an entirely different picture. As has already been highlighted, right from the strategic level of the model there are distinct differences in the approach. The most important

difference is the business feel as opposed to finance feel that the model starts to communicate. What am I saying? It is been my contention all along that the COSO model, as noble an effort as it was when it was created, was way too bean-counter–oriented to be of any value to a major business enterprise or large-scale organization of any type.

The eight bands on the COSO/ERM model are much more logically oriented toward business as opposed to finance and accounting. The order of precedence itself coming down from the top of the model is far superior to its predecessor and makes much more sense logically.

Some key differences are that you can see that ''Control Environment,'' the foundation of the COSO model, was changed to ''Internal Environment,'' giving it a much more enterprise feel. ''Objective Setting'' was injected as a new band for the purposes of establishing operating objectives that will help to attain the strategic objectives identified across the top of the cube. The next three bands (''Event Identification,'' ''Risk Assessment,'' and ''Risk Response'') are all directly related to the mission of risk assessment and management. We'll discuss some of these components in a little more detailed fashion in this chapter.

The other key observations are the order of precedence and the foundation. You can clearly see where all three of the risk-related bands precede control activities. For the first time in history, somebody has gotten the logical thought process in the correct order. *It is always risk before controls!* Regarding the foundation of the COSO/ERM cube, you can see that monitoring has now become the point of focus. Just preceding monitoring, you see the band ''Information and Communication.'' This has a logical and businesslike flow that is totally absent in the original COSO model.

The implication here is that the information and communication generated by the entity or enterprise can be utilized to evaluate the risk and the operations of the enterprise on an ongoing basis. This would be fed to the monitoring infrastructure in place in the enterprise to act as a feedback mechanism. The data and information gathered would be recycled back up to the top of the model to reset operating objectives and make necessary corrections where unacceptable risks are in evidence.

This would be in keeping with the logic that risk factors, organizational information, and data can be utilized on an ongoing basis to monitor not only risk and controls but also operational performance of the enterprise. This can be accomplished by implementing the data-centric ERM strategy detailed in Chapters 6, 7, and 8.

Illustrated in Figure 1.4 are the eight bands of the COSO/ERM model along with their detailed contents. I will not belabor the discussion. However there are some items worthy of note.

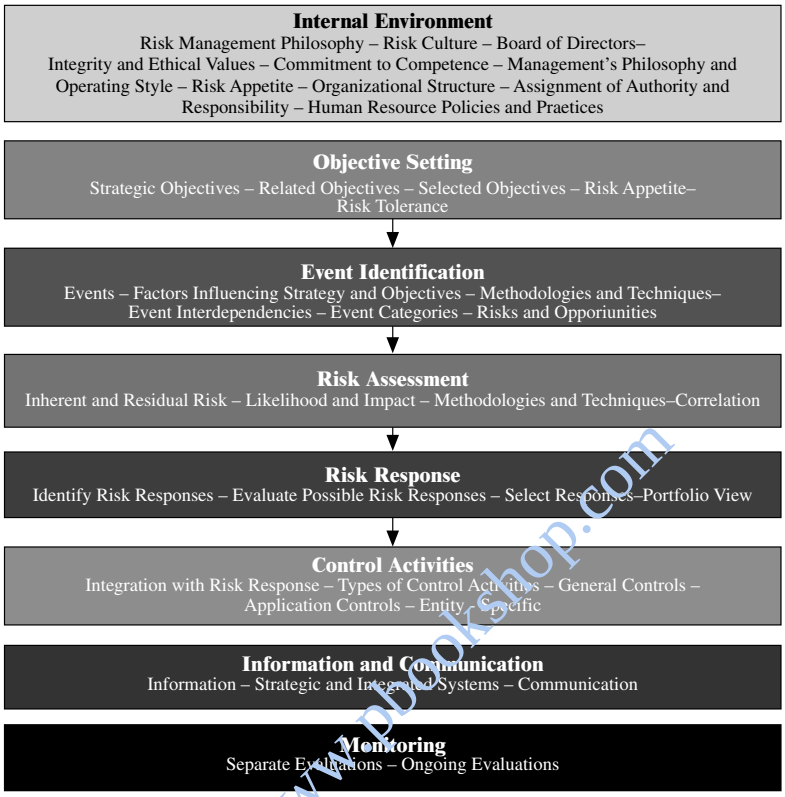

FIGURE 1.4 The Eight Bands of COSO/ERM

To put in plain terms, the COSO model for auditors, and the COSO/ERM model is for business people. This makes all the difference in the world in how the frameworks will be perceived and whether they will be embraced or not. As important as finance may be to some people, it does not create one product or get one service out the door to be sold to a customer. This has been the rub all along. Easily 90 percent of corporate executive and operations management have nothing to do with bean counting. Don't care, *may* want to know.

The unfortunate reality of what has occurred is this. In a knee-jerk reaction to try and placate the American public and shareholders in general, the federal government jumped the gun. For political expediency and gain, they allowed a couple of politicians to create a law of the land prematurely, which was then thrust upon corporate America in a totally bizarre fashion. Without getting into all the sordid details, let's just consider a few fundamental and egregious errors that occurred as a result.

First of all, the supposed fix for all of the ills that was in fact supported by all the large accounting firms and consulting houses was to strengthen financial reporting controls. As observed earlier, that is not where the problem started and did not solve the problem. I am not Monday-morning quarterbacking here. I stated categorically back when the act was first passed that this approach was wrong in my seminar ''Sarbanes-Oxley: A Road Map to Compliance,'' and I stick by that conclusion today. When I was critical of the approach and how many of the prime players who caused the events in the first place were now reaping billions while *not properly* fixing the situation, many people walked out. Could not stand the truth, I guess.

The second critical error is that the original COSO model was utilized as the compliance methodology for the act. Why would anybody do this when it had not stopped anything at all up to that point in time? I can only speculate, but one theory would be since COSO was never really embraced, all the tools that were created by the large firms and consulting houses for that purpose were never utilized. What better way to recoup your investment and make a massive profit than to lobby to make it the preferred compliance framework? It was actually mentioned in the Sarbanes-Oxley Act itself, and the big firms were off to the bank with the armored cars full of money.

Yet in 2005 the SEC and the PCAOB held a roundtable on the results of the initial compliance efforts. ''Round'' is the operative word here because the corporate executives all roundly lambasted the ineffectiveness and the cost of the effort. In fact, if you look at the actual language that came out of the session, the following observation was made:

> The feedback indicated that one reason why too many controls and processes were identified, documented and tested was that in many cases neither a top-down nor a risk-based approach was effectively used. Rather, the assessment became a mechanistic, check-the-box exercise. This was not the goal of the Section 404 rules, and a better way to view the exercise emphasizes the particular risks of individual companies. Indeed, an assessment of internal control that is too formulaic and/or so detailed as to not allow for a focus on risk may not fulfill the underlying purpose of the requirements. The desired approach should devote resources to the areas of greatest risk and avoid giving all significant accounts and related controls equal attention without regard to risk.
>
> (Source: Division of Corporation Finance, Office of the Chief Accountant, U.S. Securities and Exchange Commission, May 16, 2005)

Gee whiz, would that be a politically correct way of saying those wizards of the accounting world missed the point entirely, again? Yes, that is exactly what it is saying. The following observation to that, of course, was to direct that all efforts should be done on a top-down risk-based approach. That sounds very familiar, since that's what I was advocating back in 2002 and is what I am discussing now in this book. And yet today again they go down the road of controls irrespective of risk.

The other major fallout of this was that the billions of dollars that were ''wasted'' on the ill-gotten compliance techniques have now stymied the effort to install ERM in organizations today. What should have occurred is that no compliance should've been thrust upon corporate entities until the COSO/ERM model was completed in 2004. At that point, they could have implemented ERM as an all-encompassing governance tool as well as a business tool to run the entire enterprise. If this had been done, we would not be in the position we are today with fragmented corporate compliance—the SOX group here, the ERM group there, the compliance officer someplace else, and at the end of it all a convoluted, costly, and highly inefficient mess.

By invoking ERM early on, we could have set a pathway to corporate success by creating tools and methodologies that would have actually yielded a defined return on the investment for the business itself. Instead, what we have is a somewhat dysfunctional structure prevalent across virtually all corporate landscapes that only bring additional cost to overhead with no benefit to either the business or the shareholder. Is that what we had in mind when this act was originally brought into focus, or was it the protection of the shareholder and enhancement of value?

The upshot of this is that Sarbanes-Oxley consumed all corporate resources, and in tough economic times corporations simply cannot justify any type of large-scale expenditures to implement ERM. Unfortunately, if you were privy to a lot of boardroom conversations you would see that there is mass confusion relative to the subject matter itself. This stems again from a lot of misguided pseudo-knowledge on the part of large consulting houses who really do not understand the subject matter at all.

The only effective way to accomplish corporate governance is to design an ERM environment that is all-encompassing and not an accumulation of disjointed special-interest subsets of compliance. In Chapter 2, we will begin the discussion of what an effectively designed ERM environment should look like.