Chapter 1

Introduction

Introduction

This book contains hundreds of very specific controls over the basic processes of a business—order entry, shipping, billing, purchasing, and the like. These controls are presented in layers, beginning with those needed for a very basic paper-based system and progressing through computerized systems and the use of selected best practice enhancements to the computerized systems. Thus, users can find within these pages a variety of control systems for different levels of system complexity. As a supplement to the many controls detailed in later chapters, this chapter contains additional comments about the overall system of controls, high-risk areas, the segregation of duties, implied controls, the impact of the Sarbanes-Oxley Act, and the occasional need to deinstall controls.

1–1 Control Point

This book is entirely about the control point, which is an activity within a business process that will prevent or detect a process breakdown. For example, the requirement to have a supervisor sign checks is a control point; the key element in this control point is not the actual signing of the check, but rather the assumption that the manager will not sign the check without first reviewing the attached payment documentation to ensure that the payment is necessary. However, this control point is necessary only in a relatively disorganized purchasing environment where many people can authorize purchases. If a company were to impose a rigid requirement that all acquisitions must involve an authorizing purchase order, there is no longer a need for a control point represented by the check signer, since the purchasing department has taken over this role. Thus, control points can be activated or discarded, depending on the structure of the underlying process.

A control point itself can break down through inattention, lack of formal training or procedures, or intentionally, through fraud. To mitigate these issues, some processes involving especially high levels of asset loss are more likely to require two controls to attain a single control objective, thereby reducing the risk that the control objective will not be attained. However, double controls are not recommended in most situations, especially if the controls are not automated, since they can increase the cost and duration of the processes they are designed to safeguard.

The controls outlined in the chapters that follow are broken into two types: primary controls that usually are highlighted on a control flowchart and ancillary controls that can be added to the primary controls to provide an additional layer of security. For example, detective controls designed to find errors after they have occurred are rarely designated as primary controls (which are intended to prevent control breaches from initially occurring) and instead are to be found in the list of ancillary controls. Primary controls are more likely to be an authorization, whereby a supervisor reviews a key aspect of a transaction before it is completed, or corrective, so that an error is spotted at or close to its source and fixed immediately.

Besides the detective controls already noted, verification controls usually can be considered supplemental. For example, an inventory audit or review of a petty cash box is a verification control, but because it is not conducted as an integral part of a process flow, it is considered supplemental to the primary set of controls. For the same reason, a passive control, such as installing a surveillance camera near a cash register, is considered a supplemental control.

There are many supplemental controls to choose from. However, just having a large selection of supplemental controls does not mean that they must all be used. Quite the contrary. Most controls add to a company's costs and clutter the work required of employees, so it is best to first determine exactly what risks must be addressed and what controls are required to do so, and to avoid using all other controls to the greatest extent possible.

To some degree, the use of ancillary controls is driven by a company's control environment, which includes these elements:

- *The enforcement of ethical standards.* A company that promulgates a written ethical standard, informs employees about it regularly, and enforces its parameters has established an excellent mind-set throughout the organization that a certain ethical standard is expected. This standard should be supported by the board of directors, while the board's audit committee should be active in investigating ethical (as well as control) breaches.

- *The operating style of management*. If the management team sets unrealistic goals for bonus payments or tells employees to meet stretch targets by whatever means possible, then it is creating an environment in which employees are indirectly encouraged to breach the control system. Alternatively, a focus on long-term results and reasonable short-term objectives tends to enforce compliance with the existing control system. Further, the establishment of free lines of communication between management and staff, so that control problems can be quickly and easily communicated throughout the corporate hierarchy, is an essential element of management's operating style.
- *Structure of the organization*. If a company is highly decentralized, with minimal overview of operations by the corporate staff, then controls will likely be enforced locally with minimal rigor. Conversely, a strong interest in control compliance by corporate management, with attendant auditing reviews, will assist in achieving a strong controls environment.
- *Assignment of control responsibility*. Controls will be followed with considerably greater enthusiasm when local managers are assigned direct responsibility for their consistent application. Without local assignment of control responsibility, controls tend to be looked on as hindrances to the efficient completion of processes and so are circumvented where possible.
- *Experience and expertise of employees*. If employees have a fundamental understanding of company systems, which comes from a combination of experience and intensive training by the company, then they will understand why controls are used, as well as the ramifications of their absence. Conversely, the lack of experience or training tends to result in the lapsing of controls.

Thus, the presence of a strong control environment is directly related to a reduced need for ancillary control points.

1–2 High-Risk Areas

All areas of a company contain some control weaknesses, but some harbor key risk areas, especially the diversion of company assets or misrepresentation of financial results. Of primary concern are those areas where these two issues coincide. The paragraphs that follow note how this book's controls can mitigate these risks, but also point out areas in which problems will still exist.

A major risk area is revenue recognition, for there are a variety of ways to manipulate it to accelerate revenues improperly, thereby reporting excessively profitable financial results. The bulk of the revenue recognition controls described in this book address the mechanics of ensuring that suppliers receive an accurate invoice in a timely manner—which unfortunately addresses only part of the revenue recognition control problem. Management still may have the capability to adjust revenue with a few well-placed journal entries or by altering the timing of transactions.

Another area of significant risk is the capitalization of assets. Chapter 8 addresses the basic controls needed to properly record expenditures large enough to exceed the corporate capitalization limit. However, once again (as has been proved at WorldCom), expenses can be capitalized on a massive scale by management, completely avoiding the intentions of the existing capitalization control system.

Yet another high-risk area is the valuation of reserves, such as for bad debts, warranty claims, or product returns. Anyone responsible for these valuations can easily adjust them (within limits) to arrive at enhanced financial results. Since reserve valuations fall entirely outside of any normal process flow, they can be more easily abused.

Several other high-risk areas are also unrelated to basic process flows—the valuation of acquired assets, related-party transactions, contingent liabilities, and special-purpose entities. Thus, even with in-depth and comprehensive controls over such key processes as purchasing, billings, and cash receipts, significant areas that can be circumvented easily—usually by management—still lie outside the traditional control systems.

Consequently, this book provides only part of the controls solution: It shows how to control both basic business processes and best practice improvements to those processes, but it does not provide a control system for management. That level of control requires a different set of approaches, such as tight board oversight of operations, an active and well-funded internal audit team that reports directly to the board of directors, good recruitment procedures, clear lines of authority, constant attention to ethics training throughout the organization, a fraud hotline, and the imposition of a corporate code of ethics. Unfortunately, these approaches are much fuzzier than the precise control points laid out in this book, which still leaves room for control breaches by management. In short, all manner of controls over management can be attempted, but there will always be a higher risk of control breaches by them.

Segregation of Duties

One of the fundamental concepts of control systems is that the level of control increases when duties are segregated among employees—and the more employees, the better. By segregating duties, one person typically is responsible for handling an asset (i.e., cash), while another records the transaction and a third approves the transaction, with no one being responsible for more than one of the handling, recording, or authorization tasks. If a process flows through multiple departments, the use of duty segregation can lead to the involvement of a dozen or more people in the process.

The advantage of using segregation of duties is that a massive level of collusion would be required to commit fraud. A typical case of fraud involving collusion results in a loss averaging six times the amount lost when a single person is involved, so there is certainly a valid point behind the use of duty segregation. However, it is also an extremely expensive proposition, for the involvement of many people in a process results in lengthy wait and queue times that yield a highly inefficient operation.

Due to the exceptional cost of duty segregation, it is increasingly common to find corporate risk managers evaluating the cost and benefit of such systems and sometimes deciding against an excessive level of segregation. The deciding factor is typically the size of the potential loss; for example, the handling of corporate securities will always call for the use of a considerable degree of duty segregation, while petty cash management will not.

Implied Controls

This book contains few references to automated data entry accuracy checks, since it is assumed that they are already present. Such controls include these validations:

- *Completeness.* A transaction is not considered complete until a specific set of required fields are completed. For example, the entry of a supplier invoice requires a supplier invoice number, invoice date, and dollar amount, and the computer system should not record an entry unless all of these fields have been completed.

- *Duplication*. The computer warns of the existence of a duplicate record already containing the same information. For example, the computer should reject a supplier invoice number that has already been entered.
- *Limit*. A transaction is flagged for supervisory review or rejected outright by the computer if a numerical value is too high. An example is a payroll application where the entry of an hourly wage rate is rejected if it is higher than a predetermined amount or lower than the minimum wage.
- *Table lookups*. The computer employs table lookups to determine the validity of entered data. For example, an entered part number will be compared to the item master file and rejected if the part number does not exist.

These automated controls are extremely useful for enhancing the completeness and accuracy of entered information.

Impact of the Sarbanes-Oxley Act on Controls

The Sarbanes-Oxley Act (Sarbanes) requires that an internal control report be included in a public company's annual report that contains an assessment of the effectiveness of the company's internal control structure and procedures for financial reporting. To determine if the control system meets this requirement, it is useful to complete these five steps:

1. Determine which accounts feed into the financial statements and which disclosures are key to the overall accuracy of the statements.
2. Document the process flows that materially impact the accounts and disclosures identified in the first step.
3. Identify the key risk elements in each if the highlighted process flows.
4. Document the effectiveness of existing preventive and detective controls in mitigating the identified risks.
5. Identify the need for alternative controls to mitigate the key risk elements down to targeted levels, and implement those changes.

Since this book is a broad-based source of control concepts, it is useful for completing steps 4 and 5 of the Sarbanes review process just noted. Within these pages, readers can locate controls for many key risk elements identified during their process reviews. To accomplish step 5 in the review process, it may be useful to audit a process once the controls described in this book have been installed, in order to identify any residual risk and then to adjust the control points to achieve the targeted risk level.

Deinstalling Controls

Though this book is concerned entirely with the selection and installation of controls to a process, a further consideration is when to deinstall a control. By its nature, a control usually involves non–value-added work, which either directly or indirectly increases company expenses. Therefore, you should conduct a periodic review of the existing control structure to determine which controls are no longer needed. A good time for this is just prior to the annual audit, when the external auditors likely will want to see some documentation of the company's system of controls. Another trigger for a controls review is whenever a process flow is altered, perhaps due to the installation of a new best practice. Whatever the reason for the review, all controls should be formally documented, thereby making subsequent reviews substantially easier.

Summary

The increased emphasis on controls that is mandated by the Sarbanes-Oxley Act makes it necessary to determine carefully what risks must be guarded against throughout a company's systems and to construct a set of controls to mitigate those risks. However, a company should not be ruled by a vast array of multilayered controls, unless it wants to see its operating efficiencies vanish. A better approach is to review the need for controls continually, both on regularly scheduled dates and as new best practices are installed, to ensure that only the correct controls are used in precisely measured amounts. This book is designed for such an approach, since it describes different sets of controls, depending on what best practices are being used. The reader can then assemble and disassemble controls as needed to match the specific systems in use.

An important concept to remember when reading this book is that even the most intricate, interlocking set of controls will not ensure the complete elimination of risk from a process. On the contrary, it creates only a reasonable expectation of that achievement. The reasons that risk cannot be completely eliminated are a combination of unforeseen circumstances for which controls were not installed, the occasional breakdown of the control system, and the presence of collusion, which effectively undermines many controls.

A final thought: It is possible to continue past the scope of this book and experiment with new types of controls, which can become best practices in their own right. This endeavor is particularly useful if controls can be created that require no capital or labor cost, and that do not interfere with the natural flow of a process.