Winter 1994

The Internal Control Paradox: What Every Manager Should Know

Dana R. Hermanson
Kennesaw State University, dhermans@kennesaw.edu

Heather M. Hermanson
Kennesaw State University, hhermans@kennesaw.edu

Record: 1

Title: The internal control paradox: What every manager should know.

Authors: Hermanson, Dana R.
Hermanson, Heather M.

Source: Review of Business. Winter94, Vol. 16 Issue 2, p29. 4p.

Document Type: Article

Subjects: INDUSTRIAL management -- United States

Geographic Terms: UNITED States

Abstract: Examines some conflicting trends concerning internal control systems of companies in the 1990s. Definition of internal control; Trends toward internal control; Trends away from internal control; Balanced view of internal control; Solution to the internal control paradox.

Lexile: 1070

Full Text Word Count: 2798

ISSN: 0034-6454

Accession Number: 9510272844

Database: Advanced Placement Source

THE INTERNAL CONTROL PARADOX: WHAT EVERY MANAGER SHOULD KNOW

How extensive should my company's internal control system be? In today's environment, this is a difficult question to answer. The reason for the confusion is that some current business, legal, and social trends suggest that companies need to increase their emphasis on internal control, while other trends indicate just the opposite. The purpose of this article is to explore these conflicting trends and to offer a balanced view of internal control systems in the 1990s. This balanced view recognizes that there are costs of having too much control in a company and costs of having too little control. The key is to try to minimize your company's total costs of control by picking controls that are appropriate for the risks your company faces.

What is Internal Control?

A control is "any action taken by management to enhance the likelihood that established objectives and goals will be achieved" [Institute of Internal Auditors, 1993]. In other words, controls are designed to ensure that organizations conform to standards or plans. Examples of controls include the use of sales or expense budgets, computer passwords, or even padlocks on warehouses.

An internal control system is a collection of controls designed to provide reasonable assurance that the company meets the following objectives: (1) reliability and integrity of information, (2) compliance with policies, plans, and laws, (3) safeguarding of assets, (4) efficient use of resources, and (5) accomplishment of goals [Institute of Internal Auditors, 1993]. The major risk that companies face is that these five objectives will not be met. Therefore, the internal control system is the company's defense against risk.

An internal control system consists of three elements -the control environment, the accounting system, and the individual control procedures. The control environment includes the company's organizational structure, management's operating style, the personnel practices used, and the methods of assigning authority and responsibility to employees. The accounting system is designed to accurately identify, record, and report the company's transactions. Control procedures are detailed policies and rules, such as authorization of transactions, segregation of duties, documentation, physical controls over assets, and independent checks on performance. The debate over internal control primarily relates to finding the "right" level of control procedures.

Trends Toward Internal Control

Several trends suggest that companies should increase their emphasis on control procedures. First, companies today face substantial liability from several sources, including environmental fines, sexual harassment suits, and worker safety fines. For example, Chevron Chemical recently was fined $17 million for environmental violations [Begley, 1993]. A recent survey found that 25% of the nation's largest companies had been sued repeatedly for sexual harassment and that these companies spent an average of $6.7 million per year on costs related to sexual harassment [Moskal, 1991]. OSHA violations recently cost Cargill, Inc. nearly $1 million in fines [Garland, 1991]. It is possible that these companies' losses could have been prevented if the companies had implemented internal controls designed to prevent the environmental, harassment, and safety violations.

Second, in addition to preventing violations, internal controls also are important in calculating the fines charged to companies whose employees violate federal laws. The Federal Sentencing Guidelines of 1991 hold your company responsible if an employee violates a federal law. The fines imposed on companies can be ,as high as $290 million, depending on the seriousness of the crime and the control systems the company had in place to prevent the violation [Golden, 1993]. For example, assume that Company A and Company B each have employees who violate the same federal law. Company A had a good control system in place, but the system failed on one occasion. Company B had no controls in place to prevent the violation. Based on these facts, Company B might pay a fine 100 times greater than Company A's fine because B had shown no effort to prevent the violation. The threat of large fines has caused many companies to take a hard look at the adequacy of their controls.

A third trend pushing companies toward greater internal control is the increased risk of fraud. Recently we have witnessed a staggering number of fraudulent financial reporting cases, including ZZZZ Best, Phar Mor, Miniscribe, and numerous savings and loans. The losses from each of these external fraud cases were well into the millions of dollars. In addition, fraudulent activity within companies also appears to be on the rise. A recent study conducted by KPMG Peat Marwick [1993] indicates that 76% of responding companies had experienced one or more cases of internal fraud in the past year. The median loss per company was $200,000. In almost all instances of external or internal fraud, a weak internal control system is cited as a major contributing factor.

Fourth, the globalization of business has substantially increased the risks faced by companies. The establishment of overseas operations creates political, economic, and cultural risks not found in domestic companies. In addition, the complexity of the company's transactions often increases due to joint ventures, international tax issues, and foreign exchange transactions. Companies entering the global marketplace may require additional control systems to manage these new international risks.

Fifth, businesses today face much greater publicity, or media, risk than ever before. Companies experiencing fraud, mismanagement, litigation losses, or civil penalties often receive tremendous media attention. This attention can cause the company's stock price to change dramatically, especially when the company appears to have "lost control" of its operations. Internal controls can help to prevent these problems and can provide procedures for dealing with the press when problems do arise.

Finally, in response to the five trends above, regulators are moving toward requiring management and/or external auditors to report on the adequacy of companies' internal control systems. Under the Federal Deposit Insurance Corporation Improvement Act (FDICIA), management and auditors in the banking industry must report on companies' internal control systems. Governmental auditors may soon be required to expand their testing of governmental units' internal control systems. In addition, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) recently issued criteria by which companies' internal control systems can be evaluated. Currently, 60 percent of Fortune 500 companies voluntarily report on the adequacy of their own

internal control systems [COSO, 1992]. Many expect internal control reporting to become mandatory in the private sector in coming years.

Trends Away From Internal Control

In stark contrast to the discussion above, other current trends suggest that a reduced emphasis on controls is in order. First, one of the foundations of Total Quality Management (TQM) is that workers should be empowered, not controlled. Much of the TQM literature speaks of allowing workers to make decisions and to creatively solve problems without being constrained by a rigid system of policies and procedures. A common theme of TQM may be characterized as, "Workers are honest and talented, so let them do their jobs without interference." Such a philosophy frequently offers substantial benefits in terms of worker satisfaction and productivity, primarily in higher-performing organizations [International Quality Study, 1992]. These effects also have been found in small businesses [Nathan, 1993]. Despite these advantages, the reduced control over employees can increase the risk that employees will do something not desired by the company.

Second, the corporate reengineering movement [Hammer and Champy, 1993] includes the following concepts: (1) shift away from elaborate controls, (2) process orientation rather than task orientation, and (3) use of information technology (i.e., computers and electronic scanners) rather than humans in some areas. The purpose of reengineering is to allow the entire organization to focus on satisfying customers, creating value, and maintaining flexibility.

The shift away from elaborate controls often is done for cost and efficiency reasons. Some companies have discovered that they were spending more to prevent a loss than the loss would actually cost them. For example, it makes little sense to spend $100,000 per year on internal controls related to employee travel funds if the total travel budget each year is only $20,000. Many companies are performing cost/benefit analyses to evaluate their internal control systems.

A process orientation is designed to improve customer service and to make one person (or team) responsible for each process, such as filling customer orders. The process orientation often eliminates the errors and inefficiencies created when a process is broken down into several tasks that are performed by different people or departments. For example, Hammer and Champy [1993] discuss one manufacturer that required the involvement of 13 departments to handle a return of goods by a customer. The errors created by these 13 departments were tremendous. The company's annual cost of this ineffective and inefficient process was estimated to be over $100 million. Other companies should compare the potential savings from a process orientation to the increased risks created when duties are no longer segregated among employees. Employees who "own a process" have a much greater opportunity to defraud the company.

The third element of reengineering is the use of information technology, such as computers and electronic scanners, in place of humans. For example, several years ago Ford Motor Company's accounts payable department employed over 500 people. Many of these employees spent their time manually matching purchase orders, receiving documents, and invoices before authorizing payment to Ford's suppliers.

Today, Ford's vendor payment process requires only 125 people and one computer. When goods are ordered, the buyer enters the relevant information into a database. The receiving department consults the database each time a shipment is received. If the shipment matches the database, the receiving department enters a command, and the computer automatically sends the appropriate payment to the supplier. If the shipment does not match the database, Ford does not accept the shipment [Hammer and Champy, 1993]. The key to this new process is the use of information technology, in this case the computer.

Several other examples of information technology exist. For instance, many companies use electronic scanners for inventory control (bar codes are placed on each item) or document storage (documents are scanned and

then stored electronically), again reducing companies' reliance on humans.

The use of information technology eliminates many human errors found in manual systems. In addition, a reduction in the company's workforce can bring significant savings on salaries and fringe benefits. The main issue to consider when automating systems is whether the new technology incorporates adequate controls. In an automated environment, employee theft or destruction of information can happen very quickly. For example, Ford Motor Company must take great care to restrict access to the database described above and to make frequent backups of the database. Poor controls could allow employees to steal from the company or destroy the database.

A Balanced View of Internal Control

In the 1990s, companies are realizing that there are costs of having too little control and costs of having too much control. The costs of having too little control include unreliable information, violation of laws, loss of assets, inefficient use of resources, and failure to meet goals. More specifically, the company may face greater risk of litigation, fames, fraud, international problems, bad publicity, and unfavorable reports on its internal control system if it does not establish adequate controls. Many of these items can threaten the very existence of a company.

The costs of having too much control also are significant. Companies may stifle their workers, waste resources on redundant or unnecessary controls, overcomplicate processes, reduce customer satisfaction, or under-use information technology if they place too much emphasis on internal control. In today's competitive environment, these costs also can threaten a company's existence. Companies no longer have the luxury of supporting elaborate, unnecessary control systems.

The Solution

What is the answer to the internal control paradox? The solution has two parts. First, at a very conceptual level, companies can strive to minimize their total costs of control. In other words, companies cannot minimize the costs of too little control and the costs of too much control at the same time, but they can at least think of adding these two costs together and trying to minimize the total. This idea is analogous to many companies' approach to inventory management (or even quality). There are costs of having too much inventory (storage, insurance, and obsolescence) and costs of having too little inventory (lost sales and dissatisfied customers). To reach a "happy medium" companies try to minimize their total inventory costs by having neither too much nor too little inventory on hand. In fact the Economic Order Quantity model provides a formula to assist companies with determining optimal inventory levels.

Managers can strive for the same result in the internal control setting by trying to estimate the costs and benefits of individual controls. Unfortunately, estimating these costs and benefits is extremely difficult. Consider a clothing store that loses 5% of its revenue to shoplifters. The company can address the problem by hiring security guards, using magnetic tags or chains on garments, or even locking all of the merchandise in glass cases at all times. The direct costs of these controls are fairly easy to estimate; however, the indirect costs (such as customer frustration and lost sales) are extremely difficult to estimate. Also, the benefits of the proposed controls may be difficult to predict. Will the controls reduce the problem by 50% or 99%? In this case, the company should at least consider the costs of too much control and the costs of too little control, even though these costs are difficult to estimate.

Second, at a more practical level, companies can tailor their controls to the type of risk in question. Controls come in two forms, preventive (feedforward) controls and detective (feedback) controls. The primary difference is whether the control comes before or after the action. Preventive controls come before the action, and detective controls come alter the action.

For critical risks, such as mishandling of toxic waste [Willits and Giuntini, 1994], companies should use preventive controls. These controls are designed to prevent major problems from ever occurring. In the area of toxic waste, the company may have very explicit and detailed procedures that employees must follow at all times. Compliance with these procedures would be monitored very closely to prevent environmental liabilities from arising. Preventive controls also are used in the areas of employee safety [Derksen, 1993], strategic planning [Preble, 1992], and production [Morgan, 1992].

For less important risks, such as employees cheating on their travel expense statements, companies should use detective controls. These controls are designed to detect problems very soon after they happen. Corrective action can then be taken. A detective control over travel expenses might involve (1) detailed review of a sample of travel reports or (2) review of overall travel expenses for reasonableness every few weeks. Detective controls often are much less costly than preventive controls; however, timeliness can become an issue. Especially in production settings, it may be costly to develop detective controls that can highlight problems quickly enough to allow for correction [Koelsch, 1993].

Companies in the 1990s should try to reduce their exposure to risk by using cost-effective internal control systems. The two keys to the process are (1) balancing the estimated costs and benefits of various controls, and (2) using preventive or detective controls where they make economic sense.

References

Begley, R. 1993. EPA's enforcement sweep angers and confounds industry. Chemical Week (Oct. 13): 9.

Committee of Sponsoring Organizations of the Treadway Commission. 1992. Internal Control: An Integrated Framework. New York: AICPA.

Derksen, P. 1993. Medical surveillance: A final backup. OH&S Canada (Sept./Oct.): 128, 130.

Garland, S. B. 1991. What a way to watch out for workers. Business Week (Sept. 23): 42.

Golden, T. W. 1993. Employee crime can cost you millions. Management Accounting (August): 39-43.

Hammer, M., and J. Champy. 1993. Reengineering the Corporation. New York: Harper Business.

Institute of Internal Auditors. 1993. Codification of Standards for the Professional Practice of Internal Auditing. Altamonte Springs, FL: Institute of Internal Auditors.

International Quality Study. 1992. Best Practices Report: An Analysis of Management Practices that Impact Performance. New York: American Quality Foundation, Ernst & Young.

Koelsch, J. R. 1993. Practical adaptive control. Manufacturing Engineering (May): 61-63.

KPMG Peat Marwick. 1993. Fraud Survey Results 1993. New York: KPMG Peat Marwick.

Morgan, M. J. 1992. Feedforward control for competitive advantage: The Japanese approach. Journal of General Management (Summer): 41-52.

Moskal, B. S. 1991. Sexual harassment: An update. Industry Week (Nov. 18): 37-41.

Nathan, J. 1993. Empowerment as a workplace strategy in small business. Review of Business (Winter): 28-29.

Preble, J. F. 1992. Towards a comprehensive system of strategic control. Journal of Management Studies (July): 391-409.

Willits, S. D., and R. Giuntini. 1994. Helping your company 'go green.' Management Accounting (February): 43-47.

~~~~~~~~

BY DANA R. HERMANSON AND HEATHER M. HERMANSON

Dana R. Hermanson and Heather M. Hermanson are Assistant Professors in the Department of Accounting at Kennesaw State College, Marietta, GA.

~~~~~~~~