Strategies for Mitigating Control Risks in Organizational Settings

1. Introduction to Control Risks

Unacceptable activities may occur within organizations due to imperfections in their control function. Business entities frequently experience significant losses, waste, and damage caused by such control deficiencies. Adverse effects could have been forestalled by implementing specific corrective measures in conjunction with the entity's control system. Entities may suffer substantial consequences arising from control deficiencies, such as financial losses, business disruption, damage to the entity's reputation, the imposition of penalties, and the loss of management credibility. Similarly, the omission of any plans to counter such effects in contingency arrangements may constitute a decision taken by top management that indicates undue organizational risk. An entity that has experienced control weaknesses and has reacted to these adverse situations only after having been seriously hurt or embarrassed has usually exposed itself to unnecessary enterprise losses.

The potential magnitude of control risks is so significant that the overriding objective of an entity's control environment is to manage them effectively. This aim is important because certain control activities enable an entity to identify unpleasant surprises and, therefore, to exhibit a capacity to respond. The fundamental intention of control risks is to decrease the probability of unpleasant outcomes and to reduce their severity. These are the very elements of control risks as they exist and are understood by individuals responsible for the control function. In anticipation, in mature organizations, certain important control risks are specifically addressed in advance in comprehensive formal contingency arrangements, implemented, and updated after experiencing substantial problems to ensure viable operation of the business entity. These equitable recognition risk issues should be reflected in the management process of the organization and are essential in providing effective oversight control. Control evaluation studies have identified the current areas of business processes in which control risks exist.

1.1. Definition and Importance of Control Risks

It is fundamental that organizations have effective control systems to manage their value and risk factors. Many well-publicized failures have been accompanied by reports that the responsibilities of those charged with governance were not discharged effectively. It is usually a serious issue and may reflect poorly on the organization's management and board of directors. It is the client's overall responsibility to balance the various perspectives and principles, including legality, ethics, operational effectiveness, reporting integrity, internal control, compliance, and economic judgment. If the internal control is seen as unsatisfactory, then the auditor will need to carefully plan and perform additional work in the areas of the audit affected. This increases audit costs and can also divert time and energy from the main issues under review.

Control risk relates to the classification of monetary statement assertions that there are no internal control procedures designed to prevent, detect, and correct errors in relation to specific types of monetary misstatement. In relation to internal control systems, the audit needs to assess the initial design and implementation of the relevant procedures and the tests of the routine operation of those considerations. Relating to the operation of internal controls, the control risks are quite high, leading to the potential fraud risk.

2. Identifying Control Risks in Your Organization

Determining control risk is a difficult task for the auditor because it involves estimating, rather than measuring factors, generally viewed as within the domain of management. It's management's job to create and maintain sound internal control to minimize control risk. When management doesn't take effective responsibility for internal control, the auditor should plan to increase the assessment of control risk because more work would be required to ensure that no control risk exists. Determining control risk for a financial statement audit represents the responsibility of both management within the organization and the auditing standards generally accepted. There are many ways to identify control risks within an organization. The internal control questionnaire and the multinational internal control questionnaire are two principal methods of diagnosing internal control weaknesses and other control risk factors. The comprehensiveness of the internal control questionnaire makes it important for application to a number of companies.

The internal control questionnaire is designed to assist the auditor in identifying internal control reportable conditions, which may be relied on in evaluating control risks as a consideration in planning, performing, evaluating, and reporting his study.

The comprehensiveness of the internal control questionnaire is useful in designing control evaluation. Communication is the major intent behind any internal control study. It is important for the auditor to discuss the study with the engaged party. He should be able to obtain a clear definition of the services to be performed and carry out those services without communication barriers because of sensitivity and fairness in developing the content of the questionnaire. There would be a degree of communication between the auditor and the client companies in the discussion of the questionnaire to obtain an understanding of the system for the speed of the auditing study.

2.1. Common Types of Control Risks

All companies face control risks that are specific to their individual operations. Nevertheless, control risks are based on a common threat to organizational goals: the danger that employees, agents, management, or directors may ultimately subordinate their loyalty to their own little empire. Five common types of control risks are shown that face most companies. These control risks are (1) the threat of management fraud, (2) the excessive influence of a dominant individual, (3) management's motives to build empires, (4) the influence of corporate directors, and (5) the pressures on organizational personnel to neglect important internal controls. Each of these control risks to goal achievement is discussed in the paragraphs that follow. Since many of the terms used are related, there is some naturally occurring overlap in these definitions.

A concern pervasive to all companies is the threat of management fraud: the danger that management will use its unique position to create or perpetually distort financial reporting in order to paint a rosy picture of the company's profitability, financial stability, and growth to financial statement users. To achieve this result, management may manipulate estimated amounts, apply aggressive accounting treatments, or even break existing financial contracts or accounting rules. The result is that management will misrepresent the firm's true competitive advantage, revenue, growth, and history of earnings by portraying the firm as a stellar investment opportunity. Misrepresentations can include direct monetary transfer, converting business opportunities to personal opportunities, and manipulating results to "win support" in the form of equity, debt, or debt guarantees.

3. Tools and Techniques for Assessing Control Risks

Traditional risk assessment tools focus on identifying dimensions of risk and their impact on expected value using a predominantly fiscal framework. For example, traditional insurance industry premium assignments for property coverage are

based on underwriting survey information relating to the company's surrounding area. Detailed judgment as to the relative probability of a particular type of loss is provided by historical experience and claim data of similar facilities. More than three-fourths of the resulting premium charge, however, is based on the specific structure. A distribution of loss information accompanying the underwriting generally mentions a range of mitigation alternatives. Built-in fire protection features must be enhanced to improve the insurability figure. Costs associated with water supply capability requirements are delineated. Flexibility in customizing the insured's physical security program is discounted using readily available tools.

Developing and verifying effective mechanisms for controlling operating risks involves more than the simple calculation of expected values. Expected values must be placed in a risk framework that is broad enough to capture all the participants' expectations. This framework must also be detailed enough to make the complex model understandable by all the company's functional managers. Therefore, to comprehend organizational control strategies in a small subset of operating risk environments, one must first identify the risks that involve control mechanisms and then understand how organizations commonly cope with such risks.

3.1. Risk Assessment Frameworks

Risk is an intrinsic fact of life and operates at every level of an organization. Risk presents uncertainty, the antithesis of control, which promises certainty. Uncertainty is an intrinsic feature of modern life, as are control risks. Audit has advanced by arguing for the elimination of every business risk. Complete risk elimination is achieved through the closing down of businesses. Risk management rarely adopts such extremism, but it does begin by adopting a framework for risk assessment. The objective is not to expose every minutiae of risk assumption, but to ensure that major risks are brought to the attention of the board and disclosed in published accounts. Organizations use a number of different risk assessment techniques and risk measurements. The essence of every risk management framework, however, is the continual process of identification, assessment, control, and reassessment of the key risks. This process is supported by information systems at the operational level and control systems at the governance level. Technical developments are forward-looking and show how information technology can be used to best effect in managing inherent risk. These are usually confined to topics of specific risk. They lack any detailed and comprehensive coverage of enterprise risk management. But what is evident from these publications is the need for a common risk management language and risk management systems within business

enterprises. Data integration and an enterprise-wide risk management solution that links back to the model of governance is seen as the way forward.

4. Implementing Control Measures

Implementing control measures in a proactive way means that control strategies need to be formulated and implemented so that uncertainties and disruptions can be more readily identified, understood, and perhaps reduced to inconsequential levels for the ongoing operation. This activity essentially focuses on the "structured" use of the various management control systems identified in the control process cycle. It also means that the control support and control response systems need to be "managed" the way other management systems are managed. Processes, tools, people, and organizations need to be organized to be effective, and conditions need to be in place to sustain their effectiveness over time.

The information attracted to control systems generally consists of a mix of internally generated data and externally generated information. The internally generated data includes financial ratios of various types, workload and actual hours information on both projects and administrative tasks, and recorded utilization levels of people and machines. These data are normally easily available and are near copies of the data accountants routinely need to run a business. The main difference is that it gets reported more rapidly and in a way that can be combined, analyzed, and reported across the levels and units in the organizational hierarchy in a way that is useful for control purposes. Combined with the data are also more summary-like information about operations, process transactions, and related conditions.

4.1. Internal Controls and Their Role

Internal controls encompass those elements of an organizational structure that strive to offer support in organizing, directing, and controlling an enterprise's operational activities in order to safeguard the enterprise's assets and ensure organizational objectives are met. The internal control environment generally consists of policies and procedures that help ensure management's ability to make strategic decisions, as well as initiatives that ensure those measures can be carried out with a minimum of disruption. The control mechanisms built into this framework offer a broad management-based technique for the monitoring of all enterprise data over time. The internal control performance is indistinguishable from the traditional operational methods that are employed by organizations in these areas.

The purpose of internal controls within any enterprise is to manage risk. By employing a system of well-tested controls, management can then better ensure that the organization's financial, operational, and compliance objectives are successfully met. As management's risk stewardship tool, internal controls are tailored to particular risks and are utilized only for high-risk business areas to prevent and detect unauthorized activities. In concluding on the effectiveness of internal controls, it is important to recognize that risk exposure is not to be totally eliminated. Rather, the nature of the risk should be analyzed and accepted, or at least placed within tolerance limits. No matter what evaluation and control procedures an organization chooses to apply, risks are inherent in the concept of value-creating operations. Proper controls should provide a cushion against these risks and not hinder flexible operational processes. The risk of over-reliance on various internal control devices and structures is indeed a concern, but it is also recognized and addressed by management.

5. Building a Strong Control Environment

Although negative outcomes often receive the most attention in the business media as well as in social research on control, detrimental consequences are undoubtedly not the sole result of control activities. Moreover, the majority of people who work and conduct themselves within the confines of organizations worldwide express work-related values based on fairness, balance, and the desire to see that effective means are developed to promote accurate, reliable, and consistent organizational outcomes. In other words, there are positive and legitimate reasons for organizational members to enforce controls. Because it is not normal human behavior to universally deceive and take unfair advantage of others or to consistently tolerate what is patently unfair, organizational control can also be viewed as a social value of support to citizens and employees. Given the significant role that the control environment plays in shaping organizational behavior and risks, researchers must reassert its value in practice as well as theory. The control environment historically has played a significant role in resolving issues related to the design and operation of internal accounting systems. Although substantive changes have occurred since that time, contemporary research that addresses how the control environment can mitigate control risks has not captured the same level of attention. There are several important reasons for reinvigorating the attention that social research on the control environment can contribute to the study of control and mitigate control risks.

5.1. The Role of Leadership in Establishing a Control Culture

Within the context of frameworks for designing, implementing, and monitoring internal controls at all levels of an organization, it is becoming apparent that organizational culture plays a pivotal role in enforcing desired control behavior. An organization's culture comprises the unwritten norms, values, beliefs, and underlying assumptions shared by its employees. When an organization's culture supports shared ethical, conformance, and performance values, underpinned by systems, procedures, and compliance guidelines, it will encourage employees to become fully engaged in the control process, believing that as they perform their daily tasks, everyone within the company contributes to the quality and reliability of the data, information, and processes.

In this respect, without the active support of company leadership, organizations may find themselves more at risk of control failure - particularly in mission-critical areas where unreliable information could jeopardize the safety and health of a large group of people, the environment, and the company's financial and operational strength. In these and other high-risk industry environments, such as aerospace, general manufacturing, and pharmaceuticals, leaders (and senior management in particular) must lead by example and uphold the organization's values-based commitment to integrity, ethics, and internal control in both intent and behavior, all the while demonstrating support for enterprise-wide compliance directives by ensuring compliance with applicable laws and public policy. Such values-based compliance issues emerge from an organization's ethics infrastructure, elements of which include:

- Prize line-management accountability for ethical behavior - values-based leadership by example, reward, and sanction.
- Ensure employee performance appraisal measures ethical and internal control compliance.
- Implement compliance risk monitoring, integrating existing oversight functions with data analysis to identify weaknesses in management's effectiveness in evaluating and ensuring effective compliance risk controls and procedures.

6. Training and Education on Control Risks

There are many internal and external pressures that can lead managers to game the control system or undermine its effectiveness. It is virtually impossible to systematize the judgment, character, and integrity considerations necessary to reduce control risk. However, it is possible to assess the extent to which the pressures giving rise to the risk are properly understood, and whether an

awareness program needs to be developed that underscores the implications of such factors and clarifies the obligations associated with internal control systems. A standard approach to control risk is to mandate that more rigorous auditing and monitoring for larger multimarket corporations with multiple lines and brands be accompanied by analysis, investigation, and enforcement stages.

This service provides quality assurance, which is touted as a risk-reducing attribute of the financial statement and as a deterrent to misconduct in the formulation of financial information. But the nature of these traditional checks has not modified the environment that continues to encourage certain managers to enhance earnings management and income smoothing. Providing counseling and support at the executive, director, and stakeholder levels can also reduce control risk by helping to ground expectations and institutionalize reasonable efforts.

6.1. Employee Training Programs

Although employees may be willing to take control, they are often unprepared to assume those responsibilities. However, extensive training programs can bring employees to a level of competence that would provide substantial assurance that the control system would function as planned. Training is especially crucial in organizations with complex procedures or computerized control systems that limit the nature and quantity of decision inputs that any single employee can contribute. Employees require education concerning the controls and operational performance indicators used to monitor corporate performance, action guidance to assist them in recognizing and diagnosing unusual circumstances, and feedback about actual or simulated management decisions or other control-oriented tasks. Other investments in training programs can help employees become more familiar with the nature, source, and potential significance of the errors they confront. Periodic rotational assignments can increase employee awareness of control issues and responsibilities. For instance, gross errors do not frequently occur in situations where employees are aware that malfeasance may be quickly detected. Furthermore, when employees have the authority to make mistakes, they are more likely to contribute. Giving persons new to an assignment a feasible goal can increase general motivation, operative skill implementation, and the ability to break constraints that might otherwise hinder action and control.

7. Monitoring and Continuous Improvement

A system of internal control is expected to provide reasonable assurance to the management and governing board of an organization regarding the achievement of operational and program goals, effective and efficient use of resources, reliability of

financial reporting, and compliance with laws and regulations. Internal control is expected to help optimize an organization's capacity to make improvements to its operations and programs, to learn from experience, to innovate, and to respond to changing circumstances. An organization's system of internal control is not a fixed and unchangeable set of rules, but rather a means to an end – a dynamic, adaptable instrument to promote and achieve a more effective, efficient, and honest organization. Many of the strategies that organizations may already use to support management and continuous improvement can also be used or adapted to support internal controls and, indirectly, to support the efforts of unit managers and staff in identifying, evaluating, and mitigating control risks in day-to-day operations. This section offers some helpful lessons learned from the management literature on organizational and system learning and performance improvement that organizations may use to further enhance their internal control environment for the benefit of all engaged in achieving an organization's mission and objectives. Deciding to study or focus intently on internal control issues, control risk, engagement on internal control, or developing a risk-based approach to achieving internal control does not mean that the organization should not also study and focus intently on ways to enhance the management of the work of the organization.

7.1. The Importance of Regular Audits

Financial statements are not the only kind of document that organizations should regularly audit to detect and remedy fraud, transaction errors, problems with internal controls, and other control issues. Organizations should also establish and frequently carry out internal audit procedures for their environmental and social activities and policies. For example, one of the largest electricity producers in the United States regularly examines the effects of its electricity generation policies on various environmental and public health issues as part of its board reconfirmation processes. This and other reports are used in director self-evaluations by the organization's board of directors. Similarly, a company has regularly integrated internal review processes with outside disclosure requirements for such matters as greenhouse gas emissions and other environmental impacts. By conducting these kinds of review processes in the course of their normal activities, the organization is able to find and correct problems before they become large, expensive, and difficult to address.

8. Case Studies and Examples of Control Risk Failures

The following case of collecting fictitious lives reflects poor control over resource allocation. A well-meaning worker processing the payroll in a small office

discovered payments for full-time salaries being made to seven people, none of whom had ever collected a paycheck, paid taxes, or contributed to any welfare or pension plan. Those involved in processing the payroll had carefully recorded the seven fictitious lives in the company's personnel files. Whether the financial promoter fooled the entire company by evolving the fictitious seven fully lived lives of these individuals during a seven-year period or had all the help yet managed to escape detection seems quite incredible. A similar incident of unqualified people receiving full-time salaries would quickly come to light in an encounter with the direct supervisor or with the accuracy or frequency of the doctor's treatment or with the activities of the teachers or instructors or club members. The payroll skimmer appears, unlike popular deception techniques, coercion, or intimidation, to have been an ongoing battle of wits in the process of basic organizational functions and the desire to get away with receiving something for nothing.

Cases of other people being supported by salary payments made directly by their companies are too numerous to be accidents or indicative of an unusual lack of control. Three of the situations described involve those workers on the job at the same time, each at a different client location. The client was a defense contractor that required a national criminal search of its employees. Since most of the employees worked at least part of the time on location at various customer sites, we had not encountered this particular problem before coming up with the idea of shifting one or two known criminals to work at the same site before the check was made. All three of the criminals called home, tried to reach the college student, told the personnel head to drop his project because another project was more important, and later killed the idea entirely. Although such a plot is not especially capable of detecting criminals, the college student suggested establishing a procedure to evaluate clue-seeking shifts and was turned down flat.

8.1. Lessons Learned from Notable Control Risk Incidents

Few accounting scandals have had the same impact as the two that occurred at Enron Corporation and the company that was its auditor. While both companies no longer exist in their previous forms, many lessons can be learned by examining their rise and precipitous fall. This section explores the internal control failures that contributed to these two companies' demise, from the perspective of the control environment, risk assessment, risk response, control activities, monitoring, and information. Many of the control weaknesses identified prior to these failures are as applicable today as they ever were. The level of scrutiny, however, has significantly increased.

Historically, there have been many control risk incidents in which investigators found serious flaws in an organization's control environment. In examining these organizational failures, monitors have identified a list of best practices that organizations can implement to reduce control risk. For example, lessons learned have highlighted the importance of ethical conduct at all levels of an organization and the role that corporate culture plays in promoting honesty. The downfall of Enron was not caused by one type of unethical behavior, but by a series of unethical behaviors that ultimately led to the restatement of the company's financial statements. With this in mind, organizations can mitigate control risk exposure by promoting ethical conduct and demonstrating the importance of this behavior at all levels of the organization.

9. Conclusion

The chapter has sought to charge researchers and practitioners interested in internal and external auditing and assurance, operational excellence, risk, governance, fraud, and misreporting from countries with high and low regulatory and governance requirements to respond to the global crisis in confidence in corporate reporting to examine the effect of hierarchical level and competitive strategy on the importance given to nine predefined control goals. It has advanced three propositions which relate control goal importance to competitive organization design, environmental scanned and focused goals, and external relations goals salience, congruently. The organic flexible organization recognizes that long-term market success is a function of strategic goals congruency with scanning the needed environment to detect sub-optimal goal congruity and implementing action to correct externality problems. The organic flexible-feasible organization goal acknowledgement process is dominated by the avoidance of falls from destined success with the result that quality goals predominate.

Modern evocative industrial strength IT rationalized and performanced hierarchical level flexible dividing service role mechanistic companies closely evaluate financial profiles and make sure that resources yield returns which are relatively better than historical numbers and competitive positional; and, they have provided evidence for hierarchical level competitive strategy goal importance and organization design congruence with stated, implemented, and real events: Do companies recognize that the importance given to prevailing control goals sequences depends on hierarchical level cooperative/non-co-operative strategies? Companies signal relative goal importance by contrasting goal rankings with their organizational type, market segment served, superior and subordinate manager jobholders exclusive identified tastes; and technology choices. Companies, which central control goal narratives

imply that jobholders own highly mutual, unmotivated, and fundamental taste support evidential beliefs, choose strategies that balance market niche, superior, government, and subordinate officeholder goals.

The proposition has examined decision aid tools, informational issues, and variables: Control—goal conditions, companyscape outcomes components; who gains, provides, selects decision analysis tooling; the need information; the source, type, user, and nature of information; jobholders evoked/offered tasteful beliefs; whose tastes/constraints are satisfied; market superiority, and co-existence. There has been no evidence that corporate difference affect competitive company control goal rankings. Future researchers should develop the possibility that in personality firms a firm. This represents the first comprehensive attempt to examine the importance given to control goals sequence within modern companies and to relate advanced company typology with competitive business strategy. Generally, superior job vantage point companies value hierarchically-demanding goals relatively better than staff while superior job subordinates receive preference for goals afforded them.

9.1. Emerging Technologies for Control Risk Management

When emerging technologies move into organizational settings, it involves taking considerable risks. Various high-risk technologies emerged in the early industrial age, entering production settings before contributory research existed. High risks include the control structure of the technologies and any potential interactions with the task setting. None of the expected contributions on risk reduction were forthcoming. Hence, the paper presents a range of risk-mitigating control technologies that can be utilized across all organizational sectors.

One rationale for moving emerging high-risk technologies into organizational settings is that strategic competitive advantage can be gained. Organizations may have a first-mover advantage, temporarily leveraging technological superiority. Defensive objectives also occur to prevent economic adversaries and terrorist organizations from obtaining an advantage. Governments and professional bodies recommend the application of safety, environmental, system, and adequate software integrity standards. However, unless technology advances are linked to control risk management standards, organizations are not prompted to focus on introduced high-level hazards. Control aspects, including human and organizational factors, also receive inadequate research support. Prior research emphasizes the need to pay considerable attention to the human dimension of decision-making using risky technology in organizational and especially operational settings.