

INTERNAL AUDIT TECHNIQUES TRADITIONAL VERSUS PROGRESSIVE APPROACH

Srihadi W Zarkasyi

ABSTRACT

Internal auditors do not just audit control activities, they also monitor a company's risk profile and play a key role in identifying areas to improve risk management process. However, if they do not completely understand the risk of the business, internal auditors can perform only traditional checklist tasks. At every company, top manager should help their internal audit team transform itself into a catalyst for change as a key risk adviser. In general, it would be better if internal auditing departments are taking "an enterprise wide risk view" and adopting a more "progressive approach" to audit. We believe that internal auditors can become a cornerstone of risk management in their own companies.

Key Words: *Internal Auditor, Internal Control, Internal Audit Techniques- Progressive Approach, Internal Audit Technique-Traditional Approach, Risk Management, Risk-Based Audit, Enterprise Risk Management (ERM), Control Self Assesment (CSA), COSO (Committee of Sponsoring of the Treadway Commission)*

INTRODUCTION

Internal Auditing began as a one-person clerical function that consisted primarily of performing independent verification off bills before payment. Over the years, internal auditing has evolved into a highly professional activity that extends to the appraisal of the efficiency and effectiveness of all phases of a company's operations, both financial and non-financial. These changes have led to the formation of internal auditing departments.

The growth and importance of internal auditing to a company has been accompanied by increased professional recognition for the internal auditor. Recently, every business has complex relationship with many people, groups, and organizations in society. Some are intended and desired, others are unintentional and not desired. Whether desired or not, voluntary and involuntary, the people and organizations with which a business is involved have an interest, or stake, in the decisions, actions, and practices of the firm. Customers, suppliers, employees, owners, creditors, and local communities are affected by the economic performance of the

business. They have a stake in business, and their support can be critical to its success or failure. How the company manage risk from all these changes was critical to success. As audit professionals, we need to be able to discern significant details of business operations and look “through the windshield” for oncoming risk while communicating with operating managers in a clear and timely manner. To identify risk areas and contiously monitor the company’s risk profile, we had to transform the internal audit department from its traditional role “performing checklist activities” to one that “focused on corporate and business unit goals, strategies, and risk management processes”. To achieve this restructuring, we ask ourself these fundamental questions:

1. How do we define internal control ?
2. What best practices should we incorporate into audit’s evolving role ?
3. How can internal audit become an integral part of risk management process and maintain independence?

DEFINING INTERNAL CONTROL

The generally accepted definition of Internal Control, as outlined in Internal Control Integrated Framework, issued by the Committee of Sponsoring Organizations of Treadway Commission (COSO), consists of five related components that must be present for an entity to achieve effective internal controls: (1) the control environment, (2) risk assessment, (3) control activities, (4) information and communication, (5) Monitoring. COSO includes representatives from IMA (The Institute of Management Accountant), AICPA (American Institute of Certified Public Accountants), AAA (American Accounting Association), FEI (Financial Executives International), and IIA (The Institute of Internal Auditors). Simply testing control activities under a traditional audit system gives internal auditors a very narrow focus-this is significant problem with our former process.

To help create an auditing methodology based on process improvement an continual risk assessment, we adopted the Committee of sponsoring organization of the Treadway Commission’s (COSO) definition of internal control and incorporated it into our mission statement. In 1992 the committee of Sponsoring Organizations of the Treadway Commissions issued internal Control-Integrated Framework, whose primary objectives were to establish a

common definition of internal control and provide a standard to help auditing professionals assess control systems and determine how to improve them. COSO defines internal control as “a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable laws and regulations”. The COSO definition expands internal audit’s traditional testing of control activities, such as policies and procedures and approvals and reconciliations, to include four additional components that derive from the way management runs a business and are integrated into the management process as follows: (1) *control environment*. The tone of the organization influences the control consciousness of its people. Examples include the integrity, ethical values, and competence of employees, management philosophy, and input provided by the board of directors, (2) *risk assessments*. Identification and analysis of risks relevant to achieving corporate goals, determination of how such risks should be managed and implementation of a process to address risks associated with change, (3) control activities. Policies, procedures, and processes that help ensure a company carries out management directives. Examples include approvals, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties, (4) Information and Communications. Communication within the company and with external parties such as costumers, regulators, and shareholders. For example, reports that contain operational, compliance or financial data that share ideas or events across lines of business are generated from a company’s information systems, (5) Monitoring: Assessing the quality of company’s internal control systems. This is done through ongoing monitoring of activities within the business units and an independent evaluation of existing controls by auditors.

ADOPT BEST PRACTICE

Ever since the Asian economic crisis in 1998, risk management or rather the call for better risk management can denote the single most important answer or survival tool kit for industry. For internal auditors, our role has also expanded. Our focus and approach in considering the audit has undergone change. In assessing the adequacy and effectiveness of internal controls, we don not longer only determine internal controls and test their effectiveness. Instead, we have evolved to examine business objectives first and identify the associated risks

before proceeding to assess the business controls. In today's internal auditing, we have progressed from the compliance to risk-based auditing.

Although auditing on the level of compliance to management's policies and procedures is still important, the internal auditor's scope needs to be broadened as a high level of compliance alone is inadequate for the auditor to conclude his assessment or assurance. This is because some of the policies and procedures could be outdated, obsolete, or not well designed. Some of the controls have designed flaws while others are unnecessary or even controlled, given the risk level in terms of its significance and likelihood of happening. The other reason is that certain new and emerging risks are not well identified or fully understood by management and hence are not being addressed. This results in the absence of controls to manage such risks. Therefore, moving to risk-based auditing is the internal auditor's answer to add value to the organization and improve its operations.

However the process of migrating from compliance to risk-based auditing is a challenging journey. It is radical change that requires a shifting of paradigm from existing existing auditors. An auditor need to ensure that the current and future risk are being addressed. The risk based audit approach itself is a paradigm shift from: (1) fragmented to continuous, (2) negative to positive, (3) reactive to proactive, (4) cost-based to value driven, (5) compliance and rotational focused to risk focused, (6) mechanical to judgemental.

The internal auditor of the future will not be monotonously engaged in ticking and checking as they did in the past anymore. Today, an auditor needs to change his mindset from being a ticking auditor to a thinking auditor with the right attitude. When continuous change and transformation occur, there will be a continuum in the learning process and therefore a continuous risk assessment is needed. Retraining the auditor's skill and mind is very important to understand risk-based auditing. Hence, the auditor should be very dynamic in every angle of work and thought. We need to ensure and make our audit costumers confident with our systems of internal controls and that they are adequately in place. For internal auditors, audit customers comprise mainly the Audit Committee, Senior Management, as well as the regulators. The risk-based audit methodology should be benchmarked against best practices. It is crucial for this methodology to be systematically conducted to ensure all major risks are identified. A typical process of risk based auditing will include risk identification and assessment to come up with risk profiling. This is the most critical process and must be done comprehensively. In risk profiling, several analyses are needed, covering aspects of the business, business performance as well as

critical business processes. For example, in analyzing the business, we must consider factors such as environment, information, owners, competitors, customers, management, business processes and value. In addition, our analysis of business performance needs to cover aspects such as profitability, liquidity, asset management, asset quality, financial leverage, market valuation, and capital adequacy. In order to narrow down the risk area, the critical process also needs to be analyzed.

The processes described above are good demonstrations of how challenging risk-based auditing is. However, the benefits are obvious and will enhance value in our work. We as internal auditors, can now support our organization more effectively and assist the Board and Management to achieve corporate goals. After all, that is what an internal auditors is all about. We must use progressive approach as indicated in below tabel (Table 1).

Table 1
Internal Audit's Evolving Role
Traditional vs Progressive Approach

Traditional	Progressive/Best Practices
Audit Focus	Business Focus
Transaction based	Process based
Financial account focus	Management Focus
Compliance objective	Risk identification, process improvement objective
Policies and procedures focus	Risk management focus
Multiyear and coverage	Continual-risk assessment coverage
Policy adherence	Change facilitator
Budgeted cost center	Accountability for performance improvement results
Career auditors	Opportunities for other management position
Methodology: Focus on policies, transactions, and compliance	Methodology: Focus on goals, strategies, and risk management process

To assess how well the company in dealing with risks, we need more than “ a list of required controls”. With the COSO models as a guide, we develop the following “best practices”:

1. Monitor business activities and key performance indicators continuously. As internal auditors we must keep abreast of what happen in the organization's environment. We do this by attending executive committee meeting, obtaining important management reports, identifying and meeting with the key department heads throughout the year.
2. Coordinate with other risk management functions. In evaluating quality controls, security, asset review, etc, we try to leverage the work of other departments where possible by reviewing the scope of their activity and considering their results in our approach. For axampel, rather than just using our own samples for testing, we examine the unit's quality control program and selectively validate the results. We also can coordinate the timing of an audit with another department and suggest process improvements.
3. Develop the audit plan based on risk priorities. Rather than scheduling audits according to a standard cycle of one, two or three years rotations, we base frequency of audits on business area's risk factors such as previous poor audit rating or significant changes in personnel. This allows us to focus on the highest risk priorities within the company and to devote appropriate resources to new and changing areas. We also train managers to update their own risk assessment systems and methodologies, for example by showing them how to implement steps to monitor quality control and segregation of duties.
4. Get involved in technology projects. As internal auditos we know, we must be involved in activities such as systems development and conversions, process reengineering, new products and services, mergers, and acquisition and the analysis of new IT (Information Technology) policies.

BECOME PART OF RISK MANAGEMENT PROCESS

Risk management is an iterative process consisting of well defined steps which taken in sequence, support better decisison making by contributing a greater insight into risk and their impacts. The risk management process can be applied to any situation where an undersired or unexpected outcome could be significant or where opportunities are identified. Decisison makers need to know about possible outcomes and take steps to control their impact.

Risk management is recognized as an integral part of good management practice. To be most effective, rsik management should become part of an organization's culture. It should be integrated into the organization's philosophy, practices and business plans rather than be viewed or practiced as separate program. When this is achieved, risk management becomes the business of everyone in the organization. If for any reason, it is not possible to integrate risk management across an entire organization, it may still be possible to pally it successfully to individual departments, processes or project.

Risk management is the term applied to a logical and systematic method of establishing the context, identifying, analyzing, evaluating, treating, monitoring, and communicating risk associated with any activity, function or process in a way that enable organizations to minimize losses and maximize opportunities. Risk management is as much about identifying opportunities as avoiding or mitigating losses. The maximum benefit is usually obtained by applying the risk management process from the beginning.

The main elements of the risk management process are as follows:

- (1) **Establish the context:** Establish the strategic, organizational and risk management context in which the rest of the process will take place. Criteria against which risk will be evaluated should be established and the structure of the analysis defined,
- (2) **Identify Risks:** Identify what, why, and how things can arise as the basis for further analysis,
- (3) **Analyze risks:** Determine the existing controls and analyze risk in term of consequences and likelihood in the context of those controls. The analysis should consider the range of potential consequences and how likely those consequences are to occur. Consequences and likelihood may be combined to produce an estimated level of risk,
- (4) **Evaluate risks:** Compare estimated levels of risks against the pre-established criteria. This enable risk to be ranked so as to identify management priorities. If the levels of risk established are low, then risk may fall into category acceptable category and treatment may not be required.,
- (5) **Treat risks:** Accept and monitor low priority risks. For other risks, develop and implement a specific management plan which includes consideration of funding,
- (6) **Monitor and Review:** Monitor and review the performance of risk management system and changes which might affect it,
- (7) **Communicate and consult:** Communicate and consult with internal and external stakeholders as appropriate stage of the risk management process and concerning the process as a whole.

Risk management can be applied at many levels in organization. It can be applied at the strategic level and at operational levels. It may be applied to specific projects, to assist with specific decision or to manage specific recognized risk areas. Enterprise Risk Management (ERM) is a strategy organization that can be used to manage the variety of strategic, market, credit operational and financial risks they confront. ERM calls for high level oversight of risk on a portfolio basis, rather than discrete management by different risk overseers. The difference between ERM and more traditional ways of managing risk are as following:

Table 2

Traditional Risk Management Vs Enterprise Risk Management

Traditional Risk Management	Enterprise Risk Management
Risk as individual hazards	Risk in the context of business strategy
Risk identification and assessment	Risk portfolio development
Focus on discrete risks	Focus on critical risks
Risk Mitigation	Risk Optimization
Risk Limits	Risk Strategy
Risk with no owners	Defined Risk Responsibilities
Haphazard risk quantification	Monitoring and Measuring of Risk
"Risk is not my responsibility"	"Risk is everyone's Responsibility"

Source: KPMG

To complete the integration of COSO framework into internal audit process, we developed a strategic plan that would: (1) provide for a mix of skill sets within audit group, (2) create the audit plan by identifying audit entities and performing a formal risk assessment, (3) ensure internal auditors update risk assessment and monitor the risk indicators on an ongoing basis, (4) establish our team's communication strategies and reporting formats. In order to accomplish the first objective we assembled a new audit team with a mix of public accountants and other business professionals. Their quality and experience were critical to achieve department aims. Instead of staffing the department larger with low to mid level professionals, we began with a smaller number of mid to high level employees. As part of the upgrade, we must change job classifications and increase the skills needed to succeed.

Career paths for the team are varied: Business area professionals-from loan servicing, loan production, accounting or information technology-move into department, and auditors transfer to other functions such as treasury, accounting and lending. This cross-training adds depth to the audit team's consulting skills, enhances its ability to recruit and retain audit professionals and gives it increased understanding of risk analysis and controls in the business areas. To achieve our objectives of formal risk assessment and continuous risk monitoring, we established client service teams for specific departments or functions identified within each audit plan. These teams, typically consisting of three to seven individuals with specific skills, review the risk management as an integral part of management process. Risk management is a multifaceted

process, appropriate aspects of which are offer best carried out by a multi-disciplinary team. It is an iterative process of continuous improvement. Shacnfield (2004) use COSO's ERM framework by capturing the essence of eight components: (1) internal environment, (2) objective setting, (3) event identification, (4) risk assessment, (5) risk response, (6) control activities, (7) information and communication, and (8) monitoring.

Lawler (1980) suggested about implementing an effective control self assessment (CSA) System. CSA can be defined as a procemss whereby management and staff meet together to identify risk, assess and evaluate whether controls are in place to mitigate risks and, if not, develop action plans to introduce the requisite controls. This process is carried out in collaboration with internal auditors who act as facilitators in the process. As any new practice, there are challenges as well as benefits. Benefit of CSA: (1) to management and staff; management are encouraged to think about risks and controls and learn how to analyze and report on controls. Management then assumes responsibility and accountability for effective risk and contol management. The CSA process necessitates and has the potential to improve communication within the organization as it involves staff at all levels partaking in the process. Corrective action is more effective as participants "own" the results. It is not internal auditor telling them what they have to do; (2) to the internal auditor: This joint exercise enhances co-operation between auditors and clients. Clients are more likely to provide auditors with detailed information on their operations, increasing the auditors' understanding of the business and allowing auditors to concentrate on areas of key concern, for example, areas of highes risk. This concentration should produce higher value audits for the client. In certain cases, the need for internal audit involvement may gradually reduce, although this is not a specific strategy of the CSA process. Over time, auditors are able to take on more of a consultative role, a benefit to both the auditor and the client, (3) to the audit committee: audit committee may also be seen as benefiting from CSA being used in their organizations. Audit resources are used more efficiently with greater overall audit coverage of the organization. Information obtained is more focused on key concerns. There is greater understanding and better awareness of risks and controls within the organization as well as wider range of opinions on these controls.

CONCLUSIONS

The basic requirement for the internal audit function, as contained in the new Internal Auditor Standards, are to monitor and evaluate the effectiveness of an organization's risk management and control systems. Standard 2110 of the International Standards for the Professional Practice of Internal Auditing, for example, says the internal audit activity should help the organization manage risk by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems. Standard 2120 says the internal audit activity should evaluate the effectiveness and efficiency of the organization's control processes. The idea of viewing risk as an opportunity may surprise some internal auditor. Overall responsibility for enterprise risk is changing because of new standard from Internal Auditors. ERM require the internal audit function in a company to monitor and evaluate the effectiveness of the organization's risk management and control system. Why should Internal Auditor care about ERM? Because it will directly affect why and how they do their job.

REFERENCES

- Bahnam, Russ (2004), Enterprising Views of Risk Management, *Journal of Accountancy*, June
- Cangemi, Michael P (2003), *Managing the Audit Function: A Corporate Audit Department Procedures Guide*, John Wiley and Sons, Inc
- Cooper, DE (2004) *Ethics for Professionals in a multicultural world*, New Jersey, Pearson/Prentice Hall
- Corey G, et al (2003) *Issues and ethics in the helping professionals*, Pacific Groove, Cole Publishing Co
- Harahap, Sofyan S (2002) Corporate Accountability, *Media Akuntansi*, Desember 2002, pp 27
- Hiro Tugiman, 2003, *Peran Manajemen dalam Good Corporate Governance dan Audit Internal*, Presentasi Makalah, Unjani
- Lindow, Paul E and Jill D Race (2002), Beyond Traditional Audit Techniques, *Journal of Accountancy*, July, pp 57-58
- Matsumura, La Mae and Robert R Tucker (1992) *Fraud Detection: A Theoretical Foundation*, *The Accounting Review*, October 1992
- Malhotra, Yogesh and Dennis Galletta, (2005), A Multidimensional Commitment Model of Volitional Systems Adoption and Usage Behavior, *Journal of Management Information Systems*
- McConnell, Donald K, et al, (2003) How Sarbanes-Oxley will change the audit process, pp 37-39
- Merchant, Kenneth, *The Behavioral Dimensions of Internal Control*, Harvard University Graduate School of Business Administration, pp 269-273
- Romal, Jane B and Arlene M Hibshweiler, (2004) *Improving Professional Ethics, Step for Implementing Change*, <http://www.nysscpa.org>