Ernst and Young Top-Down, Risk Based Approach for Assessing Control

Carolyn Tsai

BADM 559

December 15,2008

Introduction

Currently all companies are paying more attention to risk management, especially ever since the emergence of the Sarbanes-Oxley Act of 2002 (SOX). SOX require companies to implement and assess internal controls. Risk management is collaboration between different elements in business, such as business operation, finance, accounting and information technology (IT). The top-down risk based approach is a control framework that addresses the financial risks involved in a business. Ernst and Young (E&Y) developed its interpretation of the top-down, risk based approach, which follows the general layout described in the PCAOB's guidance with additional components that it believes is critical for risk and control assessment. A major issue that influences the details of implementing this approach is materiality. Materiality level determines the amount of the controls that companies need to establish for preventing and detecting material misstatement risks. IT is apparent in documentation and retrieving electronic documentation for reviews on control effectiveness. In the E&Y presentation, Rich Castle, the Executive Director in the Technology and Security Risk Services practice, described the SAP control Ernst and Young uses for control testing. After a clear explanation how E&Y uses the IT system to enhance controls, the report will describe the usefulness of a risk heat map for control testing. By understanding the ultimate purpose and the components of the top-down risk based approach for assessing risk and controls, auditors can apply their information technology knowledge to effectively implement the control evaluation.

History and Purpose

After the fall of several companies due to corporate and accounting scandals, the government recognized that there is a need to assess the quality of internal controls in a company. The Enron

scandal was one of the most infamous corporate and accounting scandals. The Enron Corporation was recording illegitimate and irregular transactions to present higher profitability in its financial statements; when in fact, the company was losing money - no effective controls were executed to reveal the problem.[1] This realization resulted in the Sarbanes-Oxley Act of 2002. Section 404 addresses the criteria of internal control assessments, which required both the company's management and the external auditors, to report on the appropriateness of the company's internal controls. Many companies restructured their methodology and practices to comply with SOX Section 404.

At the very beginning, companies struggled as they tried to interpret the meaning of this new act, and incurred high compliance costs. Companies either did not have all the correct controls in place, or had ineffective controls. The guidance and practice for compliance has evolved to assist companies to lower the compliance cost by identifying the important areas and reducing unnecessary time and effort that is unlikely to support the process of assessing crucial internal controls for financial reporting.

The top-down risk-based approach takes into consideration the guidance laid out in Section 404 for management and auditors to perform the assessment. In fact, PCAOB Auditing Standard 5 encouraged management and auditors to use this assessment approach because it considers the scope and the risk involved.[2] The purpose of the approach is to provide a structured method to increase effectiveness and efficiency for the company's operations. Other benefits include improved accountability and greater transparency to identify the weakest link in the whole chain

[1] http://en.wikipedia.org/wiki/Enron_scandal

[2] http://www.nysscpa.org/cpajournal/2006/806/essentials/p36.htm

of actions in the company's operation. The alternative approach to risk management is using the bottom up approach, which begins with assessing the controls. This method works and achieves the purpose of evaluating internal controls but most likely, companies will use more controls than are needed. Companies can eliminate implementing additional controls that does not provide utility by using the top down approach because it identifies the significant accounts that need controls. Many, if not most, companies have reduced compliance cost by adopting this approach.

In general, the top down approach follows the sequence of first identifying the company-level control. Next is to identify the significant accounts and the relevant assertions, followed by identifying the significant processes. The next part is to consider the risk and identify the point in the process that an error will most likely occur. Lastly, auditors check if controls are implemented to prevent or detect fraud at the point of risk and the effectiveness of the controls.

E&Y's "Top-Down Approach"

E&Y presented its interpretation of the "Top-Down Risk-Based Approach to Assess Key Controls." The components of the framework include Financial Statement & Business Risk, Significant Accounts, Business Process, Financial Statement Assertions, What Can Go Wrong, and Controls. It is a controlled framework, shown in Figure 1, for external auditors to address risks and controls.

The approach begins with identifying the significant accounts and the related processes in the company. In the Financial Statement & Business Risk level, the procedures are to identify, understand, and evaluate if company-level control designs are effective from a financial perspective. Auditors will consider the inherent and key business risks that will affect any

processes of a company's operation. The purpose is to understand the key risks at the industry level and at the company level. For example, in the shipping industry, all companies in the industry will be negatively affected if employees at the dock went on a strike. The companies cannot receive goods shipment and will have to delay on providing the goods to their buyers.

After considering the risks, it leads to the next component of the framework, the significant accounts. Auditors select the significant accounts, the accounts where the materiality of these accounts will significantly affect the fair presentation of the company's financial statement. The significant accounts are selected in according to their qualitative and quantitative characteristics. Rich Castle described some of these characteristics as errors of importance, size and composition, susceptibility to loss or fraud, high transaction volume, subjectivity in determining account balance, and nature of account. Of all these characteristics, the main consideration is to select the accounts based on the degree of likelihood that the errors of importance could occur. As for size and composition, sometimes accounts have more than one type of account transaction. Misstatements are more likely to occur in accounts with complex structures. Subjectivity in account balances occur when there is a need to make an estimate outside of the system; for example, estimating bad debt. Management uses historical trends and professional judgment to approximate the likelihood that buyers will default on their payment but they do not know the actual amount that buyers will default until the payment deadline. The nature of accounts can be permanent or temporary. Temporary accounts are accounts that need to be cleared at the end of the fiscal year, therefore these accounts are prone to errors during the transfer.

The auditors will then consider management's financial statement assertions on the significant accounts. According to E&Y, the assertions can be explicit or implicit as long as these assertions provide coverage for the significant accounts. Auditors would classify the assertions into several

broad categories. These categories include completeness, and presentation, and disclosure. The categories of existence, valuation, rights and obligations are for assertions for accounts under the balance sheet, while occurrence and measurement are for assertions for income statement accounts. For example, when auditors assess inventory, which is a balance sheet account, they need to check if the inventory really exists (existence) and the amount is the actual quantity that management asserted in the financial statement (valuation).

The next main activity is to document processes and controls. First, auditors will identify the significant processes. E&Y defined significant process as "the point in the business process where transactions post to significant accounts represents a point where key control will most likely be defined for an assertion." Identifying the business process is also finding the major transactions of an account. The steps of identifying the significant accounts, manager's assertions, and identifying the business process are tightly linked together. E&Y recognized the "business processes as the "bridge" between significant accounts and the relevant financial statement assertions." The internal business processes are measured by key performance indicators (KPIs) to evaluate the efficiency of the process in providing value to the company's objectives. During KPI development, management will set the target result for the indicated KPI and the acceptable threshold level for performance.[3] Determining the important KPIs helps recognize where significant risks may occur. Auditors may go in depth to determine which relevant KPIs are susceptible to material misstatement. Possible misstatements for KPIs are setting KPIs that are inadequate for measuring internal business process performance, and managers manipulate KPI values to achieve the target value. PCAOB removed the requirement

[3] http://findarticles.com/p/articles/mi_km2920/is_/ai_n14719907

to identify the significant processes or major classes of transactions.[4] However, E&Y recognizes that this step is important and very useful; therefore, it kept this step in its framework. During a walk-though of the process, identifying the points in the process that impact the significant accounts can directly locate the point where risk most likely will occur.

After identifying the significant process, the auditors would ask themselves, "What Can Go Wrong (WCGW)?" The component WCGW is unique at E&Y defined as the procedure of identifying the risk that would challenge the financial statement assertions on these significant accounts and processes. The risks are the possible negative impacts associated with the specific points in the flow of transactions and accounts that will cause the management to fail to achieve its assertion.

Auditors inspect if management implemented proper controls at these points of possible risk. They would assess the effectiveness of the controls, if the controls will provide reasonable assurance; that they will prevent, detect, and correct errors. Reasonable assurance is the understanding that the likelihood that a material error has occurred is low. However this is not absolute assurance, which guarantees no errors. For example, auditors would ask themselves, how they guarantee that the level of inventory is exactly the amount in the financial statement assertion. Auditors would actually go out and count the inventory or count a sample to assess if the inventory level asserted is reasonable. Controls are designed with flexibility to apply to more than one significant account. Having one control for each significant account may run into the risk that the control will not detect a risk. Implementing more than one control on the significant accounts creates a safety net so in case one control does not expose a risk, the other control will.

[4] PCAOB Auditing Standard No 5

After the process of identifying the controls, auditors lead to actual testing to assess the operating effectiveness of the controls and the control designs for the important risks affecting the financial statements.

The framework for the top down, risk based approach helps auditors understand the client's environment and then identifying and assessing the risk and controls for the client in its specific industry. Using this approach will allow more effective and efficient compliance with SOX Section 404.

Materiality

Materiality is an important factor during the implementation of the control framework. From AICPA AU Section 312.04, it defines materiality as the magnitude of an omission or misstatement in the financial statement.[5] Considering the assumption that a reasonable person is using the financial statements, an omission or misstatement is considered material if it will change the person's judgment. It is impossible and impractical for financial statements to be error-free. The benefit from the error-free financial statement is less than the cost of the time and effort of making it free of errors. Auditors use their professionalism to determine the level of error that is acceptable and will not affect financial statement user's conclusion. Materiality is considered in many areas within the framework. It plays a major role in the course of identifying the significant accounts. The accounts with greater materiality level will be placed at higher importance for scrutiny. It will also determine the magnitude that auditors will design their testing procedures and the expected level of testing results.

[5] www.aicpa.org/download/auditstd/0210_AU310_Disposition_Oct02ASB.pdf

Auditors consider materiality in financial statements as a whole and in individual accounts. The overall material level, called planning materiality (PM), considers qualitative and quantitative factors, such as the nature of the business and industry, operating results, and the company's financial position. Auditors use their professional judgment to consider the issues that are important to potential financial statement users. The process of determining PM estimation starts with using a measurement basis, usually with the operating results, such as stable earnings.

The other materiality level considered is the tolerable error (TE), which is applied to each individual significant account. TE is the acceptable level of audit difference that an error goes undetected. Starting with the PM estimation, the tolerable error is set as a percentage of the PM, therefore, TE will always be a smaller number. The aggregation of the TE should not exceed the PM. The controls are designed to provide reasonable assurance that the level of undetected material misstatement will not affect the person's decision, therefore setting TE relies on the auditor's professional judgment. As a result the level of PM and TE is positively correlated to material misstatement, when auditors raise the level of PM and/or TE, the likelihood that a misstatement goes undetected may increase. If the auditors find that the summary of audit difference at the transaction level is significant, they will ask the client to readjust and correct their transactions.

Regarding materiality, AICPA addressed in AU Sect 312.17 that the risk of a large misstatement occurring in accounts, class of transactions, or disclosures might be very low but the risk of an extremely small misstatement occurring may be very high.[6] Rich Castle pointed out that individual error may lie below the designated threshold, however, if the error occurs frequently

[6] www.aicpa.org

and at high volume, the error may actually be significant when looking at all the errors collectively. As previously mentioned, it is unreasonable to have absolute assurance because it is time-consuming and costly. Therefore, the auditors can provide reasonable assurance as long as the summary of audit difference nominal amount is at an immaterial level.

Control

Controls are the biggest concern in the framework. Like materiality, controls are divided into two levels, the entity level controls and transaction level controls. For some time, companies overemphasized the transaction level controls but they are starting to recognize that the entity level controls cannot be ignored. For example, tone-at-the-top impacts the entire company on how effective companies prevent and detect misstatement. The SEC Management Guidance describes three types of entity level controls, indirect, monitoring and direct. Indirect controls are indirectly related to the financial statement component therefore it is not effective at preventing or detecting misstatement. Monitoring controls assess the quality of lower-level controls, determining if it will detect material misstatement risk in a timely manner. As for direct controls, these are control designs related directly to the process transaction level or application level to detect risk.

Transaction level controls are divided into several broad categories. Manual controls are controls that do not use IT. For example, in the shipping industry, companies still manually record shipping information onto logs with pen and paper. IT-dependent controls are controls over information technology situations, such as documents in electronic forms. The next type of control is application controls. These are controls set up within the application system, therefore are fully automated. Lastly, there are the end-user computing controls. These are controls for

tools used in performing daily activities such as word-processors, spreadsheet applications and databases. For example, employees in business operations and auditors all use and generate many spreadsheets. Controls are made to control all these spreadsheets being made. Auditors only care about the controls that have significant influence over financial reporting therefore it is not necessary to identify the all the transaction level controls.

Control Testing

After identify the controls, auditors test the design of the controls. Specifically, auditors look if the design of the controls meets the control design requirement, the objective of the controls, and if the design can effectively prevent or detect errors. For example, management sets a control to check the purchase receipts, not accepting receipts above a certain percentage of error. During the process of testing the design, auditors will first ask management to inquire how effective is their design of the control. Next, they would observe the design of the control and lastly go out and see the system to inspect the design of the control.

After testing the design, now auditors will go in to see if the control really works. This is called the test of operational effectiveness. In the example of the good receipts, auditors will go see if the controls previously designed really help avoid overpaying for acquired goods. Similar for test of design, auditors inquire, observe and inspect if the control works effectively. Auditor will also re-perform the control to see if it truly works.

External auditors are required to understand and evaluate the design of controls. Rich Castle stated that on average, it takes 8-10 hours to perform the whole process of both TOD and TOE. The actual amount of time spent on TOD and TOE depends on how intense auditors perform a walkthrough. A walk though is typically a combination of inquiry, inspection, and re-

performance. Auditors, using their professionalism, need to decide if they should test one or a sample. The general rule deciding to test one or a sample is that auditors should chose to take a sample if the management can easily override the requirements of the controls and if the controls vary based on transaction class. The process of taking a sample starts by using guidance from previous historical amount. In the example of the goods receipts, by default the control requires that every line item needs to have the goods receipts, but if management can easily override the order, auditors will choose to take a sample to see how well the control is working in this situation.

The different testing techniques are inquiry, observation, inspection and re-performance. Inquiry involves conducting an interview with the appropriate personnel approach. Inspection activities include reviewing documents to check if relevant documentation exists. The testing techniques provide a different level of reliability. PCAOB said, "inquiry alone does not provide sufficient evidence to support a conclusion about the effectiveness of a control", therefore auditors need to use a combination of several approaches to provide sufficient evidence to justify that the controls in place are effective.[7]

SAP Controls

Every modern company uses information technology in operations to increase efficiency. Many companies implement ERP to load account information into a database where information can be aggregated with a financial consolidation tool or general ledger system.[8] Auditors need to understand the software that companies use to organize, identify, and gather the needed

[7] www.pcaobus.org/Rules/Rules_of_the_Board/Auditing_Standard_5.pdf

[8] http://www.nysscpa.org/cpajournal/2006/806/essentials/p36.htm

documents and information needed for testing. E&Y specifically uses SAP control testing for both test of design, and test of operational effectiveness. First, auditors need to identify the type of documentation for operating transactions and the associated controls. Different documentation includes journal entries, sales orders, purchase orders, and production orders. Auditors need to understand if the client uses standard or custom document types. Usually auditors will need to take more time to understand the customized documents.

The key settings in the software are very useful during control assessment. In a database of electronic documents, the key settings can help auditors filter out the unneeded documents and locate the necessary documents. Figure 2 is a representation of the variety of information that the key settings can help auditors identify the qualitative and quantitative components for assessing the significant accounts. In SAP field status groups, controls can be set by placing criteria on different fields for documenting different classes of transactions. The field status can control which type of information is required, if it is optional, displayable, or needs to be suppressed. The ERP system can sub-classify different account groups. The key settings for account groups enable the auditors to set different controls for each sub classification.

In the software, controls can be placed in the system by defining the key settings on tolerance. The variance between inputted value for transaction and the level of tolerance can be calculated to flag any possible significant misstatements. In the key settings, auditors can specify the threshold level. The software will take into account all of the criteria and generate testing results, such as materiality level, and the location of where information was configured. SAP can display informational, warning, or error messages relating to the calculated value in relation to the defined threshold. For example, a company is quite consistent on the level of goods that it purchases from a supplier. In its ERP system, controls can be implemented by requiring

inserting a monetary value for the purchase transaction and setting an upper and lower limit to ensure the value recorded is within reasonable amount. If an employee was trying to record the transaction and accidentally added an extra zero when he or she was inserting the price of the purchase order, an error message would pop up and will not let the employee submit the value because the value was greater than the predefined upper limit. The control would have successfully prevented a material misstatement in the purchase order transaction.

Risk Heat Map

E&Y's SAP IT system is very useful for control assessment. Companies can benefit a lot by utilizing the key settings to set the criteria for controls. Depending on the level of assurance preferred, companies could use a combination of other risk assessment technologies. In risk management, another common tool that companies use is a "risk heat map".[9] It provides a visual model, mapping out all the identified risks according to their likelihood and the size of the consequences. It is based on placing higher importance on risks that are more likely to occur and the risks that have a greater affect on the company.

The technology that generates a heat map can vary from being very simplistic to complex, depending on the level of sophistication desired in the process of risk management. Figure 3 is a sample taken from the Office of Internal Audits at University of Minnesota of a heat map that identified the likelihood that the risks will occur versus the risk impact.[10] The heat map is divided into three sections, green, yellow, and red. Risks within the red zone are influential risks

[9] www.agenarisk.com/resources/Using_Risk_Maps.pdf

[10] www1.umn.edu/audit/HeatMap-Operations.html

that have the greatest probability of occurring; therefore, auditors will pay special attention to these. A heat map can provide a visual representation on the risks that auditors should prioritize.

Conclusion

The top down, risk based approach helps companies and auditors effectively and efficiently comply with SOX Sect 404 on assessing internal controls. E&Y's framework contains the components, Financial Statement and Business Risk, Significant Accounts, Business Process, Financial Statement Assertions, What Can Go Wrong, and Controls. In the course of assessing controls with the approach, auditors consider materiality in the process of identifying significant accounts and the details of control testing.

Companies and auditors have been using information technology to coordinate resources and information. ERP software collects information onto a database, where auditors can configure the specific controls by defining the key settings. Understanding the key settings feature helps E&Y auditors fully utilize the SAP software when they apply the top-down, risk based approach to assess controls. Another very useful tool that risk assessment technology can help with is a heat map. As technologies advance over the time, improvements will be made to increase the effectiveness and efficiency of control testing.

Figure 1: E&Y Framework of a top-down, Risk-based Approach

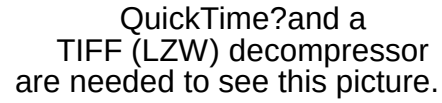

Figure 2: Ernst and Young's presentation of Key Settings

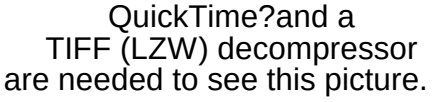

Figure 3: University of Minnesota, Department of Internal Audit Heat Map