Does Internal Control Improve the Attestation Function and by Extension Assurance Services? A Practical Approach

Linval Frazer
State University of New York (SUNY) Old Westbury

This paper demonstrates that internal control can be successfully applied to any company to foster accurate financial reporting, non-financial information, compliance with laws and operational efficiency. Furthermore, it bolsters the assurance process, in that it helps to give credibility and authenticity of information. The paper asserts that an effective internal control system reduces inherent, control and detection risks. This leads to less substantive audit procedures and lower audit fees. It also reduces compliance audits from federal, state and local authorities and garners less unethical behaviors. The paper concludes that companies that have effective internal control systems solicit more respect from stakeholders.

Keywords: internal control, attestation function, assurance services

INTRODUCTION

A major problem that stakeholders of financial reporting face is the need for credible information to assist in the decision-making process. This underscores the importance of attestation and the broader concept of assurance services. An even greater challenge is to effectively carry out these important functions adequately. Although internal control in some form has been applied universally, there is no research that focused on its effects on the attestation function from ancient time up to 1850. The limited scope of the audit objective at that time was to detect fraud. Corporate audits that encapsulated fraud and error detections objectives were instituted in response to the industrial revolution from 1850 to 1905 (Whittington & Pany, 2018). The audit process included evidence testing but there was no distinct reliance on internal control in the audit process. This persisted to some extent into the 21st century.

The development of the stock markets in 1905 to 1940 resulted in companies' activities that were complex and voluminous. As a result, the audit process incorporated increased emphasis on testing and slight reliance on controls. It was unambiguously clear from then that the audit process could not be effective if it excluded internal controls. Consequently, the audit standards were developed during the period of 1940 to 1975 and focused on determination of fairness which included reliance on internal controls (Whittington & Pany, 2018). The period of 1975 to 1985 saw where internal control was included in the audit process to determine the scope of audits. The advent of information technology and the changing environment from 1985 to 1995 triggered a demand for reporting on compliance and internal controls. The period of 1995 to present has seen major changes in the attestation function to include internal controls. The Committee of Sponsoring Organizations of the Threadwork Commission (COSO) Internal Control Framework was instituted in 1992 and was revamped in 2013 to include more defined objectives and the Sarbanes Oxley Act (SOX) of 2002 was established to aid in the reliability of

financial information and reporting processes. Both COSO and SOX overtime have been 2 of the most effective engines of internal controls and have played an indelible role in the quality and reliability of information.

The paper begins with a brief overview of the background of the problem and the distinction between assurance and attestation services. A focused discussion on COSO and SOX follows. These two institutions were created to improve the quality and reliability of information. The next sections include discussions on the external and internal audit functions. Finally, the paper briefly discusses blockchain technology.

Assurance Services

Assurance services are independent professional services that increase the reliability and quality of information received from various entities for decision makers. Users of these services rely on the information provided because providers of these services are considered independent, unbiased and qualified (Spiceland, Sep & Nelson, 2013). As such, these services help to improve the relevance, reliability, consistency and transparency of the information. An assurance engagement is a service that is designed and conducted by an accountant to improve the quality of information for decision makers and third parties against an applicable framework (criteria) such as Generally Accepted Accounting Principles (GAAP), International Financial Reporting Standards (IFRS) or Other Comprehensive Basis of Accounting (OCBOA). Assurance services are extended to include areas in risk assessment, information systems reliability and e-commerce. Some examples of assurance services are: reporting on personal financial statements; personal financial plans; compilation of financial statements; pro forma financial statements and information.

Attestation Services

An attestation engagement is a part of assurance services. It is a process where the accountant examines evidence and reports on the reliability and relevance of the information, or an assertion made by another party. There are three types of attestation services: examination, review and agreed – upon procedures. A more thorough discussion will follow regarding these services in the external function section. Pursuant to attestation standard (AT 101.1), an attest engagement is designed to issue an examination, review, or agreed upon procedures report on the subject matter that is the responsibility of another party. AICPA Code of Professional Conduct (ET 92.01) defines attestation services as engagements that require independence. Independence is defined in ET 100.06 of the AICPA as that of fact and appearance. CPAs may attest to many types of subject matters such as financial statements, financial forecasts and projections, internal control, compliance with laws regulations and contracts. The attest function adds value to information because a qualified and competent third party, the CPA, provides assurance over a subject matter prepared by management or another party responsible for the information.

Internal Controls/COSO

Internal control encompasses the policies, rules, and procedures enacted by management to provide reasonable assurance that financial reporting is reliable, the operations are effective and efficient, and the activities comply with applicable laws and regulations. Financial reporting objectives relate to the reliability, timeliness, and transparency of financial and nonfinancial reporting for internal and external uses. Operational efficiency objectives relate to the effectiveness and efficiency of operations and incorporate the achievement of financial performance goals and the safeguarding of assets. Compliance objectives relate to complying with applicable laws and regulations (COSO, 1992; 2013).

Although organizations sizes and objectives vary, they all need some form of internal control system in place to be successful at what they do. There are three types of controls used to accomplish the reliability of financial reporting, compliance and operational efficiency. These three controls are classified as corrective controls, detective controls and preventative controls. A corrective control is used to remedy or correct a misstatement. A common example of a corrective control is ensuring that the company has master files and or a backup file. In the event there is a material misstatement from data error or fraud, the

back up or master file can be used to correct this problem. A detective control is needed or used to identify misstatements after they have occurred. Bank reconciliation is a frequent example of detective control that is used to identify misstatements from cash receipts and disbursements. Preventative controls are used to prevent the occurrence of material misstatement. Most companies big and small, find ways to implement preventative controls through policies. These policies are used as preventative measures against material misstatements. A typical example of preventative control is enactment of policies to separate the authorization, custody of assets and recording functions. It is through these lens that scholars and practitioners have concluded that internal control can indeed bolster the assurance services.

In 1992, COSO established the internal control integrated framework to develop effective internal control systems. This framework provides direction to any business that wishes to establish an effective internal control system. This now recognized framework has five interrelated components: control environment, risk assessment, control activities, information and communication, and monitoring (COSO, 1992). In 2013, COSO's Board of Directors added 17 internal control principles to the five interrelated components because they are presumed very important in assessing the five components.

The five major components of COSO (1992) internal control integrated framework are part of a holistic framework needed to strengthen efficiency within the management of any organization. Throughout this holistic framework, a variety of activities and steps are taken to ensure that the organizations do not provide opportunities for the manifestation of fraudulent behaviors by employees (COSO, 1992). The framework should be assessed regularly for clarity so that the implemented internal controls function throughout the lifespans of the organizations (COSO, 1992). The five components of internal control also work harmoniously to detect, prevent, or correct errors and or misstatements in the overall business operations (COSO, 1992). For the process of internal control to be seen as viable, the financial statements generated from all business activities must be authentic and noteworthy in accounting terms.

Control Environment

The control environment is the foundation of internal control because it sets the organizational tone by influencing the control consciousness of the organizational workforce. It is the foundation for all other components of internal control because it provides discipline; structure; integrity and ethical values, employee competence, management's philosophy and operating style, and the leadership provided by senior management and the board of directors (COSO, 1992; 2013). According to COSO (2013), five basic principles are germane to the control environment of a company:

1. Demonstrates commitment to integrity and ethical values.
2. Board of directors demonstrates independence from management and exercises oversight responsibility of internal control.
3. Establishment of effective structure, including reporting lines, and appropriate authorities and responsibilities.
4. Commitment to attract, develop, and retain competent employees.
5. Holding employees responsible for internal control responsibilities.

Risk Assessment

Risk assessment is the process of identifying, analyzing, and responding to risks from external and internal sources that threaten the achievement of organizational objectives. Every organization, be it private or public, large or small, faces risks from external and internal sources that must be assessed (COSO, 1992). Because economic, industry, regulatory, and operating conditions continue to evolve, mechanisms are needed to identify and deal with the special risks associated with change. COSO (2013) identified five basic principles that companies should carry out when performing effective risk assessment.

1. Clearly specify objectives to facilitate the identification and assessment of risks related to organizational objectives.

2. Identify and analyze risks to the achievement of organizational objectives to determine how they might be managed.
3. Consider potential fraud related to the achievement of objectives.
4. Identify and assess changes that could impact internal control.

Control Activities

Control activities are policies and procedures that help to mitigate the risk that organizational objectives will not be met. These policies and procedures ensure the ways that management directives will be carried out. Control activities include approvals, authorizations, verifications, reconciliations, reviews of operating performance, safeguarding of assets, and segregation of duties. These actions dissuade fraud or theft activities that could eventually lead to losses. COSO (2013) identified three basic principles of control activities:

1. Select and develop general control activities that mitigate the risk of achieving organizational objectives to an acceptable level.
2. Select and develop general control activities over technology to support organizational objectives.
3. Deploy control activities through policies that establish what is expected and through procedures that put policies into action.

Information and Communication

Information is needed at all levels of organizations to assist managers in achieving organizational objectives. Pertinent information must be identified, captured, and communicated in forms and time frames that enable people to carry out their responsibilities. Information systems facilitate the production of operational, financial, and compliance-related reports that make it possible to run and control organizations (COSO, 1992; 2013).

Information systems deal not only with internally generated data but also information about external events, activities, and conditions necessary to inform business decision making and external reporting (COSO, 1992). Effective communication must also occur in a broader sense by flowing down, across, and up all levels in organizations (COSO, 1992). All personnel must receive a clear message from top management that control responsibilities must be taken seriously. Employees must understand their own roles in the internal control system and how individual activities relate to the work of others. In addition, they must have a means of communicating significant information upward. Effective communication also must exist with external parties, such as customers, suppliers, regulators, and shareholders (COSO, 1992). Pursuant to COSO (2013), the three basic principles of effective communication are as follows:

1. Obtaining and using relevant information to support the functioning of other internal control components.
2. Communicating internally the information necessary to support the functioning of other components of internal control.
3. Communicating with external parties regarding matters affecting the functioning of other components of internal control.

Monitoring

Monitoring is the process of determining whether all components of internal control, including the principles in each component, are in place and are functioning as intended (COSO, 2013). Monitoring assesses the quality of the internal control system's performance over time through ongoing monitoring activities, separate evaluations, or a combination of the two (COSO, 1992). Ongoing monitoring, which occurs in the course of operations, includes regular management and supervisory activities as well as other actions that personnel undertake while performing their duties. The scope and frequency of separate evaluations depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures (COSO, 1992).

Internal control deficiencies should be reported upward, with serious matters reported to top management and the board of directors (COSO, 1992). According to COSO (2013), the last two basic principles of the 17 involve (1) Selecting, developing, and performing ongoing and separate monitoring evaluations to determine that the components of internal control are present and functioning properly, and (2) evaluating and communicating internal control deficiencies in a timely manner to those responsible for taking corrective action, including senior management and the board of directors and their audit committees.

Sarbanes-Oxley Act

Sarbanes Oxley Act (SOX) contributes to internal control, and assurance services. Although SOX primarily applies to public companies and is often more expensive for private companies, some of its policies have been used by private companies in furtherance of their objectives. Sarbanes Oxley Act (SOX) was enacted in 2002 in response to corporate irregularities and the implosion of many companies in 2001. Accounting irregularities by the public accounting firm Arthur Andersen and accounting scandals with public companies such as Worldcom, Enron, Xerox, Merck and Adelphia among many, created a shockwave in the financial market. The credibility of the accounting profession and corporate America was questioned and met with public outrage and consternation. Congress had no choice but to respond to the increased pressure to pass a law that would regain creditability, and investor confidence to financial reporting process and the market. SOX was described as the most far-reaching reform of U.S. business practices since the Securities Act of 1933 (Rice & Weber, 2012).

The purpose of SOX was to improve quality and transparency in financial reporting and independent audits, strengthen the independence of firms that audit public trading companies, and increase corporate responsibility and the usefulness of corporate financial disclosure. Although SOX was passed primarily in response to wrongdoing and fiscal mismanagement in public companies, one of its outcomes has been greater accountability within the private sector, regardless of the size and status (private vs. public) of the company. Some of the key provisions are:

1. Creating the Public Company Accounting Oversight Board (PCAOB). This board has oversight and enforcement authority. It is responsible for auditing, quality control, and independence standards and rules for publicly traded companies.
2. It has implemented and is responsible for stronger independence rules for auditors auditing publicly traded companies. Examples are audit partners rotation and the prohibition of other types of accounting and consulting services while auditing firm is engaged to audit client.
3. Chief Executive Officers (CEO) and Chief Financial Officers (CFO) or other personnel that hold similar positions with similar responsibilities of publicly traded companies are required to validate and certify that financial statements and disclosures are accurate and complete. Failure to do so can lead to forfeiture of bonus or compensation associated with the restatement of a company's financial statements.
4. Publicly traded companies are required to have audit committees. Members of audit committee are required to be independent with financial expertise.
5. Code of ethics is required.

Pursuant to Section 404 of SOX, managers of public companies are required to attest to the effectiveness of the internal controls of their companies. Section 404 a controversial provision of SOX requires companies' managements maintain and document effective internal controls and report on the adequacy of the internal controls. This provision also requires auditors of publicly trading companies to express an opinion on the effectiveness of internal control over financial reporting. While academics, pundits and practitioners agree that the 404 provision was beneficial, some argued about the cost associated with implementing and maintaining the controls. The benefits outweigh the costs because companies with more effective internal control affect investors' confidence, risk assessment and ultimately the value of the companies as reflected in their stock prices (Frazer, 2018; Kim, Yeung & Zhou, 2013). The cost of section 404 compliance by public companies was high in the first couple of

years of implementation but went down significantly over a period of time. The cost of maintaining 404 compliance have been reduced also by the efficiency of internal control audits.

Section 802 of SOX amends the federal obstruction of justice statute. It is now a felony to knowingly destroy, conceal, cover up, or falsify documentation or records to impede or obstruct federal investigations. SOX imposes fines and up to 20 years in prison for knowingly destroying, altering, or falsifying records with the intent to impede or influence federal investigations, including existing government proceedings against private companies. Section 806 of SOX, under the whistleblower protection act, purports that it is against the law for employers to discriminate or take action against employees who disclose information or evidence against fraud or irregularities.

Although SOX were not expressly applicable to private companies, many of the requirements imposed by SOX have become best business practices and are now considered industry standards. The pressure on private companies to comply with SOX is coming from many different directions. Lenders, insurers, public merger partners, potential litigants, and state governments are all looking at the SOX-type control mechanisms installed by private companies. It must be noted, however, that private companies are not required to be in technical compliance with SOX. As such, private companies can pick and choose the provisions that they want to adopt. Private companies seem to be implementing most of the easier changes, such as adopting a code of ethics for officers and appointing independent directors and audit committees. The provision of SOX that affects private companies more adversely is Section 404, which requires companies to report the effectiveness of internal control over financial reporting at the end of each fiscal or calendar year. This provision requires a report of an external auditor attesting to management's assertion of the effectiveness of the internal control in the organization.

External Audit Function

The external audit function is a part of the attestation and monitoring process. Independent external auditors are required to verify if companies are adhering to accounting policies and practices consistent with GAAP, IFRS and or any other suitable criteria. Examination, review and agreed upon procedures are used to accomplish the attestation and external audit function. An audit examination is the highest level of assurance provided by CPAs. In an audit examination, the accountant gives reasonable assurance whether the presentation of the assertion, taken as a whole, conforms with the applicable criteria. An audit is the gathering and evaluation of evidence about information. Evidence is any information used by the auditor to determine whether the information being audited is consistent and stated in accordance with the established criteria. To achieve the objective of an acceptable audit, the auditor must obtain appropriate sufficient quality and volume of evidence. This process requires the auditor to be competent in evaluating whether the information gathered is analogous with the prescribed criteria (Porter, Simon & Hatherly, 2014).

There are three major types of audits that lends credibility to information. They are financial audits, compliance audits and operational audits. Financial audit is the process whereby an auditor or CPA serves as an independent intermediary, gathers and evaluates evidence of the company's financial statements, to express a professional opinion about whether the statements fairly represent the company's financial position and operation. Financial audits normally include the company's balance sheet, income statement, retained earnings and statement of cash flows. This audit is done from a historical perspective to ascertain whether the financial statements have been prepared in accordance with the prescribed criteria.

The review is an attestation function that gives limited or negative assurance. This is based on inquiry and analytical procedures. The attestation function is lower than the audit function and does not give reasonable assurance that the financial statements are in accordance with a prescribed standard. Instead, it asserts that the auditor is not aware of any information that the financial statements or subject matter are not in compliance with the applicable standard or criteria. In an engagement to review the financial statements of a company, the auditor obtains evidence from analytical procedures and inquiries. Auditors use several tools to obtain evidence such as ratio analysis, benchmarking, trend analysis, vertical analysis and horizontal analysis. The review engagement does not require the auditor to obtain an understanding of internal control, assess risk or conduct substantive audit procedures. Although the review engagement

does not require an understanding of the company's internal control, by having an effective internal control system in place, it increases the reliability of the review report. This is because there is a direct correlation with increased internal controls and the accuracy of the financial statements of companies (Rice and Weber, 2012).

Internal control improves the financial audit function by reducing the amount of audit procedures performed by an auditor. Internal control is integral to the risk assessment process. Auditors are required to assess the audit risk prior to doing the audit examination. In doing the risk assessment, auditors are required to design and implement risk assessment procedures to obtain an understanding of the client's internal control over the financial statements. Auditors test the operating effectiveness of the internal controls to determine if they prevent or detect misstatements. If the controls are working efficiently, auditors can rely on the controls, and apply fewer substantive procedures such as test of details of accounts balances, transactions and disclosures to detect material misstatement. Auditors have to consider audit risk in their risk assessment. This should be assessed throughout the audit. Importantly, external auditors must not rely exclusively on the effectiveness of internal controls to determine the accuracy of a company's financial statement without applying substantive audit procedures.

Audit Risk

Audit risk is a process whereby the auditor might incorrectly fail to modify her opinion on the financial statements that are materially misstated. That is, the auditor issues an unqualified opinion on a company's financial statements that is materially inconsistent with generally accepted accounting principles. The amount of audit evidence that is needed by the auditor is based on her assessment of the audit risk. The lower the audit risk, the less persuasive evidence is needed. The higher the audit risk the more substantive audit procedures are used. Audit risk must be assessed at the financial statements' assertion level and for all significant account balances, transactions and disclosures. Audit risk has three components; inherent risk, control risk and detection risk (AR = IR X CR X DR).

Inherent risk is the likelihood of a material misstatement of an assertion prior to considering the client's internal control. The nature of the client and its environment play an important role in assessing inherent risk. High inherent risk assessment might be determined based on misstatement detected in prior audits, going concern issues, operating activities and results tied to economic factors. Other factors include valuation, significant judgement by managers, difficult accounting issues, and human resource issues such as high turnover. The auditor uses these factors to determine if she will accept the audit engagement and if she accepts the audit engagement, the amount of audit procedures needed to obtain sufficient appropriate evidence to issue an opinion. Also, importantly the scope and cost to complete the examination.

Control risk is the risk that a material misstatement may occur at the assertion level and the internal control did not prevent or detect it in a timely manner. The auditor evaluates the effectiveness of the design and operation of the internal control to the fair presentation of the financial statements. If the auditor assesses control risk low, then she will rely on the controls and apply fewer substantive procedures. If the auditor assesses control risk high, she may not rely on the internal controls and she will have to apply more substantive procedures. Therefore, it is clear that having an effective internal control system lowers the control risk, the audit procedures and the cost associated with the audit examination.

Detection risk is the risk that the auditor's procedures will not detect a material misstatement at an assertion level. Detection risk is independent of inherent and control risks. Inherent and control risks are financial statement risks while detection risk is determined by the effectiveness of the audit procedures. Detection risk exist because of ineffective audit procedures and sampling.

Sampling

Internal control can improve the sampling process and in turn the attestation function. Sampling is the process of selecting and evaluating less than the entire amount from a population of audit evidence that represents the entire population. Complex and voluminous companies' transactions require effective sampling procedures. Attribute and discovery sampling are sampling processes used by auditors to test

controls. They test for deviation of performance from prescribed controls. Other statistical sampling includes classical variable sampling such as mean per unit estimation, ratio estimation, and difference estimation. Probability proportional to size sampling can serve a dual-purpose role as it evaluates the deviation from controls and overstatement and understatement of accounts balances. Although attribute sampling focusses on internal control, auditors use other sampling procedures to focus on amounts and transactions in the financial statements (Porter, Simon and Hatherly, 2014)

Companies with effective internal controls attract far less substantive audit procedures from auditors to issue an opinion on the financial statements. Auditors will generally rely on effective internal controls and use more sampling techniques, with smaller sample size and less substantive audit procedures. When faced with assessing a company's internal controls, auditors are faced with 2 sampling risks. The risk of assessing control risk too high or too low. Assessing control risk too high requires the auditor to assess control risk at a higher level than is needed to determine the effectiveness of the control. Assessing control risk too low forces the auditor to assess control risk at a lower level than is needed to determine effectiveness of the control. If an auditor assesses control risk too high, this will cause the auditor to use more than the required amount of audit procedures needed to express an opinion on the financial statements. In this case, the auditor performs more substantive testing than is required. These unnecessary audit procedures or testing reduce the efficiency of the audit but importantly, does not lessen the effectiveness of the audit, which is to determine if the financial statements are in conformity with the prescribed criteria. If the auditor decides to rely on the internal control systems but is dubious about operational effectiveness in some areas, she will obviously err on doing more audit procedures than less to ensure that there are no material misstatements. It is up to the companies being audited to have an effective internal control system. This would not only help in improving the auditing process and the reliability of the information provided, but also reduce the costs of the audits.

Conversely, the risk of assessing control risk too low is a very serious issue. This would mean that the auditor incorrectly reduces the extent of her substantive procedures. This invariably decreases the effectiveness of the audit process in determining if the financial statements are in conformity with prescribed standards. In this case, it is possible that the auditor will express an opinion that the financial statements are in conformity with prescribed criteria, when in fact, there is material misstatement in the financial statements. Since the attestation process does not exclusively rely on auditors to make it effective, but also on managers of the company, having a good internal control system in place reduces the likelihood of auditors assessing control risk too high or low. Companies having good internal control systems see cost benefits from an audit. Additionally, good internal controls reduce possible liability costs.

Compliance

Internal controls should be designed to ensure that companies comply with laws and contractual obligations. Internal controls may enhance the reliability of information available to compliance auditors such as Internal Revenue Service (IRS) and state auditors. More accurate and verifiable information would prevent unnecessary audits (Frazer, Winkelman and D'Amico, 2019). A compliance audit is the process whereby the auditor verifies whether the company is adhering or complying with laws, regulations or policies and procedures. Examples of compliance audits are state, local municipals and IRS audits. These audits require the auditee tax returns to be in compliance with tax laws and or IRS regulations.

The IRS uses the Discriminate Function System (DIF) to select companies for audits. The DIF is a process that involves computer scoring of mathematical formulas to select tax returns with the highest probability of errors or likely tax adjustment. It is reasonable to assume that a company selected for audit, is highly susceptible to additional tax liability. The tax returns of taxpayers with the highest scores are selected and manually screened or examined at various districts offices to determine if auditable. Effective internal controls increase the accuracy of information received by tax authorities, hence prevent extensive and costly audits. Most of the information received by tax authorities are through information reporting.

Information Reporting

Companies are required by law to report certain information that trigger tax liabilities, although they have no statutory liability for the taxes. Information reporting is required by companies that withhold salaries and wages from employees and financial institutions that pay interests and dividends. Other institutions are required to report gambling winnings, student loan interests, S Corporation and partnership income, estate and or trust distributions, interests, proceeds from sales of stocks and homes, IRA and medical savings account information. This system provides information to tax authorities that can be used to analyze and compare against the amount of tax remitted. The tax authorities will follow up on variations of amounts not being accounted for or reconciled. This follow up process is usually a desk or correspondence audit or a full-blown field audit (Burman & Slemrod, 2013; Frazer, Winkelman & D'Amico, 2018).

The quality of internal controls and information can reduce the costs associated with laborious audits from tax authorities. Information reporting discourages noncompliance and increases the detection risk at a low cost to the relevant tax authorities. Companies with effective internal controls would likely have accurate and verifiable information. This would reduce the likelihood of a compliance audit because the tax authorities would be able to reconcile or verify information received. Even if there were a mistake on the part of the reporting company, the audit would conclude in no additional tax liability. This result would serve as a record to tax authorities in determining future audits. Like any other companies, tax authorities audit companies that are likely to have additional tax liabilities and for future compliance purposes. If the tax authorities (IRS) determine compliance based on prior audits and a cost benefit model, it would be inconceivable that they would be motivated to audit a company that has a history of no changes (Frazer, et al, 2018).

Internal Audit Function

Internal auditing is defined as a process that adds value and fosters operational efficiency in companies (Hunziker, 2017). Its purpose is to have a discipline, systematic and structured approach to assess and improve the effectiveness of internal control and management and or oversight processes. Publicly traded companies are required to have an internal audit function to provide management and the audit committee with continuous assessments of the company's risk assessment and the effectiveness of internal control. One effective way of implementing and maintaining this function is the use of internal auditors.

Operational audit is normally done by internal auditors. This process determines performance measurements as it relates to effectiveness and efficiency of the overall objectives of the organization. Although operational audits are usually conducted by internal auditors and are normally applied to the internal audit function, they are often done by external auditors, especially if the company is smaller and less complex. Operational audits unlike compliance and financial audits are more subjective because criteria for operational efficiency and effectiveness are not formally established for general applicability.

Internal auditors are not independent of the company and are considered employees. However, to increase reliability of the internal audit function, they often report directly to the audit committees or the board of directors. This reporting process is done primarily because the board of directors are usually independent. Although privately held companies are not required to have the internal audit function, it is recommended. There are possible and likely limitations to having this process working in smaller less structured companies. Financial requirements, size and structures of companies are possible factors. Needless to say, the benefits of having an effective audit function, increases the reliability of the company activities and the information that is prepared for internal and external users.

Blockchain

Blockchain is a new technology that will have significant impact on the attestation function. This phenomenon is a set of coding, which encompasses blocks of transactions or distributed technology that allow companies to share information such as digital ledgers across a network of computers without compromising the integrity of the information and no central authority. No central authority suggests that

no single company or actor has the power to alter or tamper with the record. Blockchain will likely reduce the use of sampling. This is because the technology will provide verifiable and accurate information of transactions within a blockchain system. Internal controls would be effective in ensuring that these transactions are accurate. At the time of writing this article, this distributed ledger phenomenon is not yet fully understood by the profession and CPAs are bracing for its pervasive impact. Fundamental responsibilities of auditors will not change, but they will have to change the ways they carry out these responsibilities. More focus will be on internal controls and the reliability of those controls as the automation, processing and verification of transactions will be assumed by new technologies. Control environment which addresses a company's culture and operating philosophy and control activities that include segregation of duties are some of the key areas of internal control that will be very instrumental using blockchain. In contemporaneous situations like these, auditors would likely spend more time focusing on data analysis and companies' internal controls as oppose to the verification of already reliable set of information.

CONCLUSION

This paper demonstrates that internal control bolsters the assurance process, in that it helps to give credibility and authenticity to financial and non-financial information. The assurance process adds credibility to the financial statements of companies and information provided by these companies. The process increases confidence of those who use and rely on financial information, such as investors in the stock markets, private investors and creditors, managers, bankers, financial analysts and governmental agencies.

An effective internal control system reduces audit fees, compliance audits from federal, state and local authorities and unethical behaviors. It garners more respect from stakeholders for transparency and objective reporting. It decreases investors risk return premiums. Additionally, disclosure of information on soft assets such as brand knowledge and skills are more reliable. Internal control enhances the reliability of relevant nonfinancial information disclosed to investors. Examples of non-financial information that might be important to investors are operational efficiency, capital management, management strategy, credit quality and loan growth, customer satisfaction indexes, backlog information and rejection rates on goods purchased. Auditors should be aware of the challenges of the assurance services and be ready to embrace internal control as integral to the attestation function not only for public companies but private companies.

REFERENCES

American Institute of Certified Public Accountants. (1972). Statement on auditing procedure No. 48. New York, NY: Author.

American Institute of Certified Public Accountants. (2006). Communicating internal control related matters identified in an audit (Statement on Auditing Standards No. 112). New York, NY: Author.

American Institute of Certified Public Accountants. (2014). Code of Professional Conduct.

Burman, L., & Slemrod, J. (2013). *Taxes in America: What everyone needs to know*. New York: Oxford University Press.

Committee of Sponsoring Organizations of the Treadway Commission. (1992). Internal control-integrated framework (Vol. 2). New York, NY: Author.

Committee of Sponsoring Organizations of the Treadway Commission. (2013). Internal control-integrated framework. New York, NY.

Frazer, L. (2018). An empirical analysis of the effects of internal control on deviation in small restaurants. *Journal of Behavioral Studies in Business*, 10.

Frazer, L., Winkelman, K., & D'Amico, J. (2018). Do Gatekeepers of taxation need more ethics and enforcement to move the needle of compliance north? *Business and Professional Ethics Journal*, 37, 161-180.

Frazer, L., Winkelman, K., & D'Amico, J. (2019). Communication, culture, or rational actors? A review of the literature: The challenge of tax compliance. *Journal of Theoretical Accounting Research*, 15(1).

Hunziker, S. (2017). Efficiency of internal control: Evidence from Swiss non-financial companies, *Journal of Management & Governance*, pp. 401-433.

Kim, J-B., Yeung, I., & Zhou, J. (2013). *Material weakness in internal control and stock price crash risk: Evidence from SOX Section 404 Disclosure.* City University of Hong Kong; Northwestern University; National University of Singapore. http://saf.uwaterloo.ca/seminars/KYZ-ICW-Crash20130516-May20_2013.pdf. Accessed Jan 1, 2019 PCAOB (2015). AT Section 101.

Porter, B., Simon, J., & Hatherly, D. (2014). *Principles of external auditing,* 4th edition. Hoboken, NJ: John Wiley & Sons

Rice, S. C., & Weber, D. P. (2012). How effective is internal control reporting under SOX 404? Determinants of the (non-)disclosure of existing material weaknesses. *Journal of Accounting Research*, 50(3), 811–843.

Rice, S. C., Weber, D. P., & Wu, B. (2015). Does SOX 404 have teeth? Consequences of the failure to report existing internal control weaknesses. *The Accounting Review*, 90(3), 1169–1200.

Skaife, H., Collins, W., & LaFond, R. (2009). The effect of SOX internal control deficiencies on firm risk and cost of equity. *Journal of Accounting Research*, 47, 1-43.

Spiceland, J., Sepe, J., & Nelson, M. (2013). *Intermediate Accounting,* 7th ed. McGraw Hill Irwin, Avenue of the Americas, New York, NY.

Whittington, R. O., & Pany, K. (2018). *Principles of Auditing & Other Assurance Services* (21th ed.). Hoboken, NJ: John Wiley & Sons.