
AUDITING RISK IN COMPUTERIZED ACCOUNTING INFORMATION SYSTEM

By

Osim E. Etim

*Department of Accounting,
Faculty of Business Administration,
University of Uyo.*

and

Confidence Joel Ihenyen

*Department of Accounting,
Niger Delta University,
Wilberforce Island.*

Abstract

Developments brought about by information and communication technology and its increasing application in accounting information system has resulted to more risk exposures faced by business organizations, particularly risks associated with computer crimes and frauds, in addition to audit trail absence. Effective handling of risk is necessary for reduction in auditors' liability and enhancement of audited financial statements reliability for decision making. The study examines implications of business risks on audit risk and various tools used for audit in a computerized accounting system environment. Exploratory and descriptive research methods were adopted involving application of central limit theorem and Kolmogorov- Smirnov test for treatment of data gathered through questionnaire administered to forty external auditors in public practice. Results show management integrity, nature of business, quality of internal control as highly susceptible to risky transactions. It was also revealed that use of standard audit tool kits will reduce audit failure and possible liabilities; quality audit reports and reliable financial reports. It is recommended that external auditors should always evaluate risk profile every audit

Academic Excellence

engagement before accepting the audit, regular updates in ICT tools and mandatory ICT knowledge by external auditors as a compliance requirement for issuing and renewing practical licence by those responsible for that.

The accounting system consists of methods and processes established to identify, collect, classify, record and report an organization's transactions with a view to maintaining accountability for the related assets and liabilities. The activities in these methods and processes may be captured manually or electronically. When manually captured, the accounting system is said to be manual accounting information system (MAIS), characterized by the presence of audit trail (source documents) for tracking transactions from origination to completion of financial statements preparation. Computerized accounting information system (CAIS) exists where the activities are captured by use of computers.

Robinson, Davis and Alderman (1986) define accounting information systems (AIS) as encompassing the processes and procedures by which an organization's financial information is received, registered, recorded, handled, processed, stored, reported, and ultimately disposed of.

Accounting products, financial statements, are prepared for two separate user groups, each with different interests, needs, and points of view. One group is external to the corporate body in an operational sense and is concerned principally with the financial strength and performance of the business. The other group is internal management and focuses primarily on: organizational planning through the use of budgets and data refined for use in control and decision making (Etim, 2011).

In a computerized accounting system environment much of data needed for preparation of financial reports are generated automatically. The data captured and processed electronically have the advantages of being processed speedily, accurately, more reliably as well as timely provision of needed information for informed decision making.

However, along the advantages of the computerized accounting information system emerges several deadly deficiencies and threats in terms of data security and vulnerability of fraudulent practices particularly as remote terminals can serve as data entry points, thus, creating significant risks which may not have been common in a manual system.

Auditing Risk in ...

Moreso, financial statements prepared by management as stewardship reports can hardly be expected to be entirely impartial and unbiased, any more than a football coach could be expected to serve as both coach and referee in the same game. These statements may likely be prepared carelessly or intentionally either overstating assets or overlooking and omitting liabilities from the statement of financial position or due to arithmetical errors or as a result of lack of knowledge of generally accepted accounting principles (GAAP)

Consequently, there is need for independent assessment of these financial statements by an external party called the “External auditor”, who is a qualified professional (expert) in the field of accountancy with a licence to practice, to give assurance to the authenticity, and true and fair view of these statements prepared by management.

The contribution of the independent auditor is to provide credibility to information content of financial reports. Credibility in this usage, means that the information can be believed, that is can be relied upon by outsiders, such as stockholders, creditors, government regulators, customers, and other interested parties. These parties use information to take various economic decisions, such as either to invest or divest from the organization.

Implied in the above is the fact that external auditors’ opinion provides reasonable assurance of detecting material misstatements of the financial statements (both errors and fraud) and illegal acts that have a direct and material effect on the determination of financial statement amounts. Auditing arose as a result of separation of ownership and management groups in organizations, to protect stakeholders’ interest.

Statement of the Problem

With development in information technology (IT) and its increasing application in accounting information system, more risks exposure are faced by business organizations, particularly risk associated with computer crimes. Thus, the need to refocus auditing practices often associated with a manually driven accounting information system.

Thus, the CAIS is characterized by such risks of asset theft, perquisite, artificial, revenue information, expense manipulation, hacking, spam, phishing and identity y frauds. Audit risk is the risk that auditors may give an inappropriate opinion on the financial statement. It is the probability that the auditors may unknowing fail to

Academic Excellence

appropriately modify their opinion on financial statements that are materially misstated (Whittington and Pany, 2004).

Objectives of the Study

The main objective of this paper is to identify the component of auditing risk particularly as they relate to computerized accounting information system (CAIS). Other objectives include:

- i. to examine the implications of business risk on audit risk;
- ii. to find out various tools used to conduct audit in a computerized accounting information system environment.

The study will assist external auditors in planning their audit programmes to ensure reliable audit approach and reports, hence minimizing possible liabilities and audit failures as well as bridge the expectation gap which currently exist between what the auditors actually do and what the public expect of them.

Research Questions

The following research questions have been raised based on the study.

1. What is the implication of business risk on audit risk?
2. What tools are available to external auditors to carryout auditing in a computerized Accounting information system environment?

Hypothesis Development:

One hypothesis is developed for the study and stated in null form as follows:

H₀: Use of audit tool kits in a computerized account environment does not reduce audit risk.

Theoretical Framework and Review of Related Literature

Auditing functions and responsibilities are regulated by the existence of generally accepted auditing standards. The standards are evidence that the accounting profession is very concerned with maintaining a uniformly high quality of audit work by all independent public accountants. Standards are established to measure the quality of performance of individuals and organizations. Standards relating to the accounting profession are concerned with independent public accounts profession qualities. The judgment exercised by them in the performance of their engagements and a firm's quality control. These standards include Generally Accepted Auditing standards (GAAS) and Generally Accepted Accounting Principles (GAAP) issued internationally by international Auditing and Assurance standards Board (IAASB) and international

Auditing Risk in ...

Federation of Accountants (IFAC). These constitute quality control framework for all practicing public accounting firms to ensure engagement are conducted in accordance with applicable professional standards (AICPA, 2008). Applying the above requires the practitioners' independence, objectivity, integrity, due diligence as well as possession of required professional skill and knowledge in all manner of engagements.

A key point here is that independent auditors should adopt a risk based approach to conducting field work and rendering assurance services to client.

The Concept of Risk, Business Risk and Audit Risk

The word 'risk' is derived from the Italian word 'risicare', which means 'to dare'. The roots of the modern risk conception go back to eight hundred years ago, when the numbering system reached the west. From then on, scientists like Fibonacci, Paccioli, Galileo and Cardano began to develop methods of dealing with the unknown in using measurement, odds and probabilities (Ndukwe, 2009). Linsley and Shrivies (2006) note that in the pre-modern era risks were solely considered to be bad, whereas the modernist view of risk incorporates both the positive and negative outcomes of events.

Generally, risk is considered to be synonymous with uncertainty. In the early 1920's, though, Frank Knight introduced an important distinction between the two concepts. He defined 'risk' as variability that can be quantified in terms of probabilities, while immeasurable variability is best thought of as 'uncertainty'. In this context, Merije (1992) states that uncertainty reduces the predictability and therefore increases risk. Crouly, Crouly, Galai, and Mark (2006) define risk as "the volatility of returns leading to

For the purpose of this paper, we build on the risk categorization model of Crouly. (2006). These authors consider risk factors in a systematic way and group risk factors into eight categories: market risk, credit risk, liquidity risk, operational risk, legal and regulatory risk, business risk, strategic risk and reputation risk following Linsley and shrives (2006), we regroup the categories in order to obtain four risk types that impact directly on audit: financial risk, operational risk, legal, tax and regulatory risk and business risk.

Financial Risk: This risk is a broad and well-known risk category. It consists of market risk, credit risk and liquidity risk. This risk relates to price movements in financial markets (Tofik, 2006). Crouly *et al* (2006) define market risk as "the risk that changes in

Academic Excellence

financial market prices and rates will reduce the value of a security or portfolio". Market risk arises because of a number of factors such as interest rates exposures, foreign exchange exposure, commodity price-sensitive revenue or expenses, stock option plans and pension liabilities. Credit risk is the possibility that the payment of contractual obligations may not be fulfilled by the counterpart, (Chike, 2004).

Liquidity Risk: When a company is not able to meet the payment of commitments it has made, liquidity risk occurs (Cabedo and Tirado, 2004).

Operational Risk: Dozie (2007) relates operational risk to potential losses due to inadequate or failing internal processes, people and systems or resulting from external events. Crouhy, *et al* (2006) distinguishes three major types of operational risk. The first type is technology risk, principally the risks associated with computer systems. It implies the risks involved with information access, information availability and infrastructure (Linsley and Shrivess, 2006). Alozie (2001) describes technology risk as the loss events "due to piracy, theft, failure, breakdown, or other disruption technology, data or information". The second type is fraud risk by management or employees. The third type of operational risk is human factor risk; it relates to potential losses resulting from human errors (e.g. accidentally destroying a file), including external loss events (e.g. following a natural disaster).

Legal, Tax and Regulatory Risk: Legal, tax and regulatory risk arises for a whole variety of reasons. An example of legal risk is the involvement in lawsuits or the infringement of legal norms. Another example is a change in tax law which may have vast implication for a firm.

Business, Strategic and Reputation Risk: Business risk, strategic risk and reputation risk are grouped together. Following Croupy et al. (2006), these three types of risk are identified as business risk. Business risk refers to the typical risks a company faces: uncertainty about the demand for products, the price that can be charged for those products, the cost of producing, stocking and delivering the products (Croupy *et al.*, 2006). The risk associated with actions by competitors (Tofik, 2006) and potential losses of competitive advantage (Cabedo and Tirado, 2004) are other examples of business risk.

Strategic risk refers to the risk associated with significant investments for which high uncertainty exists about success and profitability (Crouhy et al 2006). A firm investing in research and development (R & D), for example, encounters uncertainty about the relation between its R & D investment and new product or process outputs (Miller, 1992).

Auditing Risk in ...

Reputation risk refers to the risk that a good reputation which can lead to value creation, turns to a bad reputation and, as a result, company value being destroyed (Ndukwe, 2009). Daferighe and Adedeji (2010), see reputation risk as a range of threats that have the potential to undermine a company's ability to function as a commercial enterprise and impair its standing to the community, an intangible asset that is very costly.

The effect of business risk is the threat that an event or action will adversely affect a business's ability to achieve its ongoing objectives, and consequently, management may tend to adopt measures that give a false impression of the financial position, hence emergence of 'Audit Risk', the probability that the auditor would draw an invalid audit conclusion and therefore, expressed an invalid audit opinion. It is the probability of reporting that financial statements present a true and fair view whereas they do not and vice versa. (Adenuyi, 2010, Babatunde, 2005, Whitigton and Pany, 2004).

The component of audit risk is expressed by the equation:

$$AR=IR \times CR \times DR$$

Where; AR=Audit Risk

IR=Inherent Risk

CR=Control Risk

DR-Detection Risk

Inherent Risk: This is the probabilities that material misstatement of financial information will occur assuming that internal controls are absent. It is the risk attached to any particular population because of its type, size and nature.

Control Risk: This is the probability that if material misstatement financial information occurs, the internal controls are weak, there is a higher risk of fraud and error, so the control risk will be high, example of control risk is lack of integrity by top management staff.

Detection Risk: This is the probability that the auditor's substantive procedures will not detect material misstatement that exist within a class of transactions or an account balance. The level of detection is determined by the uncertainties that are due to sampling risk.

Prior Empirical Studies on Risk Disclosure

In recent years, corporate reporting shifted from the disclosure of financial results toward informing the shareholders and other stakeholders about a wide variety of topics. One of these topics is risk (Ndukwe, 2009). Investors know that creating value regimes involves risk-taking and they like to know which risks the company faces and how these risks are (or will be) managed (Ekechi, 2001). As a result, there is an increasing demand for transparent risk reporting in annual reports. Bolaji (2004) defines risk disclosure as “the communication of information concerning firms’ strategies, characteristics, operations, and other external factors that have the potential to affect expected results”.

Few empirical studies have been published on the subject of corporate risk disclosure and, more specifically, on auditing risk on computerized accounting information system. A number of these rely on content analysis of annual or management reports and what external auditors do. Beattie, McLennan and Fearnley, (2004) distinguish two categories: subjective (analyst rating) and semi- objective (disclosure index studies, content analysis, readability studies, and linguistic analysis). Content analysis has been selected for this study because it has been widely used in the accounting research, particularly in corporate disclosure studies (Beretta and Bozzalan, 2004; Deumes, 2005; Linsley and Shrivies, 2006; Abraham and Cox, 2007).

A key issue is for auditors to adopt measures in conducting their audits engagement to minimize audit risk and enhance corporate risk disclosure. Linsley and Shrivies (2006) do not find a significant relationship between the extent of risk disclosure and beta coefficient which is a measure of company’s risk. Deumes (2008) and Abraham and Cox (2007), on the contrary, report a positive significant relationship between risk disclosure, systematic risk and auditors’ audit programme.

Research Design and Methodology

The research is conducted using both exploratory and descriptive research design. The population of the study is public accountants serving an external auditor. Since audit programmes are similar for all computerized accounting information system environment, forty select external auditors were chosen pinpoint key variables under study. The research questions and hypothesis were analysed using the measure of dispersion and the central limit theorem

$$Z = \frac{(x - \bar{x})}{SD}$$

Kolmogorov Smirnov test ($DN = \text{Max } |F_o(x) - F^o(x)|$)
where;

Auditing Risk in ...

Z = Z-Score Value

SD = Standard Deviation

DN = Calculated and table values for Kolmogorov-Smirnov test

F = the number of observations

$F^o(x)$ = The specified (or theoretical) cumulative frequency distribution under H_0 for any value of x .

$F_o(x)$ = The observed cumulative frequency distribution of a random sample of N observation for any value of x .

The critical value of D for sample size of $N > 35$. The decision rule is that H_0 will be rejected if the calculated D_{cal} is greater than the tabulated D_{tab} under the deviation level of 5 percent.

Results and Discussion

The data gathered are presented in tables and analysed using appropriate statistic.

Table 1: Analysis of Implication of Business Risk on Audit Risk

S/NO	Variables	x	0	(x-0)	(x-0) ²	%
1	Management Integrity	90	68.5	21.5	462	75
2	Management Competence	50	68.5	-18.5	342	62.5
3	Susceptibility to irregularities due to the nature of business	90	68.5	21.5	462	75
4	Complexity of class of transaction	30	68.5	-38.5	1482	75
5	Susceptibility of asset to loss or misappropriation	90	68.5	-21.5	462	75
6	Materiality of the Item	75	68.5	6.5	42	6.25
7	Financial Position of the Client Business	45	68.5	-23.5	552	50
8	The Company's Environment (Business)	50	68.5	-18.5	342	62.5
9	Quality of Accounting System	50	68.5	-18.5	342	62.5
10	Quality of Internal controls System	120	68.5	51.5	2652	100
	TOTAL	685			7.40	

Source: Field Survey, Data 2012.

$$\begin{aligned} 0 &= \sum \frac{x}{n} = \frac{685}{10} = 68.5 \\ &= \sum_{n-1}^n \frac{(x - \bar{x})^2}{n-1} \\ &= \frac{7140}{10-1} \\ &= \frac{7140}{9} = 793.33 \end{aligned}$$

$$\begin{aligned} \text{Standard Deviation (SD)} &= \sqrt{\frac{(x - \bar{x})^2}{n-1}} \\ &= \sqrt{793.33} \\ &= 28.17 \end{aligned}$$

Applying the central limit theorem :

$$Z = \frac{x - \bar{x}}{\text{SD}}$$

SD is exactly standardized where; $n \geq 30$

Where $x = 40$; $\text{SD} = 28.17$, $0 = 68.5$

$$Z = \frac{40 - 68.5}{28.17}$$

$$Z = -1.01$$

$$\begin{aligned} \text{Pr}(Z \geq -1.01) &= 1 - \text{Pr}(Z < -1.01) \\ &= 1 - (0.5000 - 0.45640) \\ &= 0.0436 \end{aligned}$$

From the above computations, the following statistical results are obtained:

Mean (\bar{x}) = 68.5

Standard deviation (SD) = 28.17

Distribution (Z) = 0.0436.

This implies that there is 0.436 probability that the mean will lie outside the standard deviation or 95% probability that all variables listed and studied as business risk factors affect audit risk.

It is observed from table 1 that management integrity, susceptibility to irregularities due to the nature of business, susceptibility of a set to loss or misappropriation and quality of internal controls system account for 75% implication of business risk on audit risk. Management competence, materiality of item, company's business environment and quality of accounting system accounted for 62.5%, while

Auditing Risk in ...

complexity of class of transaction and financial position of the client’s business accounted for 50% respectively.

From the Kolmogorov – Smirnov Frequency Table for the Hypothesis, the Calculated D-value is the point of greatest divergence between the cumulative observed and cumulative theoretical distributions, which is 0.15. The tabulate D from the Kolmogorov – Smirnov Test table at $\alpha = 0.05$ for sample size $N > 35$, is given as:

$$D = \frac{\alpha}{\sqrt{N}} = \frac{1.36}{\sqrt{40}} = 0.22$$

This shows that D_{cal} is greater than D_{tab} ; thus, in accordance with the decision rule, the null hypothesis (H_0) which states that “use of audit tool kits in a computerized accounting environment does not reduce audit risk” is rejected, meaning that, these tool kits are necessary for a successful audit programme in a computerized accounting system environment.

Thus, auditors have to carefully plan their work with emphasis on high risk areas, that is, must gather enough evidence to reduce audit risk to the barest minimum particularly when it has to do with reports generated from computerized accounting information system. The implication here is for external auditors to rise to the occasion of improving in their skills, knowledge and due diligence when performing audits in a computerized accounting information system environment.

Table 2: Responses on Tools Used in Computerized Accounting Information System Audits:

Alternative	Responses	Percentage %	Aggregate %
High extent	7	17.5	42.5
Moderate extent	10	25	40.5
Low extent	18	45	4.5
Not Used at all	5	12.5	12.5
Total	40		100

Source: Field Survey, Data, 2012.

The table shows that 17 respondents apply standard audit tool kits in their audit approach, representing an aggregate percentage of 42.5%. 18 respondents (45%) used these kits at low extent and 5 respondents (12.5%) do not use them at all. These imply that much needed to be done by auditors to be able to cope with challenges and risks associated with computerized accounting information system.

Test of Hypothesis

The data obtain in table 2 is used to test the hypothesis using Kolmogorov – Smirnor test.

Table 3: Responses of the Auditors on Tools Used in Computerized Accounting Information System Audits

F = Number of respondents	High extent	Moderate Extent	Low Extent	Not used At all
Choosing the alternative	7	10	18	5
$F^o(x)$ = Theoretical cumulative distribution of choices under Ho.	0.2	0.4	0.8	0.6
$F^o(x)$ = Cumulative distribution of observed choices under Ho.	0.25	0.41	0.88	0.75
$ F^o(x) - F_o(x) $	0.05	0.01	0.08	0.15

Source: Survey Data, 2012.

Data in table 3 shows that of the forty external auditors surveyed, seven use audit tool kit at high extent, ten at moderate extent, eighteen at low extent and five not at all. Applying the Kolmogorov Smirnov test, 0.05 and 0.01 for high extent and moderate extent are significant at 5 percent deviation level.

Conclusion and Recommendations

Business reporting in emerging global environment is precedent by developments in information and communication technology (ICT); has made computers pervade all human activities, including business information processing and reporting. External auditors need avail themselves with contemporary techniques and procedures required for audits in computerized accounting information system environment. The study reviewed some for the risks associated with business reporting in a system driven environment and available tools for conducting system based audits. Based on the study results, the following recommendations are made;

1. External auditors should always assess the nature of client’s business environment to have an understanding of related risks peculiar to the industry.

Auditing Risk in ...

This is to enable them know what audit programme will be suitable and whether they have the technical know-how for such engagements.

2. Regular training and retraining on contemporary audit techniques for an audit firm staff.
3. Mandatory ICT knowledge/skills is located as a prerequisite for granting of licence to practice by the relevant accounting professional bodies such as ICAN and ANAN.

References

- Abraham, S. & Cox, P. (2007). Analyzing the determinants of narrative risk information in UK FTSE 100 annual reports. *The British Accounting Review*, 227 – 248.
- Adeniyi, A. A. (2010). *Auditing and assurance services*, Lagos: Value Analysis Consult (Publishers).
- AICPA (American Institute of certified Public Accountants (2008). *Reports of the task force on risks and uncertainties*”, New York: AICPA.
- Alozie, M. C. (2001). *Separation of ownership and control*. Enugu, Gentle Publication.
- Babatunde, F. (2005). *Audit companion: Practice and revision Kit*, Lagos, FBV publications.
- Bettie, V. McLlennes, B. & S. Fearnley (2004). A methodology for analyzing and evaluating narratives in annual reports: a comprehensive descriptive profile and metrics for disclosure quality attributes”. *Accounting forum* (28), 205-236.
- Beretta, S. and Bozzolan, S. (2004). A framework for the analysis of firm risk communication”. *The International Journal of Accounting*; Vol. 39 (s); 265-288.
- Bolaji, C. A. (2004). *Disclosure level and the cost of equity capital*. Lagos: Bright Publishers.
- Cabedo, J. D. & Tirado, J. M. (2004). The disclosure of risk in financial statements, *Accounting Forum*, 28(2), 181-2000.
- Chike, K. (2004). Credit risk modeling and valuation. *Lagos: Journal of Business communication*, Vol. 142 92) 120 -157.

Academic Excellence

- Crouly, M. Galai, D. and Mark, R. (2006). *The essentials of risk management*, McGraw Hill: New York.
- Daferighe, E. & Adedeji, E. (2010). Reputational risk and impact assessment of corporate social responsibility on profitability and growth of manufacturing companies in Nigeria. *International Journal of economics development research and investment*. Vol.1 (1) p. 1-24.
- Deumes, R. & Knechel, W. R. (2005). Economic incentives for voluntary reporting on internal risk management and control systems, auditing: *A Journal of Practice and Theory*, 27(1), 35-66.
- Dozie, M. K. (2007). *The level of corporate risk disclosure in Nigeria*. Owerri, Ozbee Press.
- Ekechi, K. (2001). *Content analysis: An Introduction to its Methodology*. 5 The Sage Comm. Text series, Lagos: Sage Publications.
- Etim, E. O. (2011). Enhancing the efficiency of accounting information system in organizations. *International Journal of Economic Development Research and Investment* 2 (20) 19-27.
- Lingsley, P. M. & Shriver, P. J. (2006). Risk reporting: A study of risk disclosures in the annual reports of UK Companies. *The British Accounting Review*, 387-404.
- Merije, K. D. (1992). A framework for integrated risk-management in International Business", *Journal of International Business Studies*, 23 (2), 311-0331.
- Miller, M. J. (1992). Corporate risk reporting practices in annual reports of Japanese Companies. *Japanese Journal of Accounting* vol. 16 (1), 113-133.
- Ndukwe, A. G. (2009). Corporate risk reporting practices and their determinants. A study of selected quoted firms in Nigeria. *Nigeria research journal of accountancy* Vol.1 (1).
- Robinson, L. Davis J. & Alderman, C. (1986). *Accounting information system: A cycle approach* (2nd approach - 2nd ed). New York: Harper and Row, Publishers.

Auditing Risk in ...

Tofik, P. (2006). *The theory and practice of risk management policy*, Ibadan, University Press.

Whittington & Pany, K. (2004). *Auditing and other Assurance Services* (14th ed.) Boston: McGraw Hill.

APPENDIX I
Business Risk and Audit Risk Matrix

					Weight
1	Managing integrity	High	3	30	90
2	Management competence	Moderate	2	25	50
3	Susceptibility to irregularities due to nature of business	High	3	30	90
4	Complexity of class of transaction	Low	1	30	30
5	Susceptibility of asset to loss or misappropriation	High	3	30	90
6	Materiality of the item	High	3	25	75
7	Financial position of the client	Moderate	2	20	40
8	business	Moderate	2	25	50
9	The company's environment	Moderate	2	25	50
10	Quality of accounting system				
	Internal controls system	High	3	40	120
					685

Number of respondents = 40

Key: High risk = 3, moderate risk - 2, low risk = 1

1. Embedded audit facilities
2. Integrated test facilities (ITF)
3. System controls and review file (scare)
4. Tracing software
5. Snapshots
6. Systems software data analysis
7. Parallel simulation.