A Quantitative Approach to Information Systems Audit in Small and Medium Enterprises

Uma VIJAYAKUMAR[1], D. ILANGOVAN[2]
[1]Research & Development Centre, Bharathiar University, Coimbatore, India.
[2]Dept. of Commerce, Annamalai University, Annamalainagar, India.
bv_uma@yahoo.com, dil2691@yahoo.co.in

An Information Systems (IS) Auditor performs several audit related functions in a Small and Medium Enterprise (SME) such as preparation of a written IS audit procedure, comparison of actual IS configuration with documented configuration standards, assess whether IS assets are secure, check the access rights for users and system services, check for the presence of IS security procedures and finally analyze transactions in an information system. The current work focuses on a quantitative approach to measure the effectiveness of the IS audit functions in selected small and medium enterprises. The variations in KPI scores between sectors and regions are analyzed for the sample SMEs. Finally, the operational best practices for IS Auditors working in SMEs are suggested.
Keywords: Information Systems (IS), IS Audit, Key Performance Indicator (KPI), Small and Medium Enterprise (SME), Maturity Level Index

1 Introduction

An enterprise is mainly involved in economic activities. It can be categorized as Large, Medium or Small depending on the limits for investment, number of employees, balance sheet and total turnover. SMEs are contributing for economic development across the world. Information Systems Audit plays an important role in SMEs for running computer based application systems. Information Systems Audit ensures protection of IS assets and maintains data integrity. It also helps in achieving organizational goals and facilitates efficient *usage of resources* [1]. SMEs in the modern environment extensively make use of information system resources. This will ensure smooth flow of information between various sub systems and improves the business processes as well. An Information Systems (IS) Auditor performs several audit related functions in a Small and Medium Enterprise (SME) such as preparation of a written IS audit procedure, comparison of actual IS configuration with documented configuration standards, assess whether IS assets are secure, check the access rights for users and system services, check for the presence of IS security procedures and

finally analyze transactions in an information system.

2 Objectives

The objectives of the present work can be stated as follows:

1) To assess the existence of IS Audit expertise in SMEs with reference to the KPI- Maturity level Index.
2) To study the variations in the KPI scores between the sectors and regions.
3) Suggest operational best practices for IS Auditors with respect to Information Systems Audit in SMEs.

3 Related Work

The article by Tommie W. Singleton [2] analyses the four phases of the Controls Development Life Cycle, viz., design, implementation, operational effectiveness and monitoring. The design phase involves IS controls pertaining to Top Management, Quality Assurance Management, Operations Management, Security Management, Systems Development Management, Data Resources Management, Programming Management and User Applications Management. The implementation phase should carry out the controls listed in the

design phase. The operational effectiveness phase is concerned with ability of the controls to perform their goals (e.g. prevent a material misstatement). The monitoring phase involves continuous auditing on the controls and proper review of the change management procedures.

The monograph by Khabib [3] gives an overview of controls for applications, data centre operations and access security. It also gives an overview of computer based audit techniques to independently test computer data. Jim Kaplan proposed [4] a simplified representation of the enterprise information environment. He gave an overview of IS audit process, accuracy, consistency and reliability of data, controls for the core processes and application systems.

The fourth annual Information Systems Audit Benchmarking Survey conducted by Information Systems Audit and Control Association (ISACA and Protiviti in 2014 [5] highlights the challenges and concerns relating to computer and internet security, IS staffing and resources, IS risk assessment and IS audit reporting structure.

4 Present Scenario of Information Systems Deployment in SMEs

SMEs in the modern context are making use of IS infrastructure in a big way in their normal operations. However, the IS Audit is yet to evolve significantly in many SMEs. The internet based applications face a lot of problems related to information security in SMEs. The fraudulent websites create problems for SMEs by stealing personal and confidential data such as password, credit card number and so on. The Federal Trade Commission has stated that the number of phishing attacks have increased to a large extent during the last five years [6]. The phishing sites target individuals, banks, SMEs, e-commerce websites and government organizations. When the recipient has keyed in his/her personal details, the cyber-criminals gain access to the recipient's confidential details and cause problems relating to the recipient's money/credit/account. SMEs also face threats

from external as well as internal sources. For example, computer data are stolen using malwares like Trojans / viruses. Computer Crime as defined by the Association of Information Technology Professionals (AITP) include unauthorized actions involving usage, access, modification and destruction of hardware, software, data or network resources, release of information, copying of software tools, causing denial of service attack to genuine users and using computer & network resources to illegally obtain information [7].

SMEs face external threats from Trojans, Spyware, Viruses and Worms for their IS infrastructure. These threats penetrate into web browsers, desktop computers and e-mail servers. The common assumption that small businesses are too small to be targeted by computer threats is not true in the present scenario [8]. This is the background against which the current work will investigate the objectives listed earlier.

5 Research Methodology

This section deals with Data Collection, Sources of Data, Period of the study, Geographical area for the study and the Sampling Frame.

Data Collection: The primary data were collected from the sample respondents chosen from the Stakeholders / IS Auditors in select SMEs in India and the UAE. A Questionnaire has been prepared to administer upon them for collection of firsthand information from sample population. The strategies for evidence collection and evaluation include the following: discussion, observation, web based survey using Google Documents and telephonic interview.

Sources of Data: The sources of data about SMEs have been taken from Annual Reports of Ministry of MSME, Govt. of India, Annexure-XII and Mohammed Bin Rashid Establishment for SME Development, Dubai, UAE, for the period 2009-2010.

Period of the study: The period of the study for making worthwhile analysis has been chosen as 2010-2011.

Geographical area for the study: The geographical area for the study includes two countries, namely India and the UAE by taking into consideration the feasibility and accessibility factors. The four regions considered in India include: North, South, East and West. The four regions considered in the UAE include: Abu Dhabi, Dubai, Sharjah and Other Emirates.

Sampling Frame

STRATIFIED SAMPLING method has been deployed in the current work. The Strata considered for the study comprises of three sectors Manufacturing, Services and Trading. Equal sample selection from each stratum has been considered. Although, the strata sizes are different, it is required to compare the differences among the strata [9]. The sample size has been chosen using standard table for a given set of criteria [10]. The set of criteria considered in the present work are: Confidence level=95% and level of precision=5%.

The sample SMEs chosen in each sector has been 4. The Total number of Stakeholders / Information Systems Auditors selected from both countries (India and the UAE) has been 96. (i.e. 2 countries * 4 regions * 3 sectors * 4 SMEs/sector * 1 Stakeholder/IS Auditor per SME = 96).

Framework of Analysis

The statistical measures include the following: Measurement Scale, Mean and Two-way ANOVA. The KPI (Key Performance Indicator) considered for the stakeholder / IS Auditor has been Maturity Level Index.

Testing of Hypothesis

<u>**Hypothesis**</u>

Sectoral and Regional Variations (Two way ANOVA) within a country

The regional and sectoral KPI scores within a country do not vary or the differences between them are not significant. This is expressed as under:

H_0 : $(\mu_{s1})_{KPI} = (\mu_{s2})_{KPI} = (\mu_3)_{KPI}$

H_0 : $(\mu_{r1})_{KPI} = (\mu_{r2})_{KPI} = (\mu_{r3})_{KPI} = (\mu_{r4})_{KPI}$

H_1 : $(\mu_{s1})_{KPI} \neq (\mu_{s2})_{KPI} \neq (\mu_{s3})_{KPI}$

H_1 : $(\mu_{r1})_{KPI} \neq (\mu_{r2})_{KPI} \neq (\mu_{r3})_{KPI} \neq (\mu_{r4})_{KPI}$

μ_{s1-s3} = Sectoral Mean Score of each of the 3 sectors.

μ_{r1} - μ_{r4} = Regional Mean score of each of the 4 regions.

H_i : There is no significant interaction between the two factors sector and region. The alternate hypothesis states that there exists an interaction between the two factors sector and region. The above hypothesis is tested with the primary data pertaining to the KPI: Maturity Level Index.

Measurement Scale

Questions involving (Yes/No) responses are represented in a 3 point scale as, shown below:

Yes   No   Not Applicable
  +1   -1   0 is left for dummy response treated as neutral.

Scaling technique helps in transforming qualitative aspects into quantitative constructs. The response scores are finally converted into a cumulative score, which is then represented on a ten point scale. This is done by using the formula as stated below:

$$\text{Measurement Scale (index)} = \left[\frac{(\text{Cumulative Score})_{Actual}}{(\text{Cumulative Score})_{Maximum}} \right] \times 10 \quad (1 = \text{Low}, \ 10 = \text{High})$$

6 Questionnaire

The following questionnaire has been administered to the stakeholders / IS auditors in the sample SMEs using a web based survey.

1. Do you have a written IS audit / independent review program?
2. Do you have internal IS auditor in your organization?
3. Does IS audit coverage include a comparison of actual system configurations

to documented/baseline configuration standards?

4. Does IS audit coverage include assessing compliance with information security program requirements?

5. Does IS audit coverage include assessing users and system services access rights?

6. Is Information Systems Audit involved in your risk assessment process?

7. Do you use any IS Audit Software Tool? If Yes, specify the name.

8. Do you have documented IS Security procedures?

9. Do you have a concurrent IS audit (embedding audit modules in an application system to provide continuous monitoring of a system's transactions) mechanism for all of you?

7 Quantitative Analysis

This section deals with quantitative analysis involving the KPI - Maturity Level Index. The Maturity Level Index indicates the effectiveness of the following IS functions in a SME:

i)   Monitoring IS operations.
ii)   Compliance with IS practices.

The current work is aimed at studying the maturity level of IS Audit in sample SMEs.

The observed values for the KPI - Maturity Level Index are represented on a scale of 10. The Sectoral and Regional Variations in both the countries are analyzed using Two-way ANOVA. Finally, the hypothesis is tested and appropriate inferences are made for the KPI - Maturity Level Index. The results of the above hypothesis testing with the primary data for India and the UAE are shown below in TABLEs 1.A and 1.B.

Observation

In case of India and the UAE, the average values for Maturity Level Index observed for a given pair of sector and region are shown in TABLEs 1.A and 1.B. Their values vary between 2.778 to 5.8333.

Findings

In the case of India, the sectoral and regional variations are summarized as follows.

Between Sectors: The calculated value for F (0.55686) is less than the table value F *crit* (3.25945) *at* 5 Percent level of significance. Hence, the null hypothesis is accepted.

Between Regions: The calculated value for F (0.4569) is less than the table value F *crit* (2.86627) *at* 5 Percent level of significance. Hence, the null hypothesis is accepted.

In case of the UAE, the sectoral and regional variations are summarized as follows.

Between Sectors: The calculated value for F (5.57561) is greater than the table value F *crit.* (3.25945) *at* 5 Percent level of significance. Hence, the null hypothesis is rejected.

Between Regions: The calculated value for F (2.16098) is less than the table value F *crit* (2.86627) *at* 5 Percent level of significance. Hence, the null hypothesis is accepted.

Inference

There are no significant variations in the Maturity Level Index scores, between the three sectors in India. There are significant variations in the Maturity Level Index scores, between the three sectors in the UAE. There are no significant variations in the Maturity Level Index scores, between the four regions, in both the countries. There is no significant interaction between the two factors sector and region, in the determination of Maturity Level Index scores, in both the countries.

Table 1.A. Sectoral and Regional Variations in India - Maturity Level Index

SUMMARY	East	North	South	West	Total
Manufacturing					
Count	4	4	4	4	16
Sum	18.89	17.78	20.01	21.11	77.79
Average	4.7225	4.445	5.0025	5.2775	4.86188
Variance	3.61216	4.12923	3.71483	1.14056	2.62222
Services					

Count	4	4	4	4	16
Sum	17.78	20	22.22	21.12	81.12
Average	4.445	5	5.555	5.28	5.07
Variance	2.47903	5.36133	2.47903	0.3136	2.30656
Trading					
Count	4	4	4	4	16
Sum	15.55	18.89	18.89	17.78	71.11
Average	3.8875	4.7225	4.7225	4.445	4.44438
Variance	2.06463	3.61216	3.61216	2.47903	2.47755
Total					
Count	12	12	12	12	
Sum	52.22	56.67	61.12	60.01	
Average	4.35167	4.7225	5.09333	5.00083	
Variance	2.35583	3.62948	2.80488	1.24121	

ANOVA – Two-Factor With Replication						
Source of Variation	SS	Df	MS	F	P-value	F crit
Sample	3.24815	2	1.62408	**0.55686**	0.57786	**3.25945**
Columns	3.99764	3	1.33255	**0.4569**	0.71407	**2.86627**
Interaction	2.10395	6	0.35066	**0.12023**	0.99327	**2.36375**
Within	104.993	36	2.91648			
Total	114.343	47				

Source: Primary Data 2010-2011

Table 1.B. Sectoral and Regional Variations in the UAE - Maturity Level Index

SUMMARY	Abu Dhabi	Dubai	Other Emirates	Sharjah	Total
Manufacturing					
Count	4	4	4	4	16
Sum	20	21.1111	21.1111	18.8889	81.1111
Average	5	5.27778	5.27778	4.72222	5.06944
Variance	2.05761	1.13169	6.893	1.13169	2.29938
Services					
Count	4	4	4	4	16
Sum	21.1111	23.3333	17.7778	20	82.2222
Average	5.27778	5.83333	4.44444	5	5.13889
Variance	1.13169	2.77778	2.46914	0.41152	1.62551
Trading					
Count	4	4	4	4	16
Sum	12.2222	21.1111	15.5556	11.1111	60
Average	3.05556	5.27778	3.88889	2.77778	3.75
Variance	1.13169	1.13169	0.41152	0.41152	1.62551
Total					
Count	12	12	12	12	

Sum	53.3333	65.5556	54.4444	50		
Average	4.44444	5.46296	4.53704	4.16667		
Variance	2.24467	1.44968	3.02095	1.59933		
ANOVA - Two-Factor With Replication						
Source of Variation	*SS*	*Df*	*MS*	*F*	*P-value*	*F crit*
Sample	19.5988	2	9.79938	**5.57561**	0.00777	**3.25945**
Columns	11.394	3	3.79801	**2.16098**	0.1096	**2.86627**
Interaction	8.59053	6	1.43176	**0.81463**	0.5657	**2.36375**
Within	63.2716	36	1.75754			
Total	102.855	47				

Source: Primary Data 2010-2011

8 Operational Best Practices for IS Auditors Working in SMEs

IS Auditors can conduct audit for automated and semi-automated systems in SMEs and ensure compliance with established IS audit procedures. It is necessary that the risks relating to software applications and IT infrastructure (like security threats and viruses) are analyzed and appropriate recommendations are made to mitigate risks. IS auditor should examine the IS policies and standards followed in a SME.

Operating systems such as Windows/Linux/Mac should be well updated with the latest and necessary patches. The release of such systems should be audited at a regular basis so there are no security loopholes in them which might lead to an OS (operating system) level attack.

In-house / External applications such as ERP, HR, and Payroll etc should also be audited towards their functionality. There should be proper controls for the Information Systems which are purchased from third party vendors.

An IS auditor should examine the security of information systems in a SME, as described below:

Logical access
1. Passwords must be set according to the standards set by the IS Security department.
2. The passwords set for the last 5 times should not be the same.

3. There should be a certain time interval (say 30 to 90 days) during which the passwords must be changed.

Physical access
1. No outsider should be able to enter the company's premises until and unless the entry procedure is followed. Each and every outsider should deposit an identity.
2. Laptops must be locked to the workstations in case the owner of the laptop has gone outside.
3. The access to the server room should always be recorded and should be accessed only by the authorized personnel.
4. Server room should be protected from natural disasters.

Backup Policy
An IS auditor should examine the backup policy in a SME, as described below:
1. Frequent backup (daily, weekly, monthly basis) of the data within the systems / applications should be taken and kept in a secure place in the premises of SME.
2. For critical data, the backup can be stored additionally at a secure remote site/location.

Disaster Recovery Plan (DRP) / Business Continuity Plan (BCP)
An IS auditor should examine the DRP/BCP in a SME, as described below:
1. Availability of DRP/BCP Plan.
2. Frequency of DRP/BCP drill.
3. Results of the drill must be maintained for future reference.

9 Conclusion

This paper dealt with a quantitative approach to assess the maturity level for IS audit in sample SMEs.. The variations in KPI scores between sectors and regions have been analyzed for the sample SMEs. The operational best practices for IS Auditors working in SMEs have been suggested.

References

[1] R. Weber, Information Systems Control and Audit, Pearson Education, 2008.
[2] T. W.Singleton, "What Every IT Auditor should know about controls: The Controls Development Life Cycle", ISACA Journal Vol 3, 2009.
[3] Khabib, Information Technology Audit, General Principles, IT Audit Monograph Series, available at http;//khabib.staff.ugm.ac.id, 2010, pp. 1-25.
[4] J. Kaplan, Information Integrity Auditnet: Monograph Series, available at www.infogix.com, 2003, pp.4-24.
[5] ISACA and Protiviti, A Global Look at IT Audit Best Practices, 2014, available at www.isaca.org.
[6] Neesa Moodle & Issacs, , Banks offer new software to keep phishers out of your account, June 5, 2010, available at www.mi2g.com.
[7] J. A O'Brien & George M Marakas, Management Information Systems, 7th edition, Tata Mcgrawhill Pub., pp. 429-430, 513-515, 2009.
[8] Snap Gear Secure Computing Corporation, Security Solutions for Small Businesses and Remote Branch Offices, 2009.
[9] C.R. Kothari, "Research Methodology: Methods and Techniques", New Age International (P) Ltd., 2007, pp.63.
[10] D I Glenn, "Determining Sample Size", University of Florida IFAS Extension, April 2009, pp.9-11, available from: http://edis.ifas.ufl.edu/pd006.

Uma VIJAYAKUMAR is a Chartered Accountant, with specialization in Information Systems Control and Audit. She is a research scholar in the dept. of Commerce at Bharathiar University, Coimbatore, India. She is a Fellow Member of Institute of Chartered Accountants of India. She has 25 years of experience in finance and auditing.

Dr. **D ILANGOVAN** is a Professor in the Department of Commerce, Annamalai University, India, with specialization in Cooperation & Industrial Marketing. He has over 25 years of experience in teaching and research. He has several publications to his credit at international and national level.