Effective Operations Management Control Functions for Information Systems in Small and Medium Enterprises

V. Uma,
Chartered Accountant, Tiruchirappalli &
Research Scholar, Research and
Development Centre,
Bharathiar University, Coimbatore,
Tamil Nadu, India.
E-mail: *uma_vvk_66@yahoo.co.in*

D. Ilangovan,
Professor,
Dept. of Commerce,
Annamalai University,
Annamalai Nagar, Chidambaram,
Tamil Nadu, India.
E-mail: *dil2691@yahoo.co.in*

Abstract **- This paper aims to analyze the operations management control functions for Information Systems (IS) in small and medium enterprises (SMEs). In the current knowledge driven economy, small and medium enterprises should deploy adequate IS operations management control mechanisms in place for efficient functioning. Operations Management is responsible for carrying out the day-to-day activities involving hardware and software resources in a computer based information system. This paper begins with a brief introduction to SMEs followed by the different categories of IS operations management controls relevant to SMEs. A quantitative model for evaluating operations management controls in a SME has been suggested. The final section suggests some directions for further development in future work.**

Keywords **- Information Systems, Operations Management Controls, Small and Medium Enterprise.**

I. INTRODUCTION

An enterprise is an entity engaged in an economic activity. Enterprises can be classified as Micro, Small, and Medium and Large based on *labor employed*, *capital turnover* and *balance* sheet [1]. Small and Medium Enterprises (SMEs) play a vital role in any business in the world economy. Every country has its own identity to their SMEs based upon the standards of living of the people, extent of development in the economic sectors (manufacturing, trading & services) and pursued policies and plans. Within the same country, various supporting institutions have their own norms with regard to SMEs which will suit them for their operational convenience.

SMEs, in the modern business environment, are increasingly dependent on IS infrastructure, in their day to day operations, across the world. IS Operations Management is responsible for carrying out the day-to-day activities involving hardware and software resources in a computer based information system. However, the IS Operations Management Control functions, are yet to take off to a reasonable level in many SMEs. The widespread use of computer based information systems and internet has created a number of IS Operations Management Control related problems in SMEs across the world. A few obvious problems include the following:

1. Significant differences exist in the level of perception, awareness and acceptance of IS Operations Management Control functions, by the IS personnel and stakeholders.
2. Assessing the maturity level of IS Operations Management Control mechanism in SMEs is still in the evolving stage.

II. OBJECTIVES AND MOTIVATION

The present work is intended to meet the following objectives:

a. Examine the various categories of IS Operations Management Control functions in SMEs.
b. Evolve an objective method for measuring the effectiveness of IS Operations Management Control functions in SMEs.

SMEs in the present global economic scenario must compete with organizations of all types to meet the growing needs of an increasingly technology-empowered customer base. There is a growing need for adopting Information System Resources to speed up information flow and streamline business processes. There exists a *strong requirement* to

exercise adequate IS Operations Management Controls in SMEs, to achieve efficiency, in their regular operations. The present work is motivated by the significance and relevance of Operations Management Controls for Information Systems in SMEs.

III. PRESENT SCENARIO

In the present days, SMEs are frequently exposed to phishing attacks or identity thefts (fraudulent emails asking for personal information such as password, credit card number from unsuspecting victims) from fraudulent websites. According to Federal Trade Commission, the number of phishing attacks has increased considerably during the last five years [3]. The phishing sites target not only individuals but also banks, credit card companies, e-commerce websites, government agencies and all types of enterprises [small, medium, large]. Once the recipient has entered his/her personal information, the cyber-criminals steal the identity of the recipient and wreak havoc with credit/money/accounts [4].

SMEs in the present scenario are confronted with Computer Crimes from external as well as internal sources. Computer Crime [4] is defined by the Association of Information Technology Professionals (AITP) as follows:

1) Unauthorized use, access, modification and destruction of hardware, software, data or network resources.
2) Unauthorized release of information.
3) Unauthorized copying of software.
4) Denying an end-user to access his/her own hardware, software, data or network resources.
5) Using or conspiring to use computer or network resources to illegally obtain information or tangible property.

SMEs are presently facing threats to their IS infrastructure from external sources like Viruses, Worms, Trojans and Spyware. These threats exploit known weaknesses in web browsers, desktop computers and e-mail servers. The days of security by obscurity believed in by the small business owners for years are long gone. The common assumption that small businesses are too small and unknown to be targeted by an attack is simply not true in today's threat environment [5]. The above is the background against which the present work will analyze the IS Operations Control Management functions in SMEs.

IV. FUNCTIONS OF IS OPERATIONS MANAGEMENT CONTROLS

A Computer based Information System comprises of hardware and software resources. Operations Management [2] is responsible for carrying out the day-to-day activities involving these resources. A SME should have in place adequate controls over the following functions:

a) Computer Operations.

b) Networking.

c) Data Entry and Verification.

d) Production Control.

e) Storage Media Management.

f) Software and Documentation.

g) Help Desk / Technical support.

h) Capacity Planning and Performance Monitoring.

i) Outsourced operations.

These functions are explained briefly as follows:

A. Controls over Computer Operations

SMEs make use of personal computers and minicomputers in their regular operations. An IS auditor can observe the operators' actions relating to backup/recovery, execution of scheduled jobs and ad-hoc jobs. The Operating Systems Log, Server Log and Browser Log files can be examined regularly to monitor the system activities and prepare a summary report on a periodic basis (say daily, once a week). It is also necessary to examine the operations manual. The operations manager can give useful information about evidence of exceptional/error prone activities. The review of Log files can be documented.

In the case of manufacturing enterprises, production systems should be run according to a well defined schedule. The schedule authorizes hardware and software resources for the application systems. The schedule prepared by operations manager can be audited by IS auditor, for correctness and relevance. The IS auditor can examine the audit trial of jobs executed over a period of time and check against the authorized schedule for any evidence of irregularities (like duplicate payroll checks, invalid transactions, running of unauthorized jobs).

An IS auditor can examine the documents relating to computer hardware and software maintenance. The following set of tasks can be carried by IS auditor with regard to maintenance operations:

a) Conduct discussions with operations manager, maintenance engineers and operators regarding their activities.

b) Examine service reports/logs over a period (month/year).

c) Check if the sensitive data is not disclosed / exposed during the course of normal duties.

B. Controls over Network Operations

In the modern knowledge driven economy, SMEs deploy computer systems in a networked environment. The network can be a Local Area Network / Internet. In such a complex scenario, operations manager, in SMEs, has the responsibilities to

a) Start and stop Network operations.

b) Monitor continuously the performance of communication channels, network devices like routers & switches and network enabled programs / data files.

c) Maintain security and privacy for Information System Assets in an enterprise.

An IS auditor can use interviews, observations and review of documentation to evaluate the reliability of network control operations. The following tasks can be performed by IS auditor with respect to network operations:

a) Check for disk space usage and availability.

b) Check the Access privileges of different types of users (end user network administrator, programmer).

c) Checking the network log files of all users for identifying any irregular / unwarranted activities.

d) Check whether server machines are in a safe area.

e) Check whether authorized personnel only can enter server area.

C. Controls over Data preparation and Entry

The data entry operators should be well trained to perform data preparation and entry tasks. The batch processing of large number of records should be carefully handled in a computer based information system. The data should be backed up at regular intervals.

The keyboard and display unit and furniture should be designed ergonomically for the operators to provide maximum comfort level, while at work.

Equipments like automatic teller machines have to be serviced regularly for reliable operation.

Date Entry can be followed by Data Verification and Validation phases. This will ensure correctness of input data and eliminates errors.

D. Production Control functions

The major functions coming under production control section are listed below:

a) Receipt and Dispatch of Input and Output.

b) Job Scheduling.

c) Management of service level agreements.

d) Transfer pricing/ charge out control.

e) Acquisition of computer consumables.

An IS auditor can examine the following Operations Management tasks in SMEs:

a) Authorized personnel only give input data.

b) Logging the input data and keeping it securely.

c) Timely submission of input for processing.

d) Identifying control personnel for input.

e) Safe custody and dispatch of output to authorized outside parties and users.

f) Timely availability of output.

g) Check whether a job submitted to a computer by operations personnel has one or more programs and what resources are needed to complete the job.

h) Check the job control files of operations personnel for correct operations and ordering of programs in a job.

i) Check whether job control files are suitably backed up.

j) Identify which jobs run in the foreground (needs user attention) and which jobs run in the background. (can run without user intervention)

k) Examine service level agreements between users and operations personnel, logs of complaints from users & follow-up actions by operations personnel.

l) Examine the billing procedure for users, collecting receipts/ initiating internal transfer of funds and following up on unpaid accounts.

m) Interact with users and operations personnel for the level of services provided.

n) Check the invoices received from outsourced vendors.

o) Evaluate the procedure for purchase, storage and issue of consumables like printer stationery, disks, tapes, toner cartridges for printers and so on.

E. Control over storage media

An IS auditor can examine the following storage media related activities in SME:

a) Secure housing of storage media.

b) Labeling of media for clear identification.

c) Observe the off-site and on–site locations for housing the storage media

d) Verification of stock register entries.

e) Proper organization of files and subdirectories in storage media.

f) Permit authorized personnel to carry the storage media in and out of the server room.

g) Check the precautions to be taken while deleting old/sensitive files.

h) Evaluate the likely reliability of storage media by observing the number of read/write errors shown by operating system/diagnostic programs.

i) Examine the procedure for disposal of unreliable storage media.

F. Controls over Documentation and Program Library

An Information system in SME maintains the following items pertaining to documentation and program library:

a) Operational plan.

b) Application Systems documentation.

c) Documents relating to software utilities, user manual and technical reference manual.

d) Related books and journals for application Systems.

e) Licensed software and open source software.

An IS auditor can interview the librarians about the nature of jobs performed by them, observe the ways in which they maintain the library of licensed software and open source software and related documents. IS audit can be performed to verify the correct usage of documentation resources by authorized personnel.

G. Controls over Help Desk / Technical Support

The Help Desk/Technical support functions include the following:

a) Hardware and software installation, configuration and maintenance.

b) Attending to end users problems in their day to day operations.

IS auditors can interview end users, to determine their level of satisfaction with the service provider, by help desk / Technical support personnel. They can observe help desk/technical support personnel to see how they respond to end user's requests. They can also review the log files/registers maintained by the help desk /technical support staff to assess their effective functioning.

H. Controls over capacity planning and performance monitoring

Operations Management must ensure that hardware/ software resources are functioning well and are reliable. Hardware and software performance can be monitored continuously using control programs/monitoring tools and accordingly the system resources can be upgraded or additionally procured. IS auditor can examine capacity planning and performance monitoring tools, when they are executing in the background.

I. Controls over outsourced operations

Operations Management can exercise the following controls over outsourced operations.

a) Continuously monitor the financial viability of the outsourcing vendor.

b) Compliance with the outsourcing contract's terms and conditions.

c) Ensure the reliability of controls in the operations of outsourcing vendor through internal and external audit.

d) Have in place, well defined procedures for disaster recovery, in the event of problems with outsourcing vendor.

An IS auditor can examine the above mentioned controls by observation and interviews with the operations management personnel.

V. QUANTITATIVE MODEL FOR IS OPERATIONS MANAGEMENT CONTROL

A quantitative model is proposed in this paper for IS Operations Management Control functions in SMEs as shown in **Figure 1**. The questionnaire/schedule can be administered to IS Administrators in SMEs and the output responses obtained from them are used to compute the Operations Management Index. The scaling comprises of 3 point scales. The scoring for these is proposed to be minus one, zero and plus one as noted here under using 3 point scale:

-1: No 0: NA +1: Yes

Measurement scale

The conversion of the qualitative aspects into quantitative constructs can be carried out through scaling techniques. The response scores thus arrived at, by the usage of response scale as above, finally will result in a cumulative score. This cumulative response score for operations management control functions is converted into a measurement scale on a scale of 10. This is done by using the following formula:

IS Operations Management Control Index =

$$\frac{(\text{Cumulative Score})_{\text{Actual}}}{(\text{Cumulative Score})_{\text{Maximum}}} \times 10$$

(Here, 1 = Low, 10 = High).

If the resultant scale is negative, then it is frozen at zero on the pretext that measurement scale of 1-10 reflects the extent of effectiveness, while zero represents a state at which the effectiveness is presumed to be absent.

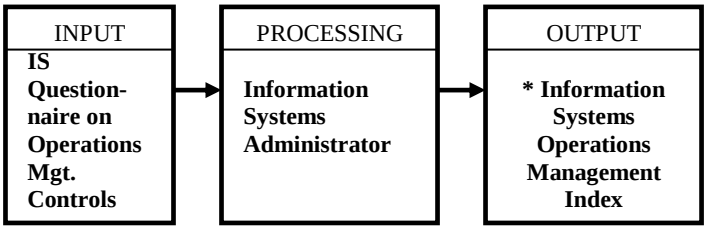

Figure 1: IS Operations Management Control Survey

VI. Questionnaire / Schedule on IS Operations Management Controls

The following questionnaire has been designed to evaluate IS operation management controls in SMEs. The responses fall under any one of the following three options: (**Y**) es, (**N**) o, **NA**.

1) Do you have IS Operational Plan in your enterprise? (Short term plan for 1 to 2 years of operations)

2) Do you maintain documents for IS policies, procedures and standards?

3) Has a network diagram, which illustrates physical and logical connections between communications equipment, available in your organisation?

4) Are authorization codes required to:

   a) Access the computer system?

   b) Access the applications programs?

   c) perform transactions

5) Does capacity planning include analyses of message length, protocol, transaction volume, and message traffic?

6) Is hardware performance compared to vendor specifications?

7) Does operations management routinely review vendor services performed?

8) Are periodic checks of the network made to verify proper operation and detect terminal/line/modem errors?

9) Are communications hardware failures documented, including corrective actions taken?

10) Have procedures been established to ensure that all transactions sent have been received? (E.g., record counts sent/received?)

11) Is there a review of all transaction messages that are unaccounted for, distorted, duplicated, or delayed?

12) Do you have policies / procedures for the proper disposal of information system's assets?

13) Does your Application System require PIN (personal identification number) to authenticate electronics fund transfer?

14) Do you have controls to ensure that privileged user (root user / super-user / application administrator) exercises his/her powers correctly?

15) Do you have LOGGING facilities for

a) System activities of all users?

b) Security-Sensitive events?

c) Hardware Malfunctions?

d) Resource Consumption Data for various users?

e) user-specified events / actions

16) Do you have controls to ensure that output / reports are provided only to authorized users?

17) Do you perform Audit Trial on Input, Processing and Output subsystems for all your applications?

(Record chronology of events from beginning to end for all transactions and processes)

18) Are back computer files created at appropriate time intervals so that damaged or lost files can be easily reconstructed?

19) Do you have a policy for Transfer Pricing / Charge out Control?

20) Do you have a policy for outsourced operations?

VII. CONCLUSION & DIRECTIONS FOR FURTHER WORK

This paper dealt with the different categories of IS Operations Management Controls as applicable to SMEs. A quantitative model for evaluating operations management controls for information systems in SMEs has been proposed for use after a formal trial.

The Questionnaire / Schedule on IS Operations Management Controls will be administered to IS Operations Management professionals in selected SMEs in India and the UAE. The SMEs will be drawn from three sectors: Manufacturing, Services and Trading. Based on the above mentioned inputs, the Operations Management Index can be computed on a measurement scale of 10. This approach will help the SMEs significantly in assessing their present maturity level in operations management controls and enhance their efficiency by deploying appropriate control measures at operations management level.

REFERENCES

1) Rana Dababneh & Farah Takan, (2007), Booklet of Standardized SMEs Definitions, [online] available at: www.SABEQ-Jordan.org, pp. 1-10.
2) Ron Weber, (2002), Information Systems Control and Audit, Pearson Education, Asia.
3) Neesa Moodle & Issacs, June 5, 2010, Banks offer new software to keep phishers out of your account, Available from: www.mi2g.com.
4) James A O'Brien & George M Marakas, 2009, Management Information Systems, 7th edition, Tata Mcgrawhill Pub., pp. 429-430, 513-515.
5) Snap Gear Secure Computing Corporation, 2009, Security Solutions for Small Businesses and Remote Branch Offices.