

How to Manage Internal Controls for an Accounting Information System; a Review

Abbas Banisharif

Department of Accounting, Payame Noor University, I.R.Iran

Abstract: for ensuring about the fact that all organizational processes are running good and the employees and staff are doing their tasks and jobs well, every system applies some internal controls. Many researchers have argued that the organizational controls will be set in the areas that the managers are interested and some of the scholars divide such controls in two categories; internal and external. The growth of computer and information technology in today's turbulent and competitive business, paves the way for using these technologies toward the goal of internal controls in the organizations. This paper discuss about the application of Accounting Information Systems (AIS) and Internal Controls, their advantages and the elimination of paper based controls.

[Abbas Banisharif. **How to Manage Internal Controls for an Accounting Information System; a Review.** *J Am Sci* 2012;8(10):351-354]. (ISSN: 1545-1003). <http://www.jofamericanscience.org>. 52

Keywords: Internal Control, Management, Accounting, Information Systems

Introduction:

Internal Accounting Controls

Creating efficient accounting processes allows an organization to set specific policies and protocols on accounting procedures, and reach its financial objectives on a regular basis. Internal accounting controls can help keep track of such areas as cash-receipt recording, payroll management, appropriate recording of grants and gifts, cash disbursements by authorized personnel, and the recording of assets. These systems also can take into account any government regulations and requirements for financial reporting.

Benefits

Internal controls of accounting provide a streamlined solution for organizing all accounting procedures and ensuring that the accounting cycle is completed consistently and successfully. Implementing a formal Accounting Procedures Manual for the organization allows the financial department to facilitate several processes and maintain rigorous standards. Internal controls also allow organizations to keep detailed records, manage and organize important financial transactions and set a high standard for the organization's financial management structure and protocols. A well-implemented system also reduces the risk of accounting errors and abuse. More companies are adopting internal controls of accounting systems and using web-based applications and computer programs to make accounting management easier. Organizations can monitor and control several accounting processes using data management systems that provide statistical reports, ensure current-day compliance and allow companies to create accurate financial assessments and forecasts with ease. As systems become computerized, the internal controls

for that system have to be adapted accordingly. This is because computerized systems bring with them certain unique problems that can only be removed or minimized by adapting the present controls and adding new controls. These problems are in a manual system there is a paper trail for the internal auditor to follow. All records and transactions are kept on paper and so an auditor has clear and documented proof of what has transpired. Computerized systems rarely have a clear paper trail to follow. Since computers do all of the sorting of the information the company rarely sorts the source documents. Also the computer does most of the calculations and processing so there would not be the amount of documentation that there would be in a manual system.

Another problem of computer systems is the fact that there can be difficulty in determining who entered the data. In a manual system the identity of the person entering the data can be identified possibly by the person's handwriting. This cannot be done in a computerized system. This makes it very difficult to determine who is responsible for errors or fraud.

Since the computers do all calculations and processing errors can occur due to bad design of the program. This can be difficult to detect especially if the error does not occur frequently and only does so under particular conditions. Computer systems also offer new opportunities for fraud. If a computerized system is not set up properly and certain checks not put in then the computer system can be used to defraud the company. The fact that it is difficult to trace who enters the data only adds to the magnitude of this.

In order to minimize the risks of errors or fraud occurring in the computer system certain controls have to be put into place. These controls can be broken up into three different categories. They are:

1. Administrative Controls

2. Systems Development Controls
3. Procedural Controls

Administrative Controls

Administrative controls are those controls are those controls that are placed on the system to ensure the proper organization and processing of data. These administrative controls are.

Division of duties

Duties are assigned to different individuals in the organization. This is done in such a way that no one person can have full control over a transaction. This ensures that an individual cannot have full control over the creation and operating of the system. One reason for this division is having one person controlling the system can result in fraud if that person is not completely trustworthy. Another reason for the division of duties is to prevent the organization from becoming totally dependent on the person controlling the computer system. If this person were to leave then the organization would have no one to run the system. The division of duties ensures that employees can leave without having any major effect on the system.

Operation Controls

Operation controls are necessary controls since they since they determine what the computer systems and the employees using the system have been doing. These controls can come in the form of

- rotation of shifts
- Duty logs
- A manual of operating instructions
- Attendance controls
- Computer logs

These controls can allow an auditor to track the exact actions of the computer systems and employees. This documentation allows the to easily spot any errors or improper actions that have occurred.

Files Controls

These controls are put in place to minimize the number of errors and omission that occur in the file system. Good file controls are:

- Availability of a skilled technician
- Proper procedures for issuing and returning files
- Proper labeling and indexing of files
- Protection of storage media from dust, humidity, fire etc.
- Procedures for returning files for certain minimum periods
- Facilities for recovering files that have been damaged or corrupted.

- Facilities for creating backup copies of files.

The placement of these controls has very serious implications. These controls that information that is vital to the organization is safe. The data in these files must be protected from errors or tampering whether intentional or accidental.

Hardware Security

The computer hardware is not only important to the processing of the information but is also a valuable fixed asset for the company. Therefore controls for the protection of the hardware must be put into place. Computer hardware must be placed in a secure area where the access to it is limited only to those who need to use it. Certain levels of security must me maintained e.g. only the systems administrator can have access to the CPU and storage systems. The computer system must also be placed in a control environment to protect it from environmental hazards e.g. dust and humidity. Arrangements should be made to protect the computer against fires and power fluctuations. There should also be some controls in place to recover the system in case the hardware fails. These controls would ensure that the breakdown of the hardware would not have a serious effect on the company.

Systems Development controls

These are the controls that are put over the design and implementation of the system. These controls ensure that the system is developed with a minimum number of errors.

Standardization

One important control is standardization. These consist of various standards that are laid down by management for the design and development of the system. These standards include the complete documentation of the development of the system. These standards would not only benefit in the correcting of problems and updating of the system, the documentation would allow the auditor to get a better idea of how the system works. This would help the auditor in spotting possible problems in the system.

Involvement of Management

The involvement of the organizations management in the development of the system is an important control. With these controls, management must have documentation such as feasibility studies, budgets and performance evaluations. These documents would allow management to decide if the system being developed would be viable and cost effective. Without such controls, expensive projects can be started and never finished, costing the

organization a great deal in time and money. These managerial controls force the development team to do a thorough job since they are accountable to management.

Testing

Testing and trials are important controls and require that systems are thoroughly tested before they become operational. The extensive testing of programs will minimize or even eliminate the errors in the computer system. The tests will show exactly what type of problems occur in the system in the processing of certain data and would also indicate any problems in the response time of the systems. Also, the benchmarks that are calculated in testing can be compared with benchmarks taken later on to see if the program has been tampered with.

Training

The training of the data processing staff is a very important control. Proper training of staff would reduce the number of errors that would occur in the system due to inadequate knowledge of the system. The trained staff would be less likely to make mistakes.

Concurrent running of old and new systems running the old and new systems concurrently is also an important control. This control would allow the organization to compare the results of the two systems when they do different tasks. These results would allow them to find any problems in the new system by validating the results of the new system with the results of the old one.

Procedural Controls

Procedural controls are one of the most important set of controls as they are the ones that are placed on the day to day running of the system. Procedural controls are particularly effective in detecting whether a system has been tampered with and so are effective in detecting fraud. Procedural controls are divided into those controls placed on input, output, processing and storage.

Input Controls

These are procedural controls that are placed on the input of data into the system. These controls are:

- Serial numbering of documents
- Validation checks on documents
- Batching documents and checking of batch totals
- authorization procedures

These controls are carried out by the user department. The Data processing depart also then gets the data and put carry out their own controls. These are:

- Vetting of batches to ensure that they are correct

- checks on data conversion methods

These checks are made so that the data that is entered is as accurate and as error free as possible.

Processing Controls

Once that data has been entered into the system and is being processed, the processing controls are used to ensure that the data is processed properly. Processing controls are divided into two categories. These are:

1. Validation tests
2. File checks

The validation checks are made on the data when it is being processed. These checks ensure that the data is processed correctly. Validation checks include

- Check digit verification
- Checks in the size of file and records
- check on mode of the file
- Check on consistency of fields in files
- Range tests on numbers and values
- Hash totals
- Control record checks
- Sequence checks to ensure that records are entered in the right order
- Error logs which contain a record of all errors that have occurred during the processing of the data.
- Transaction logs which contain a record of each transaction that has been made. This provides an audit trail for the auditor. The transaction log would contain where a particular transaction originated and who initiated it.

File checks are the controls to ensure that the integrity of the files that hold the data for the organization remain intact during processing. Some file checks are

- Use of header tables to identify files
- Use of trailer labels to ensure that the record is completely read.
- Arithmetic proof of the validation of certain fields by checking them with other fields in the record.

Output controls

The outputting of processed data also has certain controls. These output controls are used to ensure the completeness, accuracy and timeliness of the output on screen, printed form as well as on storage media. Some output control procedures are

- Initial screening of the output to detect obvious errors
- Output should only be distributed by authorized persons to authorized persons.
- Controls totals on the output should be checked against the control totals of the input to ensure the consistency of data.

- All the documents produced should be numbered and accounted for
- Highly sensitive materials should not be seen by the general data processing staff but should be outputted to a secure location.
- A feedback system must be developed between the users and the data processing department so that any errors that occur would be reported and subsequently corrected.

Storage Controls

When data is stored additional controls must be put into place to ensure that the data is stored properly and that the data is not tampered with in any way. These controls ensure that no unauthorized persons would be able to tamper with or destroy the data whether it is intentionally or deliberately. Some of these controls are

- Authorization controls to ensure that only authorized personnel are allowed to make amendments and deletions to the files
- Controls to ensure that amendments and deletions are to be thoroughly documented so that the person who made the amendments can be made accountable for the changes they made.
- Controls to ensure that there are proper facilities for the backup of files. These include ensuring that files are backed up regularly, multiple backup files are kept and that these files are kept at a secure location and are easily retrievable in case of an emergency.
- Controls that would ensure that the data can be recovered in case of disaster. This includes transaction logs of complete system dumps which will make periodic backups of all the transactions that occur within the system.

Conclusion

Computerized accounting systems bring with them a set of new and unique problems. The internal controls that have been put into place for a

manual system to help the internal auditor cannot fully prevent or minimize the possibility of errors or fraud that come with the computerized systems. Therefore the old controls must be modified for the new system and new controls must be put in. Only then can the internal auditor ensure that the number of errors that occur within the system be minimized or even eliminated. As stated in the paper, I categorized internal controls in some specific areas and discussed the functions of accounting information systems in each specific area. As stated in the paper there are many advantages for such systems but the users should be more accurate and cautious when implementing such accounting information systems due to the fact that today big vendors of enterprise resource management systems supply their own softwares and applications and some are not really working.

References:

1. Anderson, Chris. Writing Accounting Procedures for Internal Control, *Bizmanualz*, November 17, 2008.
2. Basset P.H. (1993) Computerised accounts, 3rd Edition, Manchester : NCC Blackwell. 1-85554-205-6.
3. Grudinsku G., Burch J., (1989), Information Systems Theory and Practice, 5th Edition, John Wiley and Sons, Inc. 0-471-61293-6.
4. Rezaee, Zabihollah. *Financial Statement Fraud: Prevention and Detection*. New York: Wiley; 2002.
5. International Organization of Supreme Audit Institutions (INTOSAI): Guidelines for internal control standards (1992).
6. van Creveld, Martin. *The Rise and Decline of the State*. Cambridge University Press. pp. 49. ISBN 0-521-65629-X.

8/22/2012