Lecture 7: Information System Controls

Learning Objectives

1. To understand the control policies, practices, and procedures that are important in computer-based accounting systems.
2. To learn the three functions for internal controls in information systems.
3. To categorize control policies, practices, and procedures by their scope.
4. To describe practices that control the input, processing and output of application systems.

Policies, practices and procedures adopted to prevent or detect errors and irregularities in a computer- based system are ***information system controls***.

Controls by Function

- **Preventing controls** – procedures to preventing errors and irregularities.
- **Detective controls** – procedures to detecting errors and irregularities. These procedures identify errors after they have occurred.
- **Corrective controls** – procedures to correct errors and irregularities after detection.

Controls by Scope

- **General controls** - policies, practices and procedures that prevent or detect errors and irregularities for all accounting system. They affect all transaction cycles and all application systems in each transaction cycle.
- **Applications controls** - policies, practices and procedures affect only a specific application system (such as e.g. the inventory system or cash receipts system).

General Controls

We identify four types of general controls:

1. Data Center Operations Controls

The data center is the segment of the organization that provides computer services to other segments. Data center operations controls include:

Data Backup Procedures

Data backup procedures prevent the loss of data. The backup copy is a duplicate of the original that is stored at a different location. Data backup is made in *batch processing systems, on-line real-time systems* or *local area networks (LAN).*

Contingency Plans

A contingency plan is a formal document that describes procedures to be used should a catastrophe occur at the data center. This plan should *provide adequate insurance coverage, designate alternative locations* for processing and data storage, *identify vital applications* and *assign responsibility* for recovery procedures.

Segregation of Duties

Proper segregation of duties requires that critical functions performed at the data center be separated. These functions are systems analysis and programming, machine operations and data maintenance.

2. System Software Acquisition and Maintenance Controls

These control activities requires highly specialized knowledge and usually people assigned to the data center perform them. Management should assign responsibilities for system software acquisition and maintenance and should implement appropriate policies and procedures over these activities.

Responsibilities

Responsibilities for these activities include network administration, PC technical support, database administration and web administration.

Control Policies and Procedures

Control policies and procedures involve screening personnel for system software maintenance activities, reviewing the acquisition of new system software and establishing software standards.

3. Controls over Access Security

Access controls ensure that all changes to data are authorized. These controls restrict a person's ability to modify data and to gain unauthorized use of computer equipment. Management implements access controls by establishing *segregation of duties*, by requiring *identification and authentication procedures* and by providing *physical security* for computer equipment.

4. Applications System Development and Maintenance Controls

Adequate procedures for system and program changes are preventive controls. An organization should have procedures requiring *formal review and authorization* for any new system. All procedures should have *adequate documentation*. There should be prepared a *plan for adequately testing* each new system and *procedures for authorizing and documenting changes* to existing programs and systems.

Applications Controls

Applications controls affect an individual application, such as the payroll application, sales order entry etc. We identify three ways in which applications controls prevent or detect errors and irregularities:

1. Input Controls

Input controls prevent or detect errors when the system converts data from human-readable to computer-readable form. The forms of input controls are *check digits*, *data validation*, *control totals* and *direct data entry procedures*.

2. Processing Controls

Processing controls monitor the accuracy of accounting data during computer processing. Procedures of processing controls are *sequence checks*, *control totals as run-to-run controls*, *physical file identification* and *programmed controls*.

3. Output Controls

Output controls apply to the output of a computer-based accounting system. They include those policies, practices and procedures that ensure the accuracy of the results of processing. These controls also ensure that only authorized personnel receive the reports produced by an application system.

Lecture 7 - Questions and exercises

Q 7-1: How are the information system controls categorized by:

a) Function

b) Scope?

Q 7-2: What are the contents of contingency plan?

Q 7-3: Distinguish between three kinds of applications control.

Q 7-4: Identify four types of general control.

E 7-1: Categories of controls

For items *a-g* below, identify each control as a general control or an applications control:

a) Parity check.

b) Password.

c) Turnaround document.

d) Daily file dump.

e) Edit check.

f) Software librarian.

g) Sequence check.

The main source:

BOCKHOLDT, J. L. *Accounting Information Systems: transaction processing and controls.* 5th edition, Boston: McGraw Hill Education 1999, ISBN 0-07-116098-1

The supplementary sources:

GELINAS, U. J., DULL, R. B. *Accounting Information Systems.* 8th edition, Mason: Cengage Learning, 2010, ISBN 978-0-324-66380-8

HALL, J. A. *Accounting Information Systems.* 7th edition, Mason: Cengage Learning, 2010, ISBN 978-1-4390-7857-0