Control Activities
(Relevant to AAT Examination Paper 8 – Auditing and Information Systems and PBE Paper III – Auditing and Information Systems)

Karen K.W. Li, School of Accountancy, The Chinese University of Hong Kong

Introduction

When sitting the examination, students are expected to acquire sufficient knowledge in the five components of internal controls, including control environment, risk assessment, control activities, information and communication, and monitoring. Students often mix up control activities and substantive procedures. This article focuses on control activities.

Internal Control

Control Environment			
Risk Assessment	Control Activities	Information and Communication	Monitoring

Hong Kong Standards on Auditing (HKSAs)

HKSA 315 (revised) "Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment"

HKSA 315.12 states that
"The auditor shall obtain an understanding of internal control relevant to the audit."

HKSA 700 "Forming an Opinion and Reporting on Financial Statements"

HKSA 700.26 "Forming an Opinion and Reporting on Financial Statements" requires auditors to include directors' or management's responsibility for the financial statements in the independent auditor's report.
" The directors are responsible for the preparation of financial statements that give a true and fair view in accordance with the Hong Kong Financial Reporting Standard issued by the Hong Kong Institute of Certified Public Accountants and the Hong Kong Companies Ordinance, and for such internal control as the directors determine is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error."

Auditors should be aware of the interrelationship between internal controls and the rest of the audit. They also need to develop skills in identifying control activities at the business process level.

Definition of Control Activities

Control activities are the policies and procedures to help ensure that necessary actions, whether within IT or manual systems, are taken to address risks to the achievement of the entity's objectives. The five control activities at business process level are as follows:

1. Independent checks or reviews on performance (Performance reviews)
2. Physical controls
3. Segregation of duties
4. Proper authorization of transactions
5. Adequate documents and records (Information processing)

The Five Control Activities

1. Independent checks or reviews on performance (Performance reviews)

The need for independent checks arises because internal controls tend to change over time unless there is a mechanism for frequent review. Employees sometimes may forget or intentionally fail to follow procedures, or they may simply be careless. Thus, the work of an employee should be independently verified by another member of personnel.

For example, the senior salesperson prepares the daily sales report at the end of each day. Then, the sales department supervisor checks the accuracy and completeness of the daily sales report by comparing the report to copies of sales invoices for the same day.

Often management carries out reviews on overall performance.

For example, the general manager compares the monthly sales result to budget and prior period performance. When necessary, analysis will be conducted to find out reasons behind any variances.

2. Physical controls

Use of physical precautions is the most effective measure to safeguard assets and records.

For examples:

- Storing inventory in a locked storeroom under the control of a team of competent security guards to guard against theft
- Carrying out periodic checks and counting fixed assets
- Putting important documents away in fire-proof cabinets
- Allowing only authorized personnel to have access to the accounting programs and data files
- Doing regular backups of electronic data and records and storing the backup disks and drives in some other safe locations

3. Segregation of duties

Basically, custody of assets, authorization of transactions and recording-keeping responsibility should be implemented and executed by different personnel.

- **Custody of assets** should be separated from **accounting** to prevent embezzlement.

  For example, when there is no such control, a cashier receives cash from customers and also performs the data entry. The cashier can pocket the cash received and adjust a customer's account by recording a false credit to the account.

- **Authorization of transactions** should be separated from **custody of related assets** to prevent embezzlement.
  For example, when there is no such control, the administration department supervisor can endorse a payment of an invoice and also sign a cheque to make the payment. This supervisor may open a dummy business that sends out a fake invoice to his or her employer company. He or she endorses payment of the fake invoice, signs a payment cheque, and eventually pockets the money as the owner of the fake business.

- Operational responsibilities should be separated from recording-keeping responsibility to ensure unbiased information.
  For example, when there is no such control, the sales department, not the accounting department, prepares sales reports. The sales department may choose to include the next period's sales in the current period so that their performance can be just above the benchmark to get a bonus.

- IT duties should be separated from user departments to ensure reliable information.
  For example, when there is no such control, users of IT may manipulate the information processing and management for their own benefit. Sales personnel may go into the system and lift the credit limit for an unqualified customer. When the sales order is entered, the system compares the order with this customer's credit limit, authorizes the sales, and posts the approved sales in sales journals. The company bears a greater risk that this customer may not be able to settle the outstanding amount in full.

4. **Authorization**

There are two types of proper authorization of transactions: general authorization and specific authorization.

- **General Authorization:**
  Management establishes policies and subordinates are instructed to follow these general guidelines across the board.
  For example, an entity sets a monthly credit limit of $10,000 for all customers. Then, its salespersons will allow customers to purchase on account up to the limit on a monthly basis. They do not need to ask for permission on every credit sales transaction. To be efficient, the computer system can be programmed with this credit limit. Once the sales order is entered, it will be approved.

- **Specific Authorization:**
  Management establishes policies and subordinates are instructed to implement these specific guidelines on a case-by-case basis.
  For example, an entity requires specific authorization on credit sales over the pre-determined credit limit. Then, its salespersons will need to seek management's approval on credit sales transactions over $10,000, or when a customer's outstanding balance exceeds $10,000.

5. Adequate documents and records (Information process)

Effective and user-friendly documents, whether within IT or manual systems, should be

designed and introduced to all users to ensure that all assets and transactions are correctly accounted for.

- All documents such as time cards, invoices, purchases orders and cheques should be pre-numbered to ensure fast location of any of them.
- Necessary documents should be prepared at the time of transaction to ensure completeness of information.
- All documents should be designed for multiple use to ensure that all parties involved will obtain the same information.
- All documents should be constructed to encourage correct preparation. Clear instructions are provided in the document to guide the users to complete the document step by step.

Limitations Faced By Smaller Entities

Confined by limited resources, smaller entities usually cannot implement all control activities at business process level. Segregation of duties is not feasible due to limited personnel. Their documentation is likely informal in nature since their scale or scope of business is limited. It is unrealistic to expect the limited personnel to be highly competent in all aspects concerning the business. They may make mistakes due to misunderstandings, poor or inexperienced judgment, and lack of required knowledge or skills.

Nevertheless, it cannot be definitely concluded that smaller entities are likely to experience a great deal of control deficiencies. The expertise, experience, and business network of an owner-manager is an invaluable and indispensable asset to a smaller entity. In addition normally an owner-manager has a strong will to safeguard and nurture his or her own business. Often the risks of not being able to install and launch all control activities at business process level can be mitigated by the regular and frequent involvement by management or an owner-manager in day-to-day operations.

Conclusion

Good internal control can prevent more defalcations than good auditors find on a timely basis. Auditors are required to obtain an understanding of internal control relevant to the audit. It is essential for auditors to be aware of the interrelationship between internal control and the rest of the audit; hence auditors should acquire sufficient knowledge and experience in order to comprehend the control activities at the business process level.

References

HKSA 315 “Identifying and Assessing the Risk of Material Misstatement through Understanding the Entity and Its Environment”, issued June 2009, revised July 2010, July 2012, December 2012, Hong Kong Institute of Certified Public Accountants

HKSA 700 “Forming an Opinion and Reporting on Financial Statements”, issued September 2009, revised July, October 2010, Hong Kong Institute of Certified Public Accountants