

# Computer assisted audit techniques

Finance



It is very convenient for a CPA to use Computer-Assisted Audit Techniques (CAATs) when auditing a business. CAATs may improve the effectiveness and efficiency of auditing procedures. They may also provide effective test tests of controls and substantive procedures where there are no input documents or a visible audit trail, or where population and sample are very large. The purpose of this Statement is to provide guidance on the use of CAATs. It applies to all uses of CAATs involving a computer of any type or size.

## **Description of Computer Assisted Audit Techniques (CAATs)**

CAATs are computer programs and data the auditor uses as part of the audit procedures to process the data of audit significance contained in an entity's information systems. The data may be transaction data, on which the auditor wishes to perform tests of controls or substantive procedures, or they may be other kinds of data. For example, details of the application of some general controls may be in the form of text or other files by applications that are not part of the accounting system. The auditor can use CAATs to review those files to gain evidence of the existence and operation of those controls.

### **Considerations in the use of CAATs**

- The IT Knowledge, Expertise and Experience of the Audit Team  
According to PSA 401 " Auditing in a Computer Information SystemsEnvironment" deals with the level of skill and competence the audit team needs to conduct an audit in an IT environment.
- The audit team should have sufficient knowledge to plan, execute and use the results of the particular CAAT adopted. The level of knowledge

required depends on the complexity and nature of the CAAT and of the entity's information system.

- The Availability of CAATs and Suitable Computer Facilities and Data

The auditor may plan to use the other computer facilities when the use of CAATs on an entity's computer is uneconomical or impractical.

- Impracticability of Manual Test

Some audit procedure may not be possible to perform manually because they rely on complex processing or involve amounts of data that would overwhelm any manual procedure. In addition, many computer information systems perform tasks for which no hard copy evidence is available and therefore, it may be impracticable for the auditor to perform tests manually.

- Effectiveness and Efficiency

The effectiveness and efficiency of auditing procedures may be improved by using CAATs to obtain and evaluate audit evidence.

- Timing

Certain data, such as transaction details, are often kept for only a short time, and may not be available in machine-readable form by the time the auditor wants them. Thus, the auditor will need to make arrangements for the retention of data required, or may need to alter the timing of the work that requires such data.

### **Using CAATs**

The major steps to be undertaken by the auditor in the application of a CAAT are to:

- a. Set the objective of the CAAT application

- b. Determine the content and accessibility
- c. Identify the specific files or database to be examined
- d. Understand the relationship between the data tables where a database is to be examined
- e. Define the specific tests or procedures and related transactions and balances affected
- f. Define the output requirements
- g. Arrange with the user and IT departments, if appropriate, for copies of the relevant files or database tables to be made at the appropriate cutoff date and time
- h. Identify the personnel who may participate in the design and application of the CAAT
- i. Refine the estimates of costs and benefits
- j. Ensure that the use of CAATs is properly controlled and documented
- k. Arrange the administrative activities, including the necessary skills and computer facilities
- l. Reconcile data to be used for the CAAT with the accounting records
- m. Execute the CAAT application; and
- n. Evaluate the results.

### **Using CAATs in Small Entity IT Environment**

Great emphasis on tests of details of transactions and balances and analytic review procedures, which may increase the effectiveness of certain CAATs, particularly audit software.

Where smaller volumes of data are processed, manual methods may be more cost effective. A small entity may not be able to provide adequate

technical assistance to the auditor, making the use of CAATs impracticable. Certain audit package or generalized audit software may not operate small computers, thus restricting the auditor's choice of CAATs.

### **Computer-Assisted Audit Techniques (CAATs)**

- Audit Productivity Software

Are tools used by auditors that facilitate their productivity by automating the auditing function and lessen the amount of time they spend on other administrative tasks. These tools include electronic working paper, groupware, engagement management, reference libraries and document management.

- Generalized Audit Software Tool

Is the tool use by the auditors to automate different audit task. Design to read, process and write data with the aid of functions performing specific audit routines and with self-made macros.

- Testing Computer Application Controls

Two General Approaches - Black box (around the computer) approach

- White box (through the computer) approach

- Black box approach

Auditors do not just rely on a detailed knowledge of the application's internal logic. Instead, they seek to know the functional characteristics of the application by analyzing flowcharts and interviewing knowledgeable personnel in the client's organization.

- White box approach

Relies on an in-depth knowledge of the internal logic of the application being tested.

### **COMMON TYPES OF TESTS OF CONTROLS**

- Authenticity tests – which verify that an individual, a programmed procedure, or a message attempting to access a system is authentic.
- Accuracy tests – which ensure that the system processes only data values that conform to specified tolerances.
- Completeness tests – identify missing data within a single record and entire records missing from a batch.
- Redundancy tests – determine that an application processes each record only once.
- Access tests – which ensure that the application prevents authorized users from unauthorized access to data.
- Audit trail tests – which ensure that the application creates an adequate audit trail.
- Rounding error tests – verify the correctness of rounding procedures.

### **Computer-Aided Audit Tools and Techniques for Testing**

- a. Test data method – is used to established application integrity by processing specially prepared sets of input data through production applications that are under review.
- b. Integrated test facility approach is an automated technique that enables the auditor to test an application's logic and controls during its normal operation.
- c. Parallel simulation – requires the auditor to write a program that simulates key features or processes of the application under review.

### **Continuous Auditing Techniques**

- Binary check – determine whether a control is working effectively.  
Example is the inventory count.
- Outlier – is a numerical value that is significantly different than one might expect.
- Trends – analysis software to identify trends.

### **Electronic Commerce—Effect on the Audit of Financial Statements**

The purpose of this Philippine Auditing Practice Statement is to give guidance to assist auditors of financial statements where an entity engages in commercial activity that takes place by means of connected computers over a public network. The purpose of the auditor's consideration is not to make an opinion or provide consulting services regarding the entity's e-commerce systems.

The internet refers to the worldwide network of computer networks that is nowadays very useful to the public. It is a shared public network that enables communication with other entities and individuals around the world making the world smaller for everybody. There is some risk that is inevitable when using public network that the auditor must know.

### **Skills and Knowledge**

It is important that the auditor has the skills and knowledge to perform the audit. He is also responsible to ensure that the IT personnel is suited to have business knowledge to perform the audit. They must know the what to affect the financial statements like the entity's strategy and activities, technology applied and risks that can affect the business.

**Knowledge of the Business**

The auditor must acquire knowledge of the business enough to enable the auditor to identify and understand the events, transactions, and practices that may have a significant effect on the financial statements or on the audit report. Knowledge of the business includes a general knowledge of the economy and the industry within which the entity operates. The growth of the e-commerce may have a big effect on the entity's traditional business environment.

**Risk Identification**

It is inevitable for a management to face risks relating to the business activities of the company like; loss of transaction integrity; pervasive e-commerce security risk; system availability risk; loss of information privacy; improper accounting policies; noncompliance with taxation and other legal regulatory requirements; over reliance on e-commerce when placing significant business systems; and systems and infrastructure failures or crashes.

**Internal Control Considerations**

Internal controls can be used to alleviate many of the risks associated with e-commerce activities. In accordance with PSA 400, " Risk Assessments and Internal Control," the auditor regards the control environment and control procedures the entity has applied to its e-commerce activities to the extent they are relevant to the financial statement assertions. As well as addressing security, transaction integrity, and process alignment.



### **The Effect of Electronic Records on Audit Evidence**

Electronic records of evidence can be easily destroyed or altered and there may not be any proper records for business transaction. The auditor accounts whether the entity's security of information policies, and security controls as implemented are sufficient to prevent unauthorized changes to the accounting system or records. The auditor may test automated controls to check the record integrity, digital signatures, electronic date stamps and the likes. Depending on his assessment whether to perform additional procedures or not.

### **IT Risk and Controls**

1. Identifying IT Risk – It is important to identify risks to your IT systems and data, to reduce or manage those risks, and to develop a response plan in the event of an IT crisis. IT risks include:

- Hardware and software failure- like power loss or data corruption
- Malware – malicious software designed to disrupt computer operation
- Viruses – computer code that can copy itself and scatter from one computer to another, often disrupting computer operations
- Spam, scam and phishing – unsolicited email that seeks to trick people into revealing personal details or buying fraudulent goods
- Human Error – incorrect data processing, careless data disposal, or accident opening of infected email attachments.

### **Identifying IT Controls**

They are specific activities performed by a person or system that have been designed to prevent or detect the occurrence of a risk that could threaten

your information technology infrastructure and supported business applications. The two broad categories of IT controls are; general controls and application controls. Examples of general controls are strong password policy and encryption of mobile devices. Example of application control is anomaly detection system.

### **Documenting IT Controls**

When documenting IT controls, it should include a particular description of the particular controls tested, the process used to test the controls, the number of times each control will be tested, the system used to pick the items selected, list of the item chosen, list of any exceptions, their causes and implications, and any modification or changes to our strategy resulting from our tests.

### **Monitoring IT Risks and Controls**

Is the process for tracking pinpointed risks, monitoring excess risks, identifying recent risks, play risk response plans and evaluating their effectiveness throughout the project life cycle. It is very important not only for the auditors but also for the management together with the IT controller to monitor the risks and controls that will be applied to lessen the possible future outcome that can harm the business.