1997

Information technology age : evidential matter in the electronic environment; Auditing procedure study;

American Institute of Certified Public Accountants

Auditing
Procedure
Study

AICPA

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

The Information Technology Age: Evidential Matter in the Electronic Environment

Auditing
Procedure
Study

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

The Information Technology Age: Evidential Matter in the Electronic Environment

ISBN 0–87051–182–3

1 2 3 4 5 6 7 8 9 0 AAS 9 9 8 7

Contents

Foreword

This study provides guidance to auditors in applying Statement on Auditing Standards (SAS) No. 31, *Evidential Matter,* as amended by SAS No. 80, *Amendment to SAS No. 31,* Evidential Matter, in the audit of the financial statements of an entity where significant information is transmitted, processed, maintained, or accessed electronically. It is part of the Auditing Procedure Study series of the American Institute of Certified Public Accountants (AICPA). It was prepared by the following members of the 1996 Electronic Evidence Task Force of the Auditing Standards Board:

James E. Brown, Chair
Joe E. Bolton
Thomas A. Diasio
Mark S. Eckman
Charles J. McElroy
J. Donald Warren, Jr.

AICPA staff support was provided by A. Louise Williamson, Technical Manager, Audit and Attest Standards.

The task force gratefully acknowledges the contributions of former task force members Walter R. Bogan (former Chair) and W. Ronald Walton.

January 1997

Introduction

With the increasing use of information technology in business and accounting, auditors increasingly use audit evidence in electronic form for substantive testing. However, the ability to perform an audit consisting entirely of substantive tests may be either absent or ineffective in electronic environments.

The purpose of this Auditing Procedure Study (APS) is to provide guidance to auditors in applying Statement on Auditing Standards (SAS) No. 80, *Amendment to SAS No. 31*, Evidential Matter, in audits of the financial statements of an entity in which significant information is transmitted, processed, maintained, or accessed electronically. This APS describes electronic evidence and discusses issues of concern to the auditor and illustrates implications of electronic evidence and possible audit approaches.

This APS does not attempt to address the wide variety of circumstances auditors may encounter if an entity uses computers and other information technology to transmit, process, maintain, or access accounting data. Rather, it focuses on a set of characteristics that might be encountered in a particular audit. This APS presents two case studies that demonstrate the application of the concepts described herein as well as in SAS No. 80.

RELATIONSHIP TO THE EXISTING LITERATURE

The reader of this APS should be familiar with basic information technology concepts and terminology, and the guidance provided by the following professional standards and other literature.[1]

SAS No. 31, *Evidential Matter* (AICPA, *Professional Standards,* vol. 1, AU sec. 326), as amended by SAS No. 80, *Amendment to SAS No. 31, Evidential Matter*

SAS No. 55, *Consideration of the Internal Control Structure in a Financial Statement Audit* (AICPA, *Professional Standards,* vol. 1, AU sec. 319A), as amended by SAS No. 78, *Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS No. 55* (AICPA, *Professional Standards*, vol. 1, AU sec. 622)

SAS No. 70, *Reports on the Processing of Transactions by Service Organizations* (AICPA, *Professional Standards,* vol. 1, AU sec. 324)

1. To order AICPA products, call: (800) 862–4272 (menu selection #1); write: AICPA Order Department, P.O. Box 2209, Jersey City, NJ 07303–2209; fax: (800) 362–5066.

SAS No. 73, *Using the Work of a Specialist* (AICPA, *Professional Standards,* vol. 1, AU sec. 336)

Statement on Standards for Attestation Engagements (SSAE) No. 2, *Reporting on an Entity's Internal Control Structure Over Financial Reporting* (AICPA, *Professional Standards,* vol. 1, AT sec. 400), as amended by SSAE No. 6, *Reporting on an Entity's Internal Control Over Financial Reporting: An Amendment to Statement on Standards for Attestation Engagements No. 2* (AICPA, *Professional Standards,* vol. 1, AT sec. 400)

Auditing Procedures Study, *Auditing With Computers.* New York: American Institute of Certified Public Accountants, 1994.

Auditing Procedures Study, *Auditing in Common Computer Environments.* New York: American Institute of Certified Public Accountants, 1995.

Auditing Procedures Study, *Implementing SAS No. 70,* Reports on the Processing of Transactions by Service Organizations. New York: American Institute of Certified Public Accountants, 1996.

Practice Aid, *Information Security.* New York: American Institute of Certified Public Accountants.

EDI Control, Management and Audit Issues. New York: American Institute of Certified Public Accountants.

Chapter 1

Understanding the Electronic Environment

Use of computers and other information technology has become pervasive in today's business environment. Auditors must remain aware of the related control issues and their impact on audit risk.

Information systems continue to have a greater impact on business processes, on the initiation and processing of accounting transactions, and, therefore, on auditing. Auditors must keep pace with these developments. The employment of information technology often requires the auditor to use electronic evidence to reduce audit risk to an acceptably low level. Such use raises issues and questions regarding the validity, completeness, and integrity of the evidence.

Auditors may have limited guidance about the use of electronic evidence. Information systems training and education often do not address the concepts of audit evidence in an electronic environment. Key auditing and internal control concepts, such as the segregation of duties, information security, and techniques for error correction, may not be adequately addressed or may not be given appropriate emphasis in terms of their effect on the competence of evidential matter.

This APS defines electronic evidence, compares traditional and electronic evidence in the context of six desired attributes of audit evidence, and highlights issues and related recommendations concerning the auditor and electronic evidence.

DEFINITION OF ELECTRONIC EVIDENCE

The third standard of fieldwork requires an auditor to obtain sufficient competent evidential matter to afford a reasonable basis for an opinion regarding the financial statements under audit. Statement on Auditing Standards (SAS) No. 31, *Evidential Matter* (AICPA, *Professional Standards,* vol. 1, AU sec. 326),

explains that evidential matter consists of the underlying accounting data and all corroborating information available to the auditor. In the broadest terms, four basic forms of information—text, data, video, and voice—can become electronic evidence. The intended purpose of electronic evidence does not differ from traditional forms of evidence, but it is distinguished by the need for controls to ensure its validity.

For this APS, the term *electronic evidence* means information transmitted, processed, maintained, or accessed by electronic means (for example, using a computer, scanner, sensor, or magnetic media) and used by an auditor to evaluate financial statement assertions. Many of the issues related to electronic evidence also apply to evidence in the form of computer-printed documents and reports, particularly if there is no independent review or validation of such printed information. If the integrity of evidence contained in computer files is dependent on effective internal control, printing it on paper does not overcome this dependence.

The competence of electronic evidence usually depends on the effectiveness of internal control over its validity and completeness. SAS No. 80 states that, if control risk is assessed at maximum, an auditor who performs only substantive tests of electronic evidence may not be able to obtain sufficient competent evidential matter. If the auditor is unable to obtain sufficient competent evidential matter, SAS No. 58, *Reports on Audited Financial Statements* (AICPA, *Professional Standards,* vol. 1, AU sec. 508), indicates that he or she should qualify or disclaim an opinion due to a scope limitation or withdraw from the engagement.

Information technology can be a source of electronic evidence or simply a repository of traditional evidence. Auditors understand the use of traditional evidence and the interaction of controls, such as a purchase order, with all attachments and approvals. Electronic evidence adds new dimensions for the auditor's consideration, such as the reliability of the system producing and controlling the evidence. Electronic evidence may depend on information technology for its creation, generating multiple output formats (electronic, paper, video, and audio). Electronic evidence can be used to produce "documents" that may be considered traditional evidence (for example, printouts), while traditional evidence can become a source of electronic evidence (for example, printouts used as source documents).

The following example illustrates some of the distinctions between traditional evidence and electronic evidence. A purchase order submitted and processed electronically is electronic evidence. A printout of that purchase order is electronic evidence. Approvals on the face of that printout convert the document to traditional evidence. Entering the approvals into a computer system creates new electronic evidence.

ATTRIBUTES OF AUDIT EVIDENCE

The following sections discuss certain attributes of audit evidence and highlight the differences between traditional and electronic evidence for each.

Difficulty of Alteration

Easily altered evidence lacks credibility and has reduced value to the auditor. Paper evidence is difficult to alter without detection. An auditor has a reasonable likelihood of detecting significant alterations that have been made to paper documents. This quality provides auditors with some assurance that the evidence represents the original information. The ability to alter electronic evidence is tempered by many factors, potentially including the normal operation of the information system. As a result, electronic evidence does not share this predisposition of unaltered information. However, many people perceive that information coming from a computer system is infallible. The intentional or unintentional alteration of electronic evidence can occur at selected points within a system. With effective controls, an auditor might be able to detect certain changes to electronic evidence by performing procedures such as comparing inputs and outputs. However, alterations due to the operation of the system may not be detected, unless specifically designed tests are performed.

Prima Facie Credibility

SAS No. 31, as amended by SAS No. 80, establishes a hierarchy of credibility for evidence. Increased credibility stems from the independence of the source and the auditor's ability to corroborate the evidence.

Paper documents, such as incoming purchase orders, usually have a high degree of credibility. A purchase order transmitted electronically from a customer derives its credibility primarily from the controls within the electronic environment. A fraudulent or altered electronic purchase order exhibits no apparent difference, compared to a valid purchase order, when extracted from the electronic environment of the entity. Without testing the internal control surrounding the electronic evidence (for example, controls over generation, storage, manipulation, and transmission), a lack of credibility may not be recognized by the auditor.

Completeness of Documents

Competent evidence includes the essential terms of the transaction, so an auditor can verify the validity of the transaction. Paper evidence typically includes all of the essential terms of a transaction. It also includes information regarding other parties to the transaction (for example, customer name and address), or preferred shipping methods, on the face of the document. Completeness for paper documents often includes an acknowledgment of data entry and posting. An electronic environment may mask this evidence with codes or by cross-references to other data files that may not be visible to the users of the data. For example, paper purchase orders typically have markings on the face of each document when matched to the appropriate invoice and posted to the purchases ledger. System matching of purchase order records and invoices can take place within an electronic accounts payable system, without being seen by the auditor.

Evidence of Approvals

Approvals integrated into the evidence add to the completeness of the evidence. Paper documents typically show approvals on their face. Incoming purchase orders, for example, may have marketing department price approvals and credit department approvals written on the face of each original document. The same treatment may apply to electronic approvals by integrating approvals into the electronic record. Electronic elements may require additional interpretation. For example, credit department approvals may require a single keystroke at a terminal to record the approving user. However, viewing a screen on a video terminal may not provide visibility of the approval. Without such evidence, an auditor may erroneously conclude that there was no approval.

Ease of Use

Ease of use leads to ease in evaluation and understanding. Auditors use traditional evidence without additional tools or expert analysis. For example, procedures to test cutoff can be easily performed manually by sorting or identifying vouchers based on date. If this information is maintained in electronic form, the auditor may need to request a special report by date and verify the accuracy of this report as appropriate.

Paper requires no special tools to use. Electronic evidence often requires extraction of the desired data by a knowledgeable auditor or a specialist. An internal process, such as a system-generated allocation of costs to inventory, may not be visible to the auditor attempting to trace transactions into an electronic ledger. With the proliferation of programming languages, data extraction tools, and data architectures, a unique procedure may exist for each entity, or even for each application that exists at a particular entity. The auditor may be required to use report writers, software or data-extraction tools, or other systems-based techniques in order to use information in electronic form.

Clarity

Auditors prefer easily understood evidence, allowing consistent interpretation. Competent evidence should allow the same conclusions to be drawn by different auditors performing the same task.

The nature of electronic evidence is not always clear. For example, consider the case of an auditor using electronic data interchange (EDI) purchase order information from an EDI network. EDI networks often provide a confirmation that the transaction was received by the network. With similar record formats and a lack of appropriate internal control over EDI, the auditor might mistake an EDI network transmission confirmation for an order confirmation provided by the vendor.

ISSUES CONCERNING THE AUDITOR AND ELECTRONIC EVIDENCE

Key issues which the auditor might consider because of the differences between traditional and electronic evidence include those discussed in the following sections.

Issue 1 — Electronic Information as Competent Evidential Matter

An auditor may inappropriately rely on electronic evidence without performing procedures to verify the competence of such evidence. This issue does not address the specific procedures used to test data, but rather the scope of procedures necessary to assure the competence of evidence. The validity, completeness, and other attributes of audit evidence need to be specifically considered if such evidence is produced and maintained by a computerized or other information technology system. Also, when using electronic evidence, auditors need to question the appropriateness of the traditional approach of increasing testing if ineffective controls exist, or if assessed control risk is at the maximum level. Without controls and audit procedures that assure competent evidential matter, extended testing procedures may only provide more testing of incompetent evidence.

SAS No. 58, *Reports on Audited Financial Statements* (AICPA, *Professional Standards,* vol. 1, AU sec. 508), indicates that when the auditor is unable to obtain sufficient competent evidential matter, he or she should qualify or disclaim an opinion due to a scope limitation or withdraw from the engagement.

Issue 2 — Presentation of Electronic Evidence

Presentation of the same electronic information can take different forms, at different times. The auditor may inappropriately assume that processing integrity and other controls to ensure consistency of presentation are effective without performing appropriate procedures. For example, a bank can have several similar on-line displays for presentations of a customer account that show total loans outstanding, outstanding consumer loans, outstanding real estate loans, loan payment histories, contingent liabilities, or some combination thereof, all extracted from the same data. Many banks limit the access to these displays so that each area (for example, consumer loans) can only view relevant information. An auditor using this limited presentation may not gain the full picture of the customer record.

An auditor may need to understand how electronic evidence is extracted from the information system. Computer-assisted audit techniques may be particularly useful in testing consistency of presentation.

Issue 3 — Competence of Tools Used to Access Electronic Evidence

An auditor often uses software to extract and evaluate electronic evidence, as well as for related functions such as risk assessment, audit planning, or data accumulation and analysis. Evidence produced for the auditor by software may not be competent due to the functionality of and processing used by the software. This competence issue is further complicated by the unique nature of data extraction for each entity.

As an example, consider the use of a report generator to produce an exception report from a computer file for use by the auditor. The software requires the user to identify the location of each data field in the data record and to provide specific instructions on how each field is to be processed. If the fields are not appropriately defined or the report generator software does not

appropriately process this information, the auditor may draw inappropriate conclusions from the resulting report.

The use of computer-assisted audit techniques expands the ability to analyze data, recognize patterns, and test the assertions contained in the financial statements. When used properly, these tools enhance auditor efficiency and effectiveness.

Issue 4 — Definition of Error

Electronic evidence may provide opportunities for undetected changes, alterations, or inconsistencies that do not exist in paper equivalents, thus increasing audit risk. These errors may occur subtly, with many impediments to detection. Potential errors could range from data transmission errors (for example, loss or alteration of key approval or transaction codes) to deliberate manipulation of data.

Error detection routines, such as a check digit on customer account numbers and techniques to verify the validity of transmitted data, enhance the effectiveness of internal control. Understanding how the entity assures the detection of errors may assist the auditor in identifying and evaluating control activities. To assess the operating effectiveness of these control activities, the auditor may perform tests of controls. For example, the auditor may perform tests of error detection control activities to assess their operating effectiveness. Testing through the information technology used by the entity is more likely to be effective because testing outside that technology may not detect internal routines for overriding error detection controls.

Issue 5 — Embedded or Implied Control Performance

A distinction exists between the detection of errors and embedded or implied control performance. The former addresses changes that occur to the data that are not expected while the later addresses changes to the data that are expected.

Often evidence of control performance does not appear with the transaction information. In this case, alternatives to traditional tests of controls may be needed. For example, consider a transaction in which a comparison of the sale amount to the available credit for a customer occurs as a function of the information system. If the sale does not exceed the limit, the system records the sale without the need for credit approval, and often without evidence on the transaction record. There is no evidence that the control functioned as intended or that the record was tested. This also holds true for the evidence of performance embedded on the electronic record. If the system automatically enters a credit approval on the electronic record, this approval indication alone does not provide the auditor with sufficient assurance that the control functioned as intended. An auditor ordinarily would need to test the operating effectiveness of this control and the application of the embedded credit approval before placing reliance on such evidence.

Issue 6 — Access to Evidence

Auditors require access to information to perform tests. Evidence of transactions such as those that use EDI may exist or be retained for only a short time,

limiting the period for extraction and analysis. A loss of EDI information (such as transmission rejects, transmission confirmations, and network activity) might result in greater reliance on recent transactions, rather than on those occurring throughout the remainder of the audit period. Limited access to or retention of electronic evidence may require auditors to select samples several times during the audit period, rather than at year end.

For example, an entity complies with the demands of a major customer for use of EDI to process transactions beginning six months into the fiscal year, and after the completion of audit planning. An auditor might miss the opportunity to test the transactions, limiting the scope of the audit work. The EDI transactions may not have complete details, and a test for completeness may not be possible. In such circumstances, the auditor generally should perform tests at various times during the audit period.

Chapter 2

Case Study: Ace Company

The following case study presents ways in which an auditor might approach auditing an entity if the electronic environment and the use of information technology significantly affects information and transactions. The audit strategies and related procedures described represent how an auditor might address electronic evidence in the particular engagement. It should be recognized that other approaches may also be appropriate. This case study presumes that the auditor has the appropriate level of training and proficiency needed to perform an audit of Ace Company.

Ace Company is a privately held manufacturer of pet foods for retail sale. Products are manufactured in bulk on a process basis and are packaged in various sizes for sale by various retailers, primarily on a private branding basis. Ace has five manufacturing plants located throughout the United States, each of which is capable of manufacturing the full line of Ace's products. Each of the plants is contiguous to a warehouse and distribution facility. Most products are shipped to customer locations by truck using a combination of the customer's and Ace's vehicles, a determination that is based on the availability of vehicles and back hauls. Ace's purchasing, production planning, accounting, receivable and payable functions are fully computerized and are performed at a centralized location. Shipping and receiving occurs at each plant and warehouse. The nature of Ace's products makes it necessary to make commitments for the purchase of various grains and other commodities far in advance of the time customer purchase requests or commitments are received.

A substantial majority of Ace's sales are to two customers. Each of these customers has warehouses and retail outlets throughout the United States and sells Ace's products in all of these outlets. The customers are able to give Ace forecasts of their projected needs for Ace products approximately one month in advance of the time the product must actually be at the retail outlet. However, the customer does not inform Ace of the actual quantities needed until about three days before delivery.

All communications between Ace and one of the customers occur via electronic data interchange (EDI). Most communications between Ace and the other customer also occur using EDI and are expected to occur entirely via

EDI at some point during the current year. The customer's planned sales data and inventory stocks are determined by Ace personnel by accessing the customer's internal databases. Ace then enters this information into its production planning and purchasing databases, which are used to schedule production and raw materials purchases.

Approximate quantities of each product needed are transmitted to Ace by the customer using EDI a week in advance, and Ace adjusts its production schedules using this data. The customer transmits actual delivery requirements and customer vehicle availability information to Ace via EDI about three days in advance. Ace then schedules deliveries using the information supplied by the customer and data Ace maintains about the availability of its own vehicles. Communications go back and forth between Ace and the customer on delivery schedules and mechanisms until agreement is reached. Delivery schedules are then transmitted to each warehouse of Ace and to each retail outlet of the customer.

Based on this information, goods are accumulated and shipped from Ace to the customer. Goods shipped are entered into Ace's shipping and accounting systems and at the same time are transmitted to the customer's receiving system using EDI. At this time, an invoice is also prepared and transmitted to the customer by EDI. The invoice is maintained in Ace's receivable system as unbilled until such time as receipt by the customer is indicated.

If the goods are received by the customer, each retail outlet enters receipt into the EDI system and this information is automatically transmitted to Ace. Procedures are in place to separately track and resolve any disputed goods shipped and not received or received in unacceptable condition. The unbilled invoice, which had been stored, is then adjusted for any changes in quantities and prices, billed and transmitted to the customer using EDI.

The customer compares the billings received with the receiving information transmitted to its central office by each retail outlet and to shipping records of its own vehicles and those of Ace vehicles, which it accesses from Ace's data files using EDI. Any discrepancies are resolved by either EDI or telephonic communication and each billing is approved for payment.

Payments are made electronically by the customer and are transmitted to Ace's financial institution for credit to Ace's account using EDI. At the same time, an electronic message about the payment is sent to Ace via EDI. Receipt of the payment is also verified by an EDI communication directly from the financial institution to Ace. Ace's receivable and accounting system then records the cash receipt automatically.

Ace personnel periodically review open billings and unbilled shipping indicators using Ace's computer to access the data files. Currently, Ace reconciles its bank account monthly by manually using a conventional bank statement without returned items. It is anticipated that, within the next year, the bank statement will be transmitted from the financial institution to Ace using EDI.

No paper copies are generated as part of any of these processes although the capability to do so exists at a particular point in time. Nevertheless, there is no ability to reproduce, with any assurance of accuracy or authenticity, on paper what a file looked like before it was updated or revised. The customer also operates in a paperless environment and is unable to confirm anything other than the open amounts shown in its computer system as being currently payable at any point in time. Computer files are backed up continuously.

Approximately three months' data are available in the computer systems of Ace and the customers at any point in time. After about three months have elapsed, the data are erased unless they pertain to transactions not yet settled or in dispute.

The major reasons for the extensive use of data processing and EDI for conducting business in this manner are the following:

- Ease of access to each other's information
- Convenience of communication and revision of data by the personnel of Ace and the customers

Both Ace and its customers believe that a paper trail is unnecessary and would negate the major advantages of the system. Each is concerned about proper controls but will not focus on the details of such controls until after the mechanism is fully developed and has operated for a reasonable period of time, which is anticipated to be about two years.

AUDIT IMPLICATIONS

In reviewing the case study, it is important to consider the six issues facing the auditor that are addressed in this APS. Based on a review of those issues, several implications need to be considered. First, Ace's two biggest customers (meaning trading partners) use EDI, and one used EDI for a portion of the year being audited. This consideration would affect the timing and extent of the auditor's internal control procedures and potentially the nature and extent of the substantive audit procedures to be performed. The auditor would want to further clarify if Ace and the one trading partner switched to full EDI processing of sales and purchase transactions to determine how to best accomplish the controls evaluation and substantive test procedures. Second, it appears that Ace may use the contractual services of a third-party provider of electronic mail storage and message forwarding services, and the mechanics of such a process would need further clarification.

Nevertheless, the auditor should gain an understanding of the EDI process and determine whether such a third-party value added network (VAN) provider was employed to facilitate the storing and transfer of electronic messages between Ace and its trading partners. If a VAN provider was used to facilitate EDI, the auditor may be able to rely on another auditor's report to address the sufficiency of the VAN service provider's internal control structure policies and procedures and whether these were placed into operation and operating effectively during the period covered by Ace's financial statements. SAS No. 70 should be consulted in such situations. There may be legal and audit issues concerning the nature of the trading activities between Ace and its trading partners that should have been addressed or defined in trading agreements and contracts. These contracts should be consulted and understood if they are available from or through the entity.

In summary, audit implications and potential issues relate to the competence of the evidence, the tools needed to access the evidence, and the nature

of any programmed (embedded) control procedures in use that may be relied upon that affect the competence of the electronic evidence and Ace's internal control process.

AUDIT APPROACH NUMBER 1

Since Ace's accounting processes are highly automated, the auditor has to obtain assurance that the programmed procedures are operating as prescribed. This can be accomplished using one or more of the following methodologies.

- Perform tests of controls to establish whether information technology (IT) and application controls are operating effectively.
- Perform a detailed preimplementation review of the system before it is placed in operation. The purpose of this review would be to perform the necessary procedures to ensure that the system processes as prescribed. Audit procedures may include reviewing the effectiveness of the following:
  - The system design (to ensure that appropriate controls are built in)
  - Software change management process
  - Testing strategies (to determine whether the system was adequately tested to ensure that it functions as prescribed)
  - User sign-off procedures
- Substantively test the information generated by the system (for example, to reperform the accounts receivable aging to ensure that it is complete and accurate).

Whether the system in use is a package or was developed in-house is also relevant. If the system is a package, assuming the entity has not modified it, inherent and control risk may be less than if the system was developed in-house.

IT Controls

After the system is live, it will become necessary to assess the effectiveness of the IT controls to obtain assurance that the system is continuing to process as prescribed. Generally, such an assessment would include consideration of computer operations, program change management, and information security controls for significant applications.

Application Controls

The following sections provide a brief description of key system activities and possible audit procedures.

Purchasing and Accounts Payable

The auditor may wish to examine the controls for purchasing and accounts payable.

- Similar to reviewing any purchasing cycle, an understanding of the controls in place over the purchasing cycle should be obtained, and substantive testing procedures should be performed to ensure that liabilities are completely and accurately stated; for example, the search for unrecorded liabilities.
- In terms of controls, it should be determined whether management has adequate monitoring controls in place to ensure that all purchases are properly authorized. If the system is truly paperless, determine whether system functionality is in place for management to evidence their approval of reports on-line. The system may require certain levels of management approval, based on predefined thresholds, for example, all purchases over $10,000, that must be approved by a supervisor. If authorization for purchases is performed on-line, application security should be tested to ensure that the system enforces proper segregation of duties.

Revenue

The auditor may wish to consider controls over the revenue, including the following.

- Due to the time lag between forecasted revenue (one month) versus actual purchases (three days), forecasted revenue may not match actual revenue. Analytical or other procedures to test the accuracy of forecasted revenue ordinarily should be performed.
- The integrity of the EDI transmission process is critical for Ace. The input and output controls over this process ordinarily should be reviewed, including the following.
  - Determine whether Ace uses an EDI VAN and what controls are in place.
  - Review computer operations controls over receiving and processing EDI transmissions.
  - Review the controls in place to ensure the completeness and accuracy of each EDI transmission, for example, the use of header and trailer records that indicate the number of records contained in each transmission and the total dollar value.
  - Review the controls in place to ensure the completeness and timeliness of input, for example, controls to prevent the loss of files in transmission to ensure the timeliness of data.
  - Review the controls in place to manage and monitor specific records that cannot be processed from the EDI transmissions. This would include reviewing the controls over error or suspense files to ensure that errors are dealt with completely, in a timely manner, and that their root causes are identified and addressed.
- For EDI transmissions sent from Ace, review the controls in place to ensure that transmissions received by other parties are complete and accurate. This could include receiving positive confirmation of the successful receipt of transmissions. Additionally, Ace transmissions

should include methods to determine completeness, accuracy, and timeliness, as described above.

- Review the controls in place for reconciling unbilled receivables to goods shipped to customers on a regular basis. If the system does this automatically, it may produce a report that is reviewed regularly by management to follow up on any exceptions. For example, the system might report on an exception basis items that have been unbilled for certain periods (for example, 30 to 60 days, or 60 to 90 days) so they can be followed up on.
- Review the controls over the collection of outstanding receivables after the actual invoices are transmitted via EDI.
- Review the controls in place for reconciling receipt of payments per the bank to what the customers indicate that they paid (per EDI).
- Confirm accounts receivable.

AUDIT APPROACH NUMBER 2

Once the auditor develops an audit strategy, and defines the level of control risk that is acceptable, the auditor should develop an overall approach to performing the audit considering the nature of the transactions employed by Ace and its trading partners. The audit approach should include initial procedures for developing an understanding of the entire process of initiating and executing transactions between Ace and its trading partners, including the possible use of a third-party VAN service provider. If a third-party VAN is used, the auditor should inquire about and obtain a copy of any relevant service auditor's report regarding the VAN provider's internal control. In addition, the auditor may need to gain access to electronic evidence during the year to be audited and not just at year end. Gaining access to this evidence may require the auditor to communicate with the VAN provider.

The auditor should assess the overall control environment of Ace and the ongoing monitoring procedures Ace's financial and information systems staff perform regarding the electronic transactions. In addition, the auditor should document the general information technology and application control activities that influence the EDI process. In assessing the adequacy of the internal control over Ace's EDI business process, the auditor should understand how the EDI process is reflected in Ace's accounting records and in both internal and external reports.

Specifically, the auditor should document the input, processing, and output (meaning, financial reporting) controls affecting Ace's initiation and execution of electronic transactions. The manner in which the following are met through existing control mechanisms (meaning, control activities) should be documented and evaluated:

- The control objectives of authorization, completeness and accuracy of input
- The integrity of standing data
- The completeness and accuracy of updating accounts, completeness and accuracy of accumulated data

- The access to electronic data and records

As the control activities that affect the achievement of the control objectives are documented, the auditor should determine the nature and type of electronic evidence that may be available to corroborate the understanding of Ace's control activities.

As the auditor documents and considers the internal control, consideration should be given to the methods necessary for obtaining the electronic evidence. The auditor may use a specialist trained in extracting data from information systems to gather the audit evidence. Whether the auditor extracts the data or uses a specialist for that purpose, it is important that the data extraction process also have credibility and integrity. If a data extraction program is used, the auditor should have sufficient proof that the correct data (meaning, standing and accumulated data) was accessed from which test data could be extracted.

The auditor would perform tests of controls to support any further desired reduction in the assessed level of control risk. Substantive tests, consisting of tests of details, analytical procedures, or both, should be performed to reduce detection risk to an acceptably low level.

Chapter 3

Case Study: Thompson, Inc.

The following case study presents ways in which an auditor might approach auditing an entity where the electronic environment and the use of information technology significantly affects information and transactions. The audit strategies and related procedures described represent how an auditor might address electronic evidence in the particular engagement. It should be recognized that other approaches may also be appropriate. This case study presumes that the auditor has the appropriate level of training and proficiency needed to perform an audit of Thompson, Inc.

Thompson, Inc. is a large retailer with approximately eight hundred stores located throughout the United States. Each employee is assigned an encoded identification badge that is only to be used by that individual. When an employee arrives for work, he or she runs the badge through an electronic reader that records the time of arrival. The procedure is repeated by the employee when he or she leaves work for the day. Employees are required to remain on duty at all times during their shifts.

Information gathered by the badge reader is transmitted electronically to Thompson's central office computer on a weekly basis. This computer updates the payroll files and computes and prepares weekly payroll that is subject to review and authorization electronically by Thompson's payroll section chief. After authorization, the payroll is transmitted to each employee's bank account by direct deposit using electronic funds transfer. A printout showing the payroll computation and year-to-date information is prepared and mailed to each employee by the payroll department. Employees are requested to report all suspected errors to the payroll department. Store managers can access payroll information for their location using their computer terminal. Payroll is also reflected in the monthly store profit and loss report received by each manager and regional supervisor.

During the current year, Thompson determined that the electronic funds transfer system was too inhibiting to its employees and changed its system to

smart cards[2] issued by its bank. Under the smart card system, an employee swipes his or her card through the badge reader at their store location to refill the debit function of the card with the net pay amount. The system verifies that the smart card is assigned to an employee who works at that particular store. Employees are not required to provide identification to their assigned cards. The amounts added to smart cards are transmitted electronically from the badge readers to Thompson's computer daily. The computer then totals the amounts and transmits the total electronically to Thompson's financial institution, which charges that sum to Thompson's account and credits the information to each employee's smart card available funds files.

Thompson utilizes its independent auditor only for the audit of its financial statements. All of its systems designs and changes therein are made by its own staff, which is monitored by its internal audit function.

AUDIT IMPLICATIONS

The auditor should be familiar with issues concerning the auditor and electronic evidence presented in this APS. The audit implications in the Thompson case are related to the authentication of employees who use identification badges to record attendance, and the validity of the time reported for each employee by "swiping" an identification badge during each workday. Changes or errors may occur electronically and not be detected.

There are also several implications related to embedded or implied control performance. Timing and cutoff issues may arise if employees initiate transactions close to or immediately before or after the end of a period. Because of the electronic interface between Thompson and its financial institution, the auditor should be aware of and understand the process of transmitting electronic messages between these parties. Because Thompson depends on IT controls, the auditor should be knowledgeable about how IT and application controls impact significant applications.

AUDIT APPROACH NUMBER 1

Audit approach number 1 entails the following procedures.

- Review controls in place to ensure that data is transmitted completely and accurately between the store and the central computer.
- Review controls over payroll authorization and approval.
- Review controls in place to ensure that transmissions to the bank are complete, accurate, and timely.
- Review controls in place to determine whether store payroll is being effectively monitored by budgetary comparison or other means.

2. A smart card is a card with a built-in microprocessor and memory used for identification or financial transactions. When inserted into a reader, it transfers data to and from a central computer. As a financial transaction card, it can store transactions and maintain a balance.

- Review controls in place to ensure that the database is complete and accurate with respect to employee assignment and other information.
- Determine whether the payroll system is completely and accurately updated when employees collect their pay using the smart card.
- Perform procedures to ensure that when employees terminate, the system is updated and the smart cards are revoked.
- Review controls in place to ensure that data is transmitted completely and accurately between the central computers and the financial institution.
- Perform a reconciliation of Thompson's bank account, including the smart card file.

AUDIT APPROACH NUMBER 2

Ascertain the nature of the electronic evidence and determine its availability or accessibility. In documenting the understanding of Thompson's internal control, the auditor should describe how electronic transactions are created and identify the processes that collect, process, and report such transactions throughout the periodic accounting and reporting cycle. The auditor's assessment of control risk will be influenced by the nature of the implied and embedded (programmed) control procedures. The assessment would also be supported by tests of controls that the auditor believes are warranted under the circumstances.

The auditor should understand Thompson's computer program maintenance (change management) procedures and any related controls. The auditor should also understand the control mechanisms (both embedded and implied) over access to Thompson's account at the financial institution.

The auditor should determine how Thompson's electronic records will be accessed. In addition, consideration should be given to how any technology issues may be overcome by, for example, using software extraction tools. The auditor should also determine whether it will be necessary to use the work of a specialist.

The auditor would perform tests of controls to support any further desired reduction in the assessed level of control risk. Substantive tests, consisting of tests of details, analytical procedures, or both, should be performed to reduce detection risk to an acceptably low level.