Mapping Internal Controls Using System Documentation Tools

Yan Xiong, (Email: xiongy@csus.edu), California State University, Sacramento
Merle Martin, (Email: martinm@csus.edu), California State University, Sacramento

ABSTRACT

The 2002 Sarbanes-Oxley Act requires managers to assess and attest to the internal financial controls and the IT controls within the firm. Therefore, documenting and assessing internal financial controls and IT controls has become an important and necessary task for auditors and management. This paper provides an approach for developing an internal control map using data flow diagrams. The internal control map can be used by external or internal auditors to evaluate a system's internal controls in general and also to find internal control deficiencies in the system.

INTRODUCTION

Following several high profile accounting scandals, the U.S. Congress passed the Sarbanes-Oxley (SOX) Act in 2002. One of the key provisions of this law is found in section 404, which introduces a requirement for publicly traded companies to include in their financial statements a report on the their systems of internal control for financial reporting and the effectiveness of their operation. That is, management must attest to the effectiveness and completeness of the internal control structure within the firm.

As computerization of accounting information systems continues to accelerates, the accounting profession is undergoing radical change as it strives to provide value in today's automated society. The SAS No. 94 issued in 2001 provides guidance to auditors about the effect of information technology on internal control. Especially, the statement describes benefits and risks of information technology (IT) to internal control and how IT affects the components of internal control (SAS No. 94, 2001).

To comply with Sarbanes-Oxley Section 404 requirements and SAS No. 94, auditors and managers must assess internal financial controls and IT controls. To assess internal financial controls, business processes associated with financial reporting need to be identified and documented. In addition, IT processes and controls must be documented because many companies depend on IT to process their financial information. Therefore, this paper illustrates how to develop an internal control map of an AIS using system documentation tools. Auditors can use the internal control map to examine the internal controls in general and individual business processes as well. The internal control map can be used to evaluate internal controls in general and also to find internal control "holes" by comparing where they should be as compared to where they are. Finally, this paper provides a case to demonstrate how to map internal controls using a system documentation tool.

This paper contributes to the accounting and IT professions as follows. First, the Public Company Accounting Oversight Board (PCAOB) indicated that it would be strict in monitoring external auditing firms' approach to examining and reporting on the technological aspects of their corporate clients' financial reporting processes (Krell 2004).

This paper provides an approach for developing an internal control map using system documentation tools. The internal control map can be used by external auditors or internal auditors to evaluate a system's internal controls in general and also find internal control deficiencies in the system.

Second, we tend to teach documentation techniques in an accounting information system (AIS) class as a reactive tool in system development. Students often are uninspired by this approach and may wonder why narrative documentation will not suffice. Once we have covered the early documentation chapter(s) in an AIS textbook, we may not revisit the subject through the remainder of the course. This paper provides an approach by which documentation tools can be taught in an AIS course to develop a map to facilitate learning of other course topics such as internal controls, fraud detection, auditing, procedures writing and reengineering. Finally, use of different documentation tools working in concert is common in industry and can enhance the delivery of an AIS course.

In the next section, we present an overview of both the internal financial controls and the IT controls that are to be attested to by management in compliance of the Sarbanes-Oxley Act and SAS No. 94. It describes the steps that are performed by auditors and managers to evaluate internal controls. Section three provides an overview of the system documentation. It focuses on two different system documentation tools that we use to evaluate internal controls: the REA Diagram and the Data Flow Diagram (hereafter DFD). Section 4 discusses how to prepare an internal control map using the data flow diagram while section 5 use the California State Parks case to illustrate how to develop the internal controls map using the DFD. Summary and conclusions are discussed in the final section.

INTERNAL CONTROLS

Internal controls are policies, plans, and procedures implemented by a firm to achieve three objectives: to ensure the efficiency and effectiveness of operations, to protect the assets of the organization, and to comply with applicable laws and regulations (Hall 2001). In the midst of rising concerns about accounting scandals, the 2002 Sarbanes-Oxley Act section 404 requires management to assess and attest to the effectiveness and completeness of the internal control structure. Specifically, Section 404 of SOX requires management to assess and attest to their organization's internal controls over financial reporting in an internal control report that is filed with the annual report. Furthermore, this law makes managers personally liable for the internal control structure within the firm. This act's section also requires that the external auditors report on management's internal control assessment.

With the explosive growth of IT in use, security and control over an organization's information resources is also a major concern for management. Computerized internal controls written by IT professionals are incorporated into computer programs, processes, and procedures. Therefore, the AICPA and other accounting professionals recommend that auditors acquire necessary knowledge on IT to effectively evaluate internal controls (Bagranoff et al. 2004). Accountants do not need to understand exactly how computers process the data of an accounting system, but it is important for them to be able to understand and document how this processing takes place.

To help auditors deal with the control issues surrounding the information technology use, the AICPA issued SAS No. 94 to offer guidance on how IT use in the financial information development process affects the independent audit. Specifically, the statement describes benefits and risks of information technology (IT) to internal control structure and how IT affects the components of internal control (SAS No.94).

In compliance with the Sarbanes-Oxley Act and SAS No.94, auditors and managers must assess the internal financial controls and the IT controls before attesting to them. Internal financial controls include controls on business processes related to financial statement line items, including typical processes such as revenue and expenditures. IT controls include general computer controls, application controls, data transmission controls, and database controls. To assess internal financial controls, auditors need to identify and document the business processes and controls associated with financial reporting. Furthermore, auditors need to document the IT processes and to assess IT controls. Moreover, the Sarbanes-Oxley act requires that financial data must be controlled from their point of origin, so mapping the path of a transaction from its source documents to its presentation on the financial statements is important.

After identifying and documenting all business processes and the controls surrounding these processes, auditors commonly use the risk-based audit approach to assess internal controls. The risk-based audit approach first determines the threats (i.e., errors and irregularities) facing an AIS. It then identifies a set of standard controls that would minimize each threat. Third, it compares these documented existing controls against the set of standard controls

and identifies any deficiencies and remedies for them. Finally, auditors and managers test these controls to verify if they are performing as documented. If this is the case, management can then offer a positive opinion to the control environment.

SYSTEM DOCUMENTATION

Documentation explains how AISs operate and is therefore a vital part of any accounting system (Bagranoff et al. 2004). According to Bagranoff et al. (2004), system documentation describes the tasks for recording accounting data, the procedures that users must perform to operate computer applications, the processing steps that computer systems perform to operate computer application, the processing steps that computer systems follow, and the logical and physical flows of accounting data through the system.

There are many system documentation tools used in practice, such as system flowcharts, data flow diagrams (DFDs), entity-relationship diagrams (ERD), Resource-Entity-Agent diagrams (REAs), and decision tables.

We tend to view systems documentation as a reactive tool used in accounting information system (AIS) development to describe a system that already exists or to document a proposed new system. Yet system documentation tools can be used for proactive, analytical purposes. One common example is the use of systems documentation for procedures compliance purposes (Shneiderman 1987). Separate analysts can use documentation tools to describe differences in procedural (what should be) and observed (what actually happens) information flow. Differences between these flows can indicate that (a) valid procedures are not being followed, (b) procedures are outdated, and (c) additional training may be required. System documentation tools can also serve as a map for possible reengineering efforts (Martin, 1995).

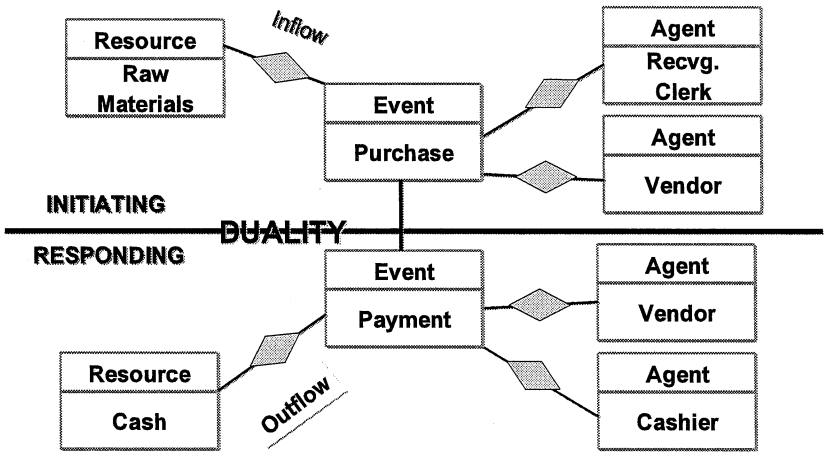
This paper focuses on mapping internal controls using system documentation tools. Specifically, this paper focuses on using REA and DFDs to prepare a Preventive-Detective-Corrective internal control map.

The REA Diagram

One of the most prevalently used documentation tools in AIS is the Resource-Event-Agent (REA) diagram. REA was proposed as a theoretical model for accounting by McCarthy (1982). Rather than focusing on debits and credits, which by design omit important data about economic events, the REA diagram capturing the details about each resource under the firm's control, the events that change the amount of each resource, and the agents who participate in these events (McCarthy 1982). Advances in database technology have now provided renewed attention on the REA as a practical alternative to the traditional accounting framework (Hall 2001).

The REA diagram is a specialized version of the Entity-Relationship-Diagram (ERD). It is ideal for an accounting-oriented topic since it stresses (a) resources that will appear in the balance sheet, (b) events (transactions) that will become journal entries, and (c) internal and external agents who promulgate the event. In addition, the REA diagram stresses the concept of duality which is the framework for the double-entry accounting model. Figure 1 shows the framework for a typical REA diagram.

Figure 1: REA Diagram



The REA diagram has been used for more than designing accounting databases. The REA diagram can be used as a guide to identify internal control opportunities in general for organization. For example, identifying the agents for each transaction or event helps control economic resources. If there is a control problem with a resource, an auditor is able to trace the transactions to employees.

However, note the diamond symbols that separate the resources, events and agents. These represent the "handoffs" which require procedures, computer programs, internal controls, reengineering opportunities, and internal audit targets. These handoff topics represent a large portion of the traditional accounting system. These diamond handoff symbols need further explosion into the detail necessary to tie together the documentation tool with more of the procedures included in the traditional accounting system.

David (1997) expands REA framework by incorporating information events in the REA diagram. The information events are defined as "procedures that are performed in organizations solely to capture, manipulate, or communicate information". This type of event is procedure or method that is used to capture data about the resources, events, and agents, as well as any report generation performed with the data in the system. One example of an information event is preparing customer invoices. However, as David (1997) emphasized in the paper, the REA diagram should not be used to document the information process because the strengths of the REA framework lie in focusing on the most basic elements in a complex organization environment and highlighting activities that consume valuable resources while adding value to organizations.

Thus, the REA diagram is not as amenable to successive refinement of detail as are other documentation tools. Yet, we can couple with the REA another documentation tool to accomplish this explosion. It is common in business to switch tools when audiences are switched. An REA diagram can be used to describe a system to non-technical users and program flow charts can be used later in a project when technical programmers are the intended audience (Martin, 1995). In an education environment such as the AIS classroom, different documentation approaches can be used in different portions of the course to differentiate conceptual from syntactic learning tasks.

We now will switch to Data Flow Diagrams (DFDs) to describe in more detail the diamond symbols shown in an REA diagram. Thus the REA diagram becomes an enterprise or overall system model while the DFD is used to explode parts of the REA diagram into further detail.

The Data Flow Diagram

The Data Flow Diagram (DFD) is one of the most commonly used systems-modeling tools, particularly for systems in which the processes of the system are of more importance and complex than the data that the system manipulates. DFDs provide process-oriented view on systems. DFDs were first introduced in the software engineering field as a notation for studying systems design issues (DeMarco 1978, Gane and Sarson 1979). DFDs were later used for structured analysis and design. DFDs show the flow of data from external entities into the system, showed how the data moved from one process to another, as well as its logical storage.

A Data Flow Diagram is a process-oriented graphical representation of an application system. The DFD is easy for non-technicians to understand because it uses only four symbols. The components of a typical data flow diagram are: the processes, the data flows, the data stores, and the external entities.

A process shows a transformation of inputs into outputs; that is, it shows how inputs are converted into outputs. There is a numbering system for the processes. The process is represented graphically as a circle.

A data flow is used to describe the movement of data or information from one part of the system to another part. Data flows represent the "hand-offs" where fumbles and interceptions can occur. The data flow is represented graphically as an arrow.

A data store is a temporary or permanent repository of data (Romney and Steinbart 2002). Data stores are typically implemented as files or databases in a computerized system; but a data store can also be data stored on punched cards, microfilm, or a variety of other electronic forms. The notation for a data store is two parallel lines.

An external entity sends data to or receives products, services, or information from the AIS. External entities are people or systems that are outside the control of the system being modeled. The external entity is graphically represented as a rectangle.

One unique characteristic associated with DFDs is that they can also be "exploded" in successive levels of increasing detail. Unlike the REA diagram, the DFD has a numbering system that facilitates successive refinement of detail ideally to the programming code level. This feature is very important and useful in analyzing a system detecting deficiencies in a system. The DFD primarily is used as a documentation tool for existing or proposed information systems. It can be used, however, as a powerful analytic tool – as a means to detect AIS deficiencies. The paper describes the DFD as an analytical tool to assess the strength of AIS internal controls.

MAPPING INTERNAL CONTROLS USING DATA FLOW DIAGRAM

As our accounting systems become increasingly more complex, we face growing risks. To assess internal controls in general, we first identify different types of threats and control opportunities for each data flow diagram element in Tables 1 and 2. Table 1 shows the threats and controls faced by external entities and data stores. The threats faced by external entities include identity theft; invalid accounts; difficult customer access; and untimely delivery. The controls used to protect the system against these risks include authentication; outsource input preparation; web-enhanced; firewalls; and data encryption.

Data storage risks include file alteration, destruction, sabotage, disaster, data theft, inaccurate update, and delayed update. The following controls should be implemented to assure the accuracy, integrity, and security of stored data files: prospecting, leveraging data, access control, consolidating files, file recovery plan.

Table 1: External Entity and Data Store Threats and Opportunities

External Entities		Data Stores	
Threats	**Opportunities**	**Threats**	**Opportunities**
- Identity fraud (spoofing) - Invalid accounts - Difficult customer access - Untimely delivery	- Authentication - Outsource input preparation - Web-enhanced - Firewalls - Encryption	- File alteration - Destruction - Sabotage - Disaster - Data theft - Inaccurate update - Delayed update	- Prospecting - Leveraging data - Access control - Consolidating files - File recovery plan

Table 2 presents threats and controls for events and relationships (diamonds). The threats faced by computer or manual processing include program alteration; pilfering (embezzlement); errors; inefficiencies; and redundancies. These problems can be minimized by implementing the following procedures: intelligent agents; outsourcing; consolidation; segregation of duties; program change/ development control; and documentation.

The data flow risks consist of input/output manipulation; interception (sniffing); delayed transmission; and improper routing. These risks can be controlled by implementing the following procedures: electronic fund transfer; data encryption; electronic monitoring; routing verification; even parity bit technique; and message verification techniques.

Table 2: Process and Data Flow Threats and Opportunities

Processes		Data Flows (handoffs)	
Threats	**Opportunities**	**Threats**	**Opportunities**
- Program alteration - Pilfering (embezzlement) - Errors - Inefficiencies - Redundancies	- Intelligent agents - Outsourcing - Consolidation - Segregation - Program change/ development control - Documentation	- Input/output manipulation - Interception (sniffing) - Delayed transmission - Improper routing	- Electronic transfer - Encryption - Electronic monitoring - Routing verification - Even parity bit - Eliminate handoffs - Message verification

Tables 1 and 2 present possible threats and a set of standard control procedures against these risks, which can be a checklist to ensure that an AIS possesses all required controls. Ideally, there should be at least one of each for each task, task hand-off, storage file, and external interface (e.g., customer, vendor).

Next we use the DFDs to map the PDC control model. The PDC model classifies controls into three different categories, including preventive, detective and corrective controls. Preventive controls prevent or deter problems before they arise, detective controls are used to discover problems as soon as they arise, while corrective controls remedy problems detected with detective controls (Romney and Steinbart, 2002).

Table 3 shows the internal control mapping structure. The internal control map is developed in the following sequence:

Table 3: Internal Control Mapping Structure

		Control Type		
Element	**DFD Symbol**	**Preventive**	**Detective**	**Corrective**
Task	**Process**	?	?	?
Task Handoff	**Data Flow**	?	?	?
Storage File	**Data Store**	?	?	?
External Interface	**External Entity**	?	?	?

? Does the current or proposed system have at least one internal control in this cell?

- Study documentation of internal controls
- Label each control sequentially within letter label
- "P" for preventive controls
- "D" for detective controls
- "C" for corrective controls
- Draw level-1 DFD for system by observing system
- Look for DFD elements (e.g., data flow) where controls are missing

In the next section, we use the California State Parks example to demonstrate the development of an internal control map using the DFD.

CALIFORNIA SATE PARKS EXAMPLE

The California Department of Parks and Recreation (DPR) manages over 260 park units, which contain diverse collections of natural, cultural, and recreational resources. DPR's workplace consists of nearly 1.3 million acres, with over 280 miles of coastline; 625 miles of lake and river frontage; nearly 18,000 campsites; and 3,000 miles of hiking, biking, and equestrian trails. During the 1998/1999 fiscal year, DPR collected over $60 million dollars of revenue from the more than 40 million visits. The remainder of the revenue was primarily from commissions on sales from contracted concessionaires. Currently, park ticket and pass revenue collection was done through non-computerized kiosks located at park entrances and staffed by Park Rangers and Park Aids. DPR called for assessing the feasibility of automating revenue collection kiosks located at state park entrances. DPR developed a requirements analysis for a proposed point-of-sale (POS) collection system for the entrance kiosks located at over 150 state parks in 2000.

The new system would work as follows:

1. *Open Shift*: The park aid would measure current park conditions (e.g., temperature, lake level) and enter it to the workstation to update the day's transaction file. Operating parameters (e.g., ticket prices) would be sent over the Internet for each park to use for that day.
2. *Process Park Visitors*: Park visitors would present entry payment or refund requests to the park aid who would enter that data to the system to update the daily transaction file and generate receipts, refunds, or entry tickets. Cash received would be placed in the cash drawer.
3. *Prepare Deposits*: Cash accumulated beyond an established limit would be prepared for deposit in a bank. The daily transaction file would be accessed to reconcile cash collections with the actual amount in the cash drawer. The system would automatically generate a deposit slip.
4. *Close Shift*: At the end of each park's operating day, the system would send the daily transaction file to (a) the district office for archiving (e.g., file recovery), and (b) park headquarters in Sacramento for update of central files and auditing.

The following internal controls were identified in the new system. The controls were classified into the three different types of controls: preventive, detective, and corrective controls.

Preventive Controls:

P1 Replace manual tickets with pre-numbered register receipts containing bolded expiration date.
P2 Control login and log-out processes by park, Ids, and passwords.
P3 Allow only authorized personnel to access subtotals and perform zero-out process for each shift.
P4 For refund procedures, print a receipt with transaction date and original transaction number. The customer has to sign the refund receipt.

Detective Controls:

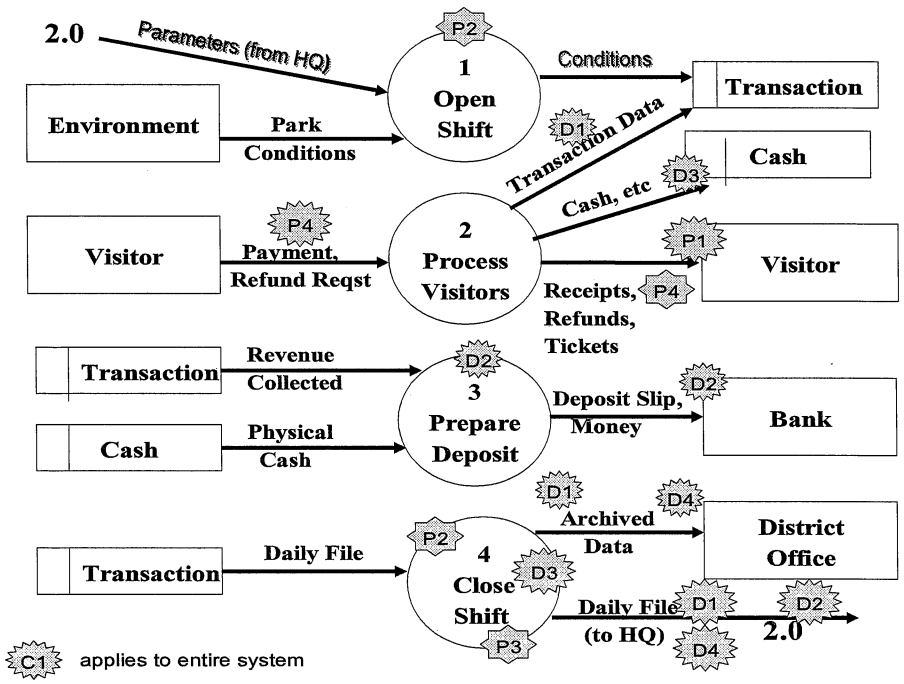
D1 Keep track of essential transaction details for each sale for review purposes,
D2 Generate physical deposit slips and the corresponding electronic records. The physical deposit slips are used to deposit cash to the bank. The electronic records of deposit are uploaded to Sacramento Headquarters for accounting functions. Deposit slips must be linked to relevant sales transactions for a proper audit trail.
D3 For the z-out process (reconciliation of cash and sales) at the end of each shift, the park aid must enter the amount of collected cash *before* the system can be instructed to z-out. The reconciliation process has to be performed at the end of each shift. Any discrepancies are recorded and must be explained.
D4 Generate exception reports by setting different data parameters and audit rules (e.g., if there are more than 5 refund transactions, generate an exception report.)

Corrective Controls:

C1 There is a mirrored manual (backup) system for the automated system.

The internal control labels (e.g., P1-4) have been added to the original requirements analysis description in order to demonstrate internal control mapping. Figure 2 shows a first-level DFD explosion for the parks operation. Each of the above proposed internal controls is shown on this DFD by means of its label (e.g., P2).

Figure 2: Parks Collection System Internal Controls Map



After evaluating the internal control map, the following examples of internal control "holes" have been identified and noted on the DFD:

- *Cash Data Store*: There is no preventive control against cash being stolen (e.g., amount over $XXX deposited or placed in safe). **
- *Visitor Payments*: There are no preventive or detective controls to prevent visitor cash payments to be pocketed and not recorded (e.g., automatic entering car counter).
- *Bad Checks*: There is no preventive control against bad checks being accepted. **
- *Reconciliation*: Revenue transactions and receipts are not reconciled. **
- *File recovery*: There is no corrective action to recover the system when it fails.

Those examples marked with an ** represent internal controls that were included in the proposed systems design, but not in the list of internal controls. These represent incomplete procedures.

SUMMARY AND CONCLUSION

Documentation tools can be used proactively for purposes such as mapping internal controls, fraud detection, auditing, procedures writing and reengineering. This paper is a demonstration of one use of documentation tools as a powerful analytical tool. The 2002 Sarbanes-Oxley Act requires managers to assess and attest to the internal financial controls and IT controls within the firm. Therefore, documenting and assessing internal financial controls and IT controls has become an important and necessary task for auditors and management. This paper provides an approach of developing an internal control map using the data flow diagrams. The internal control map can be used by external or internal auditors to evaluate a system's internal controls in general and also find internal control deficiencies in the system. In addition, use of different documentation tools (e.g.; REA and DFD) working in concert is common in industry and can enhance the development of internal control maps. Finally, this paper provides an approach whereby documentation tools can be taught in an AIS course as a map by which to facilitate other course topics such as internal controls, computer fraud and security, and auditing.

REFERENCES

1. AICPA. The Effect of Information Technology on the Auditor'sConsideration of Internal Control in a Financial Statement Audit, *SAS No. 94,* 2001.
2. Bagranoff, Nancy A., Mark G. Simkin, and Carolyn S. Norman., *Core Concepts of Accounting Information Systems*, 9th Edition. John Wiley & Sons, Inc, 2004.
3. Cannon, David M. and Glenn A. Growe., SOA compliance: Will IT sabotage your efforts? *The Journal of Corporate Accounting & Finance,* 2004.
4. David, Julie S., Three 'Events' That Define an REA Approach to Systems Analysis, Design, and Implementation, *Proceedings of the Annual Meeting of the American Accounting Association, Dallas, TX,* 1997.
5. Demarco, Tom. *Structured Analysis and System Specification*, Prentice Hall, 1978.
6. Gane, Christopher P. and Trish Sarson. *Structured Systems Analysis: tools and techniques.* Prentice Hall, 1979.
7. Hall, James A., *Accounting Information Systems,* 3rd Edition. South Western College Publishing, Inc, 2001.
8. Krell, Eric, Foolproof Compliance for Your IT Systems, *Issue of Business Finance*, Nov 2004
9. Martin, Merle P., *Analysis and Design of Business Information Systems*, Prentice Hall, 1995.
10. McCarthy, William E., The REA Accounting Model: A Generalized Framework for Accounting Systems in a Shared Data Environment, *The Accounting Review* (July), 1982.
11. Romney, Marshall B. and Paul J. Steinbart, *Accounting Information Systems.* 9th Edition. Prentice Hall. 2002.
12. Shneiderman, Ben. *Designing the User Interface.* Addison-Wesley. 1987.

NOTES