CHAPTER 9

CONTROLLING INFORMATION SYSTEMS: BUSINESS PROCESS AND APPLICATION CONTROLS

LEARNING OBJECTIVES

AFTER READING THIS CHAPTER, YOU SHOULD BE ABLE TO:

- COMPLETE THE STEPS IN THE CONTROL FRAMEWORK AND PREPARE A CONTROL MATRIX.
- WRITE EXPLANATIONS THAT DESCRIBE HOW THE BUSINESS PROCESS AND APPLICATION CONTROLS INTRODUCED IN THIS CHAPTER ACCOMPLISH CONTROL GOALS.
- DESCRIBE THE IMPORTANCE OF BUSINESS PROCESS AND APPLICATION CONTROLS TO ORGANIZATIONS WITH ENTERPRISE SYSTEMS AND THOSE ENGAGING IN E-BUSINESS.

How well do you believe that Fortune 1,000 companies manage their critical data? What percentage of that critical data do you think is accurate, 99 percent, 95 percent, or 90 percent? According to Gartner, Inc. only 75 percent of critical data within Fortune 1,000 companies is accurate. Furthermore, only 34 percent of executives responding to a 2004 PricewaterhouseCoopers survey said that they were confident in the quality of their corporate data.[1] What is the result of this problem? Internal operations that depend on accurate data do not perform as planned. For example, can we manage our inventory if we don't know exactly how much we have and where it is? Inaccurate financial reporting, uncollectible receivables, and overpayments to vendors are other problems caused by inaccurate data.

What is going on here? Haven't we had enough experience using computers to capture and store data in such a way that we have accurate data? Well, we do know how, but we do not pay sufficient attention to the controls that are needed to capture and maintain accurate data. This chapter introduces you to business process and application controls that can be applied across many types of processes to ensure that an information system captures all (i.e., *complete*) legitimate (i.e., *valid*) data and that the data is captured correctly (i.e., *accurate*) so that the data supports an organization's operations (i.e., *effectiveness*), protects its resources (i.e., *security of resources*), and does so with minimal use of an organization's resources (i.e., *efficiency*).

1 Kym Gilhooly, "Dirty Data Blights the Bottom Line," *Computerworld*, November 7, 2005, pp. 23–24.

Synopsis

CONTROLS

This chapter presents a conceptual framework for the analysis of controls in business systems. We apply the control framework by describing business process and application controls that may be found in any information system. These controls will help us *prevent* (or *detect* or *correct*) the data quality issues plaguing organizations throughout the world.

ENTERPRISE SYSTEMS

Many of the controls described in this chapter provide assurance about the quality of the data entry process. Such controls take on increased importance with *enterprise systems* because they *prevent* erroneous data from entering the system and negatively impacting the many tightly connected processes that follow the initial entry of the data. For example, good controls over the entry of customer orders will help us to perform the activities that follow the recording of that order, including the shipment; update to the inventory balance; customer invoicing; general ledger entries for sales, accounts receivable, inventory, and costs of goods sold; and the inventory replenishment process.

E-BUSINESS

Good data entry controls also are important for those engaging in *e-business*. For example, if we receive customer orders electronically, our systems must have sufficient controls within them so that they accept only authorized and accurate order data. If we don't have these controls, we may make inaccurate shipments or shipments to those who have no intention of paying for the goods being shipped.

Introduction

Having covered the control environment in Chapter 7 and pervasive and general controls in Chapter 8, we are now ready to move to the third level of control plans appearing in the hierarchy shown in Figure 7.6 (pg. 233)—business process and application control plans. We start by defining the components of a control framework and introduce the tools used to implement it. Then, we apply the control framework to two generic business processes that include controls that may be found in any information system. In Chapters 10 through 16, we will examine controls that might be found in particular business processes (e.g., order entry/sales, billing, accounts receivable, and so forth).

The Control Framework

In this section, we formally introduce the control framework that we began to discuss in Chapter 7 in the "A Framework for Assessing the Design of a System of Internal Control" section (pgs. 226–235). We recommend that you review those pages now. The control framework provides you with a structure for analyzing the internal controls of business organizations. However, structure alone is of little practical value to you. To make the framework functional, you need to become familiar with, and comfortable in using, the tools for implementing the framework. Chapter 4 introduced you to one of the key tools—the systems flowchart. Now we tell you more about a related tool—the control matrix.

The Control Matrix

As noted in Chapter 7, a *control matrix* is a tool designed to assist you in evaluating the potential effectiveness of controls in a particular business process by matching control goals with relevant control plans. PCAOB Auditing Standard Number 2 calls this

FIGURE 9.1 Lenox Control Matrix

Recommended control plans (b)	Control Goals of the Lenox Cash Receipts Business Process								
	Control Goals of the Operations Process (a)				Control Goals of the Information Process (a)				
	Ensure effectiveness of operations		Ensure efficient employment of resources (e.g., people and computers)	Ensure security of resources (e.g., checks and AR data)	For the remittance advice inputs, ensure:			For the AR master data, ensure:	
	A	B			IV	IC	IA	UC	UA
Present Controls									
P-1: Immediately endorse incoming checks				P-1 (c)					
P-2: Compare input (remittance advices [RAs]) with master data (AR master data)	P-2	P-2			P-2		P-2		
Missing Controls									
M-1 Immediately separate checks and RAs									
M-2 Compare checks and RAs									

Possible effectiveness goals include the following:

A — Timely deposit of checks

B — Comply with compensating balance agreements with the depository bank

IV = input validity

IC = input completeness

IA = input accuracy

UC = update completeness

UA = update accuracy

Note: Four elements of the control matrix:
(a) Control goals
(b) Recommended control plans
(c) Cell entries
(d) Explanation of cell entries (see Exhibit 9.1)

"Effectiveness of Control Design." Assessing the effectiveness of control design is required to comply with SOX section 404. When management and independent auditors perform this assessment, they typically use a control matrix such as the one used in our control framework.

Figure 9.1, an extension of Figure 7.7 (pg. 234), presents a "bare-bones" outline of the control matrix.[2] This control matrix includes the explanation of cell entries in

2 The update completeness (UC) and update accuracy (UA) columns of the matrix are shaded to indicate that they do not apply to this process.

EXHIBIT 9.1 Explanation of Cell Entries for Control Matrix in Figure 9.1 (d)

P-1: *Immediately endorse incoming checks.*

- *Security of Resources:* A restrictive check endorsement ["deposit only to the account of Lenox Company"] ensures security of the cash resource by preventing the check from being misappropriated.

P-2: *Compare input (remittance advices [RAs]) with master data (accounts receivable).*

- *Effectiveness Goals A and B:* By determining quickly that the input is correct, the deposit process can proceed in a timely manner.
- *Efficient employment of resources:* The automatic comparison by the computer of the input data to the master data is more efficient than a manual comparison.
- *Input accuracy:* Ensures that the correct customer number and payment amount has been entered.

M-1: *Immediately separate checks and RAs.*

- *Effectiveness Goals A and B:* Immediately separating the checks from the RAs allows the checks to be deposited without being delayed by the processing of the RAs, thereby accelerating cash flows (*Effectiveness Goal A*) and improving cash balances (*Effectiveness Goal B*).
- *Security of resources:* If the checks and RAs are processed separately, the person handling the checks (i.e., the negotiable instruments comprising the cash asset) is a different person (or process) from the one who records the checks from information on the RA. By separating these functions, we improve security of the cash asset because there is less opportunity for misappropriation of the checks to be covered up while recording the RA.

M-2: *Compare checks and RAs.*

- *Input validity:* The comparison ensures that the RA is supported by an actual payment.
- *Input accuracy:* The comparison ensures that the data on the RA that will be entered into the system is correct.

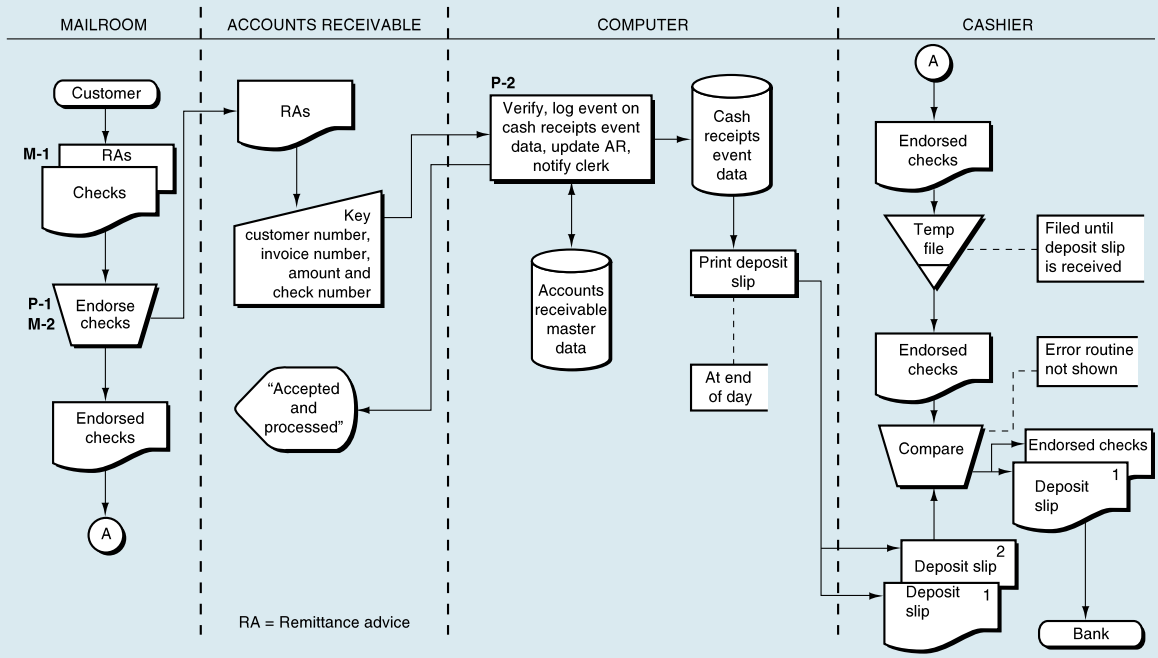
Exhibit 9.1 and Figure 9.2 (pg. 288), the "annotated" systems flowchart for the Lenox cash receipts process produced when completing the steps in the control framework and preparing the control matrix. The control matrix provides a means to explain and analyze the controls that have been annotated on a systems flowchart. We explain how to annotate a flowchart later in this section. *We cannot overemphasize that our intent in Figure 9.1 is* ***not*** *to have you learn about the control goals and control plans for a cash receipts process. Those are covered in Chapter 11. Rather, we are giving you an overview of the control matrix elements and how they relate to each other, and walking you through the steps in preparing the matrix.* Please follow along in the figure as we describe how to prepare the control matrix.

Steps in Preparing the Control Matrix

Specifying control goals represents the first step in building a control matrix. The goals are listed across the top row of the matrix; they should be familiar to you from discussions in Chapter 7 where we showed them in Figure 7.5 (pg. 229). Recall from Chapter 7 that we filled in the top row of the matrix by following these steps:

1. *Identifying operations process goals:* As noted in Chapter 7, our control framework subdivides operations process control goals into effectiveness of operations, efficient employment of resources, and security of resources (see Table 7.1, pg. 230). By

FIGURE 9.2 Lenox Company Annotated Systems Flowchart



reviewing the systems flowchart and other information about the business process, we determine the following specifics:

a. *Effectiveness goals*

i. *Effectiveness* goals describe measures of success for the operations process. These are developed during an enterprise's risk-management process. For example, see "Related Objectives" in Figure 7.1 on pg. 208.

ii. Because these goals might be difficult for you to derive without an organizational context, we will recommend some sample operations goals for each process discussed in this text.

iii. For the Lenox's cash receipts process, we include only two examples here: Goal A—Timely deposit of checks and Goal B—Comply with compensating balance agreements with the depository bank.[3] Other possible goals of a cash receipts would be shown as goals C, D, and so forth, and described at the bottom of the matrix.

b. *Efficiency goals*

i. *Efficiency* control goals relate to ensuring that resources used in the business process are being employed in the most productive manner.

3 Remember that one of the goals of any business process may be in compliance with applicable laws, regulations, and *contractual agreements*. Depending on the particular process being analyzed, we tailor the matrix to identify the specific law, regulation, or agreement with which we desire to achieve compliance. In Lenox' case, we assume that its loan agreements with its bank require that it maintain certain minimum cash balances, known as compensating balances, on deposit.

ii. In parentheses, notice that we have listed two resources of the cash receipts process for which efficiency is applicable—people and computers. In fact, people and computers would always be considered in the efficiency assessments related to accounting information systems.
iii. In other business processes, such as receiving goods and supplies, we might also be concerned with the productive use of equipment such as trucks, forklifts, and handheld scanners.

c. *Security goals*

i. *Security* control goals relate to protecting entity resources from loss, destruction, disclosure, copying, sale, or other misuse. These are meant to manage risks identified in the enterprise risk-management process.
ii. In parentheses, we have included two resources of the cash receipts process that must be secured—cash and information (accounts receivable master data). With any business process, we are concerned with information that is added, changed, or deleted as a result of executing the process, as well as assets that are brought into or taken out of the organization as a result of the process, such as cash, inventory, and fixed assets.
iii. With regard to other business processes, such as order entry and sales, we might include customer master data and inventory.

Note: The security over hard assets used to execute business processes, such as computer equipment, trucks, and loading docks, is handled through pervasive and general controls (discussed in Chapter 8).

2. *Identifying information process goals:* As noted in Chapter 7, our control framework (see Table 7.1, pg. 230) subdivides information process control goals into input control goals (*input validity*, *input completeness*, and *input accuracy*) and update control goals (*update completeness* and *update accuracy*). By reviewing the systems flowchart and other information about the business process, we determine the following specifics:

a. *Input goals*

i. *Input* goals of the information process relate to ensuring input validity (IV), input completeness (IC), and input accuracy (IA) with respect to all business process data entering the system.
ii. For Lenox's information process goals, we recognized that remittance advices, reflecting cash receipts, will be entered into the system. Notice that we specifically name the input data of concern in parentheses.
iii. With respect to other business processes, such as hiring employees, we would be concerned with other inputs, such as employee, payroll, and benefit plan data.

b. *Update goals*

i. The purpose of the *update* control goals of the information process is to ensure the update completeness (UC) and update accuracy (UA) of the business process input data. Note that these goals only apply when there is a periodic process—a delay between input and update. In Figure 9.1, the update completeness (UC) and update accuracy (UA) columns are shaded to indicate that they do not apply to this process because the input and recording of the RAs on the cash receipts event data and the update of accounts receivable master data

are simultaneous, and no additional controls, beyond those controlling the input, are required to ensure UC and UA.

ii. For the Lenox cash receipts process, we see that the receipts are coming from customers and are used to update the accounts receivable master data. Notice that we list *accounts receivable master data* in the control matrix.

iii. Other business processes, such as cash payments, would involve different update concerns, such as vendor, payroll, or accounts payable master data.

Identifying recommended control plans for the business process under evaluation is the second step in the construction of a control matrix. This step focuses on the nature and extent of control plans that should be in place to accomplish our objectives and to minimize risks to an acceptable level of residual risk. In the final analysis, the comfort level that management and auditors reach with respect to residual risk is a matter of professional judgment.

For a given business process, each operations and information process control goal should be addressed by one or more control plans. For instance one or more control plans should cover the effectiveness goals (A and B), the efficiency goal, the security goal, and each of the information process goals (IV, IC, IA, UC, and UA). The following advice will help you to structure your thinking with regard to control plans. Perhaps the most difficult part of this process, the preparation of a control matrix, is identifying controls that should be in place (we call these *present controls*) and those controls that are not in place but should be (we call these *missing controls*). Follow along as we describe a process to help you complete this task:

1. *Identify "Present" Control Plans:* Start on the upper-left column of the systems flowchart (this should be the start of the process), and identify controls that seem to accomplish one or more of the control goals. For example, ask yourself "does this control help me to protect a resource?" or "does this control improve the accuracy of the input?" and so on. Controls will fall into two categories, the generic controls that we describe later in this chapter that apply to all or most business processes and the controls that relate to a specific business process. These latter controls will be introduced in Chapters 10 through16.

   a. Reviewing the Lenox systems flowchart (Figure 9.2), you will find that the first manual process is entitled "Endorse checks." Can this help us accomplish a control goal? Sure. The endorsement will make it difficult for someone to deposit the check to his or her own account thus protecting Lenox's cash resource. Because this process appears on the flowchart, this control plan already exists, meaning, it is *present* as opposed to *missing*. Accordingly, place a *P-* beside the process, indicating that it is present, and place a *1* beside the *P*-reflecting the first present control plan on the flowchart.[4] As a result, you should have *annotated* the systems flowchart with a P-1.

   b. Continue reviewing the systems flowchart by following its sequential logic, annotating the flowchart with P-2, P-3, and so on until you have accounted for all *present* control plans. Notice in Figure 9.2 that we have found two present controls, P-1 and P-2. There are more, but we are trying to keep the example simple for now.

4 The numbering for present and missing controls is used only to cross-reference the flowchart and control matrix. The sequence of the numbers is not significant.

2. *Evaluating "Present" Control Plans:* Write the control number (P-1, P-2, P-3 through P-*n*) and name of each control plan in the left-hand column of the control matrix. Then, starting with P-1, look across the row and determine which control goals the plan addresses, and then place a P-1 in each *cell* of the matrix for which P-1 is applicable. It is possible that a given control plan can attend to more than one control goal. Continue this procedure for each of the *present* control plans. Simultaneously, in the section below the matrix (such as Exhibit 9.1), describe *how* the control plan addresses each noted control goal. Students usually have the most difficulty in providing these explanations. Yet, we believe this element is the most important part of the matrix because the purpose of the matrix is to relate plans to goals. Unless you can explain the association between plans and goals, there's a good possibility you may have guessed at the cell entry. Sometimes you'll guess right, but it's just as likely you'll guess wrong. Don't play the guessing game! Be prepared to defend your cell entries.

   a. To illustrate, we list the two illustrative control plans (P-1 and P-2) for the cash receipts process at Lenox in the left column of Figure 9.1.
   b. P-1 (Endorse checks) ensures the security of the cash (checks) by stamping the checks with a restrictive endorsement that can prevent the check from being misappropriated by an employee.
   c. P-2 (Compare input with master data) means that the system compares the input customer number and amount being paid to the accounts receivable master data. This matching reduces the possibility that the wrong customer number and account has been input. This ensures Effectiveness goals A and B and Efficient Employment of Resources by determining quickly (i.e., *timely deposit*) and automatically (i.e., *efficiently*) that the cash receipt is correct (i.e., input accuracy [IA]).

3. *Identifying and Evaluating "Missing" Control Plans:* The next step in recommending control plans is to determine whether additional controls are needed to address missing control goal areas, strengthen present control plans, or both.

   a. *Examining the controls matrix:* The first place to start is to look at the control matrix and see if there are any control goals (operations or information) that no present control plan is addressing. If so, you need to do the following:

      i. In the left-hand column of the matrix, number the first missing control plan as M-1, and label or title the plan.
      ii. Across the matrix row, place M-1 in each cell for which the missing control is designed.
      iii. In the explanation section below the matrix (such as Exhibit 9.1), explain how the missing control will address each noted control goal.
      iv. On the systems flowchart, annotate M-1 where the control should be inserted.
      v. If there are still control goals for which there is no control plan, develop another plan (M-2), and repeat the four previous steps (i through iv). Continue this procedure until each control goal on the matrix is addressed by at least one control plan.
      vi. With regard to Lenox, we have noted two missing control plans (M-1 and M-2), although more might exist. Recall that the purpose of this chapter is to offer guidelines for creating a controls matrix, not to completely analyze Lenox's cash receipts process. For missing control M-1, we note that Lenox should immediately separate checks and remittance advices to mitigate risks related to both effectiveness goals, as well as to ensure the security of

resources (i.e., the checks will be deposited quickly and cannot easily be diverted). For missing control plan M-2, we note that someone should compare the checks and the remittance advices to ensure that the amount being paid is correct. Input validity is ensured because the cash receipt (as reflected by the remittance advice) to be input into the system is supported by an actual customer payment. Input accuracy is ensured because the event (cash receipt) is correctly captured and entered into the system.

b. *Evaluating the systems flowchart:* Even though all of the control goals on the matrix are now addressed by one or more control plans, it is worthwhile to closely scrutinize the systems flowchart one more time. Such analysis can reveal areas where further controls are needed. Just because all of the control goals on the matrix have one or more associated control plans, it may be necessary to add more control plans or strengthen existing plans to further reduce residual risk to an acceptable level in certain areas. It takes training and experience to spot risks and weaknesses of this nature. In Chapters 10 through 16, you will learn more about how to make such critical internal control assessments.

When your assessment leads you to the identification (and correction) of control weaknesses, as reflected in missing control plans or recommendations for strengthening present control plans, you are essentially recommending remedial changes to the system (if necessary) to correct deficiencies in the system.

In addition to telling you about the control strengths and weaknesses of a particular system, a completed matrix and annotated systems flowchart also facilitates your evaluation from the perspectives of *control effectiveness* (are all the control goals achieved?), *control efficiency* (do individual control plans address multiple goals?), and *control redundancy* (are too many goals directed at the same goal?).

Exhibit 9.2 summarizes the steps we have just undertaken in preparing the illustrative control matrix in Figure 9.1 (pg. 286). Combined with the preceding discussion and illustration, the steps should be self-explanatory. You should take time now to study each of the steps to make sure that you have a reasonable understanding of them.

Sample Control Plans for Data Input

In the preceding section, we described the framework used to analyze business process and application controls. The framework consists of two main elements: specifying controls goals and recommending control plans. In the following sections, we describe two methods for processing input data: (1) manual and automated data entry and (2) data entry with batches of input data. For both of these methods, we describe the processing logic, present a systems flowchart, and describe and analyze the controls with a control matrix and control explanations.

Perhaps the most error-prone and inefficient steps in an operations or information process are the steps during which data is entered into a system. While much has been done to improve the accuracy and efficiency of the data entry process, problems still remain, especially when humans enter data into a system. Thus we begin our discussion of process controls by describing those controls that improve the data entry process.

As you study these controls, keep in mind the following improvements that have been made to address the errors and inefficiencies of the data entry process:

- The data entry process may be automated. Documents containing bar codes and OCR encoding may be scanned or radio-frequency identification (RFID) readers

EXHIBIT 9.2 Steps in Preparing a Control Matrix

Step I *Specifying control goals:* Review the systems flowchart and related narrative description to become familiar with the system under examination. Identify the business process (e.g., cash receipts); the key relevant resources (e.g., cash, accounts receivable master data); the input (e.g., the remittance advice); storage, if any, for the input data (e.g., cash receipts event data); and the master data being updated (e.g., accounts receivable master data). With regard to the business process under consideration:

1. Identify operations process control goals:
   a. Effectiveness goals (there may be more than one)
   b. Efficiency goals (usually people and computers)
   c. Security goals (consider all affected data and tangible assets)
2. Identify information process goals:
   a. Input goals (validity, completeness, and accuracy)
   b. Update goals (completeness and accuracy), if the process is periodic

Step II *Recommending control plans:* List a set of recommended control plans that is appropriate for the process being analyzed. The list should include both plans related to the operations process (e.g., the cash receipts process) and those related to the information processing methods (e.g., data entry controls, batch controls). In Figure 9.1 and Exhibit 9.1, we presented only two illustrative *present* plans for Lenox's system and two *missing* plans.

1. Annotate *present* controls on the systems flowchart by placing P-1, and P-2 through P-*n* beside all present controls. Start on the upper-left column of the flowchart, and follow the sequential processing logic of the flowchart.
2. Evaluate the *present* control plans by placing the number and name of the plan on the controls matrix, and explaining, in the section below the matrix, the nature and extent of the control plan on the matrix.
3. Identify and evaluate missing control plans (M-1, and M-2 through M-*n*).
   a. Examine the control matrix to determine whether there are any control goals for which no control plan exists. If so, develop a control plan designed to minimize associated risks (control goals). Explain the nature and extent of the missing plan in the section below the matrix. Repeat this procedure until all control goals on the matrix are addressed by one or more control plans.
   b. Analyze the systems flowchart for further risk exposures for which you would recommend adding additional controls or strengthening existing controls. Note any further additions or refinements on the control matrix using the same procedures described for present or missing controls plans.

may be used to obtain data from RFID chips.[5] This automation reduces or eliminates manual keying.

- Business events, such as purchases, may be initiated in one (buying) organization and transmitted to another (selling) organization via the Internet or electronic data interchange (EDI). In this case, the receiving (selling) organization need not enter the data at all. E-BUSINESS
- The multiple steps in a business process may be tightly integrated, such as in an enterprise system. In these cases, the number of data entry steps is greatly reduced. For example, there may be no need to enter a shipment (sale) into the billing system because the billing system has been integrated with the shipping system. ENTERPRISE SYSTEMS

5 See Chapter 10 for an explanation of bar codes and scanning and Chapter 12 for an explanation of RFID.

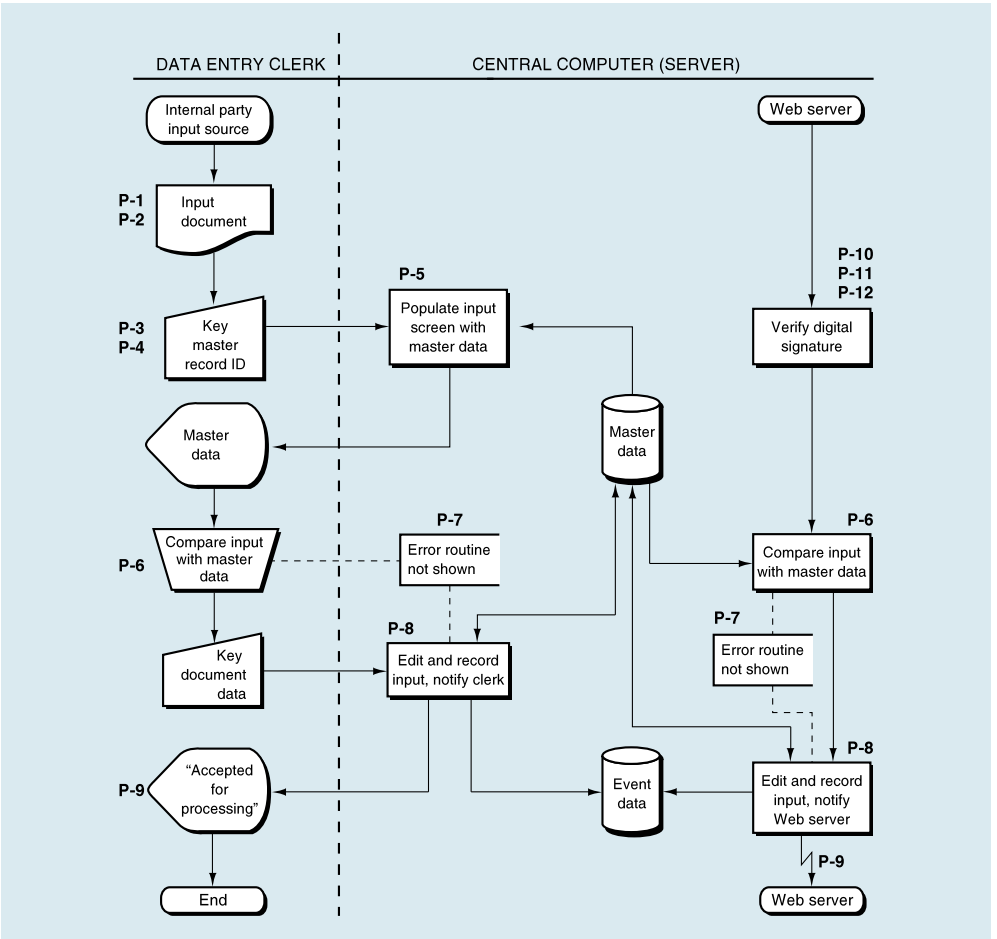
Control Plans for Manual and Automated Data Entry

In this section, we introduce you to a hypothetical system that employs manual and automated data entry techniques. We describe the system, walk you through its systems flowchart, list and explain the control plans associated with these data entry methods, and incorporate those plans into a control matrix for the system.

System Description and Flowchart

Figure 9.3 shows an annotated systems flowchart for a hypothetical system that we will use to describe our first set of controls. The processing starts in the first column of Figure 9.3 with the input document. Let's assume that the document is designed to facilitate the data entry process and that it includes the signature of an authorizing individual. The data entry program presents the clerk with a preformatted input screen and then prompts the clerk to enter certain data into fields on that screen starting with the IDs, or codes, for some master records (e.g., customer code, item numbers).

FIGURE 9.3 Systems Flowchart: Manual and Automated Data Entry



In response to keying the master record IDs, the computer populates the input screen with master data, such as a customer record. The data entry clerk compares the display to the input document to determine that the correct code has been entered. Corrective measures would be taken (see "Error routine not shown") such as entering a corrected code. The data entry clerk would then proceed to enter the remaining data such as the codes for the items that the customer has ordered (the computer would display the inventory master data as each item number is entered, and the clerk would compare each display to the input document). The computer then edits the input, records the input (if the data passes the edits, otherwise an error routine is activated), and then displays a message to the clerk indicating that the input has been accepted for processing.

On the right side of the central computer column we see an automated data entry process that roughly parallels the manual entry by the data entry clerk, with a few exceptions. As mentioned previously, automated data entry may be via RFID, OCR, bar codes, EDI or the Internet. In Figure 9.3, we assume that a business partner, such as a customer, has entered a business event (e.g., an order) on its computer system and submitted it via the Internet. The computer determines that this is an order from a legitimate customer by verifying the digital signature on the order. The computer then compares the input data to the master data. For example, the computer might match the input customer number and name to that stored in the master data. The computer then edits the input, records the input (if the data passes the edits, otherwise an error routine is activated), and sends a message back via the Web server to the business partner indicating that the input has been accepted for processing.

Our flowchart stops at this point *without* depicting the update of any master data. Certainly our system could continue with an update process. We have not shown it here so that we can concentrate on the *input* controls.

Applying the Control Framework

In this section, we apply the control framework to the generic system just described. Figure 9.4 (pg. 296) presents a sample control matrix for the systems flowchart shown in Figure 9.3. Through the symbols P-1 through P-12, we have annotated the flowchart to show where specific control plans are already implemented. The UC and UA columns in the matrix have been shaded to emphasize that they do not apply to this analysis because there is no update of any master data in Figure 9.3.

Under the operations process section of Figure 9.4, we have shown only one system goal for illustrative purposes—although there may be more than one effectiveness goal. We identify the goal as Goal A: To ensure *timely* input of (blank) event data (whatever those data happen to be). In the business process chapters (Chapters 10 through 14), we will show you how to tailor the goals to the business process discussed in those chapters.

The recommended control plans are listed in the first column in Figure 9.4 (pg. 296). Please keep in mind that the systems flowchart (Figure 9.3) and related control matrix (Figure 9.4) are shown here for illustrative purposes only; thus, they may be incomplete in some respects. To help you in future assessments of this nature, we next present a list of control issues that are representative of those commonly associated with controlling the data entry process, all of which were applied to our example.

The purpose of this presentation is to give you a sense of the multitude of control plans available for controlling data input.[6] Once again, we remind you that the plans are

6 Many of the controls in this section are adapted from material contained in *Handbook of IT Auditing 2001 Edition* (Chapters D2, D3, and D4, primarily) (Boston: Warren, Gorham & Lamont, 2000). Copyright © 2000 by PricewaterhouseCoopers L.L.P.

FIGURE 9.4 Control Matrix for Manual and Automated Data Entry

	Control Goals of the (blank) Business Process								
	Control Goals of the Operations Process				Control Goals of the Information Process (a)				
Recommended Control Plans	Ensure Effectiveness of Operations		Ensure Efficient Employment of Resources (people, computers)	Ensure Security of Resources (event data, assets)	For the (blank) inputs, ensure:			For the (blank) master data, ensure:	
	A				IV	IC	IA	UC	UA
Present Controls									
P-1: Document design	P-1		P-1				P-1		
P-2: Written approvals				P-2	P-2				
P-3: Preformatted screens	P-3		P-3				P-3		
P-4: Online prompting	P-4		P-4				P-4		
P-5: Populate input screen with master data	P-5		P-5		P-5		P-5		
P-6: Compare input data with master data	P-6	>	P-6		P-6		P-6		
P-7: Procedures for rejected Inputs						P-7	P-7		
P-8: Programmed edit checks	P-8		P-8	P-8	P-8		P-8		
P-9: Confirm input acceptance						P-9			
P-10: Automated data entry	P-10		P-10				P-10		
P-11: Enter data close to the originating source	P-11		P-11			P-11	P-11		
P-12: Digital signatures				P-12	P-12		P-12		
Missing Controls									
None noted									

Possible effectiveness goals include the following:

A = Ensure timely input of (blank) event data.

See Exhibit 9.3 for a complete explanation of control plans and cell entries.

IV = input validity

IC = input completeness

IA = input accuracy

UC = update completeness

UA = update accuracy

not unique to a specific process such as order entry/sales, billings, cash receipts, and so forth. Rather, they apply to *any* data entry process. Therefore, when the technology of a system is appropriate, these controls should be incorporated into the list of recommended control plans. Recall in the last section of this chapter, you were instructed to

look for controls that seem to address the control goals (e.g., effectiveness, efficiency, input accuracy). Begin at the upper-left column of the flowchart, and look for such controls. Then, follow along with us as we trace the sequential processing logic back and forth across and down the columns following the flow of work activities. We first define and explain these controls and then summarize, in Exhibit 9.3 (pg. 301), each cell entry in Figure 9.4, the control matrix:

- **Document design** (see Exhibit 9.3 and Figure 9.4, P-1): A control plan in which a source document is designed to make it easier to prepare the document initially and later to input data from the document. In our example, we assume that the organization has properly designed this document to facilitate the data preparation and data entry processes.
- **Written approvals** (see Exhibit 9.3 and Figure 9.4, P-2): These take the form of a signature or initials on a document to indicate that someone has authorized the event. This control ensures that the data input arises from a valid business event and that appropriate authorizations have been obtained. Another control aspect of approving an input document is that such an approval segregates authorizing events from recording events (as discussed in Chapter 8). Note: In some situations, we might use **electronic approvals** whereby business events are routed, using a computer system's *workflow* facility, to persons authorized to approve the event. For example, purchase requisitions might be routed for approval to those with budgetary authority.
- **Preformatted screens** (see Exhibit 9.3 and Figure 9.4, P-3): Control the entry of data by defining the acceptable *format* of each data field. For example, the screen might force users to key exactly nine alphabetic characters in one field and exactly five numerals in another field. Or, the system may provide drop-down lists of data that is acceptable for a given field, such as shipping methods and sales terms. To facilitate the data entry process, the cursor may *automatically move* to the next field on the screen. The program may require that certain fields be completed, thus preventing the user from omitting any *mandatory* data sets. Finally, the system may *automatically populate* certain fields with data, such as the current date, sales tax rates, and other terms of a business event. This reduces the number of keystrokes required, making data entry quicker and more efficient. Also, with fewer keystrokes and by using the default data, fewer keying mistakes are expected; thus, data entry is more accurate. To ensure that the system has not provided inappropriate defaults, the clerk must compare the data provided by the system with that of the input.
- **Online prompting** (see Exhibit 9.3 and Figure 9.4, P-4): Requests user input or asks questions that the user must answer. For example, after entering all the input data for a particular customer order, you might be presented with three options: "Accept" the completed screen, "Edit" the completed screen, or "Reject" the completed screen. By forcing you to stop and accept the data, online prompting is, in a sense, advising you to check your data entries before moving on. In addition, many systems provide *context-sensitive help* whereby the user is automatically provided with, or can ask for, descriptions of the data to be entered into each input field.
- **Populate input screens with master data** (see Exhibit 9.3 and Figure 9.4, P-5): The clerk enters the identification code for an entity, such as a customer, and the system retrieves data about that entity from the master data. For example, in our earlier example of entering a customer order, the user might be prompted to enter the customer ID (code). Then, by accessing the customer master data, the system automatically provides data such as the customer's name and address, the salesperson's name and the sales terms. This reduces the number of keystrokes required,

making data entry quicker and more efficient. With fewer keystrokes and by using the existing data, fewer keying mistakes are expected. To enable this control, numeric, alphabetic, and other designators are usually assigned to entities such as customers, vendors, and employees.

- **Compare input data with master data** (see Exhibit 9.3 and Figure 9.4, P-6): We can determine the accuracy and validity of the input data. Such comparisons may be done manually or by the computer. Here are just three types of comparisons that can be made:

  a. *Input/master data match.* These edits test that the correct identification (ID) code has been manually entered. For example, a clerk keys in a customer number, and the system displays this record on the input screen. The clerk then matches the customer data, such as name and address, to the input document. In a similar manner, the clerk could read the name and address back to a customer who is on the phone.

  b. *Input/master data dependency checks.* These edits test whether the contents of two or more data elements or fields on the event data bear the correct logical relationship. For example, input customer orders can be tested to determine whether the salesperson works in the customer's territory. If these two items don't match, there is some evidence that the customer number or the salesperson ID was input erroneously.

  c. *Input/master data validity and accuracy checks.* These edits test whether master data supports the validity and accuracy of the input. For example, this edit might prevent the input of a shipment when no record of a corresponding customer order exists. If no match is made, we may have input some data incorrectly, or the shipment might simply be invalid. We might also compare elements *within* the input and master data. For example, we can compare the quantities to be shipped to the quantities ordered. Quantities that do not match *may* have been picked from the shelf or entered into the computer incorrectly.

- **Procedures for rejected inputs** (see Exhibit 9.3 and Figure 9.4, P-7): Designed to ensure that erroneous data (i.e., not accepted for processing) are corrected and resubmitted for processing. To make sure that the corrected input does not still contain errors, the corrected input data should undergo all routines through which the input was processed originally. A "suspense file" of rejected inputs is often retained (manually or by the computer) to ensure the timely clearing of rejected items. To reduce the clutter in the simple flowcharts in this text, we often depict such routines with the annotation "Error routine not shown."
- **Programmed edit checks** (see Exhibit 9.3 and Figure 9.4, P-8): Automatically performed by data entry programs upon entry of the input data. Erroneous data may be highlighted on the input screen to allow the operator to take corrective action immediately. For automated data entry, rejected business events may be listed in a summary report periodically produced by the computer. Programmed edits can highlight actual or potential input errors and allow them to be corrected quickly and efficiently. The most common types of programmed edit checks are the following:

  a. **Reasonableness checks** also known as **limit checks**, test whether the contents (e.g., values) of the data entered fall within predetermined limits. The limits may describe a standard range (e.g., customer numbers must be between 0001 and 5000, months must be 01 to 12) or maximum values (e.g., no normal hours worked greater than 40 and no overtime hours greater than 20).

b. **Document/record hash totals** reflect a summarization of any numeric data field within the input document or record, such as item numbers or quantities on a customer order. The totaling of these numbers typically serves no purpose other than as a control. Calculated before and then again after entry of the document or record, this total can be used to determine that the applicable fields were entered accurately and completely.
c. **Mathematical accuracy checks** compare calculations performed manually to those performed by the computer to determine whether a document has been entered correctly. For this check, the user might enter the individual items (e.g., quantity purchased, unit cost, tax, shipping cost) on a document, such as an invoice, and the total for that document. Then the computer adds the individual items and compares that total to the one input by the user. If they don't agree, something has likely been entered erroneously. Alternatively, the user can review the computer calculations and compare them to totals prepared before input.
d. **Check digit verification** involves the inclusion of an extra digit—a check digit—in the identification number of entities such as customers and vendors. More than likely, you have a check digit as part of the ID on your ATM card. The check digit is calculated originally by applying a formula to an identification number; the check digit then is appended to the identification number. For instance, the digit 6 might be appended to the customer code 123 so that the entire ID becomes 1236. In this highly oversimplified example, the digit 6 was derived by adding together the digits 1, 2, and 3. Whenever a data entry person enters the identification number later, the computer program applies the mathematical formula to verify the check digit. In our illustration, if the ID were input as 1246, the entry would be rejected because the digits 1, 2, and 4 do not add up to 6. We know you are already saying to yourself, "But what about a transposition like 1326?" This would not be rejected because our example is highly oversimplified. In practice, check digits are assigned by using much more sophisticated formulas than simple cross-addition; those formulas are designed to detect a variety of input errors, including transpositions.

- **Confirm input acceptance** (see Exhibit 9.3 and Figure 9.4, P-9): This control causes the data entry program to inform the user that the input has been accepted for processing. The program may flash a message on the screen telling a user that the input has been *accepted*, or it might display a number assigned to the event. For example, after input of a customer order, the computer might display the internal sales order number that will be used to track the sale. To complete the control, the data entry clerk might write that number on the customer's order or read the number to the customer who is on the phone. For automated inputs, the computer might send the number back to the originator, such as a customer that has entered an order on a Web site.
- **Automated data entry** (see Exhibit 9.3 and Figure 9.4, P-10): This is a strategy for the capture and entry of event-related data using technology such as OCR, bar codes, RFID, and EDI. These methods use fewer human resources and capture more data in a period of time than is possible with manual entry. By eliminating the keying errors that can occur in manual data entry, these methods improve the accuracy of the entered data. Finally, in some cases, the input method can validate the authenticity of the input. For example, when the RFID chip on a box is read, we know that the box exists.
- **Enter data close to the originating source** (see Exhibit 9.3 and Figure 9.4, P-11): This is a strategy for the capture and entry of event-related data close to the place

(and probably time) that an event occurs. *Online transaction entry (OLTE)* and *online real-time processing (OLRT)* are examples of this processing strategy. When this strategy is employed, databases are more current and subsequent events can occur in a *timelier* manner. Because data are not transported to a data entry location, there is less risk that inputs will be lost. Also, the input can be more accurate because the data entry person may be in a position to recognize and immediately correct input errors. Finally, some efficiency can be gained by reducing the number of entities handling the event data or by shifting the data entry outside the organization to a business partner (e.g., customers enter orders on the Web).

E-BUSINESS

- **Digital signature** (see Exhibit 9.3 and Figure 9.4, P-12): This technology validates the identity of the sender and the integrity of an electronic message to reduce the risk that a communication was sent by an unauthorized system or user or was intercepted/modified in transit. To appreciate how digital signatures work, you first must understand the basic mechanics of *data encryption* and *public key cryptography*, topics discussed in Appendix 9A (pg. 312) at the end of this chapter.

Now that you are armed with an understanding of the basic fundamentals of these control plans, look at Exhibit 9.3, and decide if you agree with (and understand) the relationship between each plan and the goal(s) that it addresses. Remember, your ability to explain the relationships among plans and goals is more important than rote memorization.

Before we leave this discussion of controls for manual and automated data entry, let's go back to a topic that we introduced in Chapter 7 and then briefly discussed in Chapter 8. In Auditing Standard Number 2, the PCAOB asserted that auditors must consider the impact that company-level controls (i.e., control environment, pervasive, and general controls) can have on business process controls and application controls. Technology Summary 9.1 (pg. 303) describes the impact that the pervasive and general controls in Chapter 8 can have on the effectiveness of controls in this chapter, specifically the controls in Figures 9.3 and 9.4, and Exhibit 9.3.

Control Plans for Data Entry with Batches

In this section, we introduce you to a hypothetical system wherein we use the example of a shipping and billing process to illustrate certain points. The distinguishing control-related features in this system are that it processes event data in batches, uses *batch totals* as a major control, and produces an *exception and summary report* at the end of major processing steps. Once again, we describe the system, walk you through its systems flowchart, list and explain the control plans associated with batch-oriented systems, and incorporate those plans into a control matrix for the system.

System Description and Flowchart

Figure 9.5 (pg. 304) shows the systems flowchart for our hypothetical batch-processing system. Follow along in the flowchart as we describe the system and discuss some of the assumptions we used in its creation.

Processing begins in the first column of the flowchart with picking tickets that have been received in the shipping department from the warehouse. Let's assume that accompanying these picking tickets are goods that are about to be shipped to customers. Upon receipt of the picking tickets, a shipping department employee assembles them into groups or batches of 25 and calculates batch totals (the nature of the totals that could be taken is discussed in the next section).

EXHIBIT 9.3 Explanation of Cell Entries for the Control Matrix in Figure 9.4

P-1: *Document design.*

- *Effectiveness goal A, efficient employment of resources:* A well-designed document can be completed more quickly (Effectiveness goal A) and can be prepared and entered into the computer with less effort (Efficiency).
- *Input accuracy:* We tend to fill in a well-designed document completely and legibly. If a document is legible, data entry errors will occur less frequently.

P-2: *Written approvals.*

- *Security of resources, input validity:* By checking to see that approvals are present on all input documents, we reduce the possibility that invalid (unauthorized) event data will be input and that resources can be used without approval.

P-3: *Preformatted screens.*

- *Effectiveness goal A, efficient employment of resources:* By structuring the data entry process, automatically populating fields, and preventing errors, preformatted screens simplify data input and save time (Effectiveness goal A) allowing a user to input more data over a period of time (Efficiency).
- *Input accuracy:* As each data field is completed on a preformatted screen, the cursor moves to the next field on the screen, thus preventing the user from omitting any required data set. The data for fields that are automatically populated need not be manually entered, thus reducing input errors. Incorrectly formatted fields are rejected.

P-4: *Online prompting.*

- *Effectiveness goal A, efficient employment of resources:* By asking questions and providing online guidance, this plan ensures a quicker data entry process (Effectiveness goal A) and allows the user to input more data over a period of time (Efficiency).
- *Input accuracy:* The online guidance should reduce input errors.

P-5: *Populate input screens with master data.*

- *Effectiveness goal A, efficient employment of resources:* Automatic population of inputs from the master data results in fewer keystrokes, which should improve the speed and productivity of the data entry personnel.
- *Input validity:* The code entered by the user calls up data from existing records (e.g., a customer record, a sales order record), and those data establish authorization for the input event. For example, without a customer record, a customer order cannot be entered.
- *Input accuracy:* Fewer keystrokes and the use of data called up from existing records reduce the possibility of input errors.

P-6: *Compare input data with master data.*

- *Effectiveness goal A, efficient employment of resources:* Events can be processed on a timelier basis and at a lower cost if errors are detected and prevented from entering the system in the first place.
- *Input validity:* The edits identify erroneous or suspect data and reduce the possibility of the input of invalid events.
- *Input accuracy:* The edits identify erroneous or suspect data and reduce input errors.

P-7: *Procedures for rejected inputs.*

- *Input completeness, input accuracy:* The rejection procedures (i.e., ''Error routine not shown'' annotations) are designed to ensure that erroneous data not accepted for processing are corrected (accuracy) and resubmitted for processing (completeness).

P-8: *Programmed edit checks.*

- *Effectiveness goal A, efficient employment of resources:* Event data can be processed on a timelier basis (Effectiveness goal A) and at a lower cost if errors are detected and prevented from entering the system in the first place (Efficiency).
- *Input accuracy:* The edits identify erroneous or suspect data and reduce input errors.

P-9: *Confirm input acceptance.*

- *Input completeness:* By advising the user that input has been accepted, this confirmation helps ensure input completeness.

EXHIBIT 9.3 Explanation of Cell Entries for the Control Matrix in Figure 9.4 (*continued*)

P-10: *Automated data entry.*

- *Effectiveness goal A, efficient employment of resources:* Inputs are entered more quickly and with personnel resources than are inputs entered manually.
- *Input accuracy:* By eliminating manual keying and using scanning and other technology, the input accuracy is improved.

P-11: *Enter data close to the originating source.*

- *Effectiveness goal A, efficient employment of resources:* This strategy processes events immediately (i.e., no time taken to send to a data entry location). Being familiar with the input may allow the user to input the events more quickly. Finally, some efficiency can be gained by reducing the number of entities handling the event data or by shifting the data entry outside the organization to a business partner (e.g., customers enter orders on the Web).
- *Input completeness:* Because the inputs are captured at the source, they are less likely to be lost as they are transported to the data entry location.
- *Input accuracy:* Because operations personnel or business partners are familiar with the event being entered, they are less likely to make input errors and can more readily correct these errors if they occur.

P-12: *Digital signature.*

- *Security of resources, input validity:* Digital signatures authenticate that the sender of the message has authority to send it and thus prevents the unauthorized diversion of resources. This also determines that the message itself is genuine.
- *Input accuracy:* Detects messages that have been altered in transit, thus preventing input of inaccurate data.

The batch of documents is then scanned onto a magnetic disk. As the batch is recorded onto this disk, the data entry program calculates one or more totals for the batch and displays those batch totals to the shipping clerk. The clerk determines whether the displayed totals agree with the ones previously calculated. If they don't, an error-correcting routine (see "Error routine not shown") is performed. This process is repeated throughout the day as picking tickets are received in the shipping department.

Periodically, the shipment data is sent to the computer for processing by the shipment programs. This program records the inputs on the sales event data (sales journal) and updates the accounts receivable master data to reflect a new open receivable. Invoices are printed and sent to the customer. Packing slips are printed and sent to the shipping department where they are matched with the picking ticket before the goods are sent to the customer. "Further processing" includes packing and shipping the goods.

One of the system outputs is usually an **exception and summary report**. This report reflects the events—either in detail, summary, or both—that were accepted or rejected by the system. Even though the keyed input was edited and validated, some data still could be rejected at the update stage of processing where the computer *compares the input data with the master data*. In our system, a clerk in shipping compares the totals on this report to the input batch totals. Finally, picking tickets and packing slips are compared to ensure that they agree and that no picking tickets remain unshipped for an unduly long period of time.

Applying the Control Framework

In this section, we apply the control framework to the generic batch processing system previously described. Figure 9.6 (pg. 305) presents a completed control matrix for the systems flowchart shown in Figure 9.5 (pg. 304), which has been annotated to show the location of recommended control plans that exist in the system (codes P-1, P-2,. . . . P-5).

Technology Summary 9.1

CONSIDERING THE EFFECT OF COMPANY-LEVEL CONTROLS ON THE BUSINESS PROCESS CONTROLS AND APPLICATION CONTROLS IN FIGURE 9.3

The two types of business process controls in Figure 9.3 (pg. 294) are manual controls and automated (i.e., application) controls. The effectiveness of these controls can depend on the operation of several controls described in Chapter 8. In this summary, we examine some of those relationships.

Manual Controls

There are four controls in Figure 9.3 that depend, somewhat, on the ability, training, and diligence of the data entry personnel. First, *written approvals* will only be effective if the data entry clerk looks for the approval, knows which approvals are valid, and rejects input documents that are not properly approved. Second, when the data entry clerk *compares input data with master data*, we expect that the clerk will know when the inputs don't match the master data and will take action to correct errors that are discovered. Third, to complete the *procedures for rejected inputs*, the data entry clerk must know how to correct the error and will follow through to re-input the corrected document. Fourth, although the computer will *confirm input acceptance*, we must rely on the clerk to wait for the confirmation before moving on to the next input.

What controls in Chapter 8 will improve the effectiveness of these manual controls? There are several examples that we can give. There must be a *segregation of duties* between the person authorizing the input document and the data entry clerk. The organization should employ *selection and hiring* controls to ensure the hiring of quality personnel. All personnel, including data entry clerks, should receive relevant *training and education* to make sure that they *can* perform their required functions and *performance evaluations* to determine that they *do* perform their required functions. Finally, data entry clerks must be provided with *application documentation* explaining how to perform their required functions.

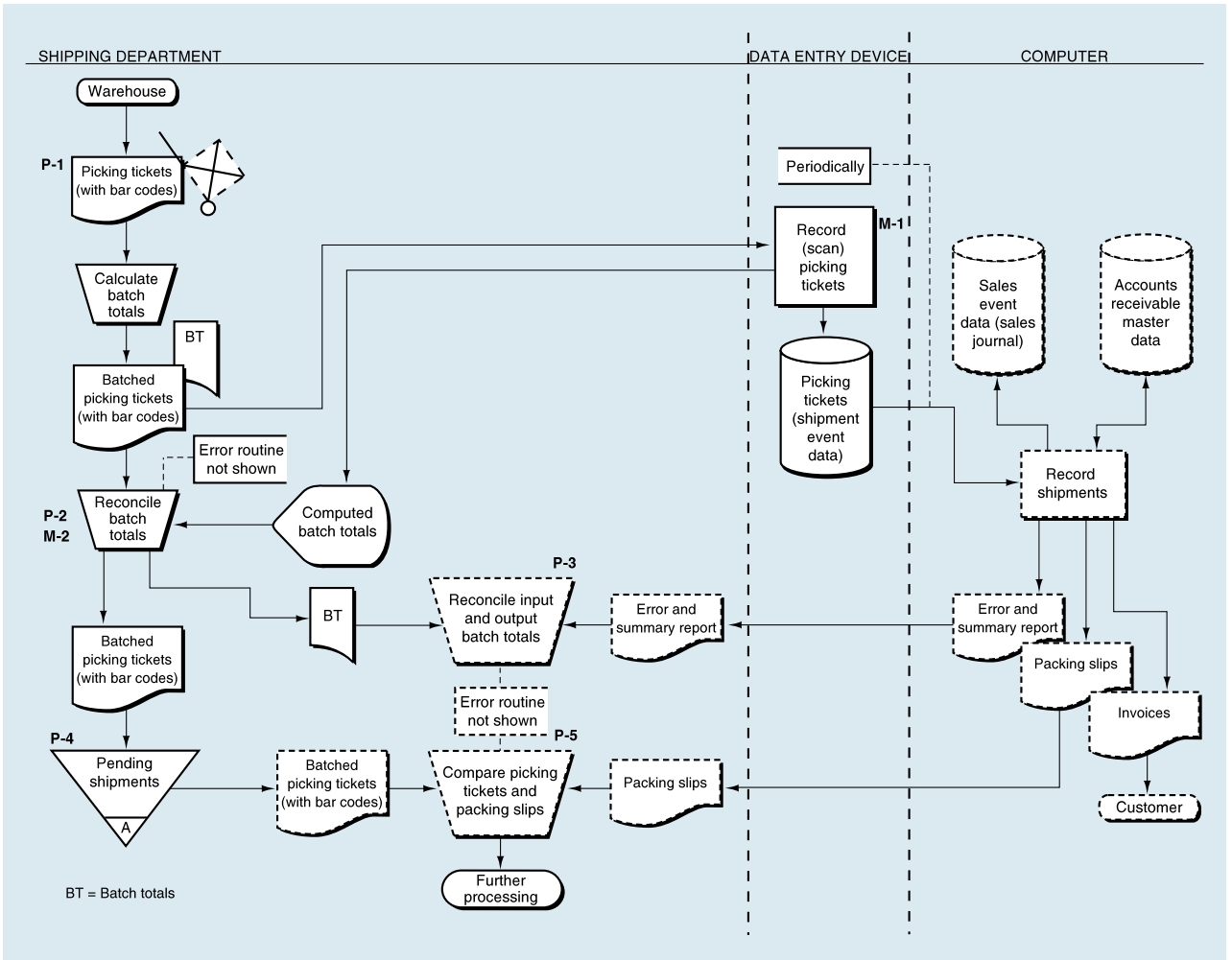
Automated Controls

All of the controls that are performed by the computer system (i.e., application controls) depend on the general controls (also known as IT general controls or ITGCs) in Chapter 8. Those controls include *electronic approvals, compare inputs with master data, programmed edits*, and *digital signatures*. How do we know that these controls and the other automated controls are working as planned? First, we need to know that the programs will perform the controls as designed. Second, we need to know that the stored data used by the computer when executing these controls is valid and accurate. We can ask such questions as ''will the business event be routed to the correct person for approval?'' and ''is the person logged on as the approver really that person or an imposter?'' and ''is the stored customer record used to validate an input a valid record or has it been added by an unauthorized person?''

On which general controls from Chapter 8 do we rely for these automated controls to be effective? There are several examples that we can give. Programs must be developed using a *systems development life cycle (SDLC)* methodology to ensure that user requirements, including controls, are included in the computer programs. Before being implemented, these programs must be tested and approved using *program change controls* to ensure that the program performs as expected and that no unauthorized elements have been included in the programs that might, for example, bypass controls. Finally, access to computer facilities, programs, and data must be restricted to prevent loss or destruction of these assets, or unauthorized changes to the programs and data. A combination of physical access controls, including *perimeter controls, building controls*, and *computer facility controls*, and logical access controls, including *firewalls, security modules*, and *intrusion detection systems (IDS)*, must be in place to protect the computing resources.

We also have some control plans that we *assume* are missing (codes M-1 and M-2) because the narrative system description did not mention them specifically. In Figure 9.4 (pg. 296) we could not complete certain parts of the top of the control matrix. However, for this example, we know the nature of the input (i.e., picking tickets), the resources that are to be protected (i.e., the inventory and the accounts receivable master data), and the

FIGURE 9.5 Systems Flowchart: Data Entry with Batches



data that is to be updated (i.e., the AR master data). Therefore, we have completed these elements in Figure 9.6 (pg. 305).

In this section, we discuss each of the recommended control plans listed in the first column of the matrix.[7] First we describe how the plans work, and then we explain (in Exhibit 9.4) the cell entries appearing in the control matrix. Be sure to trace each plan to the flowchart location where it is implemented (or could be implemented in the case of a missing plan).

Before we start, let's explain what we mean by *batch controls*. **Batch control plans** regulate information processing by calculating control totals at various points in a processing run and subsequently comparing these totals. When the various batch totals fail to agree, evidence exists that an event description(s) may have been lost

7 Many of the controls in this section are adapted from material contained in *Handbook of IT Auditing 2001 Edition* (Chapters D2, D3, and D4, primarily) (Boston: Warren, Gorham & Lamont, 2000). Copyright © 2000 by PricewaterhouseCoopers L.L.P.

FIGURE 9.6 Control Matrix for Data Entry with Batches

	Control Goals of the Shipping Business Process							
	Control Goals of the Operations Process			Control Goals of the Information Process				
Recommended Control Plans	Ensure Effectiveness of Operations	Ensure Efficient Employment of Resources (people, computers)	Ensure Security of Resources (inventory, AR master data)	For the picking ticket inputs, ensure:			For the AR master data, ensure:	
	A			IV	IC	IA	UC	UA
Present Controls								
P-1: Turnaround documents	P-1	P-1		P-1		P-1		
P-2: Manually reconcile batch totals				P-2	P-2	P-2		
P-3: Agree run-to-run totals (reconcile input and output batch totals)			P-3	P-3	P-3	P-3	P-3	P-3
P-4: Review tickler file (file of pending shipments)	P-4				P-4			
P-5: One-for-one checking (compare picking tickets and packing slips)			P-5	P-5	P-5	P-5	P-5	P-5
Missing Controls								
M-1: Sequence check				M-1	M-1			
M-2: Computer agreement of batch totals	M-2	M-2		M-2	M-2	M-2		
Possible effectiveness goals include the following: A = Ensure timely input and processing of picking tickets. See Exhibit 9.4 (pg. 310) for a complete explanation of control plans and cell entries.				IV = input validity IC = input completeness IA = input accuracy UC = update completeness UA = update accuracy				

(completeness exposure), added (validity exposure), or changed (accuracy exposure). Once established, batch totals can be reconciled manually or the computer can reconcile them. In general, for batch control plans to be effective, they should ensure that:

- *All* documents are batched; in other words, the batch totals should be established close to the time that the source documents are created or are received from external entities.
- *All* batches are submitted for processing; batch transmittals and batch logs are useful in protecting against the loss of entire batches.

- *All* batches are accepted by the computer; the user should be instrumental in performing this checking.
- *All* differences disclosed by reconciliations are investigated and corrected on a timely basis.

Batch control procedures must start by grouping event data and then calculating a control total(s) for the group. For example, Figure 9.5 (pg. 304) shows the shipping department employee preparing batch totals for the picking tickets documents to be scanned.

Several types of batch control totals can be calculated, as discussed in the following paragraphs. You will note in the following discussion that certain types of batch totals are better than others in addressing the information process control goals of input validity, input completeness, and input accuracy.

Document/record counts are simple counts of the number of documents entered (e.g., 25 documents in a batch). This procedure represents the minimum level required to control *input completeness*. It is not sufficient if more than one event description can appear on a document. For example, consider the event "sale of goods" where each document reflects a sale. If each document can include one or more line items (say, one television set and three chairs are listed as a single sale), then a document/record count would not reflect multiple sale items. Also, because one document could be intentionally replaced with another, this control is not effective for ensuring input *validity* and says nothing about input *accuracy*.

Item or line counts are counts of the number of items or lines of data entered, such as a count of the number of invoices being paid by all the customer remittances. By reducing the possibility that line items or entire documents could be added to the batch or not be input, this control improves input *validity*, *completeness*, and *accuracy*. Remember, a missing event record is a *completeness* error, and a data set missing from an event record is an *accuracy* error.

Dollar totals are a summation of the dollar value of items in the batch, such as the total dollar value of all remittance advices in a batch. By reducing the possibility that entire documents could be added to or lost from the batch or that dollar amounts were incorrectly input, this control improves input *validity*, *completeness*, and *accuracy*.

Hash totals are a summation of any numeric data existing for all documents in the batch, such as a total of customer numbers or invoice numbers in the case of remittance advices. Unlike dollar totals, hash totals normally serve no purpose other than control. Hash totals can be a powerful batch control because they can determine whether inputs have been altered, added, or deleted. These *batch* hash totals operate for a batch in a manner similar to the operation of *document/record hash totals* for individual inputs.

As we did previously with the controls for automated and manual data entry, we begin by defining and explaining the controls plans in Figures 9.5 (pg. 304) and 9.6 (pg. 305) and then summarize, in Exhibit 9.4 (pg. 296), each cell entry in Figure 9.6, the control matrix.

- **Turnaround documents** (see Exhibit 9.3 and Figure 9.4, P-1): Used to capture and input a *subsequent* event. Picking tickets, inventory count sheets, and remittance advice stubs attached to customer invoices are all examples of turnaround documents. For example, we have seen picking tickets that are printed by the computer, used to pick the goods, and sent to shipping where the *bar code* on the picking ticket is scanned to trigger the recording of the shipment. Thus, turnaround documents can facilitate *automated data entry* described in Figures 9.3 (pg. 294) and 9.4 (pg. 296). Turnaround documents can be used for the input of individual items,

rather than batches. In such cases, the scanning computer displays the scanned data, such as items and quantities to be shipped, to the data entry clerk, or shipping clerk. If the data has been scanned correctly, the clerk need only press one key or click the mouse button to record the input.

Although technically the following control is missing from the process depicted in Figure 9.5 (pg. 304), we would not advocate that it be added because we prefer to scan the documents to enhance the validity and accuracy of the data entry process. However, key verification is occasionally applied to the input of low-volume, high-value batches of events and should be described here so that you know about this powerful control.

- **Key verification:** This takes place when input documents are keyed by one individual and then re-keyed by a second individual. The data entry software compares the second keystrokes to the strokes keyed by the first individual. If there are differences, it is assumed that one person misread or miskeyed the data. Someone, perhaps a supervisor or the second clerk, would determine which keying was correct, the first or the second, and make corrections as appropriate to ensure that the input is accurate. Key verification is depicted in Figure 4.7 part e on pg. 109.

We notice, at this point, that a sequence check is not applied to the input documents. Read on about a type of control that could have been applied at this point:

- *Sequence checks* (see Exhibit 9.3 and Figure 9.4, M-1): Whenever documents are numbered sequentially—either assigned a number when the document is prepared or received from an external source or the input document is *prenumbered*—a **sequence check** can be applied to those documents to determine that all documents have been processed (*completeness*) and that no extra documents have been processed (*validity*). One of two kinds of sequence checks may be used—either a batch sequence check or a cumulative sequence check.

In a **batch sequence check**, the event data within a batch are checked as follows:

1. The range of serial numbers constituting the documents in the batch is entered.
2. Each individual, serially prenumbered document is entered.
3. The computer program sorts the input documents into numerical order; checks the documents against the sequence number range; and reports missing, duplicate, and out-of-range data.

If the documents come from an external source, and we cannot control the serial numbers of the input data, we can assign numbers to the items as the batch is prepared for processing.

A slight variation on the batch sequence check is the cumulative sequence check. The **cumulative sequence check** provides input control in those situations in which the serial numbers are assigned within the organization (e.g., sales order numbers issued by the sales order department) but later are not entered in perfect serial number sequence (i.e., picking tickets do not necessarily arrive at the shipping department in sequence). In this case, the matching of individual event data (picking ticket) numbers is made to a file that contains *all* document numbers (all sales order numbers). *Periodically*, reports of missing numbers are produced for manual follow-up.

Reconciling a checkbook is another example of a situation in which numbers (the check numbers) are issued in sequence. When we receive a bank statement, the batch may not contain a complete sequence of checks. Our check register assists us in

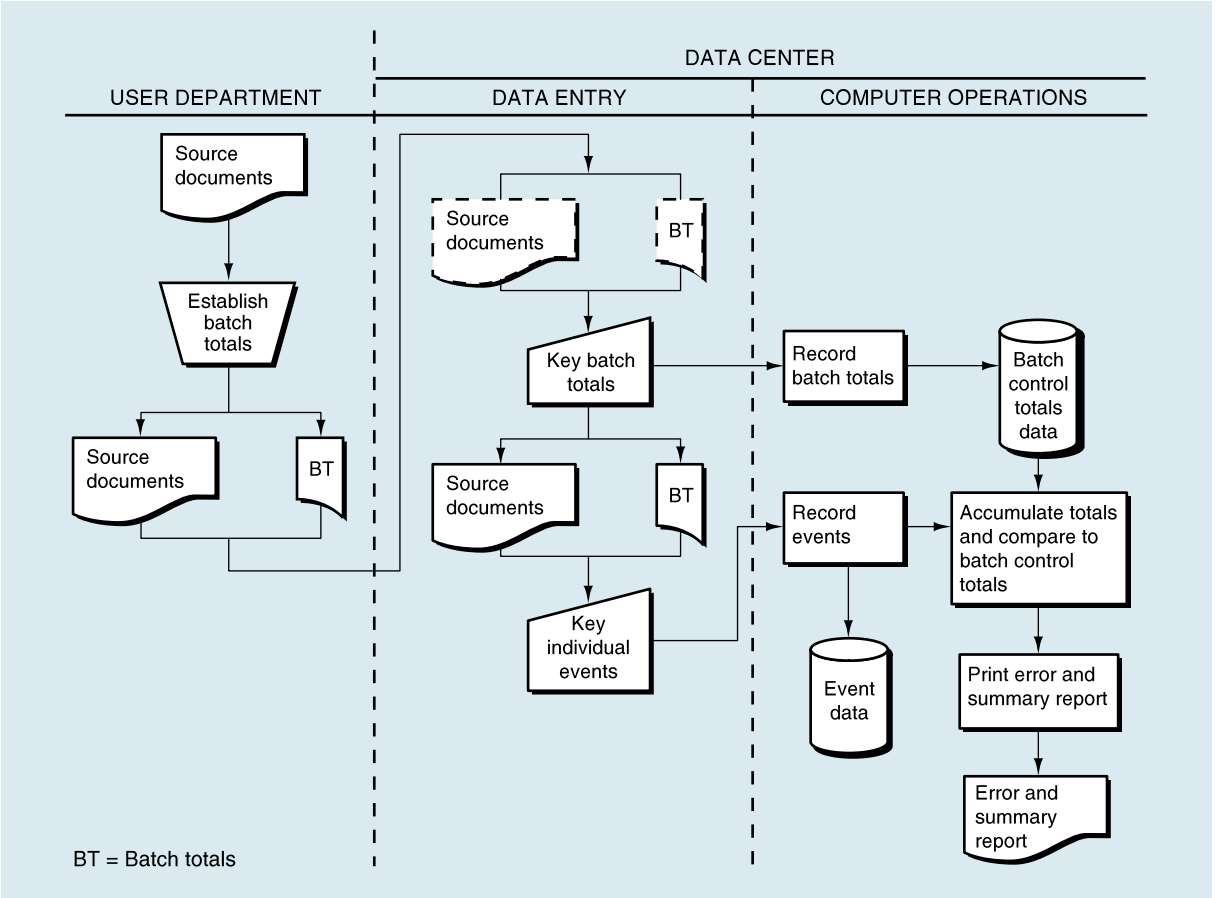
performing a cumulative sequence check to make sure that all checks are eventually cleared.

- *Manually reconcile batch totals* (see Exhibit 9.3 and Figure 9.4, P-2): The **manual reconciliation of batch totals** control plan operates in the following manner:
  1. One or more of the batch totals are established manually (i.e., in the shipping department in Figure 9.5, pg. 304).
  2. As individual event descriptions are entered (or scanned), the data entry program accumulates independent batch totals.
  3. The computer produces reports (or displays) at the end of either the input process or update process, or both. The report (or display) includes the relevant control totals that must be manually reconciled to the totals established prior to the particular process.
  4. The person who reconciles the batch total (see the shipping department employee in Figure 9.5) must determine why the totals do not agree and make corrections as necessary to ensure the integrity of the input data.

We notice, at this point, that the clerk must perform a manual reconciliation of the batch totals. Read on about a more efficient means for performing that reconciliation:

- *Computer agreement of batch totals* (see Exhibit 9.3 and Figure 9.4, M-2): This control plan does not exist in Figure 9.5 (pg. 304) and therefore is shown as a missing plan. Note in Figure 9.5 where we have placed the M-3 annotation. The **computer agreement of batch totals** plan is pictured in Figure 9.7 and works in the following manner:
  1. First, one or more of the batch totals are established manually (i.e., in the user department in Figure 9.7).
  2. Then, the manually prepared total is entered into the computer and is written to the computer batch control totals data.
  3. As individual source documents are entered, a computer program accumulates independent batch totals and compares these totals to the ones prepared manually and entered at the start of the processing.
  4. The computer prepares a report, which usually contains details of each batch, together with an indication of whether the totals agreed or disagreed. Batches that do not balance are normally rejected, and discrepancies are manually investigated. Such an analysis would be included in a report similar to the "Error and summary report" in Figures 9.5 (pg. 304) and 9.7.
- *Agree run-to-run totals (reconcile input and output batch totals)* (see Exhibit 9.3 and Figure 9.4, P-3): This is a variation of the reconciliation/agreement of batch totals controls. We **agree run-to-run totals** by reconciling totals prepared before a computer process has begun to totals prepared at the completion of the computer process. The totals may be prepared and reconciled either manually or by the computer. The post-process controls are often found on an *error and summary* report (i.e., totals prepared by the computer). When totals agree, we have evidence that the input *and* the update took place correctly. This control is especially useful when there are several intermediate steps between the beginning and the end of the process, and we want to be assured of the integrity of each process.
- *Review tickler file (file of pending shipments)* (see Exhibit 9.3 and Figure 9.4, P-4): A **tickler file** is a manual file of documents, or a computer file, that contains

FIGURE 9.7 Computer Agreement of Batch Totals Control Plan



business event data that is pending further action. Such files must be reviewed on a regular basis for the purpose of taking action to clear items from that file. Whereas Figure 9.5 (pg. 304) shows a file of picking ticket items that should be shipped ("Pending Shipments" file), tickler files also may be computer records reflecting events that need to be completed, such as open sales orders, open purchase orders, and so forth. Should tickler file documents remain in the file for an extended period of time, the person or computer monitoring the file would determine the nature and extent of the delay. In our example, after packing slips are received, the picking tickets are compared to their associated packing slips and removed from the Pending Shipments file. We are classifying this as a present control because we are assuming that the shipping clerk periodically reviews the file looking for picking tickets that have been pending for too long.

- *One-for-one checking (compare picking tickets and packing slips)* (see Exhibit 9.3 and Figure 9.4, P-5): **One-for-one checking** is the detailed comparison of the individual elements of two or more data sources to determine that they agree. This control is often used to compare a source document to an output produced later in a process. Differences may indicate errors in input or update. If the output cannot be found for comparison, there is evidence of failure to input or process the event. This procedure

EXHIBIT 9.4 Explanation of Cell Entries for the Control Matrix in Figure 9.6

P-1: *Turnaround documents.*

- *Effectiveness goal A, efficient employment of resources:* By scanning the picking ticket, we reduce the amount of data that must be input to record the shipment and improve the speed (effectiveness) and productivity of the data entry personnel (efficiency).
- *Input validity:* The turnaround documents were printed in a different functional area. This separates event authorization (as reflected by the picking ticket) from execution of the shipment (as represented by the packing slips).
- *Input accuracy:* Using a prerecorded bar code to trigger the event reduces the possibility of input errors.

P-2: *Manually reconcile batch totals.*

- *Input validity, input completeness, input accuracy:* Agreement of the batch totals at this point ensures that only valid source documents comprising the original batch have been input (*input validity*), that all source documents were input (*input completeness*), and that data elements appearing on the source documents have been input correctly (*input accuracy*).

P-3: *Agree run-to-run totals (reconcile input and output batch totals).*

- *Security of resources, input validity:* By determining that updates to the accounts receivable master data reflect goods picked and about to be shipped, we reduce the possibility of recording an invalid sales event and shipping to customers who did not order, and will not pay for, the goods.
- *Input completeness, input accuracy, update completeness, update accuracy:* By comparing totals prepared before the input to those produced after the update, we ensure that all events were input (*input completeness*), all events were input correctly (*input accuracy*), all events were updated to the master data (*update completeness*), and all events were updated correctly to the master data (*update accuracy*).

P-4: *Review tickler file (file of pending shipments).*

- *Effectiveness goal A, input completeness, update completeness:* A file of picking tickets is retained in shipping awaiting packing slips. If the packing slips are received in a timely manner, and the corresponding picking tickets are removed from the ''Pending Shipments'' file, we can ensure that goods will be shipped in a timely manner and that the picking tickets were indeed input and the master data updated. If picking slips do not receive packing slips within a reasonable period of time, then an inquiry procedure is initiated to determine the nature and extent of the delay.

P-5: *One-for-one checking (compare picking tickets and packing slips).*

- *Security of resources, input validity:* By matching details on the picking tickets with the data on the packing slips produced by the computer, we reduce the possibility that an invalid sales event has been recorded and that we will not ship goods to customers who did not order, and will not pay for, the goods.
- *Input completeness, input accuracy, update completeness, update accuracy:* By matching details on the picking tickets (i.e., the inputs) with the details on the packing slips produced by the computer, we ensure that all events were input (*input completeness*), all events were input correctly (*input accuracy*), all events were updated to the master data (*update completeness*), and all events were updated correctly to the master data (*update accuracy*).

M-1: *Sequence check.*

- *Input validity, input completeness:* By comparing an expected sequence of documents to those actually input, sequence checks can detect a second occurrence of a particular document number, which would suggest that the second event is invalid, and can detect missing document numbers, suggesting that not all events had been input.

M-2: *Computer agreement of batch totals.*

- *Effectiveness goal A, efficient employment of resources:* Had the computer been used to reconcile the control totals, the processing of the events would have been completed more quickly and with less human effort.
- *Input validity, input completeness, input accuracy:* Regarding these control goals, the effect of this control is the same as P-2. Agreement of the batch totals at this point would have ensured that only valid source documents comprising the original batch had been input, that all source documents were input, and that data elements appearing on the source documents had been input correctly.

provides detail as to *what* is incorrect within a batch. Because it's very expensive to perform, one-for-one checking should be reserved for low-volume, high-value events.

Now that we have examined what each of the recommended control plans means and how each operates, we can look at how the plans meet the control goals. Exhibit 9.4 explains the relationship between each control plan and each control goal that it helps to achieve. As you study Exhibit 9.4, we again urge you to concentrate your energies on understanding these relationships.

Summary

In this chapter, we began our study of business process control plans, the third level in the control hierarchy shown in Figure 7.6 in Chapter 7 (pg. 233). Our study of business process control plans will continue in Chapters 10 through 15, where we will apply the control framework and explore those controls that are unique to each business process. Exhibit 9.5 provides a framework for determining how well these pervasive, general, business process, and application controls can perform. That is, this framework helps us determine the "effectiveness of the design of controls" required by the PCAOB in Auditing Standard Number 2.

Before we leave this chapter, let's address one more aspect of business process controls and application controls. Many of these controls attempt to detect data that *may* be in error. For example, a *reasonableness check* may reject a price change that is beyond a normal limit, even though the price change has been authorized and correctly entered. As another example, perhaps a customer order is rejected because it does not pass the credit check, but it might be in the best interest of the company to permit the sale. In these cases, we need to be able to *override* the control and permit the event to process. If our control system is to remain effective, these overrides must be used sparingly and securely (e.g., requiring a *password* or key and signature to effect the override). Finally, a record of all overrides should be periodically reviewed to determine that the override authority is not being abused.

EXHIBIT 9.5 Level of Assurance Provided by Internal Controls

The degree of assurance, the quality, and the effectiveness of internal controls may be based on several factors:

Less Assurance	Greater Assurance
Manual control	Automated control
Control is performed by a junior, inexperienced person	Control is performed by an experienced manager
Detective control	Preventive control
Single control	Multiple, overlapping controls
Control checks some items (sampling)	Control checks all items
Control takes place after the event occurs	Control takes place as the event occurs

Source: Adapted from *Sarbanes-Oxley Act: Section 404, Practical Guidance for Management*, PricewaterhouseCoopers, July 2004, pp. 52–53.

Key Terms

document design
written approvals
electronic approvals
preformatted screens
online prompting
populate input screens with master data
compare input data with master data
procedures for rejected inputs
programmed edit checks
reasonableness checks
limit checks
document/record hash totals
mathematical accuracy checks
check digit verification
confirm input acceptance
automated data entry
enter data close to the originating sourced
digital signature
exception and summary report
batch control plans
document/record counts
item or line counts
dollar totals
hash totals
turnaround documents
key verification
sequence check
batch sequence check
cumulative sequence check
manual reconciliation of batch totals
computer agreement of batch totals
agree run-to-run totals
tickler file
one-for-one checking
data encryption

Appendix 9A

Data Encryption and Public Key Cryptography

E-Business

Data encryption is a process that employs mathematical algorithms and encryption keys to encode data (i.e., change it from plaintext to a coded text form) so that it is unintelligible to the human eye and therefore useless to those who should not have access to it. Encryption is used (or should be used) in situations where the data are of such a sensitive nature that we want to preserve the data's privacy and confidentiality. For example, people are asking for and obtaining security of their Internet transmissions through cryptography. Technology Application 9.1 (at the end of this Appendix on pg. 316) describes three methods for conducting secure electronic commerce on the Internet using data encryption and public key cryptography.

One of the earliest and most elementary uses of encryption dates back to the first century B.C. During the Gallic Wars, Julius Caesar encoded his messages by shifting the alphabet three letters forward so that an A became a D, an X became an A, and so on. For instance, if the message is NED IS A NERD—called *plaintext* in cryptography lingo—the *ciphertext* would appear as QHG LV D QHUG. The *Caesar cipher*—an example of a simple one-for-one letter substitution system—in effect used a *key* of 3 and an encrypting *algorithm* of addition. We still see examples of this type of encryption in the cryptograms or cryptoquotes that are published in the puzzle pages of our daily newspapers.

With the use of more complex *algorithms* and encryption *keys*, coding a message can be made much more powerful than in the preceding example. Figure 9.8 contains an illustration of how the message NED IS A NERD could be made more difficult to decode. Keep in mind, however, that the figure also is a very basic, rudimentary example intended to convey the bare-bones mechanics of how encryption works. In practice,

FIGURE 9.8 Example of Data Encryption

EncryptPlain (i.e., encode a message):										
1.	Plaintext message	N	E	D	I	S	A	N	E	R	D
2.	(Letter of the alphabet)	(14	5	4	9	19	1	14	5	18	4)
3.	Encryption algorithm	+	-	+	-	+	-	+	-	+	-
4.	Key	3	1	7	6	3	4	8	6	7	9
5.	(Letter of the alphabet)	(17	4	11	3	22	23	22	25	25	21)
6.	Ciphertext	Q	D	K	C	V	W	V	Y	Y	U
Decrypt (i.e., decode a message):										
7.	Ciphertext (from line 6)	Q	D	K	C	V	W	V	Y	Y	U
8.	(Letter of the alphabet)	(17	4	11	3	22	23	22	25	25	21)
9.	Decryption algorithm	-	+	-	+	-	+	-	+	-	+
10.	Key (same as line 4)	3	1	7	6	3	4	8	6	7	9
11.	(Letter of the alphabet)	(14	5	4	9	19	1	14	5	18	4)
12.	Decorded message	N	E	D	I	S	A	N	E	R	D

algorithms and keys are much more sophisticated, so much so that good encryption schemes are virtually impossible to break.

Please note the following about Figure 9.8:

- Each letter of the alphabet is assigned a number—A = 1 through Z = 26—to designate its position in the alphabet.
- If symbols as well as letters appeared in the character set, they would be designated by the numbers 27, 28, and so on.
- The key can be any string of random numbers, one number for each character in the message. In conventional, single-key encryption, the *same* key (see lines 4 and 10) is used both to encrypt and decrypt the message.
- The mathematical formula (i.e., algorithm) on line 3 is used to apply the key (line 4) to the plaintext message. In this simplistic example, we use an algorithm that alternates the basic math functions of plus and minus (i.e., plus for the first character, minus for the second, plus for the third, and so forth).
- The decryption algorithm on line 9 is the reverse of that on line 3 (i.e., each plus on line 3 is a minus on line 9, and vice versa).
- Unlike the simple puzzle-page cryptogram in our first example, a particular plaintext character—such as the N in *N*ED and in *N*ERD—does not translate on a one-for-one basis into a single ciphertext character. For instance, the first N on line 1 becomes a Q on line 6, whereas the second N becomes a V.

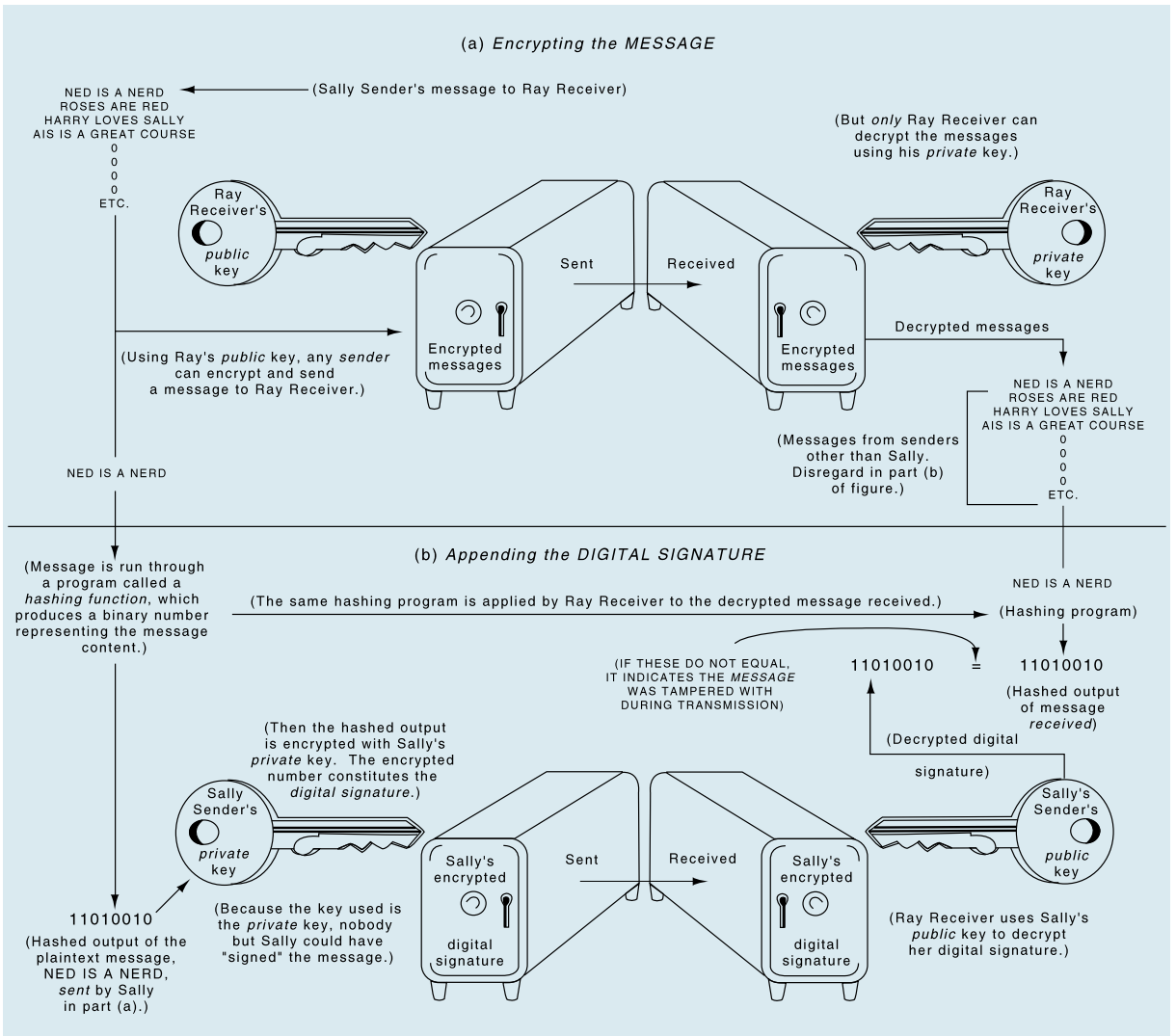
As shown in Figure 9.8, the crux of conventional encryption procedures is the *single key* used both by the sender to encrypt the message and by the receiver to decrypt it. A major drawback to such systems is that the key itself has to be transmitted by secure channels. If the key is not kept secret, the security of the entire system is compromised. *Public key cryptography* helps to solve this problem by employing a *pair* of matched keys for each system user, one private (i.e., known only to the party who possesses it) and one

public. The public key corresponds to but is not the same as the user's private key. As its name implies, the public key is assumed to be public knowledge and even could be published in a directory, in much the same way as a person's telephone number.

Figure 9.9 illustrates how public key cryptography is used both to *encrypt* messages (part (a) of the figure) and to *authenticate* a message by appending a digital signature to it (part (b) of the figure). Please note that although we show both parts (a) and (b) being executed, in practice, the parts are separable. That is, a message could be encrypted as shown in part (a) without having a *digital signature* added to it. Digital signatures enhance security by ensuring that the "signature" cannot be forged (i.e., that the message comes from an authorized source) and that the message has not been changed in any way in transmission.

The figure tells the story, so we discuss it only briefly. First note that Sally Sender and Ray Receiver each have a *pair* of keys. In part (a), Ray's *public* key is used to encrypt *all* messages sent to him. Privacy of the messages is ensured because only Ray's *private* key can decrypt the messages. The messages *cannot* be decoded using Ray's public key.

FIGURE 9.9 Illustration of Public Key Cryptography and Digital Signatures



Furthermore, the private decryption key never has to be transmitted; it is always in Ray's exclusive possession. This process ensures that only Ray can read the message using his private key.

In part (b), Sally first uses a hashing function to translate the plaintext message into a binary number. Any message *other* than NED IS A NERD would not "hash" into the number 11010010. By then using her *private* key to encrypt the binary number, Sally, in effect, has digitally "signed" the message. On the right side of part (b), Ray Receiver employs Sally's *public* key to decrypt her "signature." Because no public key except Sally's will work, Ray knows that the message comes from her. Note that *anyone* could use Sally's public key to decode her signature, but that is not important. The object is not to keep the signature secret or private but rather to *authenticate* that it was Sally, and *only* she, who "signed" the message.

To ensure the *integrity of the message* (received in part (a) of the figure), Ray does the following:

- Runs the decrypted message, NED IS A NERD, through a hashing function—the same hashing function used by Sally.
- Compares the decoded digital signature (11010010) with the hashed output of the message *received* (11010010). If the two numbers don't agree, Ray knows that the message is not the same as the one Sally sent. For example, assume that Ted Tamperer was able to intercept Sally's encrypted message in part (a) and change it so that when Ray decoded it, he read NED IS A NICE GUY. This message would *not* hash into the number 11010010; therefore, it would not match the decrypted digital signature from Sally.

The process, then, tells us if Sally sent the message and if the message has been changed.

E-BUSINESS

Some experts predict that digital signatures will soon pave the way for a truly cashless society, which has been talked about for years. The digital signatures will be used to create electronic cash, checks, and other forms of payment that can be used in electronic commerce (see Technology Application 9.1, pg. 316, for examples). Others foresee digital signatures replacing handwritten ones on a multitude of business and legal documents, such as purchase orders, checks, court documents, and tax returns. The Millennium Digital Commerce Act of 2002 makes contracts "signed" by electronic methods legally valid in all 50 states. This law was designed to accelerate the rate of growth of business-to-business (B2B) *e-business* by allowing companies to immediately execute documents online.

Digital signatures also offer an additional benefit to e-business transactions. Buyers and sellers of goods and services over the Internet can only feel comfortable about the business transaction if one party is sure that the other party will not renege on the agreement. One way for a party to back off from an agreement is to repudiate or disclaim the agreement. If the other party cannot prove that a legally binding agreement took place in the first place, the reneging party might be successful. To ward off this threat, digital signatures are used to ensure *nonrepudiation*; that is, digital signatures offer the necessary proof that a legal "meeting of the minds" took place, as neither party can successfully dispute or repudiate the existence and authenticity of a document and/or signature.

One final thought—for public key cryptography to be effective, the *private* keys must be kept *private*. To do that, we can employ a variety of techniques, some of which were introduced in Chapter 8. For example, the private key might be kept within a protected computer or device such as a *cryptographic box*. Access to the device, and to the private key, must then be protected with *passwords* or other *authentication* procedures.

TECHNOLOGY APPLICATION 9.1

USING DATA ENCRYPTION AND PUBLIC KEY CRYPTOGRAPHY FOR E-COMMERCE

Data encryption and public key cryptography are being used to secure business transactions on the Internet. Following are three examples. Although all three are currently in use, only SSL is widely used.

Case 1: SSL

The Secure Sockets Layer (SSL) handshake protocol was developed by Netscape Communications Company and uses public key cryptography to secure communications on the Internet. With SSL, a secure session is established during which messages transmitted between two parties are protected via encryption. For example, before a consumer transmits a credit card number to a merchant, the merchant's server establishes a secure session. The merchant receives the message, decrypts it, extracts the credit card number, and submits a charge to the consumer's credit card company (i.e., credit card issuing bank) to clear the transaction using traditional means. With SSL, the consumer is protected from interception and unauthorized use of the purchase and credit card information while on the Internet (i.e., from the consumer's Web browser to the merchant's Web server). Normally, the merchant cannot authenticate the transmission to determine from whom the message originated, and the consumer has only moderate assurance that he or she has sent the credit card number to a legitimate merchant.

Case 2: eCheck

The electronic check (eCheck) is a payment mechanism developed by the Financial Services Technology Consortium (FSTC). Using public key cryptography and digital signatures, trading partners and their banks can transmit secure messages and payment information. eCheck certificates are issued by banks certifying that the holder of the certificate has an account at that bank. Payments are processed automatically through the existing bank systems. Payments are checks drawn on bank accounts. A feature beyond SSL is that the eCheck protocol defines message formats, such as purchase orders, acknowledgments, and invoices, which can be processed automatically by trading parties. The basic technology developed for eCheck is being used by Xign Corp. for the Internet-based purchasing/payment system it hosts for buying and selling organizations. Also, the U.S. Department of the Treasury is developing an eProcurement system, the Internet Payment Platform (IPP), which is supported by Xign Corp.

Case 3: Smart Cards

In an increasingly online environment, where critical corporate information and business transactions are exchanged over open networks, privacy and security are essential. A possible solution to ensuring such privacy and security is a smart card, which is a small electronic device about the size of a credit card that includes embedded memory and sometimes integrated circuits. Smart cards use the public key infrastructure (PKI) technology to provide everything from digital cash, signatures, authentication, authorization, and security on a single card platform. Because PKI technology is built into smart cards, should you lose your card, no one else can use it without your private key. Smart cards are presently used in a wide array of transactions, such as telephone, banking, and healthcare—both on and off the Internet. Although the popularity of smart cards is growing rapidly in the United States, they are already used extensively in Europe and Japan. Smart cards are more reliable, can store more information, and are more tamper-resistant than magnetic stripe cards; smart cards can be disposed or reused; they can be programmed to perform single or multiple functions; and, smart cards are compatible with portable electronic devices and PCs. In fact, when President Bill Clinton signed the Millennium Digital Commerce Act of 2002, he did not use the traditional quill pen, rather, he used a smart card that contained his digital signature!

Source: As of July 2006, you can find information about these technologies at the following sites: SSL (http://www.verisgn.com); eCheck (http://www.echeck.org); Xign Corp. (http://www.xign.com); and Internet Payment Platform (http://www.ipp.gov). For information about smart cards, you might use Google to find a number of sites, including http://www.howstuffworks.com and http://www.wikipedia.org.

One such procedure involves the use of a thumbprint reader or retinal imager attached to the computer. With such devices, users must put their thumb onto the reader or eye into an imager before the private key can be used to "sign" a message. The thumbprint reader and retinal imager are examples of the *biometric* devices introduced in Chapter 8.

Review Questions

RQ 9-1 Explain the difference between the category of business process control plans and application control plans covered in this chapter and the business process controls and application controls to be covered in Chapters 10 through 16.

RQ 9-2 Describe the relationship between the *control matrix* and the *systems flowchart*.

RQ 9-3 How could the control matrix be used to recommend changes in the system to improve control of that system?

RQ 9-4 How would the control matrix be useful in evaluating control *effectiveness*, control *efficiency*, and control *redundancy*? Include in your answer a definition of these three terms.

RQ 9-5 What are the steps involved in preparing a control matrix?

RQ 9-6 Describe the four common *programmed edit checks*.

RQ 9-7 How do the 12 control plans listed in Figure 9.4 (pg. 296) work?

RQ 9-8 Name and explain four different types of batch totals that could be calculated in a batch-processing system.

RQ 9-9 How do the eight control plans (five present, three missing) listed in Figure 9.6 (pg. 305) work?

RQ 9-10 Referring to Appendix 9A, distinguish among data encryption, public key cryptography, and digital signatures.

Discussion Questions

DQ 9-1 Discuss why the control matrix is custom-tailored for each business process.

DQ 9-2 Explain why input controls are so important. Discuss fully.

DQ 9-3 In evaluating business process controls and application controls, some auditors differentiate between the point in the system at which the control is ''established'' and the *later* point at which *that* control is ''exercised.'' Speculate about the meaning of the terms *''establish a control''* and *''exercise a control''* by discussing those terms in the context of:

a. Batch total procedures
b. Turnaround documents
c. Tickler files

DQ 9-4 ''The mere fact that event data appear on a prenumbered document is no proof of the validity of the event. Someone intent on defrauding a system by introducing a fictitious event probably would be clever enough to get access to the prenumbered documents or would replicate those documents to make the event appear genuine.''

a. Do you agree with this comment? Why or why not?
b. Without prejudice to your answer to part (a), assume that the comment is true. Present (and explain) a ''statement of relationship'' between the control plan of using prenumbered documents and the information system control goal of event ''validity.''

DQ 9-5 Describe situations in your daily activities, working or not, where you have experienced or employed controls discussed in this chapter.

DQ 9-6 When we record our exams into the spreadsheet used for our grade book, we employ the following procedures:

1. For each exam, manually add up the grade and record on the front page.
2. Manually calculate the average grade for all of the exams.
3. Input the score for each part of each exam in the spreadsheet.
4. Compare the exam total on the front page of the exam to the total prepared by the computer.
5. After all the exams have been entered, compare the average grade calculated by the computer with that calculated manually.

Describe how this process employs controls discussed in this chapter.

DQ 9-7 Referring to Appendix 9A, ''Protecting the private key is a critical element in public key cryptography.'' Discuss fully.

DQ 9-8 On October 2, 2002, a clerk at Bear Stearns had erroneously entered an order to sell nearly $4 billion worth of securities. The trader had sent an order to sell $4 million worth. Only $622 million of the orders were executed, the remainder of the orders were canceled prior to execution. Reports stated that it was a human error, not a computer error and that it was the fault of the clerk, not the trader. What is your opinion of these reports? What controls could have *prevented* this error?

DQ 9-9 ''Technology Summary 9.1 seems to indicate that the business process and application control plans in this chapter cannot be relied on.'' Do you agree? Discuss fully.

DQ 9-10 ''If a business process is implemented with OLRT processing, we do not need to worry about update completeness and update accuracy.'' Do you agree? Discuss fully.

Problems

P 9-1 You worked with the Causeway Company cash receipts system in Chapter 4. The narrative of that system and its systems flowchart are reproduced in Exhibit 9.6 (pg. 320) and Figure 9.10, respectively.

Using Exhibit 9.6 and Figure 9.10, do the following:

a. Prepare a control matrix, including explanations of how each recommended control plan helps to accomplish—or would accomplish in the case of missing plans—each related control goal. Your choice of recommended control plans should come from Figure 9.1 (pg. 286)/Exhibit 9.1 (pg. 287), Figure 9.4 (pg. 296)/Exhibit 9.3 (pg. 301), or Figure 9.6 (pg. 305)/Exhibit 9.4 (pg. 310) as appropriate. Be sure to tailor the matrix columns to conform to the specifics of the Causeway system. In doing so, assume the following two effectiveness goals only:

- Timely deposit of checks
- Comply with compensating balance agreements with the depository bank

b. Annotate the systems flowchart in Figure 9.10 to show the location of each control plan listed in the control matrix.

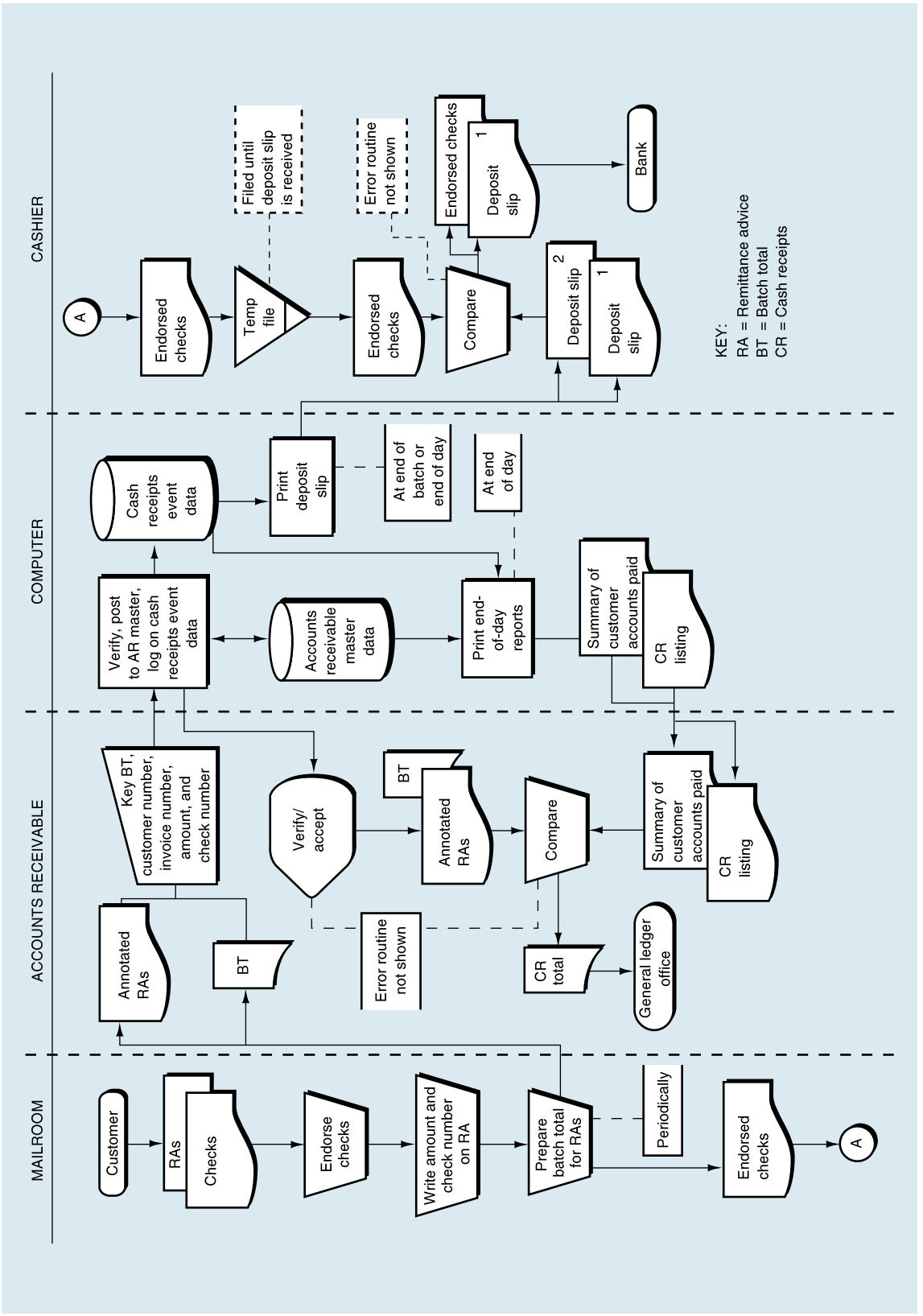


FIGURE 9.10 Causeway Company Systems Flowchart to Accompany Problem 9-1

EXHIBIT 9.6 Causeway Company System Narrative to Accompany Problem 9-1

Causeway Company uses the following procedures to process the cash received from credit sales. Customers send checks and remittance advices to Causeway. The mailroom clerk at Causeway endorses the checks and writes the amount paid and the check number on the remittance advice. Periodically, the mailroom clerk prepares a batch total of the remittance advices and sends the batch of remittance advices to accounts receivable, along with a copy of the batch total. At the same time, the clerk sends the corresponding batch of checks to the cashier.

In accounts receivable, a clerk enters the batch into the computer by keying the batch total, the customer number, the invoice number, the amount paid, and the check number. After verifying that the invoice is open and that the correct amount is being paid, the computer updates the accounts receivable master data. If there are any discrepancies, the clerk is notified.

At the end of each batch (or at the end of the day), the computer prints a deposit slip in duplicate on the printer in the cashier's office. The cashier compares the deposit slip to the corresponding batch of checks and then takes the deposit to the bank.

As they are entered, the check number and the amount paid for each receipt are logged on a disk. This event data is used to create a cash receipts listing at the end of each day. A summary of customer accounts paid that day is also printed at this time. The accounts receivable clerk compares these reports to the remittance advices and batch totals and sends the total of the cash receipts to the general ledger office.

P 9-2 The following narrative describes the processing of customer mail orders at PetChip Company:

PetChip Company is a small manufacturing operation engaged in the selling of digital identification chips that can be implanted into household pets, such as cats and dogs. Customers (e.g., veterinary clinics, animal hospitals) send orders by mail to the sales order department, where sales order clerks open the orders and review them for accuracy. For each order, the clerks enter the customer number, and the computer displays the customer record. The clerk matches the customer information on the screen with the customer order. Assuming that they match, the clerk enters the items and quantities being ordered. The computer edits the order by comparing the input data to customer and inventory master data. Assuming that the order passes the edits, the computer records the order on the sales event data and the sales order master data, and updates the inventory to allocate the ordered inventory. As the order is recorded, it is printed on a printer in the warehouse (the picking ticket). A copy of the sales order is also printed in the sales order department and is sent to the customer (a customer acknowledgment).

(Complete only those requirements specified by your instructor.)

a. Prepare a table of entities and activities.
b. Draw a context diagram.
c. Draw a physical data flow diagram (DFD).
d. Indicate on the table of entities and activities prepared for part a, the groupings, bubble numbers, and titles to be used in preparing a level 0 logical DFD.
e. Draw a level 0 logical DFD.
f. Draw a systems flowchart.

g. Prepare a control matrix, including explanations of how each recommended existing control plan helps to accomplish—or would accomplish in the case of missing plans—each related control goal. Your choice of recommended control plans may come from Figure 9.1 (pg. 286)/Exhibit 9.1 (pg. 287), Figure 9.4 (pg. 296)/Exhibit 9.3 (pg. 301), or Figure 9.6 (pg. 305)/Exhibit 9.4 (pg. 310) as appropriate. Be sure to tailor the matrix columns to conform to the specifics of the PetChip Company system. In doing so, assume the following two operations process goals only:

- To provide timely acknowledgment of customer orders
- To provide timely shipment of goods to customers

h. Annotate the systems flowchart prepared in requirement (f) to show the location of each control plan listed in the control matrix.

P 9-3 The following is a list of 12 control plans from this chapter:

Control Plans

A. Electronic approvals
B. Document design
C. Procedures for rejected inputs
D. Compare input data with master data
E. Turnaround documents
F. Digital signatures
G. Batch sequence check
H. Confirm input acceptance
I. Programmed edit checks
J. Manual agreement of batch totals
K. Online prompting
L. Cumulative sequence check

The following is a list of 10 system failures that have control implications.

System Failures

1. At Colebrook Company, customer orders are received in the mail in the Sales department where clerks enter individual orders online and then file the completed orders. For each order, the customer should receive an acknowledgement. When the customer fails to receive an acknowledgement, the customer calls to inquire. Inevitably, the sales clerk will find the customer's order filed with other customer orders that had been entered into the computer.
2. At Locust Inc., data entry clerks receive a variety of documents from many departments throughout the company. In some cases, unauthorized inputs are keyed and entered into the computer.
3. The tellers at Union Bank have been having difficulty reconciling their cash drawers. All customer transactions such as deposits and withdrawals are entered online at each teller station. At the end of the shift, the computer prints a list of the transactions that have occurred during the shift. The tellers must then review the list to determine that their drawers contain checks, cash, and other documents to support each entry on the list.

4. Data entry clerks at Reliant Company use networked PCs to enter batches of documents into the computer. Recently, a number of errors have been found in key numeric fields. The supervisor would like to implement a control to reduce the transcription errors being made by the clerks.

5. At Ducey Inc., clerks in the accounting offices of Ducey's three divisions prepare prenumbered general ledger voucher documents. Once prepared, the vouchers are given to each office's data entry clerk, who keys them into an online terminal. The computer records whatever general ledger adjustment was indicated by the voucher. The controller has found that several vouchers were never recorded, and some vouchers were recorded twice.

6. Purchase orders at Technotronics Corp. are prepared online by purchasing clerks. Recently, the purchasing manager discovered that many purchase orders are being sent for quantities far greater (i.e., incorrect quantities) than would normally be requested.

7. At Salomon Brothers, Inc., a clerk on the trading floor mistakenly entering the dollar amount of a trade into the box on the computer screen reserved for the number of shares to be sold, and then transmitted the incorrect trade to the stock exchange's computer.

8. At Washington Company, clerks in the cash applications area of the accounts receivable office open mail containing checks from customers. They prepare a remittance advice (RA) containing the customer number, invoice numbers, amount owed, amount paid, and check number. Once prepared, the RAs are sent to a clerk who keys them into the computer. The accounts receivable manager has been complaining that the RA entry process is slow and error-prone.

9. Randolph Company enters shipping notices in batches. Upon entry, the computer performs certain edits to eliminate those notices that have errors. As a result, many actual shipments never get recorded.

10. Hal the hacker gained access to the computer system of Arlington Bank and entered the data to transfer funds to his bank account in Switzerland.

Match the 10 system failures with a control plan that would *best* prevent the system failure from occurring. Because there are 12 control plans, you should have 2 letters left over.

P 9-4 The following is a list of 12 control plans from this chapter:

Control Plans

A. One-for-one checking

B. Manual reconciliation of batch totals (hash totals)

C. Turnaround documents

D. Procedures for rejected inputs

E. Digital signatures

F. Confirm input acceptance

G. Limit checks

H. Tickler files

I. Public key cryptography

J. Compare input data with master data

K. Batch sequence check

L. Manual reconciliation of batch totals (document/record counts)

Listed here are 10 definitions or descriptions of control plans.

Definitions or Descriptions

1. Determines if a customer number has been input correctly.
2. Ensures that transmitted messages can be read only by authorized receivers.
3. A control plan that cannot be implemented unless source documents are prenumbered or numbered before input.
4. In systems where accountable documents are not used, this control plan helps ensure input completeness by informing the data entry person that data have been accepted for processing by the computer system.
5. Used to detect changes in batches of events to ensure the validity, completeness, and accuracy of the batch.
6. Used to determine that a message has not been altered and has actually been sent by the person claiming to have sent the message.
7. A file of open sales orders that is periodically reviewed to ensure the timely shipment of goods.
8. Sales orders are compared to packing slips and the goods to determine that what was ordered is what is about to be shipped.
9. A system output becomes an input source in a *subsequent* event.
10. A type of programmed edit that is synonymous with a reasonableness check.

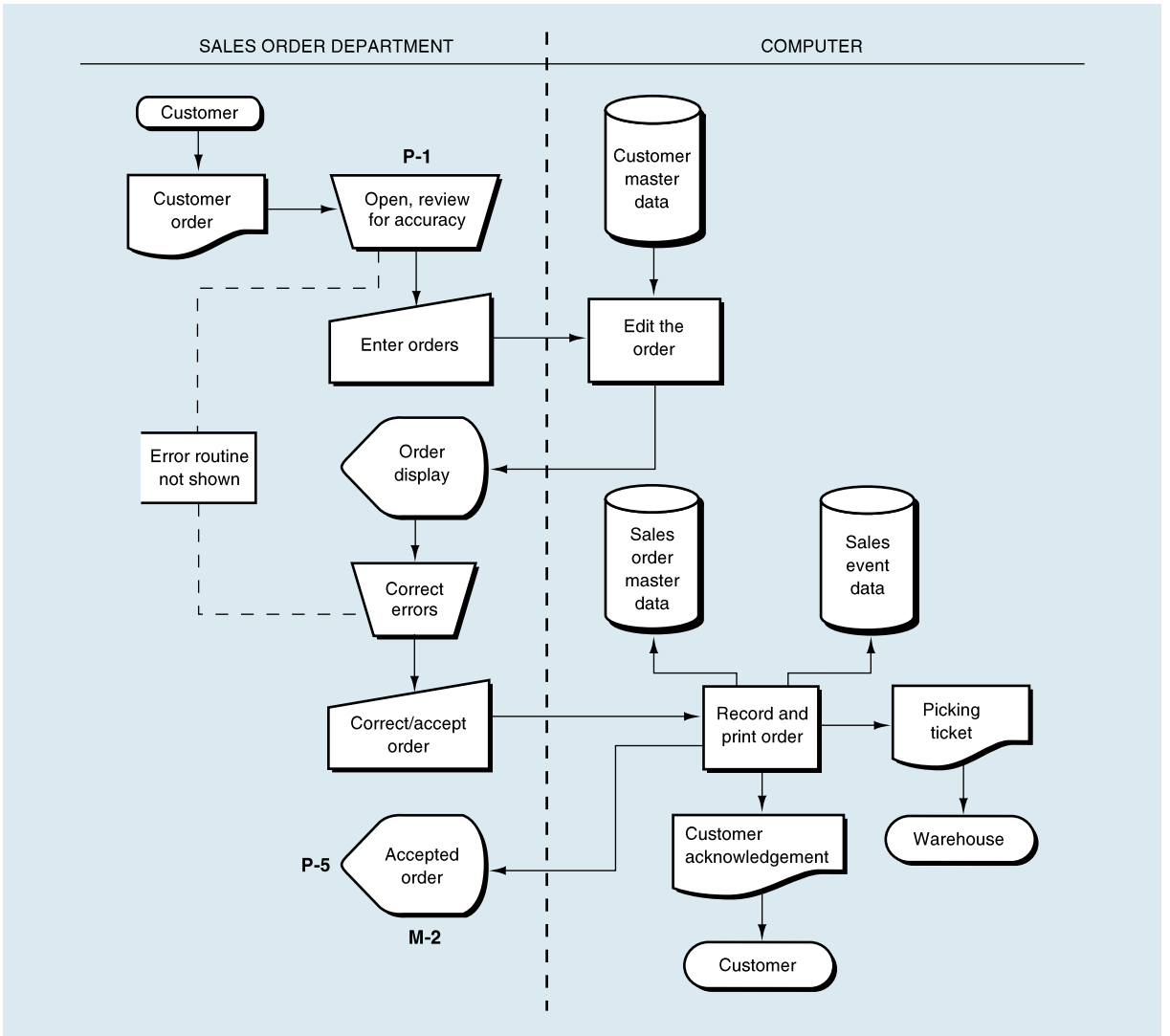
Match the 10 definitions or descriptions with a control plan that *best* matches the definition. Because there are 12 control plans, you should have 2 letters left over.

P 9-5 Big Al's Drive-In is a very popular restaurant located in Brunswick, Maine. Customers come from all over to savor Big Al's seafood delicacies. There is no inside seating area, rather, customers eat their food in their cars. Here is how the business works: A customer drives into a parking spot and orders a meal from a touch-screen pad. For instance, a customer will press a button labeled ''Scallop Dinner,'' the computer then asks ''How Many?'' and the customer presses the ''1'' key to indicate that he wants only one dinner. The same process is used for each menu item selected. When the customer finishes ordering, he presses a button labeled ''Done Ordering.'' The order shows up on a computer screen inside the restaurant where cooks prepare the meal. When the order is ready, an attendant brings the tray of food and

drinks to the car and places it near the driver's window. After the customer is finished eating (after, perhaps, ordering more food, drinks, and dessert!), the customer requests a bill on the touch pad, and the bill prints out on a small printer located below the touch pad. The customer can either pay the bill on-site with a credit card (the reader is located near the touch pad), or the attendant can collect cash payments. Once paid, the printer leaves a receipt with the customer.

Big Al has been having problems lately and is asking you for advice. First, some customers are simply driving off without paying. Also, Big Al suspects that some attendants are letting their friends eat free. Another problem is that when a customer presses ''Done Ordering'' but later orders a second round of food, the computer system treats this as two orders—each which must be paid separately. Customers are not at all happy with this situation—particularly when they order many times. Finally, Big Al has been experiencing

FIGURE 9.11 Flowchart to Accompany Problem 9-6



a growing problem with "order changes." For example, say that a customer orders a lobster roll from the touch pad. When the order arrives, the customer swears that he did not order a lobster roll; rather, he ordered a cheeseburger. Currently, the attendant takes back the lobster roll, and the cook prepares a cheeseburger instead. The lobster roll disappears (mysteriously). This repudiation problem is getting worse.

Required:

a. Draw a systems flowchart. Make reasonable assumptions where necessary.

b. Prepare a control matrix, including explanations of how each recommended control plan helps to accomplish—or would accomplish in the case of missing plans—each related control goal. Your choice of recommended control plans may come from Figure 9.1 (pg. 286)/Exhibit 9.1

FIGURE 9.12 Control Matrix for Figure 9.11 to Accompany Problem 9-6

	Control Goals of the Order Entry Business Process								
	Control Goals of the Operations Process				Control Goals of the Information Process				
Recommended Control Plans	Ensure effectiveness of operations		Ensure efficient employment of resources (people, computers)	Ensure security of resources (inventory, customer master data)	For the sales order inputs (i.e. customer orders) ensure:			For the sales order master data, ensure:	
	A	*B*			*IV*	*IC*	*IA*	*UC*	*UA*
Present Controls									
P-1: Review document for accuracy									
P-4: Procedures for rejected input									
P-5: Confirm input acceptance									
Missing Controls									
M-2: Manual reconciliation of batch totals				M-2	M-2	M-2	M-2		

Possible effectiveness goals include the following:

A = Provide timely acknowledgement of customer orders.

B = Provide timely shipment of goods to customers.

See Exhibit 9.7 (page 326) for a complete explanation of control plans and cell entries.

IV = Input validity

IC = Input completeness

IA = Input accuracy

UC = Update completeness

UA = Update accuracy

(pg. 287), Figure 9.4 (pg. 296)/Exhibit 9.3 (pg. 301), or Figure 9.6 (pg. 305)/Exhibit 9.4 (pg. 310) as appropriate. You may find other processes that have control implications. Be sure to tailor the matrix columns to conform to the specifics of Big Al's Drive-In. In doing so, assume the following operations process goal:

- To provide timely service to customers

c. Annotate the systems flowchart prepared in requirement (a) to show the location of each control plan listed in the control matrix.

d. Discuss the nature of the repudiation problem described by Big Al, and explain fully how your recommended control plan would help to assure nonrepudiation.

P 9-6 Figure 9.11(pg. 324) is a systems flowchart for the first few steps in an order entry process. Some, but not all, of the controls have been annotated on the flowchart. Figure 9.12(pg. 325) is a partially completed control matrix for the system in Figure 9.11. Some controls are not on the matrix at all. For some controls, not all of the cells have been completed. Exhibit 9.7 is a partially completed set of explanations of the cell entries in Figure 9.12.

Required:

a. Annotate the flowchart to indicate additional present and missing controls. (Some controls that are on the matrix are not annotated on

EXHIBIT 9.7 Explanation of Cell Entries for the Control Matrix in Figure 9.12 to Accompany Problem 9-6

P-1: *Review document for accuracy.*
P-2: *Preformatted screens.*

- *Effectiveness goals A and B, efficient employment of resources:* By structuring the data entry process, automatically populating fields, and preventing errors, preformatted screens simplify data input and save time (*Effectiveness goals A and B*), allowing a user to input more data over a period of time (*Efficiency*).
- *Input accuracy:* As each data field is completed on a preformatted screen, the cursor moves to the next field on the screen, thus preventing the user from omitting any required data set. The data for fields that are automatically populated need not be manually entered, thus reducing input errors. Incorrectly formatted fields are rejected.

P-4: *Procedures for rejected inputs.*
P-5: *Confirm input acceptance.*

M-2: *Manually reconcile batch totals.*

- *Security of resources:* Agreement of the batch totals at this point would ensure that only valid source documents have been input and that invalid picking tickets have not been sent to the warehouse leading to inappropriate shipments of inventory.
- *Input validity, input completeness, input accuracy:* Agreement of the batch totals at this point would ensure that only valid source documents comprising the original batch have been input (*input validity*), that all source documents were input (*input completeness*), and that data elements appearing on the source documents have been input correctly (*input accuracy*).
- *Update completeness, update accuracy:* Reconciliation of batch totals from before input to those after update would ensure a complete and accurate update of the master data.

the flowchart. Others are missing from both the flowchart and the matrix.)

b. Complete the control matrix by adding new controls (ones you added to the flowchart or ones that were on the flowchart but not on the matrix) and by adding cell entries to controls that are already on the matrix.

c. Complete the control explanations to reflect changes that you made to the flowchart and matrix.

P 9-7 Technology Summary 9.1 (pg. 303) describes the impact that pervasive and general controls from Chapter 8 can have on the effectiveness of controls in Figure 9.3, Figure 9.4, and Exhibit 9.3 (i.e., controls for manual and automated data entry). Prepare a comparable summary that describes the impact that pervasive and general controls from Chapter 8 can have on the effectiveness of controls in Figure 9.5 (pg. 304), Figure 9.6 (pg. 305), and Exhibit 9.4 (pg. 296) (i.e., controls over data entry with batches).