It was 3:55 P.M. EST, just before the 4:00 P.M. closing of the New York Stock Exchange. A clerk on the trading floor of Salomon Brothers Inc. misread a program-trading order. Instead of entering the order correctly to sell $11 million worth of this particular stock, the clerk typed 11 million into the box on the screen that asked for the number of shares to be sold. Like most such firms, Salomon has direct computer links to the New York Stock Exchange (NYSE) that allow it to process security trades with lightning speed. When a second clerk failed to double-check the order as required by company policy, most of the trade as entered—amounting to $500 million, not $11 million—was sent to the NYSE’s computer system. Although the firm’s computer system did catch the error shortly after it was made and kept at least part of the trade from being executed, it was not before the error sent the stock market tumbling and caused near chaos at the Big Board.

Synopsis

This chapter presents a conceptual framework for the analysis of controls in business systems, describing process controls that may be found in any information process. As almost all business processes incorporate information technology, many of the controls you read about are automated and do not require human intervention. As more and more business is conducted over the Internet, organizations will be increasingly reliant on computerized controls to protect both their operations processes and information processes. These controls help prevent (or detect or correct) problems such as the one that occurred at Salomon Brothers.

You should notice that 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 affecting the many tightly connected enterprise system processes that follow initial entry of the data. We want to have good controls, for example, over the entry of customer orders so that we correctly record data about the customer order, the shipment, the inventory balance, the customer’s invoice, the general ledger entries for sales, accounts receivable, inventory, cost of goods sold, and the inventory replenishment process.
Good data entry controls are also important for those engaging in e-business. For example, if we are to receive customer orders electronically, our systems must have sufficient controls within them so that they accept only authorized, accurate order data. If we don’t have these controls, we might make inaccurate shipments or shipments to those who have no intention of paying for the goods being shipped.

**LEARNING OBJECTIVES**

- To be able to prepare a control matrix
- To describe the generic process control plans introduced in this chapter
- To describe how these process controls accomplish control goals
- To describe why these generic process controls are important to organizations with enterprise systems and those that are engaged in e-business

**Introduction**

Having covered the control environment and IT control processes in Chapter 8, we are now ready to move to the third level of control plans appearing in the hierarchy shown in Figure 8.2 on page 256—process control plans (the first two were the control environment and pervasive control plans). We begin by defining the components of a control framework and introduce tools used to implement it. Then we apply the control framework to a few generic business processes. These generic processes include process controls that may be found in any information system. Later in the text, in Chapters 10 through 14, we examine process controls that might be found in particular business processes (e.g., order-to-cash, purchase-to-pay, and so forth).

**The Control Framework**

In this section, we introduce a control framework specific to the control requirements of the operations process and the information process. We again use the Causeway Company cash receipts system, this time to illustrate the control framework.

The control framework provides a structure for analyzing the internal controls of business organizations. However, structure alone is of little practical value. To make the framework functional, you need to feel comfortable using the tools for implementing the framework. In Chapter 2, you saw one of the key tools—the systems flowchart. Now we use the other important tool— the control matrix.

**The Control Matrix**

The control matrix is a tool used to analyze a systems flowchart (and related narrative) to determine the control plans appropriate to that process and to relate those...
plans to the processes control goals. It establishes criteria to be used in evaluating a particular process. We'll start by taking a look at the four essential elements of the matrix—control goals, recommended control plans, cell entries, and explanations of the cell entries. Then, we'll elaborate on the steps used to prepare the matrix.

Figure 9.1 presents a “bare-bones” outline of the control matrix, and Figure 9.2 (page 284) is the “annotated” flowchart produced as a by-product of completing the matrix. We explain how to annotate a flowchart later in this section. The intent in

**Review Question**

What are the four basic elements included in a control matrix?

**Figure 9.1 Elements of the Control Matrix**

<table>
<thead>
<tr>
<th>Control Goals of the Business Process</th>
<th>Control Goals of the Operations Process</th>
<th>Control Goals of the Information Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure effectiveness of operations by achieving the following operations process goals:</td>
<td>Ensure efficient employment of resources</td>
<td>Ensure security of resources (cash, accounts receivable master data)</td>
</tr>
<tr>
<td>A</td>
<td>B</td>
<td>For remittance advice inputs (i.e., cash receipts), ensure:</td>
</tr>
<tr>
<td>M-1</td>
<td>M-1</td>
<td>For accounts receivable master data, ensure:</td>
</tr>
<tr>
<td>P-1: Immediately endorse incoming checks</td>
<td></td>
<td>IV</td>
</tr>
<tr>
<td>M-1: Immediately separate checks and remittance advices</td>
<td>M-1</td>
<td>P-1</td>
</tr>
<tr>
<td>P-2: Plan 3 (describe)</td>
<td>P-2</td>
<td></td>
</tr>
<tr>
<td>M-2: Plan 4 (describe)</td>
<td>M-2</td>
<td></td>
</tr>
</tbody>
</table>

Four key elements:
- Control goals
- Recommended control plans
- Cell entries
- Explanation of cell entries:

Possible operations process goals include:
- A = To accelerate cash flow by promptly depositing cash receipts.
- B = To ensure minimum cash balances are maintained in our depository bank.

KEY:
- IV = input validity
- IC = input completeness
- IA = input accuracy
- UC = update completeness
- UA = update accuracy

P-1: Immediately endorse incoming checks. Security of resources: A restrictive check endorsement—“deposit only to the account of Causeway Company”—ensures security of the cash resource by preventing the check from being misappropriated.

M-1: Immediately separate checks and remittance advices.

*Operations Process 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. Decreased delays should accelerate cash flows (*Operations process Goal A*) and will improve cash balances (*Operations Process 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) than the one who records the checks from information on the remittance advices. By separating these functions, we improve security over the cash asset because there is less opportunity for misappropriation of the checks to be covered up while recording the RA.

P-2: Plan 3 (describe)
- Input Completeness:
- Input Accuracy:
- etc.

M-2: Plan 4 (describe)
- Input Validity:
- Input Accuracy:
- etc.
Part IV  Internal Control for Business Processes and Information Systems

Figure 9.2  Causeway Company Annotated Systems Flowchart

- **Customer**
  - Checks
  - Endorsed checks
  - Write amount and check number on RAs
  - Prepare batch total for RAs

- **Annotated RAs**
  - Verify, post to AR master data, log event
  - Print end-of-day reports

- **Accounts Receivable**
  - Key BT, customer number, invoice number, amount, and check number
  - Verify/accept Annotated RAs
  - Compare CR listing
  - Print end-of-day reports

- **Cash**
  - Deposit slip
  - At end of batch or end of day

- **Computer**
  - Verify posting to AR master data, log event
  - Accounts receivable master data
  - Print end-of-day reports

- **General Ledger**
  - Summary of customer accounts paid listing

- **Cash receipts event data**
  - Deposit slip
  - At end of day
  - Endorsed checks

- **Bank**
  - Deposit slip

- **Error routine not shown**

- **Key: RA = Remittance advice, BT = Batch total, CR = Cash receipts**
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 trying to give you an overview of the four control matrix elements and how they relate to each other, and to walk you through, in a very basic way, the steps in preparing the matrix. Please follow along in the figures as we describe how to prepare the control matrix.

Steps in Preparing the Control Matrix

Control goals represent the first element of the matrix. The goals are listed across the top row of the matrix; they should be familiar to you from discussions in Chapter 8. Indeed, in Figure 9.1, we have merely tailored the generic goals shown in Table 8.1 (see page 250) to Causeway’s cash receipts system. The tailoring involves:

- Identifying operations process goals for a cash receipts process; we include only two examples here—namely,
  - Goal A—to accelerate cash flow by promptly depositing cash receipts.
  - Goal B—to ensure minimum cash balances are maintained in our depository bank.\footnote{Remember that one of the goals of any business process may be 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 Causeway’s case, we assume that its loan agreements with its bank require that it maintain certain minimum cash balances—known as compensating balances—on deposit.}

- Listing the resources of interest in this process—namely, Causeway’s physical asset, cash, and an information resource, the accounts receivable master data.
- Naming the information process inputs—namely, remittance advices representing cash receipts data.
- Identifying the master data being updated in this system—namely, the accounts receivable master data.

In determining what operations process goals are appropriate for the operations process under review, you may find it helpful to first ask yourself, “What undesirable events might occur?” For example, in deciding on Causeway’s operations process goal of accelerating cash flow by promptly depositing cash receipts, we might have first speculated that there was a possibility that the mailroom could delay the processing of incoming payments, the cashier could hold endorsed checks for a time before taking them to the bank, and so forth. Noting these weak points can also be useful in deciding on recommended control plans, discussed next.

Recommended control plans, appropriate to the process being analyzed, represent the second element of the matrix. To illustrate, we list two representative plans for a cash receipts process such as Causeway’s in the left column of Figure 9.1. Each of these plans (and others) will be explained in Chapter 11. Two other plans listed in Figure 9.1 are identified merely as plans 3 and 4.
In the body of the matrix, located at various intersections of goals and plans, are cells. Cells can have entries in them (P-1, P-2, M-1, M-2), or they can be left blank. Entries in cells represent the third element of the matrix. If a recommended control plan can help to achieve a control goal (i.e., there is a relationship between that plan and a particular goal), an entry—either a P or an M—should appear in that cell. A corresponding entry (e.g., P-1, M-2) is also made on the systems flowchart for purposes of cross-referencing. We refer to this technique as annotating a systems flowchart. The process of relating the plans listed in the matrix to the point where the plans can be located on the systems flowchart is illustrated in Figure 9.2, the annotated flowchart for Causeway. Take a few moments to trace the codes, P-1, P-2, M-1, and M-2, from Figure 9.1 to their locations in Figure 9.2. From the descriptions of plans P-1 and M-1 in Figure 9.1, do you agree with where we have put them in Figure 9.2? If not, check with your instructor.

There are two types of entries that you can register in a cell. You can enter a “P,” which indicates that a particular control plan is present in the flowchart. For example, in Figure 9.1, the entries “P-1” and “P-2” indicate that those plans are present in Causeway’s system. A glance at the flowchart in Figure 9.2 shows the location of these plans. Alternatively, you can enter an “M,” which signifies that a particular, recommended control plan is missing (for example, entries “M-1” and “M-2” indicate that those plans are not present in Causeway’s system). Again, Figure 9.2 identifies the location of where these desirable, but missing, plans should be installed to control Causeway’s cash receipts process more effectively.

Because the control plans listed in the first column of the matrix are all recommended plans, entering a “P” in a cell symbolizes a strength in the system. It depicts a control plan as contributing to the accomplishment of one or more control goals. For example, in Figure 9.1, the plan “Immediately endorse incoming checks” helps to ensure that the cash resource (customer checks) will not be misappropriated. We depict this relationship by entering a “P-1” in the cell where this plan intersects with the goal of ensuring security of resources. And as importantly, at the bottom of the matrix, we provide the fourth, and final, matrix element—the explanation of how this plan helps to achieve this particular goal. In this case, a restrictive endorsement on the check (i.e., “deposit only to the account of Causeway Company”) prevents it from being diverted to any other purpose. Of the four matrix elements, many people have the most difficulty in providing these explanations. Yet this element is the most important part of the matrix because the whole 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. Be prepared to defend your cell entries.

Entering “M” in a cell symbolizes a weakness in the system. It tells us that a system does not incorporate a particular control plan that may be necessary to ensure the accomplishment of a related control goal. For example, in Figure 9.1, notice that the recommended plan, “Immediately separate checks and remittance advices,” is missing from Causeway’s system. The explanation of cell entries in Figure 9.1 goes on to explain what goals would be achieved if this plan were present.

When your assessment leads you to the identification (and correction) of control weaknesses, you are fulfilling the fourth step of the control framework: 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 also facilitates evaluation from the perspectives of control effectiveness (are all the control goals achieved?), control efficiency (do indi-
Exhibit 9.1 Steps in Preparing a Control Matrix

**Step 1** 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 important, relevant resources (e.g., cash, accountants 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).

**Step 2** List the goals that are germane to the business process under examination. The goals must be tailored to the process under study. In the business process chapters (Chapters 10–14), we suggest a few typical goals.

**Step 3** List a set of recommended control plans that is appropriate for the process being analyzed. The list could include both the 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, we presented only two illustrative plans for Causeway’s system. Later, this chapter presents controls related to the processing methods and in the business process chapters, you see controls related to those processes.

**Step 4** Examine the systems flowchart and related narrative description, looking for each of the control plans listed in the matrix in step 3. When you find an implemented control plan (i.e., a plan that is present), mark its location on the flowchart and cross-reference this information to the control matrix. Use “P-1” . . . “P-n” as identifiers. When you determine a control plan is missing, mark the location on the flowchart where it should be found and cross-reference this information to the control matrix. Use “M-1” . . . “M-n” as identifiers. As mentioned earlier, this information is used in completing step 4 of the control framework: recommending remedial action to correct deficiencies in the system. Figures 9.1 and 9.2 illustrated the technique for cross-referencing the control matrix and systems flowchart.

**Step 5** At the bottom of the control matrix, provide a short statement explaining how each existing control plan accomplishes each related control goal. Also provide a short statement explaining the significance of each missing control plan, in terms of each unmet control goal.

**Review Question**
What are the five steps involved in preparing a control matrix?

Control Plans for Data Entry without Master Data

As mentioned before, perhaps the most error-prone—and inefficient—steps in an operations process or an information process are the steps during which data is entered into a system. While a lot has been done over the years to improve the accu-
racy and efficiency of the data entry process, problems still remain, especially when
humans type data into a system. So, we begin our discussion of process controls by
describing those controls that improve the data entry process. We divide our discus-
sion of data entry controls into three parts: controls when master data is not avail-
able during data entry, controls when master data is available during data entry, and
controls when the input data may be collected into batches.

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

◇ Automation of data entry. Documents may be scanned for data entry. Docu-
ments and labels may contain bar codes that are scanned. This automation re-
duces or eliminates manual keying.

◇ Business events, such as purchases, may be initiated in one (buying) organiza-
tion and transmitted to another (selling) organization via the Internet or EDI. In
this case, the receiving (selling) organization need not enter the data at all.

◇ Multiple steps in a business process may be tightly integrated, such as in an en-
terprise 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 shipping system shares the same integrated database with the
billing system where the data have already been entered.

System Description and Flowchart

Figure 9.3 shows the systems flowchart for a hypothetical system that we will use to
describe our first set of controls. In our first pass through the system, please ignore
the control annotations, P-1, P-2, and so forth. They have been included so that we
will not have to repeat the flowchart later when we prepare the control matrix.

The processing starts in the first column of Figure 9.3 with the clerk typing in the
input data. Usually, the data entry program would present the clerk with an input
screen and then prompt the user to enter certain data into fields on that screen (e.g.,
customer code, items numbers, and so on).

Note that the first processing square in the data entry devices column “edits” the
data before they are actually accepted by the system. The editing is done through var-
ious programmed edit checks; these are discussed later in this section. Having edited
the input, the computer displays a message to the user indicating that the input ei-
ther is acceptable or contains errors. If errors exist, the user may be able to correct
them immediately. Once users have made any necessary corrections, they type in a
code or click the mouse button to instruct the system to accept the input. That ac-
tion triggers the computer to simultaneously:

◇ Record the input in machine-readable form—the event data disk.

◇ Inform the user that the input data have been accepted.

To verify that the event data were keyed correctly, the documents could be for-
warded to a second clerk who would type the data again. This procedure, called key
verification, was introduced in Chapter 2 and will be further explained below. Typi-
cally, key verification is applied only to important fields on low volume inputs.

Our flowchart stops at this point without depicting the update of any master data.
Certainly our system could continue with such a 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 described above. Figure 9.4 (page 290) presents a completed control matrix for the systems flowchart shown in Figure 9.3. Through the symbols P-1, P-2, . . . P-7, we have annotated the flowchart to show where specific control plans are implemented. We also have one control plan that we assume is missing (code M-1) because the narrative did not mention it specifically. 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.
As you recall from the previous section, step 2 in preparing a control matrix is to tailor the control goals across the top of the matrix to the particular business process under review. Because our model system does not show a specific system such as cash receipts, inventory, or the like, we cannot really perform the tailoring step. Therefore, in Figure 9.4 under the operations process section, we have shown only one operations process goal for illustrative purposes. We identify that goal as goal A: To ensure timely processing of (blank) event data (whatever those data happen to be). In the business process chapters (Chapters 10 through 14) you will see how to tailor the goals to the systems discussed in those chapters.

The recommended control plans listed in the first column in Figure 9.4 are representative of those commonly associated with controlling the data entry process. The purpose of this presentation is to give you a sense of the multitude of control plans available for controlling such systems. The plans are not unique to a specific system such as sales, billing, cash receipts, and so forth. Rather, they apply to any data entry process. Therefore, when the technology of a system is appropriate, these controls are incorporated into the list of recommended control plans (step 3 in “Steps in Preparing a Control Matrix,” Exhibit 9.1, page 287).
Let’s take a general look at how several of the control plans work. Then, in Exhibit 9.2 (page 293), we explain each of the cell entries in the control matrix. As you study the control plans, be sure to see where they are located on the systems flowchart.

**P-1: Document design.** Document design is a control plan in which a source document is designed in such a way to make it easier to prepare initially and to input data from later. We designate this as a present plan because we assume that the organization has designed this document to facilitate the data preparation and data entry processes.

**P-2: Written approvals.** A written approval takes the form of a signature or initials on a document to indicate that a person has authorized the event.

**P-3: Preformatted screens.** Preformatted screens control the entry of data by defining the acceptable format of each data field. For example, the screen might require users to key in exactly nine alphabetic characters in one field and exactly five numerals in another field. To facilitate the data entry process, the cursor may automatically move to the next field on the screen. And 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 and default shipping methods, sales tax rates, and other terms of a business event. Automatic population reduces the number of keystrokes required, making data entry quicker and more efficient. With fewer keystrokes and by utilizing the default data, fewer keying mistakes are expected. To ensure that the system has not provided inappropriate defaults, the clerk must compare the data provided by the system with that on the input.

**P-4: Online prompting.** Online prompting asks the user for input or asks questions that the user must answer. For example, after entering all the input data for a particular customer sales order, you might be presented three options: (A)cept the order, (E)dit the order, or (R)eject the order. By requiring you to stop and “accept” the order, online prompting is, in a sense, advising you to check your data entries before moving on. Many systems provide context-sensitive help whereby the user is automatically provided with, or can ask for, descriptions of data to be entered into each input field. Another way to provide choices for a field or to limit allowable choices is to restrict entry to the contents of a list that pops up. For example, a list of state abbreviations can be provided from which the user chooses the appropriate two-letter abbreviation.

**P-5: Programmed edit checks.** Programmed edit checks are edits automatically performed by data entry programs upon entry of the input data. Erroneous data may be highlighted on the terminal screen to allow the operator to take corrective action immediately. Programmed edits can highlight actual or potential input errors, and allows them to be corrected quickly and efficiently. The most common types of programmed edit checks are the following:

1. **Reasonableness checks.** 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).

---

2 Many of the controls in this section are adapted from material contained in the *Handbook of IT Auditing 2001 Edition*, (Chapters D2, D3, and D4 primarily), Copyright © 2000 by Price-waterhouseCoopers L.L.P.; published by Warren, Gorham & Lamont, Boston, MA.
2. **Document/record hash totals.** Document/record hash totals are a summary 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 all entered and were entered correctly.

3. **Mathematical accuracy checks.** This edit compares calculations performed manually to those performed by the computer to determine if 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 up 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.

4. **Check digit verification.** In many processes, an extra digit—a check digit—is included 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 complicated and secret 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 the identification number is entered later by a data entry person, 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. You are already saying to yourself, “But what about a transposition like 1326?” This entry would be accepted because of the simple method of calculating the check digit. 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.

**P-6: Interactive feedback checks.** An interactive feedback check is a control in which the data entry program informs the user that the input has been accepted and recorded. The program may flash a message on the screen telling a user that the input has been accepted for processing.

**M-1: Key verification.** With key verification documents are typed by one individual and retyped by a second individual. The data entry software compares the second entry to the first entry. If there are differences, it is assumed that one person misread or mistyped the data. Someone, perhaps a supervisor or the second clerk, would determine which typing was correct, the first or the second, and make corrections as appropriate.

**P-7: Procedures for rejected inputs.** Procedures for rejected inputs are designed to ensure that erroneous data—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 timely clearing of rejected items. To reduce the clutter in the simple flowcharts in this text, we often depict such routines with an annotation “Error routine not shown.”
Exhibit 9.2  Explanation of Cell Entries for Control Matrix in Figure 9.4

**P-1: Document design.**

*Operations process goal A, Efficient employment of resources:* A well-designed document can be completed more quickly and can be prepared with less effort.

*Input accuracy:* We tend to fill in a well-designed document completely and legibly. And, if a document is legible, data entry errors occur less frequently.

**P-2: Written approvals.**

*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.

**P-3: Preformatted screens.**

*Operations process goal A, Efficient employment of resources:* By structuring the data entry process, automatically populating fields, and by preventing errors, preformatted screens simplify data input and save time, allowing a user to input more data over a period of time.

*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.**

*Operations process goal A, Efficient employment of resources:* By asking questions and providing online guidance, this plan ensures a quicker data entry process and allows the user to input more data over a period of time.

*Input accuracy:* The online guidance should reduce input errors.

**P-5: Programmed edit checks.**

*Operations process goal A, Efficient employment of resources:* Event data can be processed on a more timely basis and at a lower cost if errors are detected and prevented from entering the system in the first place.

*Input accuracy:* The edits identify erroneous or suspect data and reduce input errors.

**P-6: Interactive feedback checks.**

*Input completeness:* By advising the user that input has been accepted, interactive feedback checks help ensure input completeness.

**M-1: Key verification.**

*Input accuracy:* By having one data entry person type the data and a second person retype that same data, we should detect the majority of keying errors.

**P-7: Procedures for rejected inputs.**

*Input completeness:* The rejection procedures (i.e., “Error routine not shown” annotations in Figure 9.3) are designed to ensure that erroneous data—not accepted for processing—are corrected and resubmitted for processing.
Review Question
How does each control plan listed in the control matrix in Figure 9.4 work?

**Explanation of control matrix cell entries.** Armed with an understanding of the mechanics of certain control plans, let’s now turn our attention to Exhibit 9.2—Explanation of Cell Entries for Control Matrix in Figure 9.4. See whether you agree with (and understand) the relationship between each plan and the goal(s) that it addresses. Remember that your ability to explain the relationships between plans and goals is more important than your memorization of the cell entries themselves.

**Control Plans for Data Entry with Master Data**

Our next set of input controls are those that may be applied when we have access to master data during the input process. The availability of such data can greatly enhance the control, and efficiencies, that be gained in the data entry process. For example, let’s say that we are entering orders from our customers. If we have available to us data entry programs such as those depicted in Figure 9.3, we can check to see if the customer number is in the range of valid numbers (i.e., a limit check) or has been entered without error (e.g., check digit verification). But, these edits determine only that the customer number might be correct or incorrect. If we have available the actual customer master data, we can use the customer number to call up the stored customer master data and determine if the customer number has been entered correctly, if the customer exists, the customer’s correct address, and so forth.

While access to master data may facilitate and control the data entry process, access to master data needs to be controlled. For example, when we allow customers or other users to communicate with us over the Web, we need to be extra cautious in protecting access to stored data. Technology Excerpt 9.1 provides some control guidelines to protect against unauthorized Internet-enabled access to stored data.

The next section describes some additional controls that become available when the master data is available during data entry.

---

**Technology Excerpt 9.1**

**Protecting Against Credit Card Fraud**

Many people are reluctant to give their credit card number over the Web because they are afraid of credit card fraud. In one sense this fear is justified, because credit card fraud is estimated to be 12 times higher for online purchases than for offline merchants, according to a recent survey by the Gartner Group. However, in either case, the holder of the card is not responsible for the fraud. In the case of face-to-face transactions, the credit card companies usually absorb the bill, but online merchants are held responsible when stolen credit card numbers are used.

Visa is beginning to require its merchants to employ a series of online controls in order to better guard its cardholders’ information. Merchants, gateways, and Internet service providers will be required to comply with Visa’s broad online security program, or face fines, sales restrictions or loss of membership. The program, summarized in the list below, is taken from Visa’s Web site.
Top Ten List

At the most basic level, the program consists of a “Top Ten” list of requirements plus several “best practices” for protecting Visa cardholder information. The Top Ten requirements include the following:

1. Install and maintain a working network firewall to protect data accessible via the Internet.
2. Keep security patches up to date.
3. Encrypt stored data accessible from the Internet.
5. Use and regularly update anti-virus software.
6. Restrict access to data by business’ “need to know.”
7. Assign unique IDs to each person with computer access to data.
8. Track access to data by unique ID.
9. Don’t use vendor-supplied defaults for system passwords and other security parameters.
10. Regularly test security systems and processes.

In addition, Visa recommends the following three “best practices”:

1. Screen employees with access to data to limit the “inside job.”
2. Don’t leave papers/diskettes/computers with data unsecured.
3. Destroy data when it’s no longer needed for business reasons.

These top level principles apply to all entities participating in the Visa payment system that process or store cardholder information and have access to it through the Internet or mail-order/telephone-order.


System Description and Flowchart

Figure 9.5 (page 296) depicts another hypothetical system. As with Figure 9.3, we make some assumptions. First, we have event data entering the system from a remote location because communications with a data entry system may be from sites away from the computer center. For instance, an existing customer might enter an order through a Web site. Second, we show that the events are typed into the system without using a source document. Naturally, source documents could be used such as they were in Figure 9.3.
Note that this system, unlike the one in Figure 9.3, validates input by reference to master data. Normally, if a user enters valid data such as a valid customer code, the system automatically retrieves certain standing master data such as the customer name and address. Having edited the input, the computer displays a message to the user indicating that the input either is acceptable or contains errors. If errors exist, the user may be able to correct them immediately. Once users have made any necessary corrections, they type in a code or click the mouse button to instruct the system to accept the input. As it did in Figure 9.3, that action triggers the computer to record simultaneously the input and inform the user that the input data has been accepted.

As with Figure 9.3, our flowchart stops at this point without depicting the update of any master data. Certainly our system could continue with such a 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 described above. Figure 9.6 presents a completed control matrix for the systems flowchart shown in Figure 9.5.
This matrix shows format and assumptions similar to those made in Figure 9.4. The recommended control plans listed in the first column in Figure 9.6 are representative of those commonly associated with controlling the data entry process when master data is available. Most of the control plans described with Figures 9.3 and 9.4 may also be applicable. But, for simplicity, we will not repeat them here.

In this section, we first see in general terms how several of the control plans work. Then, Exhibit 9.3 (page 299) describes each of the cell entries in the control matrix. As you study the control plans, be sure to track where they are located on the systems flowchart.

**P-1:** Enter data close to the originating source. This is a strategy for capture and entry of event-related data close to the place (and probably time) that an event occurs. Online transaction entry (OLTE), online real-time processing (OLRT), and online transaction processing (OLTP) are all examples of this processing strategy. When this strategy is employed, databases are more current and subsequent events can occur in a more timely manner. Because data are not transported to a data entry location, there is less of a chance that inputs will be lost (input completeness). The input can be more accurate because the data entry person may be in a position to recognize and immediately correct input errors (input accuracy). Finally,
some efficiencies can be gained by reducing the number of entities handling the event data.

**P-2**: Digital signatures. Whenever data are entered from remote locations via telecommunications channels like the Internet, there is the risk that the communication may have been sent by an unauthorized system user or may have been intercepted/modified in transit. To guard against such risks, many organizations employ digital signatures to authenticate the user’s identity and to verify the integrity of the message being transmitted. To learn more about how digital signatures work, see Appendix 9A (pages 309 through 313), and Technology Application 9.1 (page 312).

**P-3**: Populate inputs with master data. Numeric, alphabetic, and other designators are usually assigned to entities such as customers, vendors, and employees. When we populate inputs with master data, the user merely enters an entity’s identification code and the system retrieves certain data about that entity from existing master data. For example, the user might be prompted to enter the customer ID (code). Then, the system automatically provides information from the customer master data, such as the customer’s name and address, preferred shipping method, and sales terms. Fewer keystrokes are required, making data entry quicker, more accurate, and more efficient. To ensure that system users have not made a mistake keying the code itself, they compare data provided by the system with that used for input. Finally, the entry cannot proceed without valid (authorized) master data that includes such items as terms and credit limits that were previously recorded via a data maintenance process.

**P-4**: Compare input data with master data. A data entry program can be designed to compare the input data to data that have been previously recorded. When we compare input data with master data we can determine the accuracy and validity of the input data. Here are just two types of comparisons that can be made:

1. **Input/master data dependency checks.** These edits test whether the contents of two or more data elements or fields on an event description bear the correct logical relationship. For example, input sales events can be tested to determine whether the person entering the data is listed as an employee of that customer. If these two items don’t match, there is some evidence that the customer number or the salesperson identification was input erroneously.

2. **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 there is no record of a corresponding customer order. If there is no match, 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.

**Explanation of control matrix cell entries.** Armed with an understanding of the mechanics of certain control plans, let’s now turn our attention to Exhibit 9.3—Explanation of Cell Entries for Control Matrix in Figure 9.6. Notice how data entry by the customer affects these controls. See whether you understand the relationship between each plan and the goal(s) that it addresses. Remember that your ability to explain the relationships between plans and goals is most important.
Controls Plans for Data Entry with Batches

This section, as did the preceding two, presents a hypothetical system. This next flow-chart, however, uses the example of a shipping and billing process to illustrate certain points. The distinguishing control-related feature in this system is that it processes event data in batches.

Exhibit 9.3  Explanation of Cell Entries for Control Matrix in Figure 9.6

**P-1: Enter data close to the originating source.**

*Operations process goal A, Efficient employment of resources:* This strategy places users in a position to process 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 events more quickly. In this process, the direct entry of input data by customers eliminates the cost associated with the handling of the event data by additional personnel.

*Input completeness:* Because 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 customers are familiar with the event data being entered, they are less likely to make input errors and can more readily correct these errors if they occur.

**P-2: Digital signatures.**

*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.

*Input accuracy:* Detects messages that have been altered in transit, thus preventing input of inaccurate data.

**P-3: Populate inputs with master data.**

*Operations process goal A, Efficient employment of resources:* Direct entries of data by the customer should improve the speed and productivity of the event because the order entry department does not have to type in additional data about the customer’s order after the customer submits it. In addition, direct customer entry means that the department does not need to reenter the original order information.

*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 event. For example, without a customer record, the sales order cannot be entered.

*Input accuracy:* Fewer keystrokes and the use of data called up from existing records reduces the possibility of input errors.

**P-4: Compare input data with master data.**

*Operations process goal A, Efficient employment of resources:* Events can be processed on a more timely 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.
System Description and Flowchart

Figure 9.7 shows the systems flowchart for our hypothetical batch processing system. Again, please ignore the control annotations, P-1, P-2, and so forth, until we discuss them in the next subsection.

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 to be shipped to customers. Upon receipt of the picking tickets, a shipping department employee assembles them into groups or batches. Let’s assume that the employee batches the documents in groups of 25 and takes batch totals.

The batch of documents is then scanned onto a disk. As the batch is recorded, the data entry program calculates one or more totals for the batch and displays those batch totals to the shipping clerk. The clerk determines if the displayed totals agree with the ones previously calculated. If they don’t, error-correcting routines are performed. This process is repeated throughout the day as picking tickets are received in the shipping department.

Periodically, the file containing the shipment data is sent to the computer for processing by the shipment programs(s). This program records the sales event data and updates the accounts receivable master data to reflect a new sale. 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 total, or both—that were accepted by the system, and those that were 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. In our system the totals on this report are compared to the input batch totals.

Applying the Control Framework

In this section, we apply the control framework to the generic batch processing system described above. Figure 9.8 (page 302) presents a completed control matrix for the systems flowchart shown in Figure 9.7. Figure 9.7 has been annotated to show the location of recommended control plans that exist in the system (codes P-1, P-2, . . . P-5). We also have some control plans that we assume are missing (codes M-1, M-2) because the narrative system description did not mention them specifically. In Figures 9.4 and 9.6, we could not complete certain parts of the top of the control matrix. However, for this example, we have assumed that we know the nature of the input (i.e., picking tickets), we know the resources that are to be protected (i.e., the inventory and the accounts receivable master data), and we know the data that are to be updated (i.e., the AR master data). Therefore, we have completed these elements in Figure 9.8.

This section discusses each of the recommended control plans listed in the first column of the matrix, describing how the plans work. Exhibit 9.4 explains 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).

4 Ibid.
Figure 9.7 Systems Flowchart Data Entry with Batches

SHIPPING DEPARTMENT

- Warehouse
- Picking tickets (with bar codes)
- Calculate batch totals
- Batched picking tickets (with bar codes)
- Reconcile batch totals
- Batched picking tickets (with bar codes)
- Pending shipments

DATA ENTRY DEVICE

- Computed batch totals
- Batched picking tickets (with bar codes)
- Error routine not shown
- Compare picking tickets and packing slips
- Packing slips

COMPUTER

- Periodically
- Record (scan) picking tickets
- Picking tickets (shipment event data)
- Record shipments
- Error and summary report
- Packing slips
- Invoices
- Customer

BT = Batch totals
Before we start, let’s explain what we mean by *batch controls*.\(^5\) **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 (completeness problem), added (validity problem), or changed (accuracy problem). 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.

\(^5\) These batch controls apply to groups of documents. The *document/record hash totals* introduced earlier in the chapter apply to individual documents.
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 begin by grouping event data and then calculating a control total(s) for the group. For example, Figure 9.7 shows the shipping department employee preparing batch totals for the picking tickets documents to be scanned.

Several different 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. Also, because one document could be intentionally replaced with another, this control is not very 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 of 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 be used to determine if 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.

Now we proceed with an explanation of the controls plans in Figures 9.7 and 9.8.

**P-1: Turnaround documents.** Turnaround documents are printed by the computer and are used to capture and input a subsequent event. Picking tickets, inventory count sheets, remittance advice stubs attached to customer invoices, and payroll time cards are all examples of turnaround documents. For example, we have seen picking tickets that are printed by computer, are used to pick the goods, and are sent to shipping. The bar code on the picking ticket is scanned to trigger recording of the shipment. When the bar code is scanned the items and quantities that should have been picked are displayed. If the items and quantities are correct, the shipping clerk need only click one key to record the shipment.

**P-2: Manual agreement of batch totals.** The manual agreement of batch totals control plan operates in the following manner:
First, one or more of the batch totals are established manually (i.e., in the shipping department in Figure 9.7).

As individual event descriptions are entered (or scanned), the data entry program accumulates independent batch totals.

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.

The person who reconciles the batch total (see the shipping department employee in Figure 9.7) must determine why the totals do not agree and make corrections as necessary to ensure the integrity of the input data.

**M-1: Computer agreement of batch totals.** This control plan does not exist in Figure 9.7 and therefore is shown as a missing plan. Note in Figure 9.7 where we have placed the M-1 annotation. The computer agreement of batch totals plan is pictured in Figure 9.9 and works in the following manner:

**Figure 9.9** Computer Agreement of Batch Totals Control Plan

![Diagram of Computer Agreement of Batch Totals Control Plan](image-url)

- **BT** = Batch totals
First, one or more of the batch totals are established manually (i.e., in the user department in Figure 9.9).

Then, the manually prepared total is entered into the computer and is recorded on the computer as batch control totals data.

As individual event descriptions 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.

The computer then 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 9.7 and 9.9.

**M-2: Sequence checks.** Whenever documents are numbered sequentially—either assigned a number when the document is prepared or prepared using prenumbered documents—a sequence check can be applied to those documents. 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 batch is entered.
2. Each individual, serially prenumbered event is entered.
3. The computer program sorts the event data into numerical order, checks the documents against the sequence number range, and reports missing, duplicate, and out-of-range event data.

Batch sequence checks work best when we can control the input process and the serial numbers of the input data. For example, this control would not work for entering customer orders that had a variety of numbers assigned by many customers.

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 might contain broken sets of numbers). 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 an example of a situation in which numbers (the check numbers) are issued in sequence. But 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 accounted for.

**P-3: Agreement of run-to-run totals.** This is a variation of the agreement of batch totals controls. With this control, totals prepared before a computer process are compared, manually or by the computer, to totals prepared after the computer process. The controls after a process are often found on an error and summary report. 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 be-
ginning and the end of the process and we want to be assured of the integrity of each process.

**P-4:** Tickler files. A *tickler file* is a file that is reviewed on a regular basis for the purpose of taking action to clear items from that file. In Figure 9.7, we see a file of picking tickets representing items that should be shipped. Should these documents remain in this file for an extended period of time, we would fail to make the shipments or to make them in a timely manner. Tickler files may also be computer records representing events that need to be completed, such as open sales orders, open purchase orders, and so forth.

**P-5:** One-for-one checking. *One-for-one checking* is the detailed comparison of individual elements of two or more data sources to determine that they agree as appropriate. 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. While this procedure provides us details as to what is incorrect within a batch, agreement of run-to-run totals will tell us if there is any error within a batch. One-for-one checking is expensive and should be reserved for low-volume, high-value events.

Having examined what each of the recommended control plans means and how each operates, we can now 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.

**Exhibit 9.4** Explanation of Cell Entries for Control Matrix in Figure 9.8

**P-1: Turnaround documents.**

*Operations process goal A, Efficient employment of resources:* By reducing the amount of data that must be input to record the shipment, we improve the speed and productivity of the data entry personnel.

*Input accuracy:* Using a pre-recorded bar code to trigger the event reduces the possibility of input errors.

**P-2: Manual agreement of 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*).

**M-1: Computer agreement of batch totals.**

*Operations process 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.

**M-2: Sequence checks.**

*Input validity, Input completeness:* By comparing an expected sequence of documents to those actually input, the 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.

**P-3: Agreement of run-to-run 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: Tickler file of picking tickets.**

*Operations process goal A, Input completeness, Update completeness:* A file of picking slips is retained in shipping awaiting the packing slips. If the packing slips are received in a timely manner, and the corresponding picking ticket 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 updated the master data.

**P-5: One-for-one checking of 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*).

---

**Conclusions**

In this chapter, we began our study of process control plans, the third level in the control hierarchy (shown in Figure 8.2 on page 256). Our study of process control plans will continue in Chapters 10–14, where we will apply the control framework and explore controls that are unique to each business process.
Before we leave, let’s address one more aspect of process controls. Many of these controls attempt to detect data that may be in error. For example, a reasonableness test may reject a price change that is beyond a normal limit. But, it may be that 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 that it is in the best interest of the company to permit the sale anyway. 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 require a password or key and signature be necessary to effect the override. Finally, a record of all overrides should be periodically reviewed to determine that the override authority is not being abused.
Data Encryption and Public-Key Cryptography

Data encryption is a process that employs mathematical algorithms and encryption “keys” to change data from plain text to a coded text form so that it is unintelligible and therefore useless to those who should not have access to it. Encryption is useful 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) 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 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 9.10 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, the algorithms and keys are much more sophisticated; so much so that good encryption schemes are virtually impossible to break.

As shown in Figure 9.10, 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 transmit-
ted 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 9.11 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.

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. Furthermore, the private decryption key never has to be transmitted; it is always in Ray’s exclusive possession.

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.” Since 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

- runs the decrypted message, NED IS A NERD, through an encoding scheme called a hashing function—the same hashing function used by Sally—and
- 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.

Some experts predict that digital signatures will soon pave the way for a truly cashless society, 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 on page 312 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 “E-sign” law, passed by Congress in June 2000, makes contracts “signed” by electronic methods legally valid in all 50 states. This law is accelerating the rate of growth of business-to-business (B2B) e-business by allowing companies to execute
Figure 9.11  Illustration of Public-Key Cryptography and Digital Signatures

(a) Encrypting the MESSAGE

Sally Sender’s message to Ray Receiver

(Using Ray’s public key, any sender can encrypt and send a message to Ray Receiver.)

Sally’s Sender’s private key

(Then the hashed output is encrypted with Sally’s private key. The encrypted number constitutes the digital signature.)

(b) Appending the DIGITAL SIGNATURE

(The same hashing program is applied by Ray Receiver to the decrypted message received.)

Ray Receiver’s public key

(Ray Receiver uses Sally’s public key to decrypt her digital signature.)

NED IS A NERD
ROSES ARE RED
HARRY LOVES SALLY
I LOVE COMPUTERS
0
0
0
0

ETC.

Decrypted messages

Sally’s encrypted

acceptable

Sally’s encrypted

digital signature

(Sent

Received

Ray Receiver’s private key

11010010

11010010

NED IS A NERD
ROSES ARE RED
HARRY LOVES SALLY
I LOVE COMPUTERS
0
0
0
0

ETC.

(Hashed output of the plaintext message, NED IS A NERD, sent by Sally in part (a).)

(Decrypted digital signature)

Ray Receiver uses Sally’s public key to decrypt her digital signature.)

11010010

(Hashed output of message received)

If these do not equal, it indicates the message was tampered with during transmission)

(Sent

Received

Decrypted messages

NED IS A NERD
ROSES ARE RED
HARRY LOVES SALLY
I LOVE COMPUTERS
0
0
0
0

ETC.

(Ray Receiver uses Sally’s public key to decrypt her digital signature.)

11010010

(Hashed output of message received)

(Decrypted digital signature)

Ray Receiver uses Sally’s public key to decrypt her digital signature.)

11010010

(Hashed output of message received)

(Decrypted digital signature)

Ray Receiver uses Sally’s public key to decrypt her digital signature.)

11010010

(Hashed output of message received)

(Decrypted digital signature)

Ray Receiver uses Sally’s public key to decrypt her digital signature.)

11010010

(Hashed output of message received)

(Decrypted digital signature)

Ray Receiver uses Sally’s public key to decrypt her digital signature.)
Using Data Encryption and Public-Key Cryptography for Electronic Commerce

Data encryption and public-key cryptography are being used to secure business transactions on the Internet. Below are three examples. The first two are in use, and the latter one was piloted until July 2001. The eCheck technology has been applied for online payments by firms such as Xign (http://www.xign.com/) and Clareon (http://www.clareon.com). Only SSL is widely used.

Case 1: SSL
The secure sockets layer (SSL) protocol was developed by Netscape Communications Company (now owned by America Online) 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 decrypts the message, 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. SSL protects the consumer from interception and unauthorized use of the purchase and credit card information while it is 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 they have sent their credit card number to a legitimate merchant.

Case 2: SET
The secure electronic transaction (SET) protocol was developed by MasterCard and Visa to secure credit card transactions on the Internet involving three parties: the consumer, the merchant, and one or more credit card issuing banks. With SET, the consumer separately encrypts the purchase message and the credit card number. The merchant decrypts the purchase message to proceed with the sale and submits a charge to the consumer’s credit card company (i.e., credit card issuing bank) to clear the transaction using traditional means. However, unlike SSL, SET-based clearing will pass through the merchant and go directly to the consumer’s credit card issuing bank. The consumer and the merchant sign their messages with certificates obtained from financial institutions that certify that the consumer holds the credit card in question and that the merchant has a credit card clearing relationship with the issuing bank. SET protects merchants and credit card issuing banks from unauthorized purchases, and consumers from credit card fraud.

Case 3: 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. As with SET, eCheck certificates would be issued by banks certifying that the holder of the certificate has an account at that bank. And, payments would be processed automatically through the existing bank systems. Unlike SET, however, payments would be checks drawn on bank accounts. And, a feature beyond SSL and SET is that the eCheck protocol defines message formats, such as purchase orders, acknowledgments, and invoices, that can be processed automatically by trading parties. eCheck provides protections similar to those obtained with SET. That is, merchants and banks are protected from unauthorized use of checks, and the consumer is protected from check fraud.

documents online immediately. (Review Technology Excerpt 8.4 for more on E-sign and digital signatures.)

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 smartcard, or cryptographic box. Access to the device, and to the private key, must then be protected with passwords or other authentication procedures. One such procedure involves the use of a thumbprint reader attached to the computer. With this device users must put their thumb onto the reader before the private key can be used to “sign” a message. The thumbprint reader is an example of the biometric devices introduced in Chapter 8.


Review Question
Distinguish among data encryption, public-key cryptography, and digital signatures.

**REVIEW QUESTIONS**

RQ9-1 Explain the difference between the category of process control plans covered in this chapter and the process controls to be covered in Chapters 10 through 14.

RQ9-2 a. Describe the relationship between the control matrix and the control framework.
   b. What are the four basic elements included in a control matrix?
   c. Describe the relationship between the control matrix and the systems flowchart. What does it mean to “annotate” the systems flowchart?
   d. What are the five steps involved in preparing a control matrix?

RQ9-3 Explain how a manager would use the control matrix in performing step 4 of the control framework.
   a. How could the matrix be used to recommend changes in the system in order to improve control of that system?
   b. How would the matrix be useful in evaluating control effectiveness, control efficiency, and control redundancy? Include in your answer a definition of these three terms.

RQ9-4 What are two common programmed edit checks? Describe each check.

RQ9-5 How does each control plan listed in the control matrix in Figure 9.4 (page 290) work?

RQ9-6 How does each control plan listed in the control matrix in Figure 9.6 (page 297) work?

RQ9-7 In examining the systems flowchart in Figure 9.7 (page 301), how would you discern from the symbols used (or perhaps the lack of certain other symbols) that the
system (a) employs online data entry; (b) uses data communications technology; (c) processes events individually, rather than in groups of similar events; and (d) updates master data continuously?

**RQ9-8** Name and explain three different types of batch totals that could be calculated in a batch processing system.

**RQ9-9** How does each control plan listed in the control matrix in Figure 9.8 (page 302) work?

**RQ9-10** (Appendix 9A) Distinguish among data encryption, public-key cryptography, and digital signatures.

---

### DISCUSSION QUESTIONS

**DQ9-1** Discuss why the control matrix is custom-tailored for each process.

**DQ9-2** Explain why input controls are so important for controlling an online system.

**DQ9-3** Review the controls included in the Visa Top Ten and Best Practice Lists in Technology Excerpt 9.1 on page 294. Classify each item in the two lists according to the following categories:

- Preventive, detective, or corrective controls.
- Control environment, pervasive controls, or process controls.

**DQ9-4** “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 so as to make the event appear genuine.”

- Assume for a moment that the comment is true. Present (and explain) a “statement of relationship” between the intended control plan of using prenumbered documents and the information process control goal of event “validity.”
- Do you agree with this comment? Why or why not?

**DQ9-5** Describe a situation in your daily activities, working or not, where you have experienced or employed controls described in this chapter.

**DQ9-6** When we record our exams into the spreadsheet used for our gradebook, we employ the following procedures:

- For each exam, manually add up the grade for each exam and record on the front page.
- Manually calculate the average grade for all of the exams.
- Input the score for each part of each exam into the spreadsheet.
- Compare the exam total on the front page of the exam to the total prepared by the computer.
e. 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 introduced in this chapter.

DQ9-7 “My top management is demanding Web access to reports that would contain very sensitive data. They want to be able to call them up while they travel to get up-to-the-minute information about the company. Our auditors advise us not to make this data available over the Web because of security concerns. But if top management doesn’t get what they want, I may lose my job! What can I do?” What would you advise this manager to do?

PROBLEMS

P9-1 You worked with the Causeway Company cash receipts system in Chapter 2. The narrative of that system and its systems flowchart are reproduced in Exhibit 9.5 and Figure 9.12, respectively.

Using Exhibit 9.5 and Figure 9.12, do the following:

a. 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 controls introduced in this chapter.

Exhibit 9.5 Causeway Company System Narrative to Accompany Problem 9-1

The 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 terminal 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.
Figure 9.12 Causeway Company Systems Flowchart to Accompany Problem 9-1

**Customer:**
- Write amount and check number on RA
- Periodically

**MAILROOM:**
- Customer
- RA checks

**ACCOUNTS RECEIVABLE COMPUTER CASHIER:**
- Key BT, customer number, invoice number, amount, and check number
- Verify acceptance

**COMPUTER:**
- Accounts receivable master data
- Compare
- Summary of customer accounts paid listing
- Print end-of-day reports
- CR listing

**ACCOUNTS RECEIVABLE:**
- Annotated RA

**CASHIER:**
- Endorsed checks
- Print deposit slip
- At end of day
- Error routine not shown

**DEPOSIT:**
- Bank
- Deposit slip
- At end of day
- Error routine not shown

**KEY:**
- RA = Remittance advice
- BT = Batch total
- CR = Cash receipts

**Error routine not shown**
control plans should come from Exhibits 9.2, 9.3, or 9.4 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 operations process goals only:

• To deposit cash receipts on the same day received.
• To ensure that customer balances in the accounts receivable master data reflect account activity on a timely basis.

b. Annotate the systems flowchart in Figure 9.12 to show the location of each control plan you listed in the control matrix.

P9-2 The following narrative describes the processing of customer mail orders at Phoenix Company.

Phoenix Company is a small manufacturing operation engaged in the selling of widgets. Customer mail orders are received in the sales order department, where sales order clerks open the orders and review them for accuracy. The clerks enter each order into the computer, where they are edited by comparing them to customer master data (stored on a disk). The computer displays the edited order on the clerk’s screen. The clerk reviews and accepts the order. The order is then added to the sales event data (stored on a disk) and updates the sales order master data (also stored on a disk). 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 should come from Exhibits 9.2, 9.3, or 9.4 as appropriate. Be sure to tailor the matrix columns to conform to the specifics of the Phoenix 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.

P9-3 The following is a list of 14 control plans from this chapter:

Control Plans

A. Populate inputs with master data
B. Online prompting
Listed below are 10 system failures that have control implications. On your solution sheet, list the numbers 1 through 10. Next to each number, insert the capital letter from the list above for the best control plan to prevent the system failure from occurring. (If you can’t find a control that will prevent the failure, then choose a detective plan or, as a last resort, a corrective control plan.) A letter should be used only once, with four letters left over.

**System Failures**

1. At Datatech 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.

2. Data entry clerks at the Visitron Company use networked PCs to enter data 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.

3. Purchase orders are prepared online by purchasing clerks. Recently, the purchasing manager discovered that many purchase orders are being sent to the wrong vendor, for the wrong items, and for quantities far greater than would normally be requested.

4. The tellers at Bucks Bank have been having difficulty reconciling their cash drawers. All customer events are entered online at a teller terminal. At the end of the shift, the computer prints a list of the events that have occurred during the shift. The tellers must then review the list to determine that their drawer contains checks, cash, and other documents to support each entry on the list.

5. At Helm Inc., clerks in the accounting offices of Helm’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. Then, 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. At the Baltimore 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 an online computer terminal. The accounts receivable manager has been complaining that the RA entry process is slow and error-prone.

7. Occasionally, the order entry system at Dorsam Inc. fails to record a customer order. After failing to receive an acknowledgment, the customer will call to inquire. Inevitably, the sales clerk will find the customer’s order filed with other customer orders that had been entered into the computer. In each case, all indications are that the order had been entered.

8. The Stoughton 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.

9. A computer hacker gained access to the computer system of Big Bucks Bank and entered an event to transfer funds to his bank account in Switzerland.

10. Refer to the vignette at the beginning of the chapter. It describes a botched securities trade caused by a clerk’s 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 transmitting the incorrect trade to the stock exchange’s computer.

**P9-4**

The following is a list of 12 controls from Chapter 9:

**Controls**

A. Turnaround documents  
B. Tickler files  
C. Public-key cryptography  
D. One-for-one checking  
E. Batch sequence check  
F. Document/record counts  
G. Written approvals  
H. Hash totals (for a batch)  
I. Limit checks  
J. Procedures for rejected inputs  
K. Digital signatures  
L. Interactive feedback checks

Listed below are 10 definitions or descriptions. List the numbers 1 through 10 on your solution sheet. Next to each number, insert the capital letter from the list above for the term that best matches the definition. A letter should be used only once, with two letters left over.

**Definitions or Descriptions**

1. Ensures that transmitted messages can only be read by authorized receivers.  
2. A control plan that cannot be implemented unless source documents are prenumbered.
3. In systems where accountable documents are not used, this control plan helps assure input completeness by informing the data entry person that events have been accepted by the computer system.

4. Used to determine that a message has not been altered and has actually been sent by the person claiming to have sent the message.

5. A process control plan that implements the pervasive control (see Chapter 8) of general or specific authorization.

6. Data related to open sales orders is periodically reviewed to ensure the timely shipment of goods.

7. Used to detect changes in batches of events to ensure the validity, completeness, and accuracy of the batch.

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 test.

P9-5 The following is a description of seven control/technology descriptions and a list of seven control/technology names.

Control/Technology Descriptions

| A. | When you type a customer code into the enterprise system the matching master data is called up to the screen. |
| B. | All enterprise systems can be programmed to consider a number of pieces of stored data and real-time calculations as business event data are being entered into the system. |
| C. | Access to the company network from the Internet is through a server on which there are programs to monitor the traffic, coming and going. |
| D. | Workflow software within enterprise systems can be used to route business events to those who must work on the business event data, or approve the business event before it is finalized. |
| E. | A standard practice at most firms is to develop profiles for each employee to grant them access to the appropriate computer resources. |
| F. | To make changes to production programs, a copy of the program is moved successively through “development,” “testing,” and “staging,” before the modified program is moved into production. |
| G. | Enterprise system software can be configured to require that certain fields be completed on an input screen before being allowed to move on to the next screen. |

Control/Technology Names

| 1. | Firewall |
| 2. | Preformatted screens |
| 3. | Compare input data with master data, programmed edits, customer credit check |
| 4. | Populate inputs with master data |
| 5. | Program change controls |
| 6. | Approvals, such as POs |
| 7. | Security module |

Listed below are five potential risks or systems failures that can be addressed with a control or a technology from the lists above.

A. On the blank line to the left of each number (the “Description” column), insert the capital letter from the list above for the control/technology that best addresses the risk. A letter should be used only once, with two letters left over.
B. In the column titled “Explanation,” provide an explanation of why you selected that control/technology description. You need to specifically describe how the control/technology addresses the risk.

C. In the right column (titled “Name”) insert the number from the list above corresponding to the control/technology name for the answer provided in part A.

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>POTENTIAL RISKS</th>
<th>EXPLANATION</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. A computer programmer altered the order entry programs so that the credit-checking routine was bypassed for one of the customers, a company owned by his uncle.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. A hacker accessed the Web site at Dorothy’s Gifts &amp; Flowers and changed some of the graphics. Several customers, confused by the graphics, took their business elsewhere.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Roxy’s Retailing maintains an extensive and valuable repository of information about its customers. Tricky Nick was fired from Roxy’s and now works at a competing firm. Last night Nick dialed into the Roxy computer system and downloaded some valuable customer data to his own computer.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. Cash application clerks at the Blanford Company have been posting payments to the incorrect customer accounts because the customer account numbers are being keyed in incorrectly.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e. At Natick Company, customers who are four months late in making payments to their accounts are still able to have their orders accepted and goods shipped to them.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>