SOLUTIONS FOR CHAPTER 7

Each end-of-chapter question in the Solutions Manual is tagged to correspond with AACSB, AICPA and CISA standards, allowing professors to more easily manage the task of reporting outcomes to these professional and accrediting bodies. Please see the corresponding spreadsheet file for the tagging information.

Discussion Questions

DQ 7-1 *Recently, the U.S. federal government and the American Institute of Certified Public Accountants (AICPA) have taken aggressive steps aimed at ensuring the quality of organizational governance. What are these changes, how might they change organizational governance procedures, and do you believe that these actions will really improve internal control of business organizations?*

ANS. First, the U.S. Congress passed the Sarbanes-Oxley Act of 2002 (SOX). This groundbreaking legislation is intended to set the foundation for improved organizational governance. Most notably, SOX disallows auditors of public companies from performing most consulting services with their audit clients; establishes a Public Company Accounting Oversight Board (PCAOB) to watch over the auditing profession; requires CEOs and CFOs to sign quarterly and annual financial statements submitted to the SEC (by signing, the CEOs and CFOs are certifying that the financial statements are correct in all material respects); and requires CEOs, CFOs, and independent auditors to sign an internal control report that details the presence and effectiveness of the company's internal controls.

The AICPA has developed a special portal on its Web site devoted to SOX implementation activities, enhanced its ethics enforcement process, and voiced its strong intention to further strengthen the independence of public auditors and the integrity of all CPAs.

Will these steps improve internal control of business organizations? [Let the students express and support their opinions. This should generate insightful discussions.]

DQ 7-2 *"Enterprise Risk Management is a process for organizational governance." Discuss why this might be correct and why it might not.*

ANS. Let's look at the elements of the definitions of these two concepts side-by-side:

Organizational Governance	Enterprise Risk Management	Comment
A process.	A process.	Both are clear that governance is an ongoing endeavor.
	Effected by an entity's board of directors, management, and other personnel.	ERM explicitly places the responsibility for governance at the top of the organization.
Organizations select objectives.	Applied in strategy setting and across the enterprise.	Both assert that strategy and objectives must be chosen first and be the basis for governance.
	Identify potential events that may affect the entity.	ERM describes a process for establishing what processes (and controls) must be put in place, considering risk, to provide a reasonable assurance of achieving objectives. Although not part of the definition, monitoring is one of ERM's eight elements.
	Manage risk to be within its risk appetite.	
Establish processes to achieve objectives.	Provide reasonable assurance regarding achievement of entity objectives.	
Monitor performance.		
	Categories of management objectives: strategic, operations, reporting, compliance.	These ERM categories provide a useful template for selecting objectives.

DQ 7-3 *"If it weren't for the potential of computer crime, the emphasis on controlling computer systems would decline significantly in importance." Do you agree? Discuss fully.*

ANS. Without computer crime, and the attendant, fascinating stories, public awareness of the importance of controlling computer systems might decline. However, while the dollar loss from each incident of computer crime is high, the *total* of the losses from unintentional errors is higher than the total of the losses from computer crimes. Also, as described in this chapter, control systems help an organization achieve organizational goals and objectives, only one of which is to reduce the incidence of computer crime.

DQ 7-4 *Provide five examples of potential conflict between the control goals of ensuring effectiveness of operations and of ensuring efficient employment of resources.*

ANS.

1. By striving to answer many customer telephone calls, a customer service representative rushes each call. These hurried phone calls reduce the level of customer service.
2. To reduce the investment in inventory, stock levels are kept low. These levels are inadequate and a high number of back orders results.
3. Although the batch printing of shipping documents is an efficient use of computer resources, shipments are delayed.
4. Ensuring effectiveness of operations may require that we hire an additional employee and purchase an additional computer to respond to customer inquiries. This may not be an efficient use of resources.
5. To adequately segregate duties and ensure effectiveness of operations, we may hire an additional employee. However, this may lead to an inefficient use of personnel resources.

DQ 7-5 *Discuss how the* efficiency *and* effectiveness *of a mass-transit system in a large city can be measured.*

ANS. The main purpose of this question is to reinforce the ideas that (1) effectiveness must be judged in light of objectives and (2) efficiency is the relationship of inputs to outputs.

A mass-transit system may be established with many purposes. For example:

- To reduce traffic on the highways just enough to preclude highway expansion
- To provide affordable transportation to all residents
- To encourage inner-city travel and tourism
- To assist in the economic development of certain areas

Effectiveness is judged in light of the objectives of the system. For example, does mass transit reduce traffic on the highways?

The efficiency of the mass transit system could be measured in terms of cost per passenger mile.

DQ 7-6 *"If* input data *are entered into the system completely and accurately, then the information system control goals of* ensuring update completeness *and of* ensuring update accuracy *will be automatically achieved." Do you agree? Discuss fully.*

ANS. No, we do not agree. The text distinguishes input and update because these steps are often separate and because successful update does not necessarily follow from successful input. The computer system could fail to completely or accurately update the master data.

DQ 7-7 *"Section 404 of SOX has not been a good idea. It has been too costly and it has not had its intended effect." Do you agree? Discuss fully.*

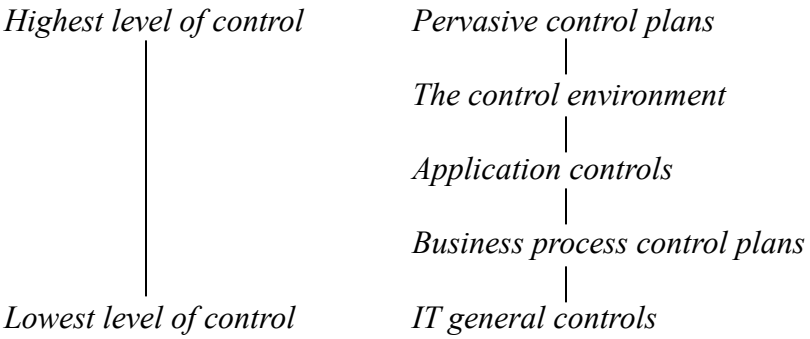
ANS. As reported in the chapter, reviews of the results of SOX Section 404 are mixed. Certainly, its implementations have been quite costly. Also, some foreign firms are delisting their stocks from U.S. exchanges or are halting efforts to list on the exchanges to avoid SOX requirements. Some firms are going private or not becoming public to avoid the requirements of SOX, especially Section 404. On the other hand, some control systems have been improved, and firms are improving their business processes as a result of their SOX 404 efforts. Bottom line, it is a matter of opinion as to whether SOX Section 404 has been worth the effort. AS5, which requires a top-down, risk-based approach to the integrated audit, is expected to further reduce the time and cost of complying with SOX Section 404.

DQ 7-8 *How does this text's definition of internal control differ from COSO? How does it differ from the controls that are subject to review under Section 404 of SOX?*

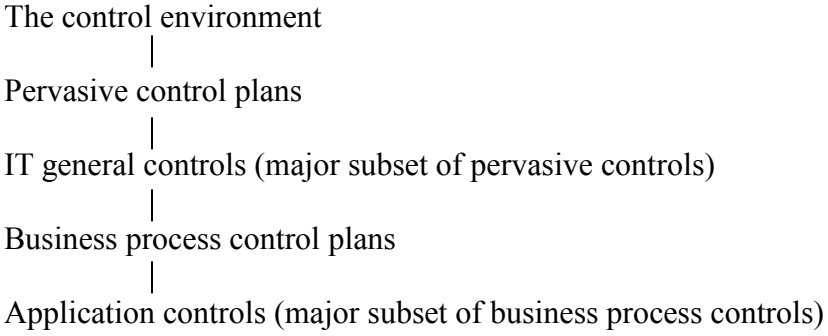
ANS. The text's definition of internal control is aimed at *all* reporting, not just *financial* reporting. Both COSO and SOX 404 are interested only in controls over the information systems and output reporting that are related to financial reporting.

The text's definition of internal control, like COSO, includes efficiency and effectiveness of operations, whereas the PCAOB has explicitly stated that the controls that are to be reviewed pursuant to SOX Section 404 are only those that affect financial transactions and financial reporting. COSO and this textbook, on the other hand, are interested in the overall system of internal control and all organizational processes. As such, these definitions apply to all processes, all controls, and to all types of audits of these processes and controls, including financial statement audits; internal audits for efficiency, effectiveness, and compliance; and IT audits for overall efficiency, effectiveness, and security of IT resources and operations.

DQ 7-9 *What, if anything, is wrong with the following control hierarchy? Discuss fully.*

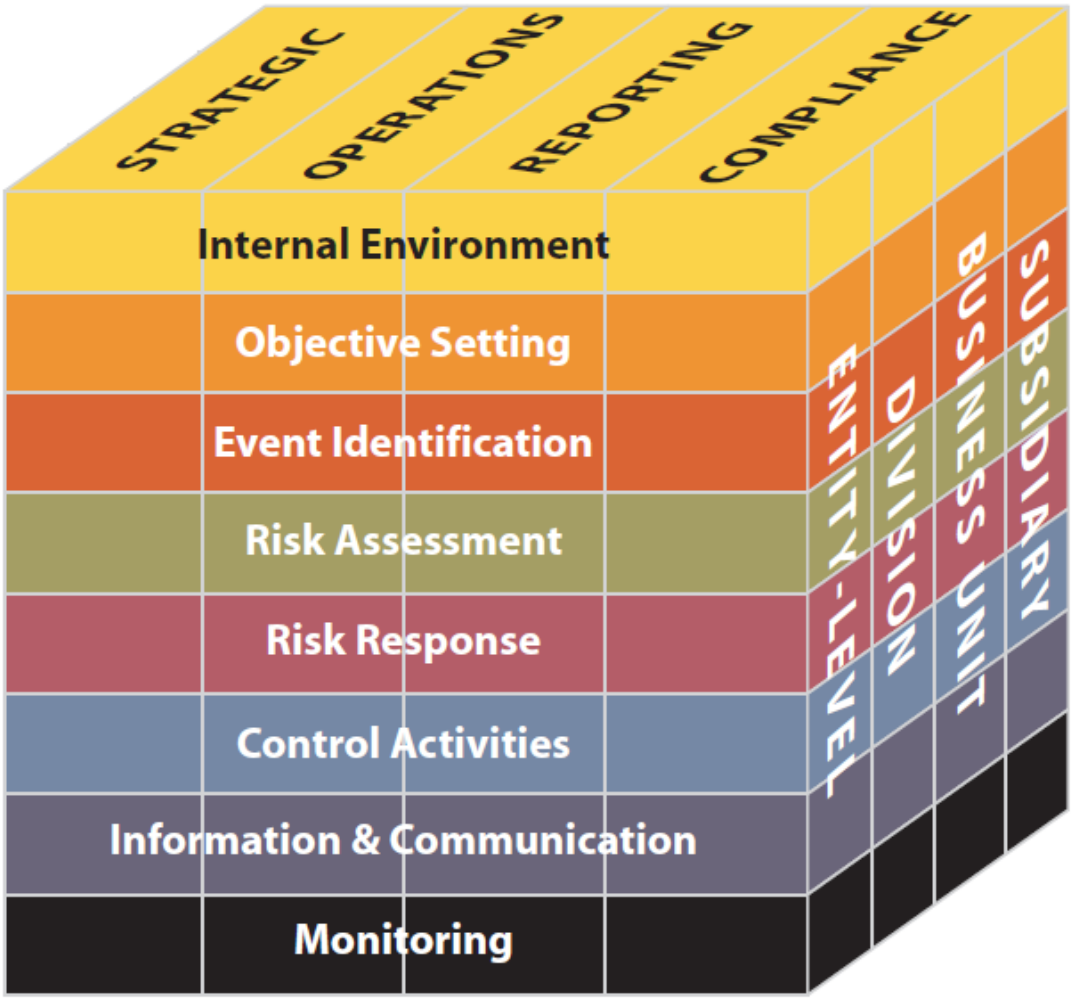


ANS. The correct order from highest to lowest level of control is (see also Figure 7.6) the following:



Short Problems

SP 7-1 ANS. The answer should note the differences in the following two internal control cubes: that of SAS 78 followed by that of the ERM. Note that the latter basically builds on the former.



SP 7-2 ANS.

F 1.

B 2.

A 3.

C 4.

E 5.

SP 7-3 ANS.

F	1.
C	2.
E	3.
D	4.
B	5.

SP 7-4 ANS. Answers will vary among students.

Problems

P 7-1 ANS.

E	1.
H	2.
B (and I)	3.
L	4.
G	5.
K	6.
D	7.
A (and I)	8.
C	9.
F	10.

P 7-2 ANS. The major implication is that management can be held legally accountable for the organization's control system. Under the Foreign Corrupt Practices Act (FCPA), for example, an officer of an organization must ensure that the organization maintains adequate accounting records. Recently, Section 404 of the Sarbanes-Oxley Act of 2002 has reinforced this management responsibility by requiring that organizations develop a system of internal control, report on that system in their annual report, and have their independent auditors assess the effectiveness of that system. So, as this chapter points out, an organization must develop and maintain a system of controls to ensure the effectiveness of the accounting information system that will maintain the accounting records. Should management not fulfill this obligation, they can be fined and imprisoned.

Management discharges this responsibility by doing the following:

- Constructing an internal control system, including an internal audit department.
- Establishing a control environment incorporating audit committees, nonconflict of interest affidavits, control policies, and reward systems that support, rather than undermine, the control policies.
- Being actively and continuously involved in the design, operation, review, and modification of the organization's systems and related control systems. This may involve participation in—or at least approval of—the systems development process.

In addition to the legal responsibility for control, increasing pressure is being applied to the board of directors and management by the public, stockholders, and the other stakeholders of organizations. These stakeholders want to be confident that the organization is well managed and that its assets are protected. Several control frameworks have been issued that provide guidance to boards and management. In addition to COSO, introduced in this chapter, and COBIT, introduced in Chapter 8, the following frameworks have been published:

- From Canada, the Canadian Institute of Chartered Accountants Guidance on Assessing Control
- From the United Kingdom, the Turnbull Report: Revised guidance for Directors on the Combined Code
- From South Africa, The King II Report on Corporate Governance for South Africa, 2007

P 7-3 ANS.

Situation	Control Goal	Explanation
1.	E and A	Checking to make sure that shipping notices are received for *all* sales orders issued addresses the goal of ensuring that event data inputs (i.e., shipping notices representing actual sales) are *completely* recorded. Answer A is appropriate here if we assume- that timely shipments to customers are a measure of a system's *effectiveness*.
2.	F and D	Double checking unit prices helps to ensure that the prices actually billed are *accurate*. Answer D is appropriate if we explain that checking prices against an *authorized* price list helps to ensure that the event was an authorized one (input *validity*).
3.	G and H	If the dollar change to AR does not equal the dollars of payments, then the updates were either incomplete, inaccurate, or both. For example, let's say that payments in the cash receipts event data equal $600, and the starting balance in AR, before the update run, was $4,500. Then the ending balance in AR, after the update run, must equal $3,900. If not, something went wrong during the run. Some payments were not posted (UC), or some were posted incorrectly (UA).
4.	D	The fact that the shipments were bogus means that they did not represent real, actual events and were therefore, by definition, *invalid* event data.
5.	E	A vendor is unlikely to send two *different* invoices with the same number. Thus, the second instance of invoice #12345 is probably a duplicate of the first. The second invoice should be rejected to ensure that the invoice is processed once and only once (*input completeness*).
6.	F	Under the definitions given in the chapter, data elements missing from an input document are instances of lack of input *accuracy* as opposed to input *completeness*, which relates to recording all events that occurred.
7.	A and B	Speeding up the cash deposits has to do with achieving timeliness in cash receipts processing, an operations process by which we judge system *effectiveness*. Answer B is appropriate if we explain that it is more *efficient* to have the computer prepare documents than it is to prepare them manually.
8.	C	The restrictive endorsement prevents the checks from being misappropriated, thereby helping to ensure security over the cash asset.

P 7-4 ANS.

	Description Answer
1.	J
2.	C
3.	F
4.	H
5.	D
6.	B
7.	G
8.	I

P 7-5 ANS.

Part A: Current Scenario:

Dollar loss (sales) per hour of downtime		$10,000
Internal downtime incidents per year	50	
External downtime incidents per year	50	
Total downtime incidents per year		100
Expected Gross Risk		$1,000,000
Preventative Measures		
Annualized cost of redundant technology	$150,000	
Annualized cost of ISP	100,000	
Total annualized cost of preventive measures		250,000
Residual Expected Risk		$1,250,000

Part B: Additional Redundant Technology

Dollar loss (sales) per hour of downtime		$10,000
Internal downtime incidents per year	15	
External downtime incidents per year	50	
Total downtime incidents per year		65
Expected Gross Risk		$650,000
Preventive Measures		
Annualized cost of redundant technology	$250,000	
Annualized cost of ISP	100,000	
Total annualized cost of preventive measures		350,000
Residual Expected Risk		$1,000,000

Part C: Additional Redundant Technology and Additional ISP Support

The answer to Part C of problem 7-6 depends on the organization's level of risk tolerance.

If the company remains with the current ISP contract of no more than 50 downtime incidents, the residual expected risk is (see Part B above).	$1,000,000
If the company moves to a higher support level of no more than 40 downtime incidents, the residual expected risk is (see Part C.1 below).	950,000
If the company moves to a higher support level of no more than 30 downtime incidents, the expected residual risk is (see Part C.2 below).	900,000
If the company moves to a higher support level of no more than 20 downtime incidents, the residual expected risk is (see Part C.3 below).	900,000
If the company moves to a higher support level of no more than 10 downtime incidents, the residual expected risk is (see Part C.4 below).	925,000
If the company moves to a higher support level of no more than 0 downtime incidents, the residual expected risk is (see Part C.5 below).	950,000

Guarantees of either 20 or 30 maximum downtime incidents per year each yield an expected residual risk of $900,000.00. Thus, management would be prudent to pay for a guarantee of only 20 rather than 30 incidents because the former would also result in less customer dissatisfaction if and when downtime incidents occur.

Part C.1: Additional Redundant Technology and Additional ISP Support for 40 Downtime Incidents

Dollar loss (sales) per hour of downtime		$10,000
Internal downtime incidents per year	15	
External downtime incidents per year	40	
Total downtime incidents per year		55
Expected Gross Risk		$550,000
Preventive Measures		
Annualized cost of redundant technology	$250,000	
Annualized cost of ISP	150,000	
Total annualized cost of preventive measures		400,000
Residual Expected Risk		$950,000

Part C.2: Additional Redundant Technology and Additional ISP Support for 30 Downtime Incidents

Dollar loss (sales) per hour of downtime		$10,000
Internal downtime incidents per year	15	
External downtime incidents per year	30	
Total downtime incidents per year		45
Expected Gross Risk		$450,000
Preventive Measures		
Annualized cost of redundant technology	$250,000	
Annualized cost of ISP	200,000	
Total annualized cost of preventive measures		450,000
Residual Expected Risk		$900,000

Part C.3: Additional Redundant Technology and Additional ISP Support for 20 Downtime Incidents

Dollar loss (sales) per hour of downtime		$10,000
Internal downtime incidents per year	15	
External downtime incidents per year	20	
Total downtime incidents per year		35
Expected Gross Risk		$350,000
Preventive Measures		
Annualized cost of redundant technology	$250,000	
Annualized cost of ISP	300,000	
Total annualized cost of preventive measures		550,000
Residual Expected Risk		$900,000

Part C.4: Additional Redundant Technology and Additional ISP Support for 10 Downtime Incidents

Dollar loss (sales) per hour of downtime		$10,000
Internal downtime incidents per year	15	
External downtime incidents per year	10	
Total downtime incidents per year		25
Expected Gross Risk		$250,000
Preventive Measures		
Annualized cost of redundant technology	$250,000	
Annualized cost of ISP	425,000	
Total annualized cost of preventive measures		675,000
Residual Expected Risk		$925,000

Part C.5: Additional Redundant Technology and Additional ISP Support for 0 Downtime Incidents

Dollar loss (sales) per hour of downtime		$10,000
Internal downtime incidents per year	15	
External downtime incidents per year	0	
Total downtime incidents per year		15
Expected Gross Risk		$150,000
Preventive Measures		
Annualized cost of redundant technology	$250,000	
Annualized cost of ISP	550,000	
Total annualized cost of preventive measures		800,000
Residual Expected Risk		$950,000

P 7-6 ANS. We might compare the elements of these two control matrices as follows:

Figure 7.7 (the textbook)	Figure 7.8 (PwC)	Comment
Control goals of the Lenox cash receipts business process.	Subprocess.	Both name the process.
Control goals of the operations process.	NA	PwC matrix relates to controls over financial reporting and operations are beyond the scope of the PwC matrix.
Ensure effectiveness of operations (and effectiveness goals).	NA	Operations are beyond the scope of the PwC matrix.
Ensure efficient employment of resources.	NA	Operations are beyond the scope of the PwC matrix.
Ensure security of resources.	Information processing objective (restricted access).	PwC's objective is to restrict access to information resources. Figure 7.7's objective also includes other assets.
Control goals of the information process.	Control objective.	PwC states an overall objective for each process. In Figure 7.7, this is a heading for more specific control goals.
Input validity.	Information processing objective (validity).	Same.
Input completeness/update completeness.	Information processing objective (completeness).	Same, but PwC does not address updates.
Input accuracy/update accuracy.	Information processing objective (accuracy).	Same, but PwC does not address updates.
Recommended control plans.	Description and frequency of control activity.	Figure 7.7 does not address frequency of the control activity.

Figure 7.7 (the textbook)	Figure 7.8 (PwC)	Comment
NA	Financial statement area.	PwC matrix is for controls over financial reporting and states the area of interest.
NA	Assertions.	These are the financial statement assertions that guide testing in a financial statement audit. Testing of controls is beyond the scope of the AIS text.
NA	P or D.	Figure 7.7 does not specifically classify controls as preventive, detective, or corrective.
NA	A or M.	Figure 7.7 does not classify controls as automated or manual.

The overall assessment is that the matrices are quite similar. In fact, the control matrix for this textbook was adapted from earlier versions of a PwC matrix (one that was developed by Coopers & Lybrand, one of the firms that became part of PwC). The PwC matrix, focused as it is on the financial statement audit, has information that is related to that endeavor. The matrix from this textbook is more expansive in that it looks at controls over efficiency and effectiveness of operations *and* controls related to financial reporting.

SOLUTIONS FOR CHAPTER 8

Each end-of-chapter question in the Solutions Manual is tagged to correspond with AACSB, AICPA and CISA standards, allowing professors to more easily manage the task of reporting outcomes to these professional and accrediting bodies. Please see the corresponding spreadsheet file for the tagging information.

Discussion Questions

DQ 8-1 *"The Enterprise Risk Management (ERM) framework introduced in Chapter 7 can be used by management to make decisions on which controls in this chapter should be implemented." Do you agree? Discuss fully.*

ANS. Several issues might be included in an answer to this question. Here are some of those issues:

- The quote implies that not all controls need to be implemented. Perhaps the costs and benefits of controls should be considered.
- Using the ERM framework provides an alternative whereby the benefits, or return on investment, might be difficult to determine. Using the ERM framework will focus attention on management of risk by employing certain control techniques and security measures.
- Security measures might be implemented on the basis of the probability of loss or disruption (i.e., risk assessment).
- Security measures should be directed at information assets that must be protected to help achieve objectives (and strategies).
- Security measures must address business requirements. Information security is a business problem.

DQ 8-2 *"In small companies with few employees, it is virtually impossible to implement the* segregation of duties *control plan." Do you agree? Discuss fully.*

ANS. Obviously, whether one agrees or disagrees with the statement depends on how few "few" employees actually are. (Forty-seven percent of all U.S. employers have fewer than five workers. *Source:* Jim Hopkins, "How Small Firms Lock Data Down," *USA Today*, July 19, 2006, p. 6B.) Ideally, to maximize segregation of duties, the four events-processing functions would reside in four separate individuals. However, the plan can be implemented with as few as three employees, as follows (the employees are called A, B, and C in the following example and a cash payment is used as an illustrative transaction):

Function Number	Function Description	Performed by Employee
1	Authorize the cash payment.	A*
2	Execute (make) the cash payment.	B
3	Record the cash payment.	C
4	Safeguard the cash asset (i.e., have custody of blank checks).	B**

Notes:

* Employee A might very well be the sole proprietor of the organization or hold an equivalent supervisory position.

** To *compensate* for the fact that functions 2 and 4 both reside in employee B, the monthly bank statement is mailed by the bank directly to employee A, who prepares the independent bank reconciliation. In the chapter, we discussed such an alternative under the rubric of *compensatory controls*.

Assuming that employee A is the sole proprietor, we could even collapse the four functions into two employees by having A perform functions 1 and 3 and having B perform functions 2 and 4. But note that if we do that, we are really substituting a personnel control plan (i.e., trust in employee B's honesty) for a segregation of duties control plan.

DQ 8-3 *"No matter how sophisticated a system of internal control is, its success ultimately requires that you place your trust in certain key personnel." Do you agree? Discuss fully.*

ANS. Yes and no. We say no because we believe that a control system should monitor the quantity, quality, and legitimacy of each employee's work. Procedures should be in place, therefore, to make sure that each employee performs his/her duties as planned. We say yes because many control procedures are performed by an organization's employees and we must assume that control procedures will be performed as prescribed. That assumption is invalidated when employees conspire—collude—to bypass control procedures. We do have to trust that key personnel will not collude to bypass prescribed procedures.

DQ 8-4 *"If personnel hiring is done correctly, the other personnel control plans are not needed." Do you agree? Discuss fully.*

ANS. Emphatically no. While sound hiring practices are a crucial personnel policy, employees can change over time. An employee's need for ongoing training might not be addressed (a *personnel development control plan*), or they may become disgruntled due to lack of advancement or appropriate raises (*retention control plans*). Outside factors such as a change in the employee's personal life might cause a change in the employee's work attitude or behavior. These changes should be noticed during performance evaluations (*personnel development control plan*) or supervision (*personnel management control plan*). Further, while hiring good people is important to a company, keeping good people (e.g., preventing turnover of trained employees) is equally important. This is addressed with use of appropriate *development* and *retention control plans*.

DQ 8-5 *"Monitoring must be performed by an independent function such as a CPA." Do you agree? Discuss fully.*

ANS. All internal controls need to be reviewed periodically to determine that they continue to function effectively and efficiently. This review may be one of three types.

First, the business process owner or IS organization may perform a so-called control self-assessment. The benefits of this approach include acceptance on the part of these entities of the ownership of the internal controls and development of an appreciation for how control systems can help entities achieve their objectives.

Second, an entity's internal audit function may add objectivity to the monitoring operation. If organizationally independent of the units being reviewed, the internal auditor can also provide an independent assessment.

Third, a function independent of the entity, such as a CPA or consultant, can provide an objective and independent monitoring function to complement the self-assessments and internal audits.

DQ 8-6 *Compare and contrast the COBIT definition of control in this chapter with definitions in Chapter 7 for ERM, the COSO definition of internal control, and this textbook's definition of internal control.*

ANS. Some common elements, and some differences, are summarized in the following table:

ERM	**COSO**	**Textbook**	**COBIT**
Process.	Process.	Process.	Policies, procedures, practices, and organizational structures.
Effected by an entity's board of directors, management, and other	Effected by an entity's board of directors, management, and other	Effected by an entity's board of directors, management, and other personnel.	

ERM	COSO	Textbook	COBIT
personnel.	personnel.		
Applied in strategy setting and across the enterprise.			
Identify potential events that may affect the entity.			Undesired events will be prevented or detected and corrected.
Manage risk within the risk appetite.			
Reasonable assurance.	Reasonable assurance.	Reasonable assurance.	Reasonable assurance.
Achievement of entity objectives.	Achievement of objectives.	Achievement of objectives.	Business objectives will be achieved.
Strategic—high-level goals, aligned with and supporting its mission.			
Operations—efficient and effective use of resources.	Effectiveness and efficiency of operations.	Effectiveness and efficiency of operations.	Effectiveness and efficiency are qualities of information that are to be achieved.
Reliability of reporting.	Reliability of financial reporting.	Reliability of reporting.	Reliability of information and integrity are qualities of information that are to be achieved.
Compliance with applicable laws and regulations.	Compliance with applicable laws and regulations.	Compliance with applicable laws and regulations.	Compliance is a quality of information that is to be achieved.
			Availability is a quality of information.
			Confidentiality is a quality of information.

DQ 8-7 *A key control concern described in Table 8.2 regarding the systems development manager is that "systems development can develop and implement systems without management approval." Discuss a control described in this chapter that reduces the risk that unauthorized systems will be implemented.*

ANS. *Program change controls* address this risk. As depicted in Figure 8.6, any new or revised programs must go through three sets of hands. First, a programmer must write or revise a program. Then the new or revised program must be tested, typically by Quality Assurance with input from the business process owner.

Finally, management, including the business process owner, must give their approval before the new/revised program can be put into production. Collusion between two or more of these individuals could circumvent this control. But an audit trail of changes to production programs would allow the eventual detection of any unauthorized program changes.

DQ 8-8 *Debate the following point: "*Business continuity planning *is really an IT issue."*

ANS. Yes. IT needs to ensure the continued operation of IT, one of the organization's major resources.

No. Management and IT users are responsible for planning, and in many ways implementing, the *business continuity plan*. This plan will include, in addition to plans for IT, plans for the continued availability of people, documents, offices, communications, and so on. It is, after all, a *business* continuity plan, not an *IT* continuity plan.

DQ 8-9 *"Contracting for a* hot site *is too cost-prohibitive except in the rarest of circumstances. Therefore, the vast majority of companies should think in terms of providing for a* cold site *at most." Discuss fully.*

ANS. The key discussion point in this question should be the trade-off between timely recovery of critical business functions on the one hand and the cost of providing the backup facilities on the other. As mentioned in the chapter, in some industries, such as the airline industry's reservation system, near-immediate recovery is a must. In that situation, the remedy is even more expensive than *contracting* for a backup hot site; the airline itself owns and maintains duplicate processing facilities.

Therefore, the quotation must be discussed in relative rather than absolute terms. For some companies (or some applications within a company), a cold site recovery strategy would be adequate or more than adequate. For other companies or applications, more immediate recovery is required because the exposures of a serious business disruption carry a cost that exceeds the cost of providing the backup facility.

The solution to this question is strengthened if one emphasizes the importance of risk analysis in developing the contingency plan.

DQ 8-10 *"Preventing the unauthorized disclosure and loss of data has become almost impossible. Employees and others can use iPods, flash drives, cameras, and PDAs, such as BlackBerries and Treos, to download data and remove it from an organization's premises." Do you agree? Describe some controls from this chapter that might be applied to reduce the risk of data disclosure and loss for these devices.*

ANS. These devices can certainly be used to circumvent physical access controls and logical access controls, such as physically restricting access to a computer facility, library controls, and access control software with identification and authentication techniques. However, some controls that might be used to reduce the risks of disclosure and loss include the following:

- Implement portable device policies and education programs for employees.
- Encrypt flash drives to protect data in the event that the device is lost.
- Dismiss employees violating portable device policies.
- Some organizations have gone to the extreme of limiting their network's capability to write to portable storage devices.

DQ 8-11 *Your boss was heard to say, "If we implemented every control plan discussed in this chapter, we'd never get any work done around here." Do you agree? Discuss fully.*

ANS. Yes and no. In rebutting your boss's statement, you could point out at least two things:

1. The authors never intended that the plans be applied to all situations in all companies. Some are appropriate for some environments, whereas others are geared to different environments. Although the four broad categories of control plans should be considered by all organizations, the specific plans within those categories must be tailored to each particular organization. For example:
    - Many of the plans presented in the chapter relate to computerized operations. Naturally, they would not be appropriate for manual systems.
    - Several of the specific control plans were discussed in the context of an information systems organization such as that depicted in Figure 8.2. Many of those plans would not be suitable for organizations whose ISs were organized differently (e.g., a decentralized organization with IS functions located throughout the organization).
2. The authors recognize that some plans simply cannot be employed in some situations because it is impossible or impractical to do so. For instance, as discussed in the chapter, smaller companies may not have the personnel to fully implement the segregation of duties control plan. In that case, they have to consider alternative, compensatory controls, such as greater care in their selection and hiring procedures and closer managerial supervision of their personnel.

On the other hand, your boss is right on the money if his or her remark was intended to identify the following interdependent issues:

1. *Assessing risks before deciding on which controls to implement:* Recall from Chapter 7 that Enterprise Risk Management describes a process for

identifying and responding to risks. For example, some organizations, by the very nature of their businesses, are simply more vulnerable or susceptible to loss or injury than other organizations. Naturally, they should consider instituting tighter controls than would those subject to less risk.

2. *Control redundancy:* As discussed in Chapter 7, situations can exist where multiple plans are directed at the same control goal, in which case, the organization could suffer from control overkill. For instance, this chapter discusses many different backup and recovery strategies. No single entity would ever contemplate using all of these strategies; doing so is impractical, unnecessary, and cost-prohibitive.

   Also, because over-control has the potential to encourage unwanted, negative behavioral reactions, it often can be as injurious to an organization as can under-control. Employees may rebel at controls that they perceive as unduly constraining or distasteful. Their rebellion might well manifest itself in petty acts of fraud, thievery, or other forms of covert and overt resistance.

3. *Balancing effectiveness and efficiency:* This topic was also mentioned in Chapter 7, when the authors talked about controls being built in rather than built on. Controls impose some overhead on a firm. Therefore, management must attempt to integrate the *control system* as seamlessly as possible with the *work system* so that normal operations are not unduly burdened or impeded.

4. *Cost/benefit analysis:* Closely related to the previous three issues is management's evaluation of the costs and benefits associated with any control plans being contemplated. Control plans cost money. Therefore, to justify the expenditure of resources, management should be convinced that the benefit to be derived will exceed the cost involved. Calculations such as *residual expected risk* can help in making a determination that enough controls have been put in place.

DQ 8-12 *For each of these control plans suggest a monitoring activity:*

a. Credit approval

ANS. A list of new customers for the last month and the supporting documentation used to approve credit reviewed by the CFO.

b. Removal of terminated employee access to computer system

ANS. A list of employees terminated in the last month supplied by personnel and a list of access level changes supplied by the security manager are compared by the chief information officer.

c. New employee background check

ANS. The applications of newly hired employees for the last month are compared to the supporting documentation of the reference checks by each employee's manager.

Short Problems

SP 8-1 ANS.

Control Situation	Control Plan
1.	E
2.	F
3.	A
4.	D
5.	C

SP 8-2 ANS.

Control Situation	Control Plan
1.	B
2.	A
3.	E
4.	F
5.	D

SP 8-3 ANS.

1. CAEMWLVGPE, A becomes C by adding 2, C becomes A by subtracting 2, C becomes E by adding 2, O becomes M by subtracting 2, etc.
2. Depends on professor name.

SP 8-4 ANS. Students' solutions will vary, of course. At a minimum, each answer should include (1) a brief description of the case, including the IT involved; (2) the pervasive controls that failed; (3) how the pervasive controls failed; (4) lower-level controls affected; and (5) sources.

Problems

P 8-1 ANS.

Note: This problem and solution were adopted from Thomas Wailgum, "Security: 50-Cent Holes," *CIO Magazine*, October 15, 2005.

A. The personal information can be used to perpetrate identify theft. Releasing the data may violate privacy laws and regulations. To prevent this problem, train employees and customers on how to recognize and respond to phishing and other related attacks. Install systems to screen out suspicious e-mails.

B. The default password can be used by hackers to gain access to her network and intercept her transmissions. The data accessed in this manner can be used for a variety of fraudulent activities or to create a competitive advantage. To prevent this problem, employees need to be trained on how to set up and secure (passwords, firewall, antivirus, etc.) a wireless network. Perhaps the organization can provide assistance to employees to ensure their proper installation.

C. The use of the consumer-grade IM precludes the organization from enforcing virus, spam, and regulatory compliance. Also, the user can take their IM name, and therefore their customers, with them when they leave the organization. To prevent these problems, organizations should establish policies for acceptable use of IM. Organizations can also deploy security functions such as blocking file transfers or mapping IM names to identifiers (e.g., user IDs) assigned by the organization. Or the organization can replace the consumer-grade IM with an enterprise-grade system.

D. The information on the laptop can be used to perpetrate identify theft. Releasing the data may violate privacy laws and regulations. To prevent this problem, management should perform risk assessment to determine what data must be protected and then implement security policies based on that assessment. Security protection may include password protection, encrypted data, and biometric access.

E. A hacker, or any individual for that matter, could use the passwords to access computer systems and cause many kinds of problems. To prevent this problem, establish an organization-wide policy prohibiting the creation and storage of electronic files listing passwords. Educate employees as to the importance of this policy, and enforce the policy by taking disciplinary action against those violating the policy (assumes that network files are scanned on a regular basis, looking for files that violate the policy).

Management might consider implementing single sign-on systems to reduce the number of passwords that individuals must create and remember.

F. The information on the backup disks can be used to perpetrate identify theft and execute fraudulent credit card charges. Releasing the data may violate privacy laws and regulations and subject the company to financial loss as it indemnifies customers for any losses. To prevent this problem, the credit card company should send the data encrypted and electronically.

G. Such e-mails would violate privacy laws and regulations and cause embarrassment to the senders and recipients of the messages. To prevent this problem, establish an organization-wide policy that explicitly states what can and cannot be sent via e-mail or instant messaging. Educate employees as to the importance of this policy, and enforce the policy by taking disciplinary action against those violating the policy. Management might consider scanning messages for violation of the policy. For example, systems can scan for messages with 16-digit numbers (i.e., credit card numbers).

H. The account information can be used to steal funds from the individuals' accounts and to perpetrate identify theft. To prevent this problem, establish an organization-wide policy specifying who can access what information, how they can access it, and how often. Then implement the policy through library controls and access control software to limit employee access to data. An employee education program about the importance of this policy should be conducted.

I. The credit card data can be used to perpetrate identify theft and execute fraudulent credit card charges. Releasing the data may violate privacy laws and regulations and subject the company to financial loss as it indemnifies customers for any losses. To prevent this problem, the organization needs to implement policies and procedures, such as firewalls, access control software, and other access controls, to limit access to data to authorized users for authorized purposes.

J. The business related e-mails could find their way into competitors' hands and be used to gain a competitive advantage. Some data may be sensitive or subject to privacy laws and regulations. Organizations should establish and enforce policies related to the use and return of laptops, cell phones, and other information devices. Assuming that this individual has left the organization, a personnel termination procedure should include handing in the cell phone.

P 8-2 ANS.

P & D	1.	P & D	11.
P	2.	P & C	12.
P	3.	P & D	13.
C	4.	P	14.
C	5.	P & D	15.
C	6.	P	16.
P & C	7.	C	17.
P	8.	P	18.
P & D	9.	P & D	19.
P	10.	P & D	20.

Note: We have offered multiple possibilities for answers to some of the preceding items:

- *Item 1:* Library controls will manage access to programs and data and thus prevent unauthorized access. These controls also log all uses of programs and data and thus can detect any unauthorized uses that may take place.
- *Item 7:* The service level agreement may provide for a minimum level of service, may prevent service disruptions, may have sanctions for nonperformance, and may be a corrective control.
- *Item 9:* A security officer may prevent intruders as well as detect intruders after they have gained access.
- *Items 11, 13, and 15:* These may encourage personnel to perform their jobs well (or discourage bad behavior) or provide a means to detect poor performance and bad behavior.
- *Item 19:* May prevent unauthorized personnel from gaining access to a computer system or detect attempts to gain unauthorized access.
- *Item 20:* May prevent poor personnel performance by ensuring that employees are trained to perform their jobs or may detect poor performance through ongoing evaluation.

P 8-3 ANS.

Control Situation	Control Plan
1.	H
2.	F
3.	B
4.	G
5.	C
6.	J
7.	I
8.	L
9.	K
10.	E

P 8-4 ANS.

Option	Manager	Matthew	Mark
1	No	No	No
2	No	Yes	No
3	Yes	No	No
4	No	No	Yes
5	No	No	No
6	Yes	Yes	Yes
7	Yes	Yes	Yes

Explanation:

Option 1, vendor data maintenance, should be performed by the purchasing office. By doing so, we separate authorization to engage in business with a particular vendor from the approval to create accounts payable records and to disburse payments.

Menu options 2, 3, and 4 could be segregated among the three accounts payable personnel. One clerk records invoices, one clerk selects invoices for payment, and the manager makes required adjustments. This authorization pattern prevents any one person from entering *and* paying (or otherwise eliminating) a vendor invoice.

Option 5, check printing, should be reserved for the treasurer's office.

Option 7, accounts payable reports, should be available to all three accounts payable personnel. This read-only option provides information necessary for each person to perform his or her functions.

P 8-5 ANS.

Employee	Function
Nathan	1, 6, 7
Jordyn	2, 3, 10
James	4, 5, 8, 9

Comment: The preceding solution represents but one of many possible solutions. Our primary goal in solving this problem should be to segregate the handling of cash from the recording of the cash-related transactions. This solution segregates duties as follows:

a. Nathan performs cashier (i.e., treasurer) functions, such as receiving the checks from the customers (function 1), depositing checks in the bank (function 6), and signing and mailing checks to vendors (function 7).

b. Jordyn performs accounting (i.e., controller) functions, such as approving vendor invoices for payment (function 2) and approving credit memos (function 3). This employee also reconciles the bank account (function 10). The bank reconciliation safeguards the cash, for example, by comparing the checks deposited by Nathan to the customer payments recorded by James. We prefer to have a fourth person, independent of the treasurer and controller functions, to reconcile the bank account.

c. James is a clerk who performs all recordkeeping (i.e., controller) functions (4, 5, 8, 9).

P 8-6 ANS.

Domain	Process	Plans
Plan and Organize Domain	Establish Strategic Vision for Information Technology	An inventory of IT capabilities
		Statement of IT goals and strategies
	Develop Tactics to Plan, Communicate, and Manage Realization of the Strategic Vision	Segregation of duties within the IT department
		A quality assurance plan
Acquire and Implement Domain	Identify Automated Solutions	A new system requirements definition document
		Feasibility studies
	Develop and Acquire IT Solutions	An assessment of how new hardware might affect existing hardware
		Application documentation
	Integrate IT Solutions into Operational Processes	A process for testing a new system.
		A postimplementation review
	Manage Changes to Existing IT Systems	A process to select and prioritize user requests for system changes
		Program change testing
Deliver and Support Domain	Deliver Required IT Services	Define service levels
		Perform preventive maintenance
	Ensure Security and Continuous Service	Complete a disaster recovery plan
		Biometric security devices
	Provide Support Services	Help desk
		User training classes
Monitor and Evaluate Domain	Monitor and Evaluate the	Report on response times

	Processes	
		An IT security audit

P 8-7 ANS.

1. Controls related to the control environment	H O	Establishment of a code of conduct Use of control frameworks such as COBIT and COSO
2. Controls over management override	K N	Segregation of duties Supervision
3. The company's risk assessment process	G C	Development of a business interruption plan A report on IT risks and a risk action plan
4. Centralized processing and controls, including shared service environments	E J	A systems development life cycle methodology (SDLC) Program change controls
5. Controls to monitor the results of operations	F M	Budgetary controls Service level agreements and reporting processes
6. Controls to monitor other controls, including activities of the internal audit function, the audit committee and self-assessment programs	B A	A report of all employees not taking required vacation days A file of signed code of conduct letters
7. Controls over the period-end financial reporting process	I	Not covered
8. Policies that address significant business control and risk management practices	D L	Access control software Selection and hiring control plans

P 8-8 ANS.

1. *Security officer:* Business continuity planning can help an organization recover quickly from natural disasters such as hurricanes and losses of data and computing resources such as those perpetrated by hackers.
2. *Chief Information Officer (CIO):* The Strategic IT Plan sets the long-term agenda for the IS organization. When synchronized with the organization's

strategic plan, the Strategic IT Plan (along with the IT steering committee) directs IS resources toward the achievement of the organization's mission.

3. *Systems development manager:* This control concern is directed at the potential exposure—such as fraud—that could result should systems development personnel make unauthorized changes to computer programs. To *prevent* systems development personnel from developing and implementing systems without authorization, duties are segregated *within* the information systems function. For example, we prevent computer programmers from installing their own programs on the computer or having access to production data (primary copy) for testing purposes.
4. *Quality assurance:* Internal audit's monitoring of projects, including systems development projects, should improve the efficiency and effectiveness of those undertakings. Internal audit can, for example, review project documentation to determine that the project team is following prescribed procedures.
5. *Systems programming:* Fidelity bonding can minimize (i.e., *correct*) the financial impact of any fraudulent manipulations perpetrated by a systems programmer. Also, if we have adequate staff, we can review and monitor their work.

P 8-9 ANS. Student solutions will vary, of course. At a minimum, each answer should include (1) a description of the incident(s), with background; (2) how long the site(s) were not available; (3) how they came to be out of service; (4) which controls would have *prevented*, *detected*, or *corrected* the outages; and (5) sources.

P 8-10 ANS. Student solutions will vary, of course. At a minimum, each answer should include (1) a description of the incident(s), with background; (2) how long the site(s) were not available; (3) how they came to be out of service; (4) which controls would have *prevented*, *detected*, or *corrected* the attacks/outages; and (5) sources.

P 8-11 ANS. As of this writing, the main Web page for Trust Services Principles and Criteria is found at www.aicpa.org/InterestAreas/InformationTechnology/Resources/TrustServices/Pages/default.aspx. A link to Trust Services Principles and Criteria is also found on this Web page.

a. The Trust Services Principles and Criteria are the following:

- *Security:* The system is protected against unauthorized access, both logical and physical.
- *Availability:* The system is available for operation and use as committed or agreed.
- *Processing integrity:* System processing is complete, accurate, timely, and author*ized.*

- *Confidentiality:* Information designated as confidential is protected as committee or agreed.

- *Privacy.* Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles issued by the AICPA and CICA.

b. SysTrust and WebTrust are the two types of Trust Services based on the Trust Services Principles and Criteria. Links to these services may also be found on this page.

c. It should be interesting and informative to discuss the types of additional assurance services that the students offer. Be sure that they apply the five principles (listed previously) to the services they recommend. Students might suggest (or you could suggest these to them) services to examine performance of members of supply chain collaborations. Or they could suggest services related to compliance with HIPAA (the Health Insurance Portability and Accountability Act) or FERPA (the Family Educational Rights and Privacy Act).

SOLUTIONS FOR CHAPTER 9

Each end-of-chapter question in the Solutions Manual is tagged to correspond with AACSB, AICPA and CISA standards, allowing professors to more easily manage the task of reporting outcomes to these professional and accrediting bodies. Please see the corresponding spreadsheet file for the tagging information.

Discussion Questions

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

ANS. The control matrix is customized for each business process because the following elements of the control goals vary depending on the process being analyzed:

- Process name
- Effectiveness goals
- Resources (for security and efficiency)
- Inputs
- Master data

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

ANS. Perhaps the most error-prone and inefficient steps in an operations or information process are the steps during which data is entered into a system. Although much has been done to improve the accuracy and efficiency of the data entry process, problems still remain, especially when humans enter data into a system.

Once input, event data will affect a number of processes and will cause the update of master data. For example, upon input, a shipping notice will affect the OE/S process, the billing/accounts receivable/cash receipts process, the inventory process, and, possibly, the general ledger process. The shipping notice will likely cause the update of the sales order data, the accounts receivable master data, the inventory master data, and, possibly, the general ledger master data. Therefore, input controls must ensure that the shipping notice is valid and accurate at the time of input. Otherwise, all master data must be corrected, and until they are corrected, the effect could be significant.

Should the data be input to an *enterprise system,* the impact would certainly be significant. The processes/subsystems are tightly connected, and each depends on receiving accurate, valid data from other portions of the system. If the data is input to an application that is connected to other organizations, such as with *e-business*, the data needs to be accurate and valid. Otherwise, we may undertake a purchase or a sale with a trading partner that is not in our best interest (because it is based on invalid or inaccurate data).

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

a. Batch total procedures

ANS. We *establish* the control when we calculate the original batch total. We *exercise* the control when we reconcile the original batch total with a total calculated at some later point in the process.

b. Turnaround documents

ANS. We *establish* the control when we prepare a turnaround document, typically by having a document printed by a computer, as, for example, the stub of a customer invoice. We *exercise* the control when we use that document for input to a subsequent process. For example, we use the invoice stub (i.e., the remittance advice or RA) that is received from the customer with their payment as the input to record the payment.

c. Tickler files

ANS. We *establish* the control when we create a record in a file that can be used as a tickler file. We *exercise* the control when we go through the file to ensure that the record is cleared (i.e., a subsequent action is taken in a timely manner). For example, we review the sales order master data to find sales orders that have not yet been shipped to follow up and ensure timely shipment.

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

a. Do you agree with this comment? Why or why not?

ANS. To some extent, we agree. An individual inside the organization or normally authorized to use the prenumbered document could obtain a blank document and complete the document to create an invalid event.

b. Without prejudice to your answer to part (a) , assume that the comment is true. Present (and explain) a "statement of relationship" between the control plan of using prenumbered documents and the information system control goal of event "validity."

ANS. If an individual gains access to a prenumbered document and uses that document to initiate an unauthorized event, the prenumbered document could not help *prevent* or *detect* the invalid event. However, if an individual were to replicate a prenumbered document in an attempt to initiate an unauthorized event, the prenumbering would help *detect* the invalid event because two documents with the same number should not be acceptable to the system.

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

ANS. Many students will have worked in retail as cashiers, wait staff, and so on. They will also likely have engaged in retail as consumers. Therefore, situations that might be mentioned include the following. Most retail sites on the Internet use *encryption* to transmit sensitive data such as credit card numbers. Bank tellers and retail clerks use *batch totals* to reconcile their cash drawers at the end of a shift. We use a *cumulative sequence check* when we balance our checkbook. We often use a *turnaround document* to submit payments for credit cards and utilities.

Students often have experience with software, such as Peachtree, Great Plains, or SAP®, at school or at work. In those cases, they may cite the following control examples recalled from that experience: *preformatted screens*, *online prompting*, *populate input screens with master data*, *compare input data with master data*, and *confirm input acceptance*.

DQ 9-6 *Refer to Exhibit 9.5. For each pair of factors describe why you believe the factor in the right column provides a higher level of assurance. That is, why do these factors indicate a stronger control?*

ANS. With manual controls there is the risk of human error, while automated controls will—depending on the effectiveness of IT general controls—perform consistently.

1. An experienced manager's knowledge, background, and skills make him or her a better candidate to perform a control than would an inexperienced person.

2. In most circumstances we would prefer to prevent errors from entering into a system, especially with *OLRT* systems and systems with integrated modules such as in an *enterprise systems*. In these cases an erroneous input can quickly spread throughout a system and be difficult to detect.

3. While we might prefer the efficiency of a single control, the one control may not be effective in detecting all errors. For example, programmed edit checks followed by manual review of output would be more effective than either control on its own.

4. Sampling, especially statistical sampling, may provide comfort that there are no errors in some situations, such as manufacturing. But if we need to know with certainty that *all valid* business events are being processed *correctly*, we need to review every event.

5. As discussed with the control *enter data close to the originating source*, it is much easier to detect and correct errors as the event occurs. For example, in the shipping department, at the time and place of the shipment, we can match one-for-one the picking ticket, packing slip, and goods to detect and correct any errors before the input takes place.

DQ 9-7 *Referring to Appendix 9A, discuss fully the following statement: "Protecting the private key is a critical element in public key cryptography."*

ANS. If we receive a transmission and open it with a public key (say Bob's public key), we assume that the document was locked with the corresponding private key (i.e., Bob's private key). If someone other than Bob has that private key, we are not sure who sent and locked the message. Also, we are not sure that someone has not tampered with the message. Therefore, protecting the private key to prevent unauthorized use of that key is critical to the integrity of public key cryptography.

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

ANS. If the clerk misread the order and input the order for $4 billion, rather than $4 million, there is a human error. But it is not clear whose error this is. Was the order handwritten and was the trader's handwriting legible (i.e., *document design*)? Should trades of this size be reviewed and approved by a second party (*written approvals* or *electronic approvals*)? Should the computer have immediately recognized the size of the trade and stopped it before execution (a *reasonableness test*)? Perhaps the trades were entered a few million dollars at a time, and the computer would not be able to determine that the total was unreasonable.

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

ANS. No, we do not agree. As indicated in Figure 7.6, the hierarchy of controls has business process and application control plans at the bottom. Does that mean that they cannot be relied on? No, but it does mean that we need to be aware of the impact that strong or weak pervasive and general controls (and IT general controls) can have on the potential effectiveness of business process and application controls. At the same time, we need to be aware of the impact that the control environment can have on the potential effectiveness of pervasive and general controls. For example, if management sets a positive tone-at-the-top of the organization (i.e., *control environment*) by establishing a code of conduct, setting a positive example regarding following established policies and procedures, and performing their duties to the best of their abilities, for example, it is more likely that pervasive and general controls will be performed as required (e.g., use the *SDLC* when developing systems, follow *program change controls* when implementing a new system). When an organization adopts and follows these pervasive controls, and others, we can accept that application controls such as *programmed edit checks* and other automated controls will be effective.

We should also mention that controls in the hierarchy do not replace controls below them. For example, a positive tone at the top does not mean that we do not need *program change controls*. Also, if we have program change controls, we still need *programmed edit checks* and other automated controls to ensure that data is processed properly. So it is with a *combination* of controls from the three levels in the hierarchy that we obtain a reasonable level of assurance that control objectives are achieved.

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

ANS. No, we do not agree. Our control framework looks separately at update completeness (UC) and update accuracy (UA) only when there is a delay between input and update. In those cases, controls need to be in place to ensure that *all* data (UC) that is recorded on an input/event data store (i.e., an event data store or transaction file) is subsequently updated *correctly* (UA) to the relevant master data. If the controls over input completeness and input accuracy are in place, and the updates to the master data occur in the same step as the input is accepted for processing, then the input controls should ensure UC and UA.

Note: This is a simplification of the matter of UC and UA that we have made to help the students learn the framework without undue complications involving the details of the processing of business events.

Short Problems

SP 9-1 ANS.

Assertion	Information Quality	Explanation
A	1 and 2	When input data is restricted to "actual economic events and objects" (IV) that are recorded "only once" (IC), the resulting financial data will contain only assets and liabilities that exist (actual objects) and transactions that have occurred (actual events).
B	2	When controls are in place to ensure that all economic events are recorded (IC), the resulting financial data will be complete.
C	1, 2, and 3	To assert that an entity has rights to an asset, controls must be in place to accurately capture (IA) only real events (IV). To assert that liabilities are the obligations of the entity, controls must be in place to accurately capture (IA) all economic events (IC). *Note:* We are not so concerned about incomplete assets and invalid liabilities.
D	3	Including these components in the financial statements at "appropriate" amounts relates mostly to accurate data capture (IA).
E	2 and 3	To be properly classified and described, controls must be in place to capture all data accurately (IA). To be able to disclose all components, controls must be in place to capture all relevant events (IC).

SP 9-2 ANS.

1. No. Only someone with Sally's private key (D) can open the message. (This assumes that only Sally has her private key.)
2. No. Anyone with Sally's public key (C) can send this message.
3. No. Anyone with Harry's public key (A) can open the digital signature message.
4. No. Only Harry's private key could have been used to send this message. (This assumes that only Harry has his private key.)
5. If the hash total (HT) that she calculates from the message (M) matches the hash total contained in the digital signature. If they are not equal, the message, or the digital signature hash total, have been changed.
6. Questions 2 and 4 ask about authenticity (who sent the message).
7. Question 5 asks about integrity.
8. Questions 1 and 3 ask about confidentiality.

SP 9-3 ANS.

Control Plan	Input Validity	Input Completeness	Input Accuracy
Document design			1
Written approvals	2		
Preformatted screens			3
Limit check			4
Confirm input acceptance		5	
Digital signature	6		7
Reconciliation of batch totals (document count)	8	9	
Turnaround documents	10		11
Sequence check	12	13	
Populate input screens with master data	14		15

FIGURE SM-9.1 Short Problem 3 Completed Table

Description of table entries (number 1 and 2 were given):

1. A well-designed document can be filled in completely and legibly and be input to the computer with fewer errors.
2. Approvals indicate authorization for a document or business event, thus reducing the possibility of processing invalid events.
3. Preformatted screens ensure that entries are made in all required fields and that data is properly formatted.
4. Limit checks review input data to determine that it falls within predetermined limits, reducing the possibility of input erroneous data.
5. With this control the data entry clerk is informed by the computer that an input has been accepted, thus ensuring that all inputs are recorded.
6. Opening the digital signature (hash total) message with sender "A's" public key ensures that the signature message (and the related encrypted message) was actually sent by "A," thus ensuring the validity of the message.
7. By matching the hash total in the signature message with the hash total of the encrypted message, we can ensure that the message was not altered in transmission.
8. If we reconcile the count documents before entry with the total number of documents accepted by the computer, we have some evidence (but not strong evidence) that no *invalid* documents were entered.
9. If we reconcile the count documents before entry with the total number of documents accepted by the computer, we have some evidence (but not strong evidence) that all documents were entered once and only once.
10. Turnaround documents, when they are created by one functional area and input by another, can ensure authorization (i.e., validity) of the input.
11. Using the prerecorded data on the turnaround document reduces input errors.

12. By comparing an expected sequence of documents with those actually input, we can detect a duplicated (i.e., incomplete [input more than once]) or unexpected (i.e., invalid) document.
13. By comparing an expected sequence of documents with those actually input, we can detect missing or duplicated documents.
14. When the computer displays a master record, such as a customer master record, when a clerk inputs a customer number for a sale, we can be sure that we will be executing a sale for an authorized customer, thus ensuring the validity of sale.
15. When the computer displays a master record, such as a customer master record, when a clerk inputs a customer number for a sale, fewer keystrokes will be required to enter the sales data, thus improving the accuracy of the input.

Problems

P 9-1

a. ANS. The control matrix is shown in Figure SM-9.2, and the explanations of the cell entries are contained in Exhibit SM-9.1. Wherever the system narrative is not explicit about whether a plan is present or missing, we have made assumptions, as indicated by our labels P-*n* or M-*n*.

b. ANS. See Figure SM-9.2.

	Control Goals of the Causeway Cash Receipts Process								
	Control Goals of the Operations Process				Control Goals of the Information Process				
	Ensure effectiveness of operations:		Ensure efficient employment of resources (people, computers)	Ensure security of resources (cash, accounts receivable master data)	For the remittance advice inputs (i.e., cash receipts), ensure:			For the accounts receivable master data, ensure:	
Recommended control plans	**A**	**B**			**IV**	**IC**	**IA**	**UC**	**UA**
Present Controls									
P-1: Preformatted screens	P-1	P-1	P-1				P-1		
P-2: Online prompting	P-2	P-2	P-2				P-2		
P-3 Programmed edit checks.	P-3	P-3	P-3				P-3		
P-4: Manual agreement of RA batch totals				P-4	P-4	P-4	P-4	P-4	P-4
P-5: Manual agreement of deposit batch totals				P-5	P-5	P-5	P-5		
Missing Controls									
M-1: Turnaround documents	M-1	M-1	M-1				M-1		

	Control Goals of the Causeway Cash Receipts Process								
	Control Goals of the Operations Process				Control Goals of the Information Process				
	Ensure effectiveness of operations:		Ensure efficient employment of resources (people, computers)	Ensure security of resources (cash, accounts receivable master data)	For the remittance advice inputs (i.e., cash receipts), ensure:			For the accounts receivable master data, ensure:	
Recommended control plans	**A**	**B**			**IV**	**IC**	**IA**	**UC**	**UA**
M-2: Enter cash receipts in the mailroom	M-2	M-2	M-2			M-2	M-2		
M-3: Computer agreement of batch totals	M-3	M-3	M-3	M-3	M-3	M-3	M-3	M-3	M-3

Possible effectiveness goals include the following:
A – Timely deposit of checks
B – Comply with compensating balance agreements with the depository bank

IV = input validity
IC = input completeness
IA = input accuracy
UC = update completeness
UA = update accuracy

See Exhibit SM-9.1 for a complete explanation of control plans and cell entries.

FIGURE SM-9.2 Problem 1 Part a Solution (Partial)—Control Matrix for Causeway Company

Exhibit SM-9.1 Problem 9-1 Part a Solution (Partial)—Explanation of Cell Entries

Discussion and Explanation of Recommended Control Plans

P-1: *Preformatted screens.*

System goals A and B, efficient employment of resources: By structuring the data entry process and by preventing input errors, data entry is simplified, time saved, and checks deposited in a timely manner so as to comply with balance agreements.

Input accuracy: As each data field is completed, the cursor moves to the next field on the screen, thus preventing the user from omitting any data set.

P-2: *Online prompting.*

System goals A and B, efficient employment of resources: Asking the user for input or asking questions that the user must answer can ensure a quicker and more efficient data entry process. By saving time, we can ensure that checks are deposited in a timely manner so as to comply with balance agreements.

Input accuracy: The online guidance should reduce input errors.

P-3: *Programmed edit checks.*

Effectiveness goals A and B, efficient employment of resources: Event data can be processed on a timelier basis when errors are identified and the input clerk can take corrective action immediately. Event data can be processed on a timelier basis and at a lower cost per input if errors are prevented from entering the system in the first place. By saving time, we can ensure that checks are deposited in a timely manner so as to comply with balance agreements.

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

P-4: *Manual agreement of RA batch totals*. (*Solution Note:* The following discussion assumes that the batch totals are *hash totals*. If the batch totals consisted of *document/record counts* and/or *item/line counts* only, those types of batch totals would address only the goals of input validity, input completeness, and update completeness.)

Security of resources: A complete and accurate record of RA amounts, when compared to the deposit amounts, should ensure that all cash received is deposited.

Input validity, input completeness, input accuracy: The output reports prepared at the end of the day are compared by an accounts receivable clerk to the batch totals of the RAs that were input to the system. When the various batch totals fail to agree, evidence exists that event(s) may have been added (*validity*), input more than once (*completeness*), lost (*completeness*), or changed (*accuracy*).

Update completeness, update accuracy: Because the Causeway system *reconciles* batch totals after *both* the event *recording* and master data *update* steps have been performed, *update completeness (UC)* and *update accuracy (UA)* are ensured.

P-5: *Manual agreement of deposit batch totals.*

Note: We assume that the cashier is reconciling batch totals. Perhaps this control is a one-for-one comparison of the checks on the deposit slip to those in the temporary file.

Security of resources: The deposit slip is compared by the cashier to the batch totals of the checks received from the mailroom. If the totals do not agree, checks may have been lost.

Input validity, input completeness, input accuracy: If the batch totals fail to agree, there would be evidence that cash receipts data may have been added (*validity*), input more than once (*completeness*), lost (*completeness*), or changed (*accuracy*).

Note: We cannot show UC or UA because no cash update is shown.

M-1: *Turnaround documents.*

Effectiveness goals A and B, efficient employment of resources, input accuracy: A document, printed by the computer, is used to capture and input a subsequent transaction. Often, companies use remittance advice "stubs" attached to customer invoices for subsequent input of cash receipts. If Causeway used such a procedure, it would ensure a quicker data entry process; reduce the keying necessary, and therefore be more efficient; and reduce the input errors that might be made, such as incorrect customer number, invoice number, or amount due. By saving time, we can ensure that checks are deposited in a timely manner so as to comply with balance agreements.

M-2: *Enter cash receipts in the mailroom.*

Effectiveness goals A and B, efficient employment of resources: If the cash receipts were to be entered immediately upon receipt at the organization, the cash could be deposited more quickly and the updates to customer balances recorded in a timelier manner so as to comply with balance agreements.

Input completeness: If the cash receipts are captured in the mailroom, there is less chance that they will be lost as they are transported to the data entry location.

Input accuracy: Because the mailroom personnel would have both the check and the RA, they would be in a position to correct many input errors "on the spot" and thus improve input accuracy.

M-3: *Computer agreement of batch totals.* (*Solution Note:* The following discussion assumes that the batch totals are *hash totals*. If the batch totals consisted of *document/record counts* and/or *item/line counts* only, those types of batch totals would address only the goals of input validity, input completeness, and update completeness.)

Effectiveness goals A and B, efficient employment of resources: Had the computer been used to reconcile the batch totals, the processing of event data would have been completed more quickly and with less human effort. By saving time, we can ensure that checks are deposited in a timely manner so as to comply with balance agreements.

Security of resources: A complete and accurate record of RA amounts, when compared to the deposit amounts, should ensure that all cash received is deposited.

Input validity, input completeness, input accuracy: The output reports prepared at the end of the day are compared by an accounts receivable clerk to the batch totals of the RAs that were input to the system. When the various batch totals fail to agree, evidence exists that event(s) may have been added (*validity*), input more than once (*completeness*), lost (*completeness*), or changed (*accuracy*).

Update completeness, update accuracy: Because the Causeway system *reconciles* batch totals after *both* the event *recording* and master data *update* steps have been performed, *update completeness (UC)* and *update accuracy (UA)* are ensured.

Note: Additional controls that could be discussed include procedures for rejected inputs, compare input data with master data, and tickler files.

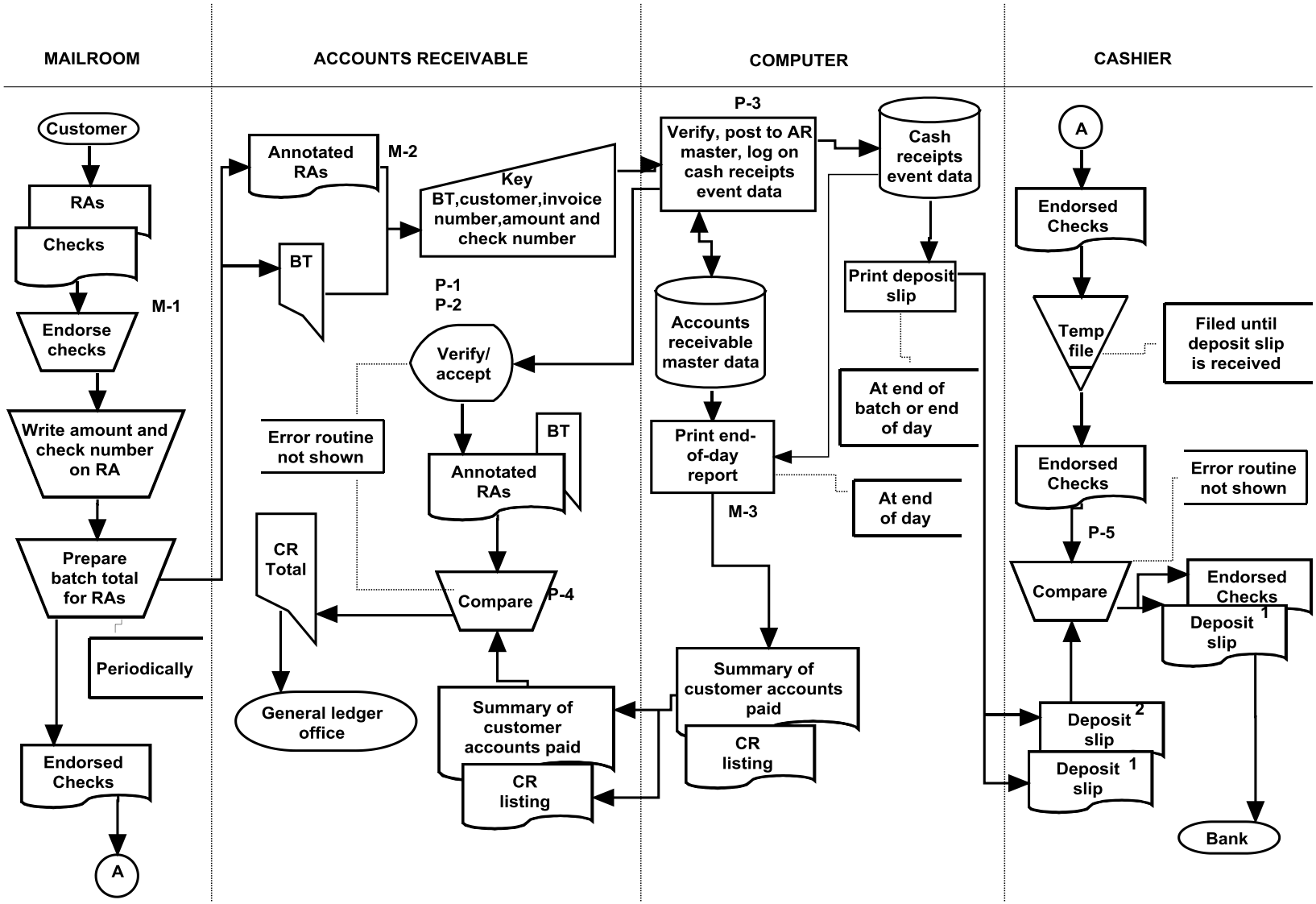


Figure SM-9.3 Problem 1 Part b Solution—Annotated Systems Flowchart for Causeway

P 9-2 a. ANS. Table of Entities and Activities for ePetID Company

Entities	Para	Activities
Customer	1	1. Send orders by mail.
Sales order clerks	1	2. Open and review orders for accuracy.
	1	3. Enter customer number into the computer.
Computer	1	4. Display customer record.
Sales order clerks	1	5. Match customer data onscreen with customer order.
	1	6. Enter items and quantities ordered.
Computer	1	7. Compare input data to customer and inventory master data.
	1	8. Record order on sales event data and sales order master data, update inventory master data.
	1	9. Print picking ticket in warehouse.
	1	10. Print customer acknowledgement in sales order department.
Warehouse	1	
Sales order clerks	1	11. Send customer acknowledgement to the customer.

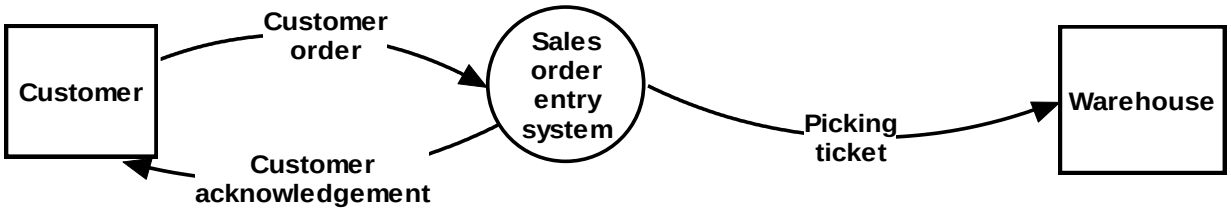


FIGURE SM-9.4 Problem 2 Part b Solution—Context Diagram for ePetID Company

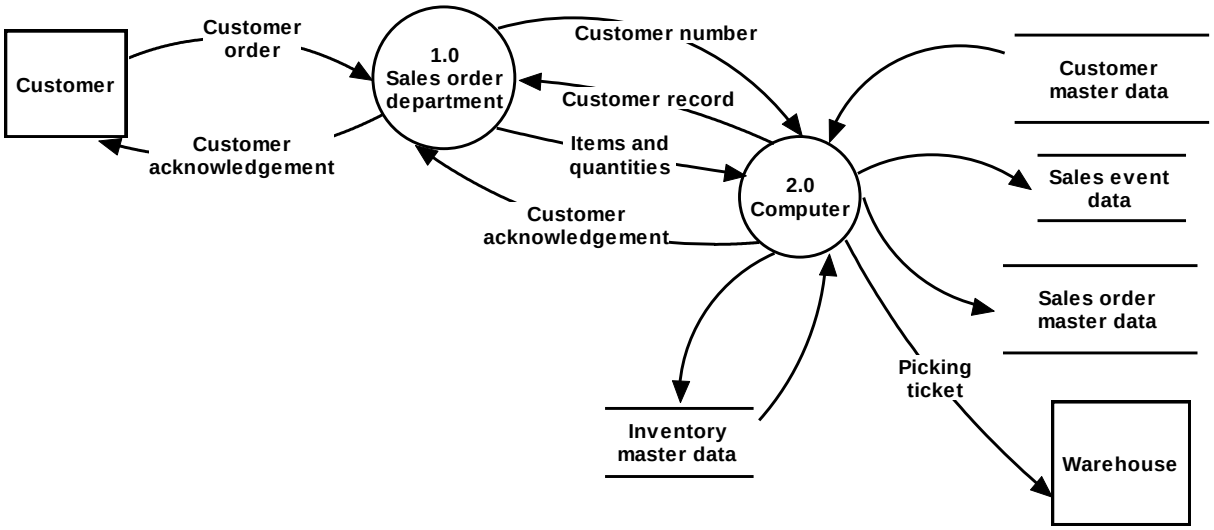


FIGURE SM-9.5 Problem 2 Part c Solution—Physical DFD for ePetID Company

d. ANS. Table of Entities and Activities (Annotated) for ePetID Company

Entities	Para	Activities	
Sales order clerks	1	2. Open and review orders for accuracy.	
	1	3. Enter customer number into the computer.	
Computer	1	4. Display customer record.	***1.0 Capture Customer Order.***
Sales order clerks	1	5. Match customer data on the screen with customer order.	
	1	6 Enter items and quantities ordered.	
Computer	1	7. Compare input data to customer and inventory master data.	
	1	8. Record the order on the sales event data and the sales order master data.	***2.0 Edit and Record Sales Order.***
	1	9. Print picking in the warehouse.	
	1	10 Print customer acknowledgement in the sales order department.	

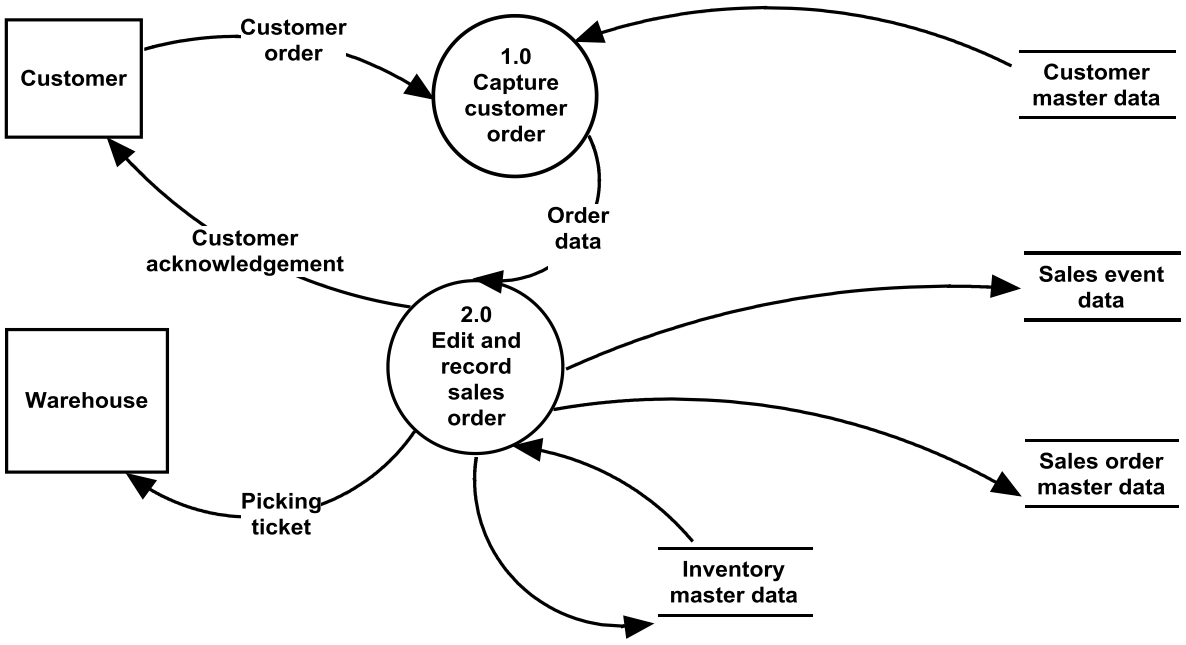


FIGURE SM-9.6 Problem 2 Part e Solution—Logical DFD for ePetID Company

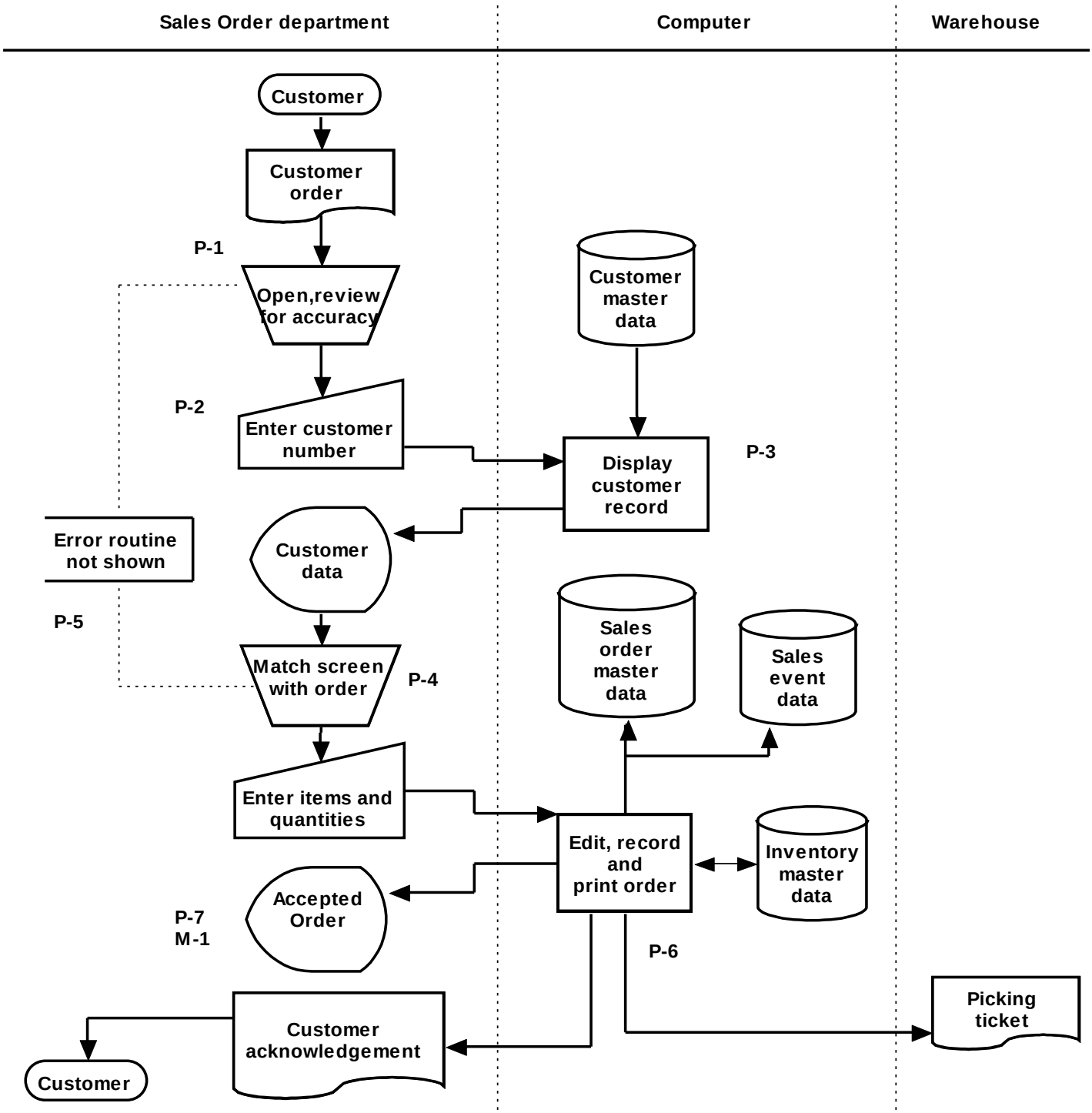


FIGURE SM-9.7 Problem 2 Parts f and h Solutions—Annotated Flowchart for ePetID Company

	Control Goals of the ePetID Order Entry Process								
	Control Goals of the Operations Process				Control Goals of the Information Process				
	Ensure effectiveness of operations:		Ensure efficient employment of resources (people, computers)	Ensure security of resources (customer master data, inventory)	For the sales order inputs (i.e., customer orders), ensure:			For the sales order master data, ensure:	
Recommended control plans	**A**	**B**			**IV**	**IC**	**IA**	**UC**	**UA**
Present Controls									
P-1: Review order for accuracy.	P-1	P-1	P-1				P-1		
P-2: Enter customer orders close to their originating source.	P-2	P-2	P-2			P-2	P-2		
P-3: Populate input screens with master data.	P-3	P-3	P-3	P-3	P-3		P-3		
P-4: Compare input data with master data.	P-4	P-4	P-4	P-4	P-4		P-4		
P-5: Procedures for rejected inputs.						P-5	P-5		
P-6: Programmed edit checks.	P-6	P-6	P-6	P-6	P-6		P-6		
P-7: Confirm input acceptance.						P-7			
Missing Control									
M-1: Manual agreement of batch totals.					M-1	M-1	M-1		

Possible effectiveness goals include the following:
A – To provide timely acknowledgement of customer orders
B – To provide timely shipment of goods to customers

IV = input validity
IC = input completeness
IA = input accuracy
UC = update completeness
UA = update accuracy

See Exhibit SM-9.2 for a complete explanation of control plans and cell entries.

FIGURE SM-9.8 Problem 2 Part g Solution (Partial)—Control Matrix for ePetID Company

Exhibit SM-9.2 Problem 9-2 Part g Solution (Partial)—Explanation of Cell Entries

Notes:

1. The columns for update completeness and update accuracy are shaded and not used in Figure SM-9.8 because the update of the sales order master data occurs simultaneously with the input and acceptance of the customer order. Therefore, the input controls will be sufficient to ensure update completeness and update accuracy.
2. Several controls could be added to this analysis, including preformatted screens and online prompting.

Discussion and Explanation of Recommended Control Plans

P-1: *Review order for accuracy.*

Effectiveness goals A and B (timeliness): By reviewing the customer order early in the order entry process, we preclude delays that will occur when incorrect orders are entered into the computer, rejected, and must be corrected and reentered.

Efficient employment of resources: It will take less time to review and correct the orders now than to do so later in the process.

Customer order input accuracy: By reviewing the orders before they are entered into the computer, we reduce the possibility that errors will go undetected later in the process and improve the chances of correct data entry.

P-2: *Enter customer orders close to their originating source.*

Effectiveness goals A and B (timeliness), efficient employment of resources: Customer mail orders are entered into the computer in the sales order department rather than being sent to a separate data entry department for input. In addition, the direct entry of input data by sales personnel provides for a more timely process and efficient employment of resources because they will be more familiar with orders and customers and able to input, edit, and correct orders more quickly.

Customer order input completeness: Because the customer orders are captured upon arrival in the organization, they are less likely to be lost as they are transported to the data entry location.

Customer order input accuracy: Because sales personnel are familiar with the type of data being entered, they are less likely to make input errors and can correct these errors immediately if they occur.

P-3: *Populate input screens with master data.*

Effectiveness goals A and B (timeliness), efficient employment of resources: When the sales order clerk enters the customer's number, the computer retrieves

standing data from the customer master file. Because the clerk does not have to key all this data, there are fewer keystrokes, which improves the speed and productivity of the sales clerks.

Security of resources and customer order input validity: The code entered by the sales clerk calls up the existing customer record, which establishes authorization for the sales event. Selling to an existing, authorized customer reduces the possibility of shipping inventory and not being paid for it.

Customer order input accuracy: Fewer keystrokes means less chance for input errors. By using existing *standing data*, data that has previously been entered and validated, we reduce input errors.

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

Effectiveness goals A and B (timeliness), efficient employment of resources, customer order input accuracy: Sales orders can be processed on a timelier basis and at a lower cost if errors, such as entering the wrong customer number, are detected and prevented from entering the system in the first place.

Security of resources and customer order input validity: By comparing the customer order to the customer data, the clerk ensures that the order is from a valid, authorized customer. Selling to an existing, authorized customer reduces the possibility of shipping inventory and not being paid for it.

P-5: *Procedures for rejected inputs.Customer order input completeness, customer order input accuracy:* The rejection procedures (i.e., "Error routine not shown" annotations) are designed to ensure that erroneous data not accepted for processing are corrected (*accuracy*) and resubmitted for processing (*completeness*).

P-6: *Programmed edit checks.*

Effectiveness goals A and B (timeliness), efficient employment of resources: The computer would detect erroneous data, and the clerk can take corrective action ("Error routine not shown") immediately, for a more timely input process. Furthermore, the customer order can be processed on a timelier basis and at lower cost if errors are detected and prevented from entering the system in the first place.

Security of resources, customer order input validity, customer order input accuracy: Should a discrepancy arise between the entered data and the customer or inventory master data, the order entry process would not continue, thus ensuring that ePetID does not create an incorrect order (e.g., inventory items numbers are incorrect or quantities are unreasonable—*accuracy*), an order for a bogus customer, a customer with inadequate credit (*validity*), and so on, so that ePetID does not ship goods to a bogus customer (*security*).

P-7: *Confirm input acceptance.*

Customer order input completeness: By flashing a message on the screen telling the sales clerk that the customer order has been *accepted* and *recorded*, the computer informs the user of acceptance of the order.

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

Customer order input validity, customer order input completeness, customer order input accuracy: Mail orders are received in the sales order department, where a clerk opens the mail and checks the orders for accuracy. Because orders are processed in groups, we have an opportunity to exercise certain batch-oriented control plans, such as calculating batch totals and later agreeing those totals with similar totals of the customer orders accepted by the computer. However, such batch totaling procedures are *not* performed in this system. Dollar totals or hash totals (i.e., totals of customer numbers, totals of inventory ID numbers, and the like) help to preclude invalid orders from being added to a batch (*validity*), orders being entered more than once (*completeness*), orders being lost from a batch (*completeness*), or orders being changed (*accuracy*), either accidentally or intentionally. On the other hand, document/record counts and/or item/line counts would ensure input completeness *only.*

P 9-3 ANS.

System Failure	Control Plan	Notes
1	B	
2	G	
3	D	This is better than reviewing the detail in the list as they are doing at present.
4	H	*J* is another possible answer if that is not chosen for number 3.
5	F	A batch sequence check (*A*) will not work in this situation because three sets of voucher numbers are used by the three divisions.
6	C	*E* would ask the operator to review the input to determine if quantities were greater than normal (but *E* is used for number 7), and *G* (which is used for number 2) would ensure that the PO was reviewed before being sent.
7	E	This could also be *C* (programmed edit checks—reasonableness test), but this is used for number 6.
8	K	Could also be document design (*H*), if that is not chosen for number 4.
9	I	
10	L	

P 9-4 ANS.

1.	D	6.	K
2.	C	7.	B
3.	E	8.	G
4.	L	9.	I
5.	H	10.	A

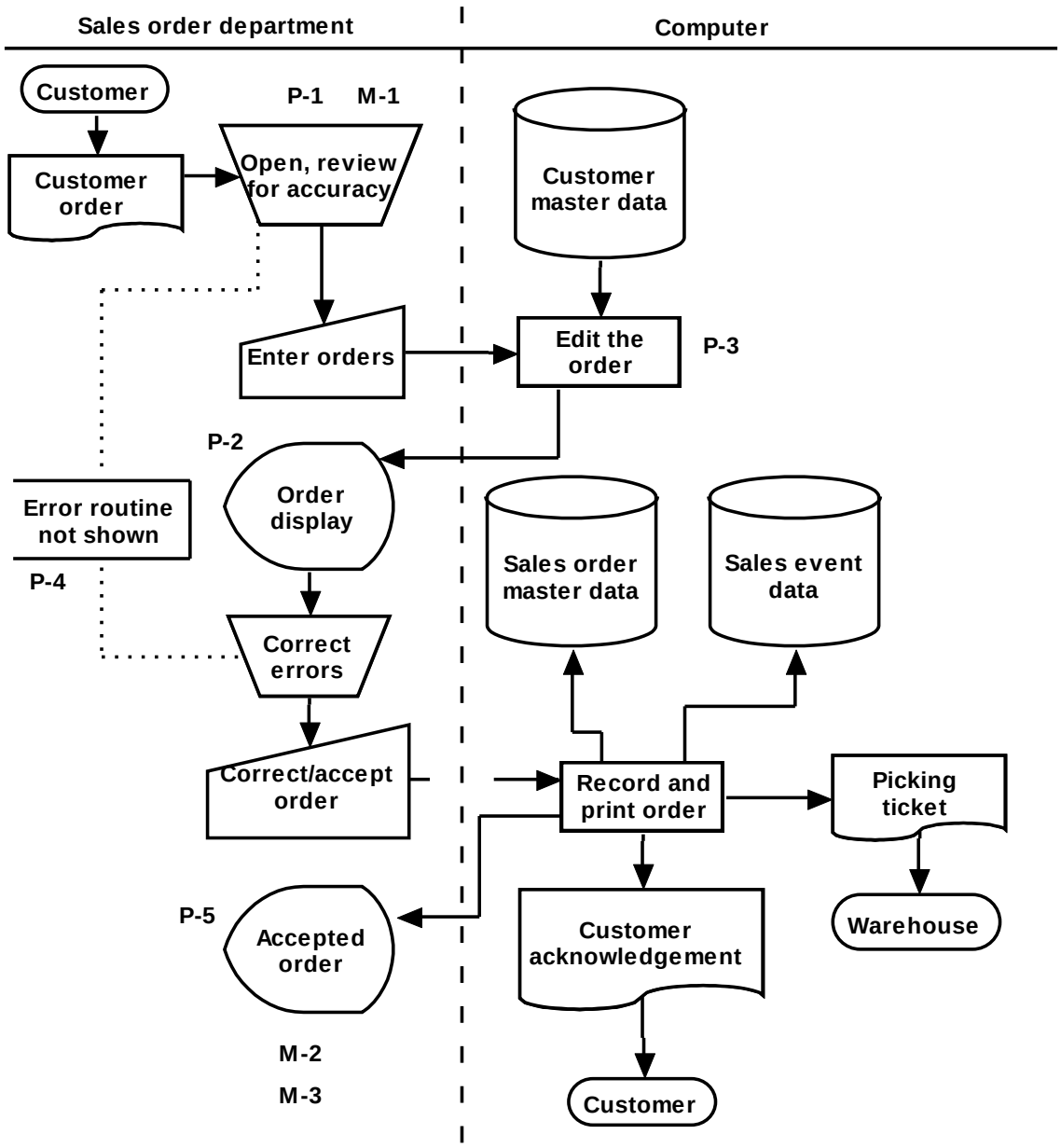


FIGURE SM-9.9 Problem 5 Part a Solution—Annotated Systems Flowchart

	Control Goals of the Order Entry Business Process								
	Control Goals of the Operations Process				Control Goals of the Information Process				
	Ensure effectiveness of operations:		Ensure efficient employment of resources (people, computers)	Ensure security of resources Inventory, customer master data)	For the sales order inputs (i.e., customer order) - ensure:			For the sales order master data, ensure:	
Recommended control plans	**A**	**B**			**IV**	**IC**	**IA**	**UC**	**UA**
Present Controls									
P-1: Review document for accuracy	P-1	P-1					P-1		
P-2: Preformatted screens	P-2	P-2	P-2				P-2		
P-3: Programmed edit checks	P-3	P-3	P-3		P-3		P-3		
P-4: Procedures for rejected input						P-4			
P-5: Confirm input acceptance						P-5			
Missing Controls									
M-1: Enter data close to the location where the customer order is prepared	M-1	M-1	M-1			M-1	M-1		
M-2: Manual reconciliation of batch totals				M-2	M-2	M-2	M-2		
M-3: Computer agreement of batch totals	M-3	M-3	M-3	M-3	M-3	M-3	M-3		

Possible effectiveness goals include the following:
A – Provide timely acknowledgement of customer orders.
B – Provide timely shipment of goods to customers.

See Exhibit SM-9.5 for a complete explanation of control plans and cell entries.

IV = input validity
IC = input completeness
IA = input accuracy
UC = update completeness
UA = update accuracy

FIGURE SM-9.10 Problem 5 Part b Solution—Control Matrix for Figure SM 9.9

Exhibit SM-9.5 Problem 9-5 Part c Solution—Explanation of Cell Entries

Discussion and Explanation of Recommended Control Plans for Figure SM 9.10

P-1: *Review document for accuracy.*

Effectiveness goals A and B: By reviewing and correcting errors on the document before input, the clerk should make the subsequent processes quicker.

Customer order input accuracy: By correcting errors on the document before input, the clerk should increase the accuracy of the input data.

P-2: *Preformatted screens.*

Effectiveness goals A and B, and efficient employment of resources: By structuring the data entry process, automatically populating fields, and preventing errors, preformatted screens simplify data input and save time (*Effectiveness goals A and B*), allowing a user to input more data over a period of time (*efficiency*).

Customer order 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.

Note: P-2 could also be "Online prompting." The same control goals apply but with a slightly different description.

P-3: *Programmed edit checks.*

Effectiveness goals A and B, and efficient employment of resources: Event data can be processed on a timelier basis (*Effectiveness goals A and B*) and at a lower cost if errors are detected and prevented from entering the system in the first place (*efficiency*). It will be more time consuming and costly to detect and correct errors after the fact.

Customer order input validity: The programmed edits appear to include a matching of the order with the records in the customer master data table. The matching will confirm the existence of the customer and that there was a prior approval to do business with the customer—both measures of the validity of the customer order.

Customer order input accuracy: The edits identify erroneous or suspect data and reduce input errors.

Note: Students will not be able to describe the input validity described previously until after covering the controls in Chapter 10.

P-4: *Procedures for rejected inputs.*

Customer order input completeness: The rejection procedures (i.e., "Error routine not shown" annotations) are designed to ensure that erroneous data not accepted for processing are corrected and resubmitted for processing.

P-5: *Confirm input acceptance.*

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

M-1: *Enter data close to the location where the customer order is prepared.*

Effectiveness goals A and B, and 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 the events more quickly.

Customer order input completeness: Because the inputs are captured at the source, they are less likely to be lost as they are transported to the data entry location.

Customer order input accuracy: Because operations personnel are familiar with the type of event being entered, they are less likely to make input errors and can more readily correct these errors if they occur.

M-2: *Manual reconciliation of batch totals.*

Security of resources: Agreement of the batch totals at this point would ensure that only valid source documents have been input and that invalid picking tickets have not been sent to the warehouse, leading to inappropriate shipments of inventory.

Customer order input validity, customer order input completeness, customer order input accuracy: Agreement of the batch totals at this point would ensure that only valid source documents comprising the original batch have been input (*input validity*), that all source documents were input once and only once (*input completeness*), and that data elements appearing on the source documents have been input correctly (*input accuracy*).

M-3: *Computer agreement of batch totals.*

Effectiveness goals A and B, 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.

Security of resources: Reconciliations can discover anomalies thus preventing additional losses. When the reconciliation is computer-based, it should be quicker than a manual reconciliation, providing improved security of resources.

Customer order input validity, customer order input completeness, customer order input accuracy: Regarding these control goals, the effect of this control is the same as M-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.

P 9-6 ANS. The two types of business process controls in Figure 9.5 (and analyzed in the control matrix in Figure 9.6 and Exhibit 9.4) are manual and automated (i.e., application) controls. The effectiveness of these controls can depend on the operation of several controls described in Chapter 8. In this summary we examine some of those relationships.

Manual Controls

Five *controls* in Figure 9.6 depend, somewhat, on the ability, training, and diligence of the shipping personnel. First, *Manually reconcile batch totals* will only be effective if the shipping clerk correctly prepares and then reconciles the input batch totals and rejects input batches for which the totals do not agree. Second, when the shipping clerk *Agrees run-to-run totals (reconcile input and output batch totals)*, we expect that the shipping clerk will perform this task correctly and will reject batches for which the totals do not agree. Third, the shipping clerk *Reviews the tickler file (file of pending shipments)* to ensure that all packing slips arrive from the computer. We expect that the shipping clerk will perform this task correctly and will follow up on open shipments when a packing slip does not arrive in a timely manner. Fourth, the clerk performs a *One-for-one checking (compare picking tickets and packing slips)* to ensure that the two documents agree and that the goods will be shipped to the correct customer. Fifth, while not explicitly noted, the clerk will need to complete *Procedures for rejected inputs* at each location that there is an "Error routine not shown." The clerk must know how to correct each error and follow through to re-input the corrected documents.

What controls in Chapter 8 will improve the effectiveness of these manual controls? We can give several examples. The organization should employ *selection and hiring* controls to ensure the hiring of quality personnel. All personnel, including shipping clerks, should receive relevant *training and education* to make sure that they *can* perform their required functions and *performance evaluations* to determine that they *do* perform their required functions as required. Finally, shipping clerks must be provided with *application documentation* explaining how to perform their required functions.

Automated Controls

All of the controls that are performed by the computer system (i.e., application controls) depend on the general controls (also known as IT general controls or ITGCs) in Chapter 8. Several controls not mentioned in this analysis that might be included here include *Compare inputs with master data* and *Programmed edits* at

the point that shipments are recorded. Also, we would look for controls in the scanning devices used to record the picking tickets to ensure accurate capture and recording of the picking ticket data. How do we know that these controls and the other automated controls are working as planned? First, we need to know that the programs will perform the controls as designed. Second, we need to know that the stored data used by the computer when executing these controls is valid and accurate. We can ask such questions as "Is the stored customer record used to validate an input a valid record or has it been added by an unauthorized person?" and "Is the scanning device working correctly?"

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