

Systems Design, Implementation, and Operation

Learning Objectives

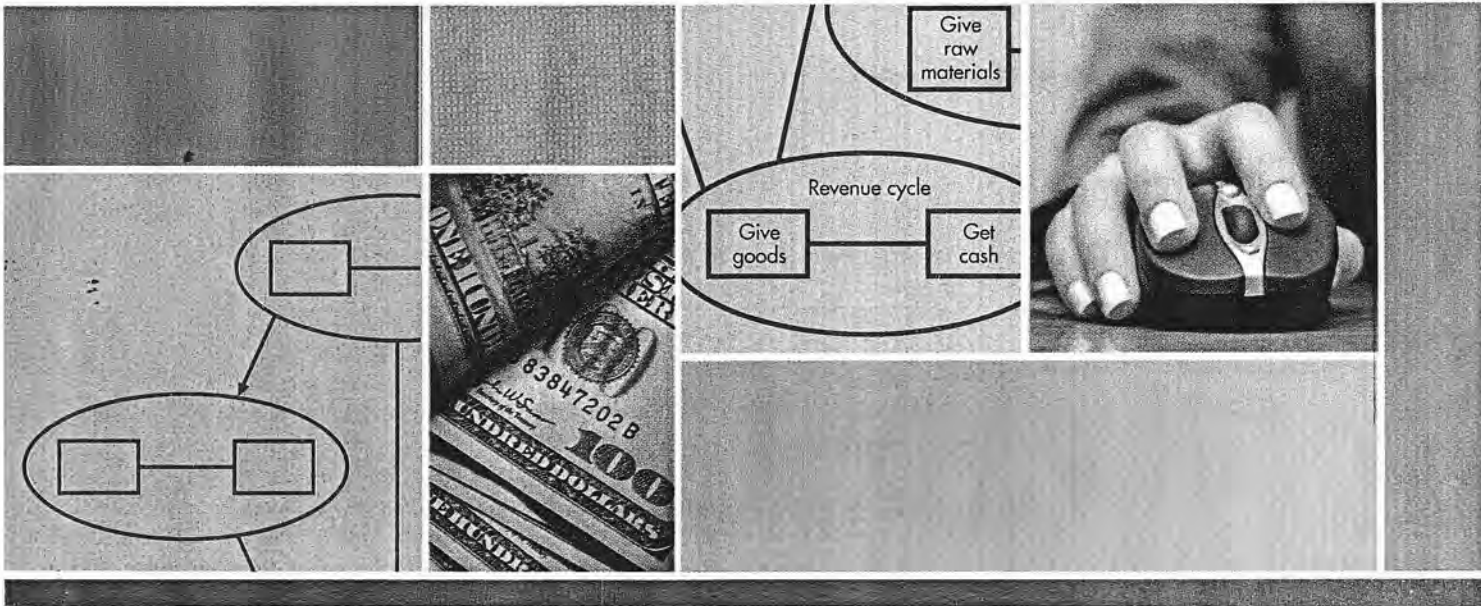
After studying this chapter, you should be able to:

1. Discuss the conceptual systems design process and the activities in this phase.
2. Discuss the physical systems design process and the activities in this phase.
3. Discuss the systems implementation and conversion process and the activities in this phase.
4. Discuss the systems operation and maintenance process and the activities in this phase.

INTEGRATIVE CASE SHOPPERS MART

Ann Christy received permission to develop a new AIS (Chapter 20 conclusion) for Shoppers Mart (SM). Ann is concerned because many development projects bog down during the design and implementation phases, and she does not want a runaway project that she cannot control. She wants to plan the rest of the project so that it is completed correctly, and her first task is to determine what type of system will best meet SM's needs. She scheduled a meeting with the head of systems development to discuss the following questions:

1. Should her team develop what it considers the best approach to meeting SM's needs, or should they develop several approaches?
2. How can she ensure that system output will meet user needs? When and how should input be captured, and who should capture it? Where should AIS data be stored, and how should it be organized and accessed?
3. How should SM convert from its current to its new AIS? How much time and effort will be needed to maintain the new AIS? In what capacity should Ann's accounting staff participate?



Introduction

Effective systems analysis and design can help developers correctly define business problems and create a system to solve those problems. As discussed in Chapter 20, system requirements are defined during systems analysis. This chapter discusses the other four systems development life cycle (SDLC) steps (see Figure 20-1): conceptual systems design, physical systems design, systems implementation and conversion, and operation and maintenance. Chapter 21 discusses how some SDLC steps can be shortened or made more effective.

Conceptual Systems Design

In *conceptual systems design*, the developer creates a general framework for implementing user requirements and solving the problems identified in the analysis phase. Figure 22-1 shows the conceptual design steps: evaluating design alternatives, preparing design specifications, and preparing the conceptual systems design report.

Evaluate Design Alternatives

There are many ways to design an AIS, so systems designers must make many design decisions. For example, should SM mail hard-copy purchase orders, use electronic data interchange (EDI), or enter orders over the Internet? Should SM have a large centralized mainframe and database or distribute computer power to the stores using a network of servers and PCs? Should data entry be by keyboard, optical character recognition, point-of-sale devices, barcodes, radio-frequency identification (RFID) tags, the Internet, or some combination?

There are many ways SM can approach the systems development process. It can purchase software, ask in-house information systems (IS) staff to develop it, or hire an outside company to develop and manage the system. The company could modify existing software or redesign its business processes and develop software to support the new processes. These conceptual design alternatives are discussed in Chapter 21.

The following standards should be used to evaluate design alternatives: (1) how well it meets organizational and system objectives, (2) how well it meets user needs, (3) whether it is economically feasible, and (4) how advantages weigh against disadvantages. The steering committee evaluates the alternatives and selects the one that best meets the organization's needs.

Table 22-1 summarizes design considerations and alternatives.

FIGURE 22-1
Conceptual Systems
Design Activities

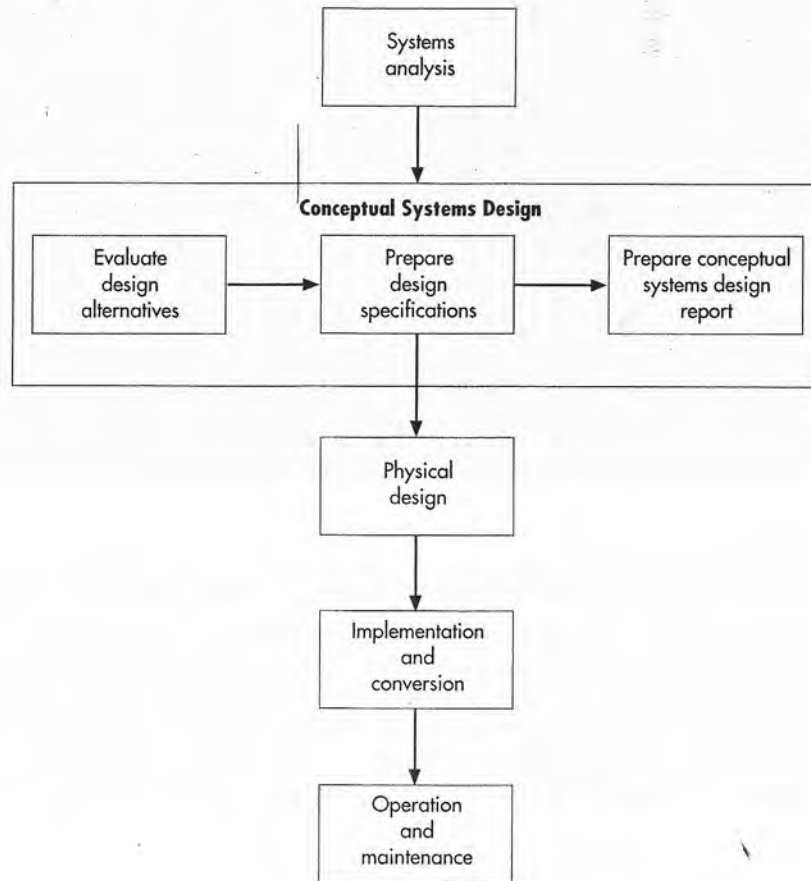


TABLE 22-1 Design Considerations and Alternatives

Design Considerations	Design Alternatives
Communications channels	Telephone, Internet, cable, fiber optics, or satellite
Communications network	Centralized, decentralized, distributed, or local area
Data storage medium	Tape, disk, hard drive, CD, or paper
Data storage structure	Files or database
File organization and access	Random, sequential, or indexed-sequential access
Input medium	Keying, optical character recognition (OCR), magnetic ink character recognition (MICR), point-of-sale (POS), EDI, or voice
Input format	Source document, turnaround document, source data automation, or screen
Operations	In-house or outsourcing
Output and update frequency	Instantaneous, hourly, daily, weekly, or monthly
Output medium	Paper, screen, voice, CD, or microfilm
Output scheduling	Predetermined times or on demand
Output format	Narrative, table, graph, file, or electronic
Printed output format	Preprinted forms or system-generated forms
Processing mode	Manual, batch, or real time
Processor	Personal computer, server, or mainframe
Software acquisition	Canned, custom, or modified
Transaction processing	Batch or online

Prepare Design Specifications and Reports

Once a design alternative is selected, *conceptual design specifications* are created for the following elements:

1. **Output.** Because the system is designed to meet user information needs, output specifications are prepared first. To evaluate store sales, SM must decide (a) how often to produce a sales analysis report, (b) what the report should contain, (c) what it will look like, and (d) whether it is a hard-copy or screen (or both) output.
2. **Data storage.** Data storage decisions include which data elements must be stored to produce the sales report, how they should be stored, and what type of file or database to use.
3. **Input.** Input design considerations include which sales data to enter, sale location and amount, and where, when, and how to collect the data.
4. **Processing procedures and operations.** Design considerations include how to process the input and stored data to produce the sales report, and in which sequence the processes must be performed.

A *conceptual systems design report* summarizes conceptual design activities, guides physical design activities, communicates how all information needs will be met, and helps the steering committee assess feasibility. The main component is a description of one or more recommended system designs. Table 22-8, in the chapter summary, shows what this report contains.

Physical Systems Design

During *physical systems design*, the broad, user-oriented AIS requirements of conceptual design are translated into detailed specifications that are used to code and test the computer programs. Figure 22-2 shows the physical system design phases that are described below in detail.

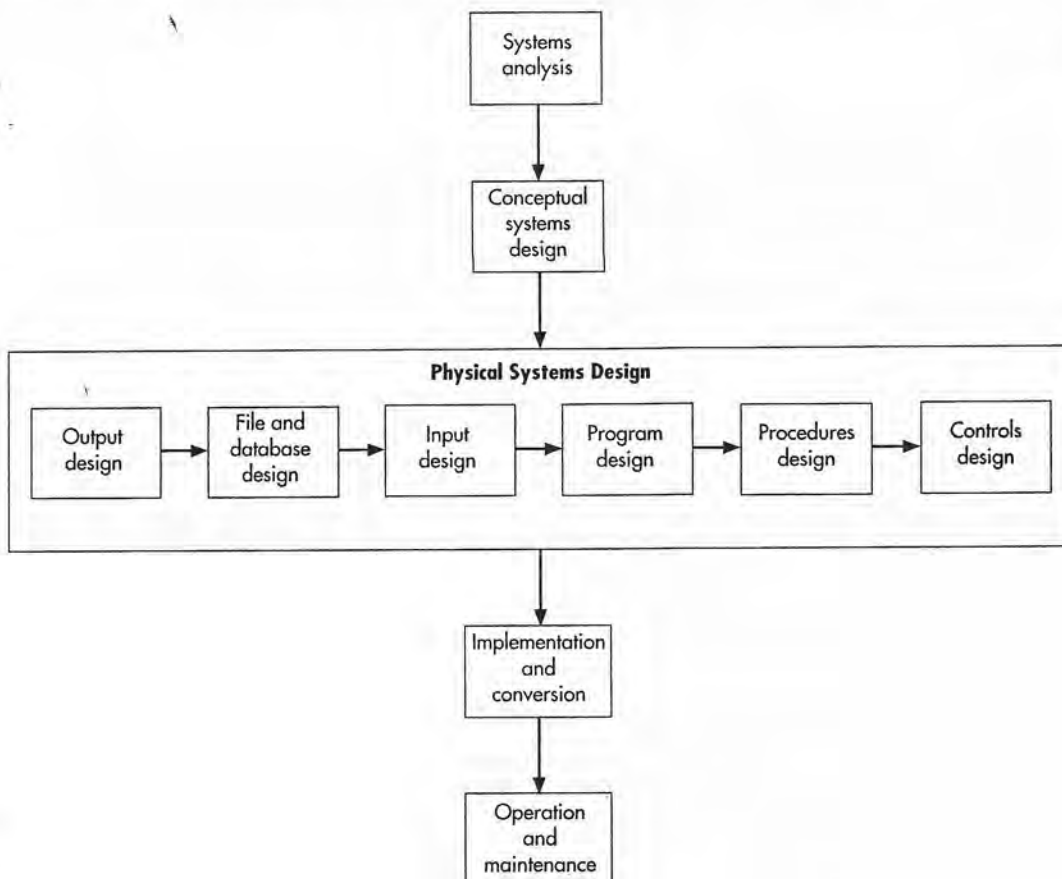


FIGURE 22-2
Physical Systems
Design Activities

Failing to take sufficient time on conceptual and physical design can cause problems. A rush to implement an enterprise resource planning (ERP) package at Overstock.com caused early design problems. The result was a mistake-laden Oracle implementation. The ERP package was out-of-sync with the accounting software, causing the order tracking system to go down for a week. Ultimately, five years of earnings had to be restated, with revenue reduced by \$12.9 million and increased losses of \$10.3 million.

Output Design

The objective of output design is to determine the nature, format, content, and timing of reports, documents, and screen displays. Tailoring the output to user needs requires cooperation between users and designers. Important output design considerations are summarized in Table 22-2.

Output usually fits into one of the following four categories:

1. *Scheduled reports* have a prespecified content and format and are prepared on a regular basis. Examples include monthly performance reports, weekly sales analyses, and annual financial statements.
2. *Special-purpose analysis reports* have no prespecified content or format and are not prepared on a regular schedule. They are prepared in response to a management request to evaluate an issue, such as which of three new products would provide the highest profits.
3. *Triggered exception reports* have a prespecified content and format but are prepared only in response to abnormal conditions. Excessive absenteeism, cost overruns, inventory shortages, and situations requiring immediate corrective action trigger such reports.
4. *Demand reports* have a prespecified content and format but are prepared only on request. Both triggered exception reports and demand reports can be used effectively to facilitate the management process.

Designers often prepare sample outputs and ask users to evaluate whether they are complete, relevant, and useful. Unacceptable output is modified and reviewed again as many times as necessary to make it acceptable. To avoid expensive time delays later in the SDLC, many organizations require users to sign a document stating that the output form and content are acceptable.

File and Database Design

Data in various company units should be stored in compatible formats to help avoid the problem AT&T faced: 23 business units, a jumble of incompatible systems and data formats, and an inability to communicate and share data with other units. AT&T spent five years creating a “single view” of each customer so customer data could be shared across business units.

Chapter 4 discusses files and databases and how to design them. Important file and database design considerations are summarized in Table 22-3.

TABLE 22-2 Output Design Considerations

Consideration	Concern
Use	Who will use the output, why and when do users need it, and what decisions will they make based on it?
Medium	Use paper, screen, voice, e-mail, or some combination?
Format	Will narrative, table, or graphic format best convey information?
Preprinted	Use preprinted forms? Turnaround documents?
Location	Where should output be sent?
Access	Who should have access to hard-copy and screen output?
Detail	Should a summary or table of contents be included with lengthy output? Should headings organize data and highlight important items? Should detailed information be placed in an appendix?
Timeliness	How often should output be produced?

TABLE 22-3 File and Database Design Considerations

Consideration	Concern
Medium	Store data on hard drive, disk, CD, tape, or paper?
Processing mode	Use manual, batch, or real-time processing?
Maintenance	What procedures are needed to maintain data effectively?
Size	How many records will be stored in the database, how large will they be, and how fast will the number of records grow?
Activity level	What percentage of the records will be updated, added, or deleted each year?

Input Design

Input design considerations include what types of data will be input and the optimal input method. Considerations for input design are shown in Table 22-4.

FORM DESIGN Although systems are moving away from paper documents and toward source data automation, forms design is still an important topic. Forms design principles are summarized in Table 22-5.

COMPUTER SCREEN DESIGN It is more efficient to enter data directly into the computer than onto paper for subsequent entry. Computer input screens are most effective when these procedures are followed:

- Organize the screen so data can be entered quickly, accurately, and completely. Minimize data input by retrieving as much data as possible from the system. For example, entering a customer number could cause the system to retrieve the customer's name, address, and other key information.
- Enter data in the same order as displayed on paper forms that capture the data.
- Group logically related data together. Complete the screen from left to right and top to bottom.
- Design the screen so users can jump from one data entry location to another or use a single key to go directly to screen locations.
- Make it easy to correct mistakes. Clear and explicit error messages that are consistent across all screens are essential. There should be a help feature to provide online assistance.
- Restrict the data or the number of menu options on a screen to avoid clutter.

Program Design

Program development, one of the most time-consuming SDLC activities, takes place in the eight steps shown below. Step 1 is part of the systems analysis phase. Step 2 begins in

TABLE 22-4 Input Design Considerations

Consideration	Concern
Medium	Enter data using a keyboard, OCR, MICR, POS terminal, barcodes, RFID tags, EDI, or voice input?
Source	Where do data originate (computer, customer, remote location, etc.), and how does that affect data entry?
Format	What format (source or turnaround document, screen, source data automation) efficiently captures the data with the least effort and cost?
Type	What is the nature of the data?
Volume	How much data are to be entered?
Personnel	What are data entry operators' abilities, functions, and expertise? Is additional training necessary?
Frequency	How often must data be entered?
Cost	How can costs be minimized without adversely affecting efficiency and accuracy?
Error detection and correction	What errors are possible, and how can they be detected and corrected?

TABLE 22-5 Principles of Good Forms Design**General Considerations**

- Are preprinted data used as much as possible?
- Are the weight and grade of the paper appropriate for the planned use?
- Do bold type, lines, and shading highlight different parts of the form?
- Is the form a standard size?
- Is the form size consistent with filing, binding, or mailing requirements?
- If the form is mailed, will the address show in a window envelope?
- Are copies printed in different colors to facilitate proper distribution?
- Do clear instructions explain how to complete the form?

Introduction

- Does the form name appear at the top in bold type?
- Is the form consecutively prenumbered?
- Is the company name and address preprinted on forms sent to external parties?

Main Body

- Is logically related information (e.g., customer name, address) grouped together?
- Is there sufficient room to record each data item?
- Is data entry consistent with the sequence the data is acquired?
- Are codes or check-offs that are used instead of written entries adequately explained?

Conclusion

- Is space provided to record the final disposition of the form?
- Is space provided for a signature(s) to indicate transaction approval?
- Is space provided to record the approval date?
- Is space provided for a dollar or numeric total?
- Is the distribution of each copy of the form clearly indicated?

conceptual systems design and may carry over to physical design. Most of steps 3 and 4 are done during systems design and are completed during systems implementation. Steps 5 and 6 are begun in systems design, but most of the work is done during systems implementation. Step 7 is done during systems implementation and conversion. Step 8 is part of operation and maintenance.

1. **Determine user needs.** Systems analysts consult with users and reach an agreement on user needs and software requirements.
2. **Create and document a development plan.**
3. **Write program instructions (computer code).** Program preparation time may range from a few days to a few years, depending on program complexity. Programming standards (rules for writing programs) contribute to program consistency, making them easier to read and maintain. Computer programs should be subdivided into small, well-defined modules to reduce complexity and enhance reliability and modifiability, a process called *structured programming*. Modules should interact with a control module rather than with each other. To facilitate testing and modification, each module should have only one entry and exit point.
4. **Test the program.** *Debugging* is the process of discovering and eliminating program errors. A program is tested for logic errors using test data that simulate as many real processing situations and input data combinations as possible. Large programs are often tested in three stages: individual program modules, the linkages between modules and a control module, and interfaces with other application programs.

It is important to find errors as soon as possible during the development process. The Gartner Group estimates that bugs discovered later in the SDLC cost 80% to 1,000% more to fix than those discovered earlier. Focus 22-1 discusses the difficulty of testing software and the consequences of releasing software with undetected errors. Between 20% and 30% of software development costs should be allocated to testing, debugging, and rewriting software.


FOCUS
22-1

Software Bugs Take Their Toll

An \$18.5 million rocket explodes seconds after liftoff. Because of three missing digits in several million lines of programming code, telephone networks crash, leaving 10 million customers without service. A nuclear plant releases hundreds of gallons of radioactive water near Lake Huron. A device that uses X-rays to treat cancer victims delivered a radiation overdose, killing one patient and leaving two others deeply burned and partly paralyzed. A software error prevents a Patriot missile from destroying an incoming Iraqi Scud missile that kills 28 people.

These events have one disturbing fact in common. They were caused by program errors called bugs. The term *bug* was coined during World War II when a researcher, puzzled by a computer shutdown, removed a moth stuck between two electric relays. A program containing bugs can work adequately for quite some time until, with no warning, the bug triggers something, and the computer goes haywire. One incorrect letter—even a missing period—can cause a computer to issue an incorrect command or no command at all.

Bugs exist in most software, and it is almost impossible to eliminate all of them. The sheer volume of software code in a complex program makes finding bugs difficult. There are over 2.5 million lines of code in systems that check for cracks in the engine wheel of the space shuttle and 12 million in a phone company's call-switching computer. Finding a flaw in

this code is as difficult as looking for one misspelled name in the New York City phone book. It is estimated that flawed or bug-ridden software cost businesses worldwide over \$175 billion last year.

Programmers go to great pains to detect and eliminate bugs, but no one has the time or money to find every bug or to simulate every situation the program will encounter in the real world. Instead, software is tested with assumptions about how it will be used and what processing volumes it must handle.

One product manager estimated that his company often found 5,000 bugs in each product. They fixed serious flaws and ignored minor flaws that were unlikely to cause a problem. If developers took the time to find and correct every flaw, they would risk not getting their product to market on a timely basis and losing market share.

Software developers also cannot predict whether computer users will work faster than the software itself. The linear accelerators that killed and maimed cancer patients were controlled by an operator who typed extremely fast. She accidentally selected the X-ray mode and then switched to the electron beam. The software was not quick enough to recognize the change, and the machine beamed radiation at full power to a tiny spot on the patients' bodies. The bug was so subtle it took programmers a year to detect and eliminate it.

5. **Document the program.** Documentation explains how programs work and is used to correct errors. Program documentation includes flowcharts, data flow diagrams, E-R diagrams, data models, record layouts, and narrative descriptions. These items are stored in a documentation manual.
6. **Train program users.** Program documentation is often used to train users.
7. **Install the system.** All system components, including the programs and the hardware, are combined, and the company begins to use the system.
8. **Use and modify the system.** Factors that require existing programs to be revised, referred to as *program maintenance*, include requests for new or revised reports; changes in input, file content, or values such as tax rates; error detection; and conversion to new hardware.

Procedures and Controls Design

Everyone who interacts with a system needs procedures that answer the who, what, when, where, why, and how questions related to IS activities. Procedures should cover input preparation, transaction processing, error detection and correction, controls, reconciliation of balances, database access, output preparation and distribution, and computer operator instructions. Procedures documentation and training may take the form of system manuals, user instruction classes, training materials, or online help screens. Developers, users, or teams representing both groups may write procedures.

The adage "garbage in, garbage out" emphasizes that improperly controlled input, processing, and data storage functions produce unreliable information. Controls must be built into an AIS to ensure its effectiveness, efficiency, and accuracy. They should minimize errors as well as detect and correct them when they occur. Accountants play a vital role in this area. Important control concerns are summarized in Table 22-6. Controls are discussed in detail in Chapters 7 through 11.

TABLE 22-6 Controls Design Considerations

Consideration	Concern
Validity	Are system interactions valid (e.g., all cash disbursements are made to legitimate vendors)?
Authorization	Are input, processing, storage, and output activities authorized by the appropriate managers?
Accuracy	Is input verified to ensure accuracy? Are data processed and stored accurately?
Security	Is the system protected against (a) unauthorized physical and logical access to prevent the improper use, alteration, destruction, or disclosure of information and software and (b) the theft of system resources?
Numerical control	Are documents prenumbered to prevent errors and fraud and to detect when documents are misused, missing, or stolen?
Availability	Is the system available at times set forth in service-level agreements? Can users enter, update, and retrieve data during the agreed-upon times?
Maintainability	Can the system be modified without affecting system availability, security, and integrity? Are only authorized, tested, and documented changes made? Are resources available to manage, schedule, document, and communicate the changes?
Integrity	Is data processing complete, accurate, timely, and authorized? Is data processing free from unauthorized or inadvertent system manipulation?
Audit trail	Can transactions be traced from source documents to final output?

Failing to produce good policies and procedures and failing to implement controls can be devastating. Nonexistent governance kept Kaiser Kidney Transplant Center from developing good policies and procedures. As a result, hundreds of patients did not receive life-saving transplant surgeries, and the transplant center was forced to close two years after opening. Inadequate controls at Heartland Payment Systems, a credit card processor, allowed hackers to steal sensitive information from more than 100 million credit card accounts.

A *physical systems design report* summarizes what was accomplished and serves as the basis for management's decision whether or not to proceed to the implementation phase. Table 22-8 shows a table of contents for the report prepared at Shoppers Mart.

Systems Implementation

Systems implementation is the process of installing hardware and software and getting the AIS up and running. Implementation processes are shown in Figure 22-3 and described below. Focus 22-2 describes the improvements the state of Virginia made to its AIS.

Implementation Planning and Site Preparation

An *implementation plan* consists of implementation tasks, expected completion dates, cost estimates, and who is responsible for each task. The plan specifies when the project should be complete and when the AIS is operational. The implementation team identifies factors that decrease the likelihood of successful implementation, and the plan contains a strategy for coping with each factor.

AIS changes may require adjustments to a company's existing organizational structure. New departments may be created, existing ones may be eliminated or downsized, or the IS department itself may change. Technical staff at Blue Cross and Blue Shield of Wisconsin who did not understand the company's business or vision contracted for a \$200 million system that did not work properly. It sent checks to a nonexistent town, made \$60 million in overpayments, and resulted in the loss of 35,000 clients. One reason the system failed was that its implementation should have included an organizational restructuring.

Site preparation is a lengthy process and should begin well in advance of the installation date. A large computer may require extensive changes, such as additional electrical outlets, data communications facilities, raised floors, humidity controls, special lighting, air conditioning, fire protection, and an emergency power supply. Space is needed for equipment, storage, and offices.

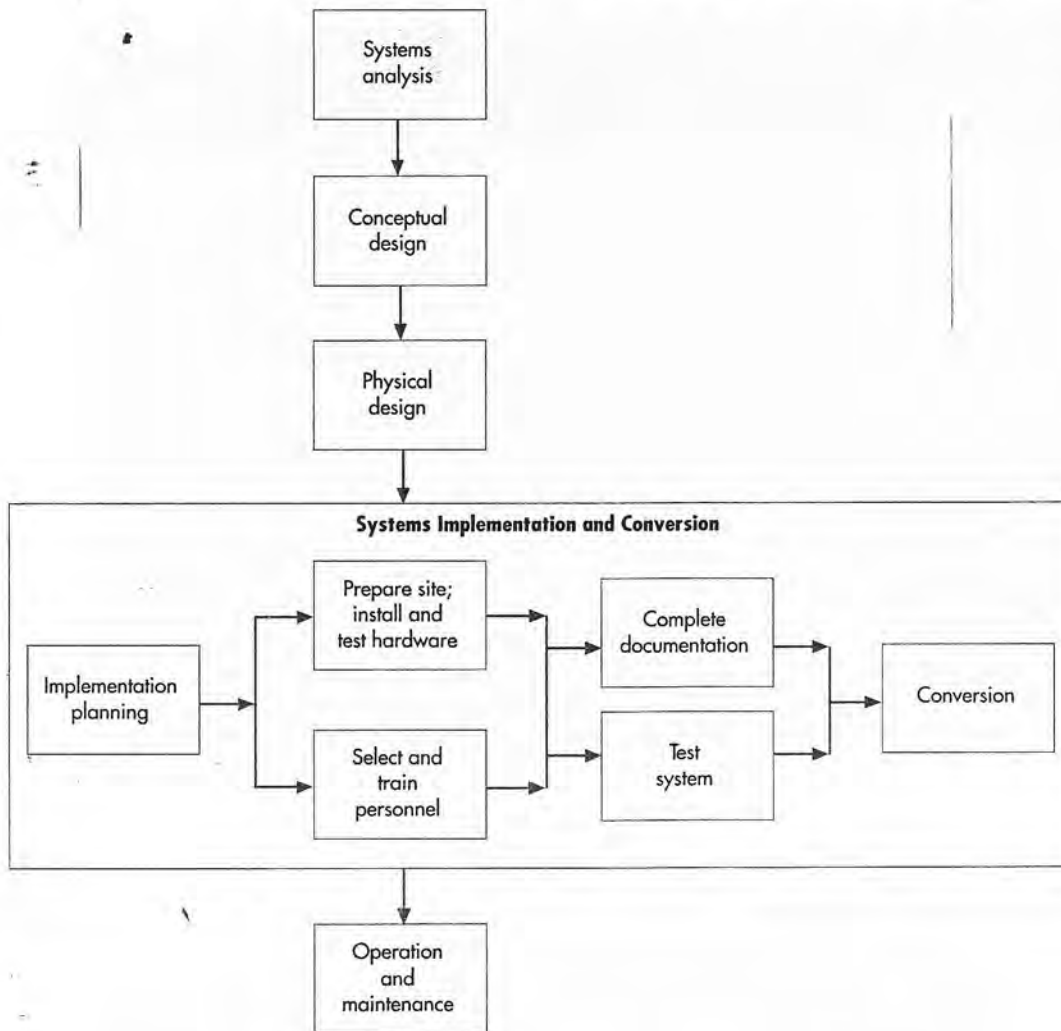


FIGURE 22-3
Systems
Implementation
Activities

Selecting and Training Personnel

Employees are hired from outside the company or transferred internally, which often is the less costly alternative because they already understand the firm's business and operations. Transferring employees who are displaced because of the new system could boost employee loyalty and morale.

When users are not adequately trained, the company will not achieve the expected benefits and return on its investment. Companies provide insufficient training because it is time-consuming and expensive. The hidden cost of inadequate training is that users turn for help to coworkers who have mastered the system, decreasing the productivity of coworkers and increasing company costs.

Employees must be trained on the hardware, software, and any new policies and procedures. Training should be scheduled for just before systems testing and conversion. Many training options are available, such as vendor training, self-study manuals, computer-assisted instruction, videotape presentations, role-playing, case studies, and experimenting with the system under the guidance of experienced users.

Boots the Chemists, a British pharmacy chain with over 1,000 stores, developed a novel approach to training employees nervous about a forthcoming system. They were invited to a party at a store where a new POS system had been installed. They were invited to try to harm the system by pushing the wrong buttons or fouling up a transaction. Employees quickly found they could not harm the system and that it was easy to use.


FOCUS
22-2

STARS Saves Virginia \$80 Million

Most Virginia taxpayers receive tax refunds within a week of filing instead of the usual two to three months thanks to Jane Bailey, director of AIS at the Department of Taxation. Bailey managed the development of the State Tax Accounting and Reporting System (STARS), a multisystem project that took nine years to complete. STARS was so successful that the IRS, 27 states, and a Canadian province sent teams to Richmond to see whether STARS could improve their systems development and implementation efforts.

The state's IT group had strongly recommended outside contractors for the job, saying Bailey's six-person staff was far too small and unsophisticated to overhaul the state's disjointed manual and batch systems. Bailey insisted on going with an inside job. She was able to convince management by stating that she would maintain the system and respond quickly to tax law changes.

Bailey insisted on hiring first-rate people, and her staff eventually swelled to 45 employees. If she could not hire the experts and specialists she needed, she retained them as

consultants and used them to train her staff. She recruited five management analysts to redesign business processes, write user documentation, and train users. Ten people from her staff are management analysts who work full-time on user procedures and issues. Seeing user involvement as crucial, Bailey succeeded in getting six managers from user areas assigned full-time to the project.

Over the years, STARS expanded to encompass more functions and more users, and its budget climbed from \$3 million to \$11 million. A new piece of software was installed every three to six months. Users had to adapt, often getting 15 new screens at a time. The megaproject eventually involved putting together 1,500 programs, 40 IBM databases, and 350 online screens in 25 applications for 1,800 users.

The state asked for a Chevrolet and got a Cadillac; the payoff has been impressive. STARS users estimate that it saved the state \$80 million over five years, most of it from added collections from would-be tax cheats.

Complete Documentation

Three types of documentation must be prepared for new systems:

1. **Development documentation** describes the new AIS. It includes a system description; copies of output, input, and file and database layouts; program flowcharts; test results; and user acceptance forms.
2. **Operations documentation** includes operating schedules; files and databases accessed; and equipment, security, and file-retention requirements.
3. **User documentation** teaches users how to operate the AIS. It includes a procedures manual and training materials.

Testing the System

Inadequate system testing was another reason for the Blue Cross and Blue Shield system failure. The developers underestimated system complexity and promised an unrealistic delivery time of 18 months. One shortcut they took to meet the deadline was to deliver an untested system. Documents and reports, user input, controls, operating and processing procedures, capacity limits, recovery procedures, and computer programs should all be tested in realistic circumstances. Following are three common forms of testing:

1. **Walk-throughs** are step-by-step reviews of procedures or program logic to find incorrect logic, errors, omissions, or other problems. The development team and system users attend walk-throughs early in system design. The focus is on the input, files, outputs, and data flows of the organization. Subsequent walk-throughs, attended by programmers, address logical and structural aspects of program code.
2. **Processing test data**, including all valid transactions and all possible error conditions, is performed to determine whether a program operates as designed; that is, valid transactions are handled properly and errors are detected and dealt with appropriately. To evaluate test results, the correct system response for each test transaction must be specified in advance.
3. **Acceptance tests** use copies of real transactions and files rather than hypothetical ones. Users develop the acceptance criteria and make the final decision whether to accept the AIS.

Chemical Bank did not adequately test an ATM upgrade, and customers who withdrew cash had their accounts debited twice. Over 150,000 withdrawals with a total value of \$8 million were posted twice. Thousands of small accounts were overdrawn or emptied, which annoyed and angered customers. Chemical Bank lost a great deal of customer credibility because of the glitch.

Even software purchased from an outside vendor must be tested thoroughly before being installed. As soon as Kane Carpets installed an AIS custom tailored to the floor-covering industry, its inventory control system told salespeople that orders could not be filled when the product was available, and vice versa. As a result, Kane lost many of its customers.

Systems Conversion

Conversion is changing from the old to the new AIS. Many elements must be converted: hardware, software, data files, and procedures. The process is complete when the new AIS is a routine, ongoing part of the system. Four conversion approaches are used:

- **Direct conversion** terminates the old AIS when the new one is introduced. For example, Shoppers Mart could discontinue its old system on Saturday night and use its new AIS on Monday morning. Direct conversion is appropriate when a new system is so different that comparisons between the two are meaningless. The approach is inexpensive, but it provides no backup AIS. Unless a system has been carefully developed and tested, direct conversion carries a high risk of failure. Focus 22-3 discusses the problems at an Egyptian University, caused in part by attempting a direct conversion.
- **Parallel conversion** operates the old and new systems simultaneously for a period. For example, Shoppers Mart could process transactions with both systems, compare the output, reconcile the differences, correct problems, and discontinue the old system after the new system proves itself. Parallel processing protects companies from errors, but it is costly and stressful to process transactions twice. Because companies often experience problems during conversion, parallel processing has gained widespread popularity.

FOCUS 22-3

Dangers of Direct Conversion to an ERP SAP Implementation

In 2004, a not-for-profit university in Egypt that follows the American accreditation system decided to upgrade its aging financial system by implementing an advanced integrated financial system. The project steering committee (ST) selected the SAP finance module. Egypt's IBM branch was selected as the implementer. The ST was made up of representatives from IBM, the university's finance department, the university IT unit, and senior administrators. The SAP project was viewed by the top administrators as a business project, being directly linked to the finance operations. The end users thus had a key role in deciding the project outcomes, being the stakeholders in accepting or rejecting the new SAP operational processes. The ST considered two alternative conversion approaches to the new system: direct or parallel conversion. The finance end users adamantly supported direct conversion against the recommendation of the senior administrators, the IT unit, and IBM representatives.

Despite the opposition, the direct approach prevailed. The IT unit and IBM representatives warned that thorough and meticulous testing plans, using synthetic and/or historical

data, should be developed before the conversion. However, these warnings were not heeded because of time and cost pressures. As a consequence, the old system was plugged off, and transactions subsequent to the kick-off date were to be posted to the new system.

The university experienced serious problems from day one of the conversion. A defective process workflow led to transaction entry errors to the General Ledger, Accounts Payable, and Accounts Receivable modules, and missing financial reporting forced the university to revert to manual operation. With no rollback plan to the old system, financial reporting and payroll had to be prepared hastily using Excel spreadsheets. After spending more than \$20 million on the system, the university had to bring in another implementer to fix the dysfunctional finance system. A new steering committee was formed, with more power given to the IT organization to challenge any flawed technical decisions.

This case highlights how strategic decisions can determine the success or failure of the implementation process. It also highlights the need for testing before conversion.

- *Phase-in conversion* gradually replaces elements of the old AIS with the new one. For example, Shoppers Mart could implement its inventory system, then disbursements, then sales collection, and so forth, until the whole system is functional. Gradual changes allow data processing resources to be acquired over time. The disadvantages are the cost of creating the temporary interfaces between the old and the new AIS and the time required to make the gradual changeover.
- *Pilot conversion* implements a system in one part of the organization, such as a branch location. For example, Shoppers Mart could install its new POS system at one of its stores using a direct, parallel, or phase-in approach. When problems with the system are resolved, the new system could be implemented at the remaining locations. This localizes conversion problems and allows training in a live environment. The disadvantages are the long conversion time and the need for interfaces between the old and the new systems, which coexist until all locations have been converted. Owens-Corning Fiberglass implemented its accounts payable, travel expense, and payroll systems by getting the system up and running in one plant and then moving it to all the others.

Data conversion can be time-consuming, tedious, and expensive; its difficulty and magnitude are easily underestimated. Data files may need to be modified in three ways. First, files may be moved to a different storage medium—for example, from tapes to disks. Second, data content may be changed—for example, fields and records may be added or deleted. Third, file or database format may be changed.

The first step in data conversion is to decide which data files need to be converted. Then the data are checked for completeness and errors, and inconsistencies are removed. Following data conversion, the new files are validated to ensure data were not lost during conversion. If data conversion is lengthy, the new files must be updated with the transactions that occurred during data conversion. Once the files and databases have been converted and tested for accuracy, the new system is functional. The system should be monitored for a time to make sure it runs smoothly and accurately. The final activity is to document the conversion activities.

Operation and Maintenance

The final SDLC step is to operate and maintain the new system. A *post-implementation review* is conducted to determine whether the system meets its planned objectives. Important review considerations are listed in Table 22-7. Problems uncovered during the review are brought to

TABLE 22-7 Factors to Investigate During Post-Implementation Review

Factors	Questions
Goals and objectives	Does the system help the organization meet its goals, objectives, and overall mission?
Satisfaction	Are users satisfied? What would they like changed or improved?
Benefits	How have users benefited? Were the expected benefits achieved?
Costs	Are actual costs in line with expected costs?
Reliability	Is the system reliable? Has it failed? If so, what caused its failure?
Accuracy	Does the system produce accurate and complete data?
Timeliness	Does the system produce information on a timely basis?
Compatibility	Are hardware, software, data, and procedures compatible with existing systems?
Controls and security	Is the system safeguarded against errors, fraud, and intrusion?
Errors	Do adequate error-handling procedures exist?
Training	Are systems personnel and users trained to support and use the system?
Communications	Is the communications system adequate?
Organizational changes	Are organizational changes beneficial or harmful? If harmful, how can they be resolved?
Documentation	Is system documentation complete and accurate?

TABLE 22-8 Table of Contents for Shoppers Mart Reports

Conceptual Systems Design Report	Physical Systems Design Report	Postimplementation Review Report
Table of Contents	Table of Contents	Table of Contents
I. Executive Summary of Conceptual Systems Design II. Overview of Project Purpose and Summary of Findings to Date III. Recommended Conceptual Design(s) A. Overview of Recommended Design(s) B. Objectives to Be Achieved by Design(s) C. Impact of Design(s) on Information System and Organization D. Expected Costs and Benefits of Design(s) E. Audit, Control, and Security Processes and Procedures F. Hardware, Software, and Other Resource Requirements G. Processing Flows: Relationships of Programs, Databases, Inputs, and Outputs H. Description of System Components (Programs, Databases, Inputs, and Outputs) IV. Assumptions and Unresolved Problems V. Summary VI. Appendixes, Glossary	I. Executive Summary of Physical Systems Design II. Overview of Project Purpose and Summary of Findings to Date III. Physical Design Recommendations A. Output Design B. Input Design C. Database Design D. Software Design E. Hardware Design F. Controls Design G. Procedures Design IV. Assumptions and Unresolved Problems V. Summary VI. Appendixes, Glossary	I. Executive Summary of Postimplementation Review II. Overview of Development Project III. Evaluation of the Development A. Degree to Which System Objectives Were Met B. Analysis of Actual Versus Expected Costs and Benefits C. User Reactions and Satisfaction IV. Evaluation of Project Development Team V. Recommendations A. Recommendations for Improving the New System B. Recommendations for Improving the System Development Process VI. Summary

management's attention, and the necessary adjustments are made. Table 22-8 illustrates what the *post-implementation review report* should contain. User acceptance of the report is the final activity in the systems development process.

Control of the AIS is passed to the data processing department, but work on the new system is not finished. Over the life of a typical system, 30% of the work takes place during development, and 70% is spent on software modifications and updates. At Hartford Insurance Group, 70% of its personnel resources are devoted to maintaining an inventory of 34,000 program modules containing 24 million lines of code. The job is even more difficult because changes in insurance regulations and business strategies reduced the structure of the code and increased its complexity.

Summary and Case Conclusion

Ann Christy tackles the sales processing system first. She gives the project development team her systems analysis report and accompanying data. During conceptual systems design, the team visits stores with similar operations and identifies ways to meet AIS requirements. Alternative approaches are discussed with users, management, and the steering committee. They are narrowed down to Ann's original approach. Ann has considered buying software but does not find a package that accomplishes what she and the company want. The team develops conceptual design specifications for the output, input, processing, and data storage elements.

The company decides to use screen-based output and to capture data electronically using point-of-sale (POS) devices. Data that cannot be captured electronically will be entered using PCs. Each store will have a network that connects its PCs and POS devices to a local database. The POS cash registers will capture and feed sales data electronically to this database. Each store will be linked to the central office using a wide area network. All sales data, store orders, and other summary-level information will be uploaded to the corporate database daily. The corporate database will download the information needed to manage the store. The central office will use electronic data interchange to order goods and pay suppliers.

During physical design, the development team designs each report identified during conceptual design. Users and designers rework the reports until everyone is satisfied. The team

designs all files, databases, and input screens. Then they design the software programs that collect and process data and produce the output. The team develops new procedures for handling data and operating the AIS. The accountants and the internal audit staff are especially helpful during the design of the controls needed to protect the system against errors and fraud.

Implementation planning starts early. A location for the new mainframe is identified, and site preparation begins during the design phase. The hardware and software are installed and tested and then the entire AIS is tested. The new AIS is staffed with existing employees that are trained as the system is tested. System documentation is completed before data from the old AIS are converted to the new one.

For the corporate system, the new and old systems are operated in parallel for a month, and the results compared. The bugs are ironed out, and the old AIS is discontinued. For the store systems, a pilot approach is used. The AIS is installed at three stores, and all problems are resolved before the system is implemented at the remaining stores. Conversion requires a fair amount of overtime and duplicate processing. After a few months, Ann and her staff conduct a post-implementation review and make some adjustments to enhance the high user acceptance of the new AIS.

Ann makes a final presentation to top management after the AIS is installed and operating. She is widely congratulated and even hears the president mention that she "is worth keeping an eye on" for even more responsibility in the firm. Table 22-8 is a summary of the contents of the conceptual, physical, and post-implementation reports.

Key Terms

conceptual systems design 661	demand report 664	acceptance test 670
conceptual design specifications 663	structured programming 666	conversion 671
conceptual systems design report 663	debugging 666	direct conversion 671
physical systems design 663	program maintenance 667	parallel conversion 671
scheduled report 664	physical systems design report 668	phase-in conversion 672
special-purpose analysis report 664	systems implementation 668	pilot conversion 672
triggered exception report 664	implementation plan 668	post-implementation review 672
	walk-through 670	post-implementation review report 673
	processing test data 670	

AIS IN ACTION

Chapter Quiz

- The developers of your new system have proposed two different AIS designs and have asked you to evaluate them. This evaluation process is most likely to be a part of which SDLC step?
 - systems analysis
 - conceptual design
 - physical design
 - implementation and conversion
 - operation and maintenance
- What is the purpose of the conceptual systems design report?
 - to guide physical systems design activities
 - to communicate how management and user information needs are met
 - to help the steering committee assess system feasibility
 - a and b
 - a, b, and c

3. Which of the following is the correct order of the steps in physical systems design?
 - a. input, file and database, output, controls, procedures, program
 - b. file and database, output, input, procedures, program, controls
 - c. output, input, file and database, procedures, program, controls
 - d. output, file and database, input, program, procedures, controls
4. A monthly payroll register showing all hourly employees, the number of hours they worked, their deductions, and their net pay is most likely which of the following?
 - a. scheduled report
 - b. special-purpose analysis
 - c. triggered exception report
 - d. demand report
5. Which of the following is NOT a consideration in input design?
 - a. Which errors are possible, and how can they be detected and corrected?
 - b. How can data be entered (keyboards, OCR, or POS terminal)?
 - c. Which format efficiently captures the input data with the least effort and cost?
 - d. How often should the system produce reports?
6. Which of the following is most likely to help improve program development?
 - a. physical model
 - b. IT strategic plan
 - c. walk-through
 - d. record layout
7. Which of the following statements is true?
 - a. The Gartner Group estimates that programming bugs not found until later in the SDLC cost 25% to 30% more to correct than if they had been found earlier in the SDLC.
 - b. Direct system conversion is the least risky of the system conversion methods.
 - c. Many software developers state that 5% to 10% of software development costs should be allocated to testing, debugging, and rewriting software.
 - d. Over the life of a system, only 30% of information systems work takes place during development; the remaining 70% is spent maintaining the system.
8. Which of the following describes the systems testing approach that uses real transactions and files rather than hypothetical ones?
 - a. walk-through
 - b. processing of test transactions
 - c. acceptance test
 - d. parallel conversion test
9. What is the process of discontinuing an old system as soon as a new one is introduced?
 - a. direct conversion
 - b. parallel conversion
 - c. phase-in conversion
 - d. pilot conversion
10. Which of the following describes designing a program from the top down to more detailed levels?
 - a. hierarchical program design
 - b. top-down program design
 - c. parallel program design
 - d. unstructured program design

Case 22-1 Hershey's Big Bang ERP

Halloween is the biggest candy season of them all, with \$1.8 billion in sales. For Hershey's, Halloween 1999 was the scariest of all time. Hershey's had planned to implement a \$112 million ERP system in 48 months. Instead, it was implemented in an accelerated 30-month time frame. Hershey's "flipped the switch" in July 1999, right during its busiest ordering season. Issues with inventory and ordering processes promptly gummed up the order-distribution system. By August 1999, Hershey's was 15 days behind in shipping orders. Many distributors who placed orders in September were still waiting for their shipment at Halloween. Hershey had plenty of candy in inventory; it just could not move the candy from its

warehouses to its customers. The implementation problem contributed to a 19% drop in revenue. It took a full year for the company to bounce back.

The new ERP system employed over 5,000 PCs, network hubs, and servers. The ERP software was supplied by three firms and implemented by a large consulting firm. Despite the system's size and complexity, Hershey chose to implement most of it in one step called the "big bang."

Required

What could Hershey have done to properly design, implement, and operate this new ERP?

Discussion Questions

- 22.1. Prism Glass is converting to a new information system. To expedite and speed up implementation, the CEO asked your consulting team to postpone establishing standards and controls until after the system is fully operational. How should you respond to the CEO's request?
- 22.2. When a company converts from one system to another, many areas within the organization are affected. Explain how conversion to a new system will affect the following groups, both individually and collectively.
- Personnel
 - Data storage
 - Operations
 - Policies and procedures
 - Physical facilities
- 22.3. The following notice was posted in the employee cafeteria on Monday morning:
- To: All Accounting and Clerical Employees*
From: I.M. Krewel, President
Subject: Termination of Employee Positions
- Effective this Friday, all accounting and clerical employees not otherwise contacted will be terminated. Our new computer system eliminates the need for most of these jobs. We're grateful for the loyal service you've rendered as employees and wish you success. You may wish to pick up your final checks on Friday before you go.*
- Discuss the president's approach to human resource management. What are the possible repercussions of this episode? Assuming that job termination is the best alternative available, how should management approach the situation?
- 22.4. In which phase of the systems development cycle would each of the following positions be most actively involved? Justify your answers.
- Managerial accountant
 - Programmer
 - Systems analyst
 - Financial vice president
 - Information systems manager
 - Internal auditor
- 22.5. During which of the five SDLC stages is each task, labeled (a) through (m), performed? More than one answer may apply for each activity.
- | | |
|--|---|
| — 1. Systems analysis | a. Writing operating procedures manuals |
| — 2. Conceptual (general) systems design | b. Developing program and process controls |
| — 3. Physical (detailed) systems design | c. Identifying alternative systems designs |
| — 4. Implementation and conversion | d. Developing a logical model of the system |
| — 5. Operation and maintenance | e. Identifying external and administrative controls |
| | f. Testing the system |
| | g. Training personnel |
| | h. Evaluating the existing system |

- i. Analyzing the achievement of systems benefits
- j. Modifying and altering programs
- k. Analyzing total quality management (TQM) performance measures
- l. Conducting a feasibility analysis
- m. Aligning AIS development plans with business objectives

Problems

22.1. You were hired to manage the accounting and control functions at the Glass Jewelry Company. During your introductory meeting, the president asked you to design and implement a new AIS within six months. Company sales for the past year were \$10 million, and they are expected to double in the next 18 months.

Required

- a. Outline the procedures you would follow to complete the assigned project. Include a description of the following:
 - 1. Sources of information
 - 2. Methods of documenting information collected
 - 3. Methods of verifying the information collected
- b. The accounts payable system will contain a number of programs, including Enter Invoices and Print Payable Checks. For each program, describe its purpose, and outline application control considerations. (*SMAC Examination, adapted*)

22.2. Wang Lab's tremendous growth left the company with a serious problem. Customers would often wait months for Wang to fill orders and process invoices. Repeated attempts by Wang's understaffed IS department to solve these problems met with failure. Finally, Wang hired a consulting firm to solve its revenue tracking problems and expedite prompt receipt of payments. The 18-month project turned into a doubly long nightmare. After three years and \$10 million, the consultants were dismissed from the unfinished project.

The project failed for many reasons. The systems development process was so dynamic that the failure to complete the project quickly became self-defeating as modifications took over the original design. Second, management did not have a clear vision of the new AIS and lacked a strong support staff. As a result, a number of incompatible tracking systems sprang from the company's distributed computer system. Third, the project was too large and complex for the consulting firm, who had little experience with the complex database at the heart of the new system. Finally, the project had too many applications. Interdependencies among subprograms left consultants with few completed programs. Every program was linked to several subprograms, which in turn were linked to several other programs. Programmers eventually found themselves lost in a morass of subroutines with no completed program.

The IS department finally developed a system to solve the problem, but their revenue tracking system suffered quality problems for years.

Required

Wang asked you to write a memo explaining the failure of the systems development project.

- a. Why did the development project fail? What role did the consultants play in the failure?
- b. Identify the organizational issues that management must address in the future.
- c. Recommend steps the company could take to guarantee consulting service quality.

22.3. Tiny Toddlers, a manufacturer of children's toys and furniture, is designing and implementing a distributed system to assist its sales force. Each of the 10 sales offices in Canada and 20 in the United States maintains its own customers and is responsible for granting credit and collecting receivables. Reports used by each sales office to maintain the customer master file and to enter the daily sales orders are shown in Figures 22-4 and 22-5.

Required

Evaluate the reports shown in Figures 22-4 and 22-5 using the following format:

Weakness	Explanation	Recommendation(s)
		(SMAC Examination, adapted)

22.4. Mickie Louderman is the new assistant controller of Pickens Publishers. She was the controller of a company in a similar industry, where she was in charge of accounting and had considerable influence over computer center operations. Pickens wants to revamp its information system, placing increased emphasis on decentralized data access and online systems. John Richards, the controller, is near retirement. He has put Mickie in charge of developing a new system that integrates the company's accounting-related functions. Her promotion to controller will depend on the success of the new AIS.

Mickie uses the same design characteristics and reporting format she used at her former company. She sends details of the new AIS to the departments that interface with accounting, including inventory control, purchasing, human resources, production control, and marketing. If they do not respond with suggestions by a prescribed date, she will continue the development process. Mickie and John have established a new schedule for many of the reports, changing the frequency from weekly to monthly. After a meeting with the director of IS, Mickie selects a programmer to help her with the details of the new reporting formats.

Most control features of the old system are maintained to decrease the installation time, with a few new ones added for unusual situations. The procedures for maintaining the controls are substantially changed. Mickie makes all the AIS control change and program-testing decisions, including screening the control features related to payroll, inventory control, accounts receivable, cash deposits, and accounts payable.

FIGURE 22-4
Customer Maintenance Form for Tiny Toddlers

CUSTOMER MAINTENANCE FORM	
New Customer?	<input type="checkbox"/> Yes _____ <input checked="" type="checkbox"/> No 24671
Name	The Little Ones Furniture Store
New Address	5 St. Antoine Street N. Quebec City
Old Address	305 St. Antoine Street S. Quebec City
Salesperson #	02
Requested Credit Limit	50,000
Sales Office	Eastern Canada
Pricing Code	25
Estimated Sales	300,000
Credit Limit	10,000
Currency	U.S.A. <input type="checkbox"/> , Canada <input type="checkbox"/>
Bank	Canadian Credit Bank 50 St. Antoine Street Quebec City
Bank Line	
Rating	Satisfactory
_____ Sales Manager	
_____ Credit Manager	

SALES ORDER FORM			
Customer: 24671 The Little Ones Furniture Store 5 St. Antoine Street N. Quebec City		Date: _____	
Product Code	Description		Quantity
24571	Crib		4
M0002	Mattress		102
HG730	High chair—white		32
HG223	High chair—natural wood		22
CT200	Changing table		300
D0025	Desk—modern design		2
C9925	Chair—modern design		5
BP809	Bumper pads		1200
Salesperson No.: _____			
Entered by: _____			

FIGURE 22-5
Sales Order Form for Tiny Toddlers

As each module is completed, Mickie has the corresponding department implement the change immediately to take advantage of the labor savings. Incomplete instructions accompany these changes, and specific implementation responsibility is not assigned to departmental personnel. Mickie believes operations people should learn as they go, reporting errors as they occur.

Accounts payable and inventory control are implemented first, and several problems arise. The semimonthly payroll runs, which had been weekly under the old system, have abundant errors, requiring numerous manual paychecks. Payroll run control totals take hours to reconcile with the computer printout. To expedite matters, Mickie authorizes the payroll clerk to prepare payroll journal entries.

The new inventory control system fails to improve the carrying level of many stock items. This causes critical stock outs of raw material that result in expensive rush orders. The new system's primary control procedure is the availability of ordering and user information. The information is available to both inventory control and purchasing personnel so that both departments can issue timely purchase orders. Because the inventory levels are updated daily, Mickie discontinues the previous weekly report.

Because of these problems, system documentation is behind schedule, and proper backup procedures have not been implemented. Mickie has requested budget approval to hire two systems analysts, an accountant, and an administrative assistant to help her implement the new system. John is disturbed by her request because her predecessor had only one part-time assistant.

Required

- List the steps Mickie should have taken while designing the AIS to ensure that end-user needs were satisfied.
- Identify and describe three ways Mickie violated internal control principles during the AIS implementation.
- Identify and describe the weaknesses in Mickie's approach to implementing the new AIS. How could you improve the development process for the remaining parts of the AIS?
(CMA Examination, adapted)

22.5. Ryon Pulsipher, manager of Columbia's property accounting division, has had difficulty responding to the following departmental requests for information about fixed assets.

- The controller has requested individual fixed assets schedules to support the general ledger balance. Although Ryon has furnished the information, it is late. The way the records are organized makes it difficult to obtain information easily.

2. The maintenance manager wants to verify the existence of a punch press that he thinks was repaired twice. He has asked Ryon to confirm the asset number and the location of the press.
3. The insurance department wants data on the cost and book values of assets to include in its review of current insurance coverage.
4. The tax department has requested data to determine whether Columbia should switch depreciation methods for tax purposes.
5. The internal auditors have spent significant time in the property accounting division to confirm the annual depreciation expense.

Ryon's property account records, kept in an Excel spreadsheet, show the asset acquisition date, its account number, the dollar amount capitalized, and its estimated useful life for depreciation purposes. After many frustrations, Ryon realizes his records are inadequate and that he cannot supply data easily when requested. He discusses his problems with the controller, Gig Griffith.

RYON: Gig, something has to give. My people are working overtime and can't keep up. You worked in property accounting before you became controller. You know I can't tell the tax, insurance, and maintenance people everything they need to know from my records. Internal auditing is living in my area, and that slows down the work. The requests of these people are reasonable, and we should be able to answer their questions and provide the needed data. I think we need an automated property accounting system. I want to talk with the AIS people to see if they can help me.

GIG: I think that's a great idea. Just be sure you are personally involved in the design of any system so you get all the info you need. Keep me posted on the project's progress.

Required

- a. Identify and justify four major objectives Columbia's automated property accounting system should possess to respond to departmental requests for information.
 - b. Identify the data that should be included in the database for each asset. (*CMA Examination, adapted*)
- 22.6. A credit union is developing a new AIS. The internal auditors suggest planning the systems development process in accordance with the SDLC concept. The following nine items are identified as major systems development activities that will have to be completed.
1. System test
 2. User specifications
 3. Conversion
 4. Systems survey
 5. Technical specifications
 6. Post-implementation planning
 7. Implementation planning
 8. User procedures and training
 9. Programming

Required

- a. Arrange the nine items in the sequence in which they should logically occur.
 - b. One major activity is to convert data files from the old system to the new one. List three types of file conversion documentation that would be of particular interest to an auditor. (*CMA Examination, adapted*)
- 22.7. MetLife, an insurance company, spent \$11 billion to acquire Travelers Life and Annuity from Citicorp in one of the largest insurance company acquisitions of all time. The Metlife CIO estimated it would take three years to integrate the two systems. Because the integration project was especially critical, he figured he could



accomplish the integration in 18 months if he pulled out all the stops. The MetLife CEO gave him nine months to complete the task. To pull off the integration in nine months, he had to:

- Integrate over 600 IS applications, all with their own infrastructure and business processes. The new systems had to comply with “One MetLife,” a company policy that all information systems had to have a common look and feel companywide and be able to function seamlessly with other MetLife systems.
- Work with over 4,000 employees located in 88 offices scattered all over the globe.
- Supervise an oversight team and 50 integration teams in seven project management offices.
- Work with hostile, uncooperative Travelers employees for the six months it took to get regulatory approval and close the deal. The systems had to be integrated three months after the deal closed.
- Identify integration deliverables (144 in total) and manage the process to deliver them.
- Negotiate with Citicorp for hundreds of transition services that would not be immediately converted to MetLife’s systems

Required

- a. What tasks would MetLife have to perform to integrate the Traveler systems into MetLife’s?
- b. Search the Internet for articles that describe the integration process. Write a two-page summary of the problems and successes that MetLife experienced while integrating the two systems.

22.8. During final testing, just before launching a new payroll system, the project manager at Reutzel Legal Services found that the purchased payroll system was doing the following:

- Writing checks for negative amounts
- Printing checks with names and employee numbers that did not match
- Making errors; for example, \$8 per hour became \$800 per hour if a decimal point was not entered
- Writing checks for amounts greater than a full year’s salary

Fortunately, payroll was still installed on time, and only 1.5% of the checks had to be manually reissued every payday until the problem was solved.

Other problems were that no one had made sure the new system was compatible with the existing payroll database, and there appeared to be no formal transition between the development of the project and the implementation of the project. The system was never run in parallel.

Although the programming manager lost his job, the payroll problems helped raise awareness of the company’s growing dependence on IT. Lacking a major problem, there was a perception that the information system did not affect operations.

Required

- a. What does “the system was never run in parallel” mean?
- b. If the company had run the system in parallel, what should have occurred?
- c. What other testing methodologies could have been used by the firm?
- d. What other types of problems are evident from reading the case?

22.9. A new program at Jones and Carter Corporation (JCC) was supposed to track customer calls. Unfortunately, the program took 20 minutes to load on a PC, and it crashed frequently. The project did not have a traditional reporting structure, and it appeared that no one was actually in charge. The lead project manager quit halfway through the

project, the in-house programmers were reassigned to other projects or let go, and two layers of management loosely supervised the systems analyst.

Management hired consultants to fix the application, but after three months and \$200,000, the project was discontinued. JCC did not check the references of the consulting firm it hired to create the new system. The consultants, who were located two states away, made many programming errors. Although the systems analyst caught some of the consultant's mistakes, they grew increasingly distant and difficult to work with. They would not even furnish the source code to the project managers, most likely because they were afraid of revealing their incompetence.

Required

- Identify potential causes for the system implementation failure.
- What steps should JCC have taken to successfully design and implement the call tracking system?

Case 22-2 Citizen's Gas Company

Citizen's Gas Company (CGC) provides natural gas service to 200,000 customers. The customer base is divided into the following three revenue classes:

Class	Customers	Sales in Cubic Feet	Revenues
Residential	160,000	80 billion	\$160 million
Commercial	38,000	15 billion	\$ 25 million
Industrial	2,000	50 billion	\$ 65 million
Totals		145 billion	\$250 million

Residential customer gas usage is highly correlated with the weather. Commercial customer usage is partially weather dependent. Industrial customer usage is governed almost entirely by business factors.

The company buys natural gas from 10 pipeline companies in the amounts specified in contracts that run for 5 to 15 years. For some contracts, the supply is in equal monthly increments; for other contracts, the supply varies according to the heating season. Supply over the contract amounts is not available, and some contracts contain take-or-pay clauses. That is, the company must pay for the gas volume specified in the contract, regardless of the amount used.

To match customer demand with supply, gas is pumped into a storage field when supply exceeds customer demand. Gas is withdrawn when demand exceeds supply. There are no restrictions on the gas storage field except that the field must be full at the beginning of each gas year (September 1). Consequently, when the contractual supply for the remainder of the gas year is less than that required to satisfy projected demand and fill the storage field, CGC curtails

service to industrial customers (except for heating quantities). The curtailments must be carefully controlled to prevent either an oversupply at year-end or a curtailing of commercial or residential customers so the storage field can be filled at year-end.

In recent years, CGC's planning efforts have not been able to control the supply during the gas year or provide the information needed to establish long-term contracts. Customer demand has been projected only as a function of the total number of customers. Commercial and industrial customers' demand for gas has been curtailed. This has resulted in lost sales and caused an excess of supply at the end of the gas year.

To correct the problems, CGC has hired a director of corporate planning. She is presented with a conceptual design for an information system that will help analyze gas supply and demand. The system will provide a monthly gas plan for the next five years, with particular emphasis on the first year. The plan will provide detailed reports that assist in the decision-making process. The system will use actual data during the year to project demand for the year. The president has indicated that she will base her decisions on the effect alternative plans have on operating income.

Required

- Discuss the criteria to consider in specifying the structure and features of CGC's new system.
- Identify the data that should be incorporated into CGC's new system to provide adequate planning capability. Explain why each data item is important and the level of detail needed for the data to be useful. (*CMA Examination, adapted*)

AIS IN ACTION SOLUTIONS

Quiz Key

1. The developers of your new system have proposed two different AIS designs and have asked you to evaluate them. This evaluation process is most likely to be a part of which SDLC step?
 - a. systems analysis [Incorrect. During systems analysis, analysts identify user requirements and establish objectives and specifications for the design phases of the SDLC.]
 - ▶ b. conceptual design [Correct. During conceptual design, users develop and evaluate appropriate design alternatives.]
 - c. physical design [Incorrect. During physical design, the company translates the broad, user-oriented requirements of the conceptual design into detailed specifications that are used to develop and test computer programs.]
 - d. implementation and conversion [Incorrect. During implementation and conversion, the company installs and tests hardware, software, and procedures, as well as converts from the old system to the new system.]
 - e. operation and maintenance [Incorrect. During operation and maintenance, the company runs the system and performs ongoing maintenance and minor modifications.]
2. What is the purpose of the conceptual systems design report?
 - a. to guide physical systems design activities [Incorrect. The conceptual design report also includes communicating how management and users' needs are met and helping the steering committee assess system feasibility.]
 - b. to communicate how management and user information needs are met [Incorrect. The conceptual design report also includes guiding physical systems design activities and helping the steering committee assess system feasibility.]
 - c. to help the steering committee assess system feasibility [Incorrect. The conceptual design report also includes communicating how management and users' needs are met and guiding physical systems design activities.]
 - d. a and b [Incorrect. The conceptual design report also includes helping the steering committee assess system feasibility.]
 - ▶ e. a, b, and c [Correct. The conceptual design report guides physical systems design activities, communicates how management and users' needs are met, and helps the steering committee assess system feasibility.]
3. Which of the following is the correct order of the steps in physical systems design?
 - a. input, file and database, output, controls, procedures, program [Incorrect. See Figure 22-2.]
 - b. file and database, output, input, procedures, program, controls [Incorrect. See Figure 22-2.]
 - c. output, input, file and database, procedures, program, controls [Incorrect. See Figure 22-2.]
 - ▶ d. output, file and database, input, program, procedures, controls [Correct. See Figure 22-2.]
4. A monthly payroll register showing all hourly employees, the number of hours they worked, their deductions, and their net pay is most likely which of the following?
 - ▶ a. scheduled report [Correct. Scheduled reports have a specified content, format, and delivery time. A monthly payroll register exhibits these characteristics.]
 - b. special-purpose analysis [Incorrect. A special-purpose analysis has no specified content, format, or delivery schedule.]
 - c. triggered exception report [Incorrect. A triggered exception report has specified content and format, but it is generated only if a certain event occurs.]
 - d. demand report [Incorrect. A demand report has specified content and format, but it is generated only on request.]
5. Which of the following is NOT a consideration in input design?
 - a. Which errors are possible, and how can they be detected and corrected? [Incorrect. Error identification and correction should be considered during input design. See Table 22-4.]

Case 22-1 Solution

To properly design, implement, and operate this new ERP system, Hershey could have taken the following steps.

Conceptual Design

In designing its new ERP system, Hershey should have looked at all possible designs, evaluated their strengths and weaknesses, and selected the best one. Once the system was selected, Hershey needed to address the design specifications, such as what distribution output is needed to meet customer demands, how to store order and shipping data, how to input order and shipping data, and how to process the inputs and data to produce the outputs. Hershey should have prepared a detailed report to guide the physical design phase and communicate with management and the steering committee the project's progress, requirements, and feasibility.

Physical Design

Once the conceptual design was approved, physical design should have been planned. During this design phase, the following should have been created: order and shipment output documents, reports, files and databases; and the input forms and computer screens needed to capture order and shipment data. Hershey needed to choose which ERP modules to implement and to decide how to structure and modify those modules to meet its needs. Hershey also needed to decide how employees will interact with the system and to develop policies and procedures to formalize that interaction. Controls should have been designed to make sure those procedures and the system in general perform as intended and to prevent fraud and abuse. All of the physical design elements also should have been put into a report to guide Hershey in the actual implementation of the system.

Systems Implementation

Once the new ERP system had been designed and created, the actual hardware, software, procedures, and controls should have been implemented. An installation plan includes all tasks needed to prepare the physical location of the new ERP system, train managers and users to operate the ERP system, document the system, and test it. Based on the information in the case, it appears that Hershey failed to test its new ERP system adequately before converting from the old system.

System Conversion

Of the four primary system conversion approaches, Hershey chose direct conversion—the highest-risk approach. Hershey called the approach the “big bang”—and the big bang that was heard was a drop in market capitalization (stock price) and a damaged reputation due to the loss of orders and the loss of supplier confidence. In hindsight, Hershey should have used one of the other three approaches—parallel, phase-in, or pilot—with the parallel approach probably being the most effective. If Hershey had been able to convert to the new ERP system more successfully, it could have then focused on operating and maintaining the new system and making improvements to make it more effective and efficient.

Glossary

A

acceptance tests Tests of new systems using specially developed transactions and acceptance criteria. The test results are evaluated to determine whether the system is acceptable.

access control list (ACL) A set of rules that determines which packets of information transmitted over a network are allowed entry and which are dropped.

access control matrix An internally maintained table specifying which portions of the system users are permitted to access and what actions they can perform. The matrix contains a list of user codes, a list of all files and programs maintained on the system, and a list of the accesses each user is authorized to make.

accounting information system (AIS) A system that collects, records, stores, and processes data to produce information for decision makers. AIS components include: people, procedures and instructions, data, software, information technology infrastructure, and internal controls and security measures.

accounts receivable aging schedule A report listing customer account balances by length of time outstanding. The report provides useful information for evaluating current credit policies, for estimating bad debts, and for deciding whether to increase the credit limit for specific customers.

activity-based costing (ABC) A cost system designed to trace costs to the activities that create them. Once costs are traced to their specific activities, they are allocated to their corresponding products or departments.

Address Resolution Protocol (ARP) spoofing Sending fake ARP messages to an Ethernet LAN. ARP is a computer networking protocol for determining a network host's hardware address when only its IP or network address is known.

ad hoc queries Nonrepetitive requests for reports or answers to specific questions about the contents of the system's data files.

adware Spyware that (1) causes banner ads to pop up on a monitor as a user surfs the Internet; and (2) collects information about the user's Web-surfing and spending habits and forwards it to the company gathering the data, often an advertising or media organization. Adware usually comes bundled with freeware and shareware downloaded from the Internet.

agents In the REA data model, the people and organizations who participate in events and about whom information is desired.

aggression Resistance to change intended to destroy, cripple, or lessen the effectiveness of a system. It may take the form of increased error rates, disruptions, or deliberate sabotage.

analytical review The examination of the relationships between different sets of data.

application The data processing task to which a computer's processing power is applied.

application controls Controls that prevent, detect, and correct transaction errors and fraud in application programs. They are concerned with the accuracy, completeness, validity, and authorization of the data captured, entered into the system, processed, stored, transmitted to other systems, and reported. Contrast with *general controls*.

application programmer A person who uses a programming language to write an application program.

application service provider (ASP) A company that provides access to and use of application programs via the Internet. The ASP owns and hosts the software; the contracting organization accesses the software remotely via the Internet.

application software The programs that perform data or information processing tasks, such as accounts receivable and payable, inventory control, and payroll.

archive A copy of a database, master file, or software that is retained indefinitely as a historical record, usually to satisfy legal and regulatory requirements.

asymmetric encryption systems See *public key infrastructure (PKI)*.

asynchronous transmission Data transmission in which each character is transmitted separately. A start bit is required before the character and a stop bit after it because the interval of time between transmission of characters can vary. Contrast with *synchronous transmission*.

attributes Characteristics of interest in a file or database; the different individual properties of an entity. Examples of attributes are employee number, pay rate, name, and address.

audit committee The committee responsible for overseeing a corporation's internal control structure, financial reporting process, and compliance with related laws and regulations. It is usually made up of outside members of the board of directors.

audit hooks A concurrent audit technique that embeds audit routines into application software to flag transactions that might indicate an error or fraud.

- audit log** A log of all transactions that have audit significance.
- audit trail** A path that allows a transaction to be traced through a data processing system from point of origin (whether paper or electronic) to final output or backwards from from final output to point of origin. It is used to check the accuracy and validity of ledger postings and to trace changes in general ledger accounts from their beginning balance to their ending balance.
- auditing** A systematic process of (1) objectively obtaining and evaluating evidence regarding assertions about economic actions and events to ascertain the degree of correspondence between those assertions and established criteria; and (2) communicating the results to interested parties.
- authentication** Verifying the identity of the person or device attempting to access the system.
- authorization** Granting an employee power to perform certain organizational functions, such as purchasing or selling on behalf of the company. Employees who are allowed to handle routine transactions without special approval have *general* authorization. An employee needing approval to handle a transaction receives *specific* authorization.
- automated decision table programs** Programs that generate a decision table representing the program's logic.
- automated flowcharting program** A program that interprets the source code of a program and generates a flowchart of the logic used by the program.
- avoidance** A way of resisting change by not using the new system.

B

- back door** See *trap door*.
- back order** A document authorizing the purchase or production of items that is created when there is insufficient inventory to meet customer orders.
- background check** An investigation conducted by a potential or current employer regarding a prospective or current employee. A background check often involves verifying the educational and work experience data on the person's resume, talking to references, checking for a criminal record, checking credit records, and checking other publicly available information about the individual.
- backup** A copy of a database, file, or software program.
- balance-forward method** Method of maintaining accounts receivable in which customers typically pay according to the amount shown on a monthly statement, rather than by individual invoices. Remittances are applied against the total account balance, rather than specific invoices.
- balanced scorecard** A management report that measures four dimensions of performance: financial, internal operations, innovation and learning, and customer perspectives of the organization.
- bandwidth** The difference between the highest and the lowest frequencies of a communications channel. Usually expressed in cycles per second (hertz).
- bar code** An identification label found on most merchandise with vertical lines of differing widths that represent binary information that is read by an optical scanner.
- batch processing** Accumulating transaction records into groups or batches for processing at a regular interval such as daily or weekly. The records are usually sorted into some sequence (such as numerically or alphabetically) before processing.
- batch total** The sum of a numerical item for a batch of documents. These totals are calculated prior to processing the batch and are compared with machine-generated totals at each subsequent processing step to verify that the data was processed correctly.
- behavioral aspects of change** New systems can change organizations, which may result in people changing their behavior. Organizations must be sensitive to and consider the feelings and reactions of persons affected by such changes.
- belief system** A corporate attitude instilled by upper management that communicates company core values to employees and inspires them to live by these values. A belief system should draw attention to how the organization creates values and help employees understand the direction management wants the company to take.
- benchmark problem** A data processing task executed by different computer systems. The results are used to measure systems performance and to make comparative evaluations among systems.
- bill of lading** A legal contract that defines responsibility for goods while they are in transit. It identifies the carrier, source, destination, shipping instructions, and the party (customer or vendor) that must pay the carrier.
- bill of materials** A document that specifies the part number, description, and quantity of each component used in a product.
- biometric identification** Using unique physical characteristics such as fingerprints, voice patterns, retina prints, and signature dynamics to identify people.
- bits** Binary digits are the smallest storage location in a computer. A bit may be either "on" or "off," or "magnetized" or "nonmagnetized." A combination of bits (usually eight) is used to represent a single character of data.
- bits per second (BPS)** A unit of measurement describing the number of bits of data transmitted electronically in one second.
- blanket purchase order or blanket order** A commitment to purchase specified items at designated prices from a particular supplier for a set time period, often one year.
- block code** Blocks of numbers within a numerical sequence that are reserved for categories having meaning to the user.
- border router** A device that connects an organization's information system to the Internet.
- boundary system** An established system that helps employees act ethically by setting limits beyond which an employee must not pass. Employees can solve problems and meet customer needs as long as they operate within certain limits, such as meeting minimum standards of performance, shunning activities that are off limits, and avoiding courses of action that would damage the company's reputation.
- broadband lines** Communications channels capable of handling high-speed data transmissions.
- budget** The formal expression of goals in financial terms. Budgets are financial planning tools. Contrast with *performance report*.
- buffer overflow attack** When an attacker sends a program more data than it can handle. Buffer overflows may cause the system to crash or may provide a command prompt that gives the attacker full administrative privileges and control of the device.
- business continuity plan (BCP)** A plan that specifies how to resume all business processes in the event of a major calamity.
- business cycle** A group of related business processes. The major business cycles are sales and cash receipts, purchasing and cash disbursements, production and inventory control, human resources and payroll, and finance.

business process A set of related, coordinated, and structured activities and tasks that help accomplish a specific organizational goal.

business intelligence Accessing and using data for strategic decision making. There are two main business intelligence techniques: online analytical processing (OLAP) and data mining.

business process management (BPM) Managing the process of improving business processes. Software has been developed to automate business process improvement tasks.

business process management system (BPMS) System that automates and facilitates business process improvements throughout the SDLC. It can improve communication and collaboration, automate activities, and integrate with other systems and with other partners in the value chain.

business process reengineering (BPR) The thorough analysis and redesign of business processes and information systems to achieve dramatic performance improvements.

byte A group of adjacent bits (usually eight) used to represent an alphabetic, numeric, or special character, or even two numeric characters "packed" into a single eight-bit byte.

C

callback system A routing verification procedure. After the user dials in and is authenticated, the computer disconnects and calls the user back as an additional security precaution.

Caller ID spoofing Displaying an incorrect number on the recipient's caller ID display to hide the identity of the caller.

canned software Programs for sale on the open market to a broad range of users with similar needs.

capital budgeting model An estimate of funds to be appropriated for the acquisition of major capital assets and for investment in long-term projects. The estimated benefits are compared with the costs to determine if the system is cost beneficial.

cardinality A property of a database relationship indicating the number of occurrences of one entity that may be associated with a single occurrence of the other entity. Three types of cardinalities are one-to-one, one-to-many, and many-to-many.

cash flow budget A budget that shows projected cash inflows and outflows for a specified period so that an organization can anticipate the need for short-term borrowing.

centralized system or network A system where user terminals are linked to the centralized host computer so that users can send data to the host computer for processing and access data as needed. It provides an "economy of scale" advantage in data processing operations.

central processing unit (CPU) The hardware that contains the circuits that control the interpretation and execution of instructions and that serves as the principal data processing device. Its major components are the arithmetic-logic unit, the memory, and the control unit.

certificate authority An independent organization that issues public and private keys and records the public key in a digital certificate.

change control The process that ensures that hardware, software, or process modifications do not reduce systems reliability. Careful testing prior to implementing changes reduces the likelihood of changes that cause system downtime. Companies with a good change control process are less likely to suffer financial or reputational harm from security incidents.

change management Making sure that system changes minimize negative effects on users and do not negatively affect systems reliability, security, confidentiality, integrity, and availability.

character A letter, numeric digit, or symbol that is entered into a computer system.

chart of accounts A listing of all balance sheet and income statement account number codes.

check digit ID numbers (such as employee number) can contain a check digit computed from the other digits. For example, the system could assign employees a nine-digit number, calculate a tenth digit from the nine, and append it to form a ten-digit ID number.

check digit verification Recalculating a check digit to verify that an error has not been made. This calculation can be made only on a data item that has a check digit.

checkpoint The point(s) during a long processing run where a copy of all data values and status indicators of a program are captured. If a system failure occurs, the system is backed up to the most recent checkpoint and processing restarts at the checkpoint rather than at the beginning of the program.

ciphertext Plaintext that was transformed into unreadable gibberish using encryption.

client/server system A system where information requested by a user is processed as much as possible by the server and then transmitted to the user.

closed-loop verification An input validation method that uses data entered into the system to retrieve and display other related information so the accuracy of the input data can be verified.

cloud computing Purchasing software, storage infrastructure, or platforms from a third-party (referred to as the cloud provider) on a pay-for-use or subscription basis. Cloud providers use virtualization technology to economically provide shared access simultaneously to multiple customers. The resulting economies of scale mean that organizations can often cut their total costs for IT with cloud computing and transforms IT into a utility.

coding (1) The systematic assignment of numbers or letters to items to classify and organize them. (2) Writing program instructions that direct a computer to perform specific data processing tasks.

cold site A location that provides everything necessary to quickly install computer equipment in the event of a disaster.

collusion Cooperation between two or more people in an effort to thwart internal controls.

Committee of Sponsoring Organizations (COSO) A private-sector group consisting of the American Accounting Association, the AICPA, the Institute of Internal Auditors, the Institute of Management Accountants, and the Financial Executives Institute.

compatibility check (or test) Determining whether a person attempting to access an information system resource is authorized to do so. The computer matches the user's authentication credentials against the access control matrix to determine whether the employee is allowed access to that resource or to perform the requested operation.

compensating controls Control procedures that compensate for the deficiency in other controls.

completeness test (or check) An online data entry control in which the computer determines whether all data required for a particular transaction have been entered.

compliance audit Determines compliance with applicable laws, regulations, policies, and procedures. These audits often result in

- recommendations to improve processes and controls that ensure compliance with regulations.
- compliance objectives** Objectives to help the company comply with applicable laws and regulations.
- computer-assisted audit techniques (CAATS)** Audit software, often referred to as generalized audit software (GAS) or computer audit software (CAS), that uses auditor-supplied specifications to generate a program that performs audit functions, thereby automating or simplifying the audit process.
- computer crime** Any illegal act for which knowledge of a computer is essential for the crime's perpetration, investigation, or prosecution.
- computer forensics specialists** Computer experts whose job entails discovering, extracting, safeguarding, and documenting computer evidence so that its authenticity, accuracy, and integrity will not succumb to legal challenges.
- computer fraud** See *computer crime*.
- computer incident response team (CIRT)** A team that is responsible for dealing with major security incidents. The CIRT should include technical specialists as well as senior operations management, because some security incident responses may have significant economic consequences.
- computer-integrated manufacturing (CIM)** A manufacturing approach in which much of the manufacturing process is performed and monitored by computerized equipment, in part through the use of robotics and real-time data collection of manufacturing activities.
- computer operators** People who operate the company's computers. They ensure that data are properly input to the computer and processed correctly, and needed output is produced.
- computer programmers** Persons who develop, code, and test computer programs.
- computer security** The policies, procedures, tools, and other means of safeguarding information systems from unauthorized access or alteration, intentional or unintentional damage, or theft.
- computer security officer** An employee independent of the information system function who monitors the system and disseminates information about improper system uses and their consequences.
- concatenated key** Two or more primary keys of other database tables that, together, become a unique identifier or primary key of another table. A multiple-attribute primary key.
- conceptual design specifications** System requirement specifications for systems output, data storage, input, processing procedures, and operations.
- conceptual-level schema** The organization-wide view of the entire database. It lists all data elements and the relationships between them. Contrast with *external-level schema* and *internal-level schema*.
- conceptual systems design** The systems development life cycle phase in which a general framework is created to implement user requirements and solve problems identified in the analysis phase.
- conceptual systems design report** A document specifying the findings and results of conceptual systems design. The report is used in physical systems design to identify the hardware, software, and procedures necessary to deliver the system.
- concurrent audit techniques** Software that continuously monitors an information system as it processes live data in order to collect, evaluate, and report information about system reliability.
- concurrent update controls** Controls that lock out users to protect individual records from errors that could occur if multiple users attempted to update the same record simultaneously.
- context diagram** The highest data flow diagram level. It provides a summary-level view of a system. It shows the data processing system, system input(s) and output(s), and the external entities that are the sources and destinations of the input(s) and output(s).
- continuous and intermittent simulation (CIS)** A concurrent audit technique that embeds an audit module into a database management system, rather than the application software.
- control account** A general ledger account that summarizes the total amounts recorded in a subsidiary ledger. The accounts payable control account in the general ledger represents the total amount owed to all vendors. The balances in the subsidiary accounts payable ledger indicate the amount owed to each specific vendor.
- control activities** Policies, procedures, and rules that provide reasonable assurance that control objectives are met and their risk responses are carried out.
- control environment** The organization's environment relating to controls, including management's philosophy, the audit committee, and the organizational structure.
- Control Objectives for Information and related Technology (COBIT)** An information systems security and control framework that allows (1) management to benchmark the security and control practices of IT environments, (2) users of IT services to be assured that adequate security and control exist, and (3) auditors to substantiate their internal control opinions and advise on IT security and control matters.
- control risk** The risk that a significant control problem will not be prevented or detected by the internal control system.
- control totals** Batch totals used to ensure that all data are processed correctly. Examples are the number of transactions processed and the dollar amount of all updates.
- conversion** The process of changing from one computer format to another.
- cookie** A text file created by a Web site and stored on a visitor's hard drive. Cookies store information about who the user is and what the user has done on the site.
- corrective controls** Procedures that remedy problems that occur.
- cost driver** Anything that has a cause-and-effect relationship to costs. For example, the number of purchase orders processed is a purchasing department cost driver.
- cracking** See *hacking*.
- credit limit** The maximum allowable credit account balance for each customer, based on past credit history and ability to pay.
- credit memo** A document authorizing the billing department to credit a customer's account. Usually issued for sales returns, for allowances granted for damaged goods kept by the customer, or to write off uncollectible accounts. Approved by the credit manager.
- critical path** The path requiring the greatest amount of time to complete a project. If an activity on the critical path is delayed, the whole project is delayed. If possible, resources are shifted to critical path activities to reduce project completion time.
- cross-footing balance test** A procedure in which worksheet data are totaled both across and down. Then, the total of the horizontal totals is compared to the total of the vertical totals to ensure that the worksheet balances.
- cross site scripting (XSS)** Exploits Web page security vulnerabilities to bypass browser security mechanisms and create a malicious link that injects unwanted code into a Web site.
- cryptography** See *data encryption*.

customer relationship management (CRM) systems Software that organizes information about customers in a manner that facilitates efficient and personalized service.

custom software Software developed and written in-house to meet the unique needs of a particular company.

cyber-bullying Using computer technology to harm another person.

cycle billing Producing monthly statements for subsets of customers at different times. For example, each week monthly statements would be prepared for one-fourth of the customers.

D

data Facts that are collected, recorded, stored, and processed by an information system to produce information.

data administrator (DA) The person responsible for developing general policies and procedures governing all organizational data, not just what is stored in the database. The DA is responsible for understanding the organization's information needs and deciding what should be included in the database.

database A set of interrelated, centrally controlled data files that are stored with as little data redundancy as possible. A database consolidates records previously stored in separate files into a common pool and serves a variety of users and data processing applications.

database administrator The person responsible for coordinating, controlling, and managing the database.

database management system (DBMS) The program that manages and controls the data and the interfaces between the data and the application programs.

database query language An easy-to-use DBMS language that lets users ask questions about the data stored in a database.

database system The combination of the database, the database management system, and the application programs that access the database through the database management system.

data communications The transmission of data from a point of origin to a point of destination.

data communications network A communication system that bridges geographical distances, giving users immediate access to a company's computerized data. It allows multiple companies or computer services to be linked to information.

data control group The group charged with ensuring that source data have been properly approved, monitoring the flow of work through the computer, reconciling input and output, maintaining a record of input errors to ensure their correction and resubmission, and distributing systems output.

data definition language (DDL) A DBMS language that ties the logical and physical views of data together. It is used to build the data dictionary, initialize or create the database, describe the logical views for each individual user or programmer, and specify any limitations or constraints on security imposed on database records or fields.

data destination An entity outside the system that receives data produced by the system. A component of a data flow diagram.

data dictionary A description of each data element that is stored in the database. For example, customer numbers are stored in the database and there is a record in the data dictionary describing that data element.

data diddling Changing data before, during, or after it is entered into the system. The change can be made to add, delete, or alter system data.

data flow The data flow diagram component that represents data flowing into or out of a process.

data flow diagram (DFD) A graphical description of the flow of data within an organization. It is used to document existing systems and to plan and design new ones.

data independence Storing data such that the data and the application programs that use it are independent. This means that one may be changed without affecting the other.

data leakage The unauthorized copying of company data, often without leaving any indication that it was copied.

data loss prevention (DLP) Software which works like antivirus programs in reverse, blocking outgoing messages (e-mail, instant messages, etc.) that contain key words or phrases associated with intellectual property or other sensitive data the organization wants to protect.

data maintenance The periodic processing of transactions to update stored data. The four types of data maintenance are create, read, update, and delete (often referred to as CRUD).

data manipulation language (DML) A DBMS language used create, read, update, and delete items in the database.

data mart A smaller data warehouse for functions such as finance and human resources.

data masking A program that protects privacy by replacing customers' personal information with fake values before sending that data to the program development and testing system. For example, a real Social Security number might be replaced with a different set of numbers that have the same characteristics, such as 123-45-6789.

data mining Accessing information stored in a data warehouse through statistical analysis or artificial intelligence techniques to "discover" unhypothesized relationships in the data.

data model An abstract representation of the contents of a database.

data modeling Defining a database so that it faithfully represents all key components of an organization's environment. The objective is to explicitly capture and store data about every business activity the organization wishes to plan, control, or evaluate.

data processing center The room that houses the hardware, software, data, and people who operate a computer system.

data processing cycle The operations performed on data to generate meaningful and relevant information. It has four stages: data input, data storage, data processing, and information output.

data processing schedule A schedule of data processing tasks designed to maximize the use of scarce computer resources.

data query language (DQL) A high-level, English-like, DBMS language that retrieves, sorts, orders, and presents subsets of the database in response to user queries.

data redundancy The storage of the same data item in two or more files within an organization.

data source The entity that produces or sends the data that is entered into the system. A component of a data flow diagram.

data store The place or medium where system data is stored. A component of a data flow diagram.

data transmission controls Methods of monitoring the network to detect weak points, maintain backup components, and ensure that the system can still communicate if one of the communications paths fails.

data value The actual value stored in a field. It describes a particular attribute of an entity.

- data warehouses** Very large databases that contain detailed and summarized data for a number of years and that are used for analysis rather than transaction processing.
- debit memo** A document used to record a reduction to the balance due to a vendor.
- debugging** The process of checking for and correcting the errors found in a computer program.
- decentralized system** An information system that has an independent CPU and data processing manager at each location.
- decision support system (DSS)** An interactive computer system designed to help with the decision-making process by providing access to a database or decision-making model.
- decryption** Transforming ciphertext back into plaintext.
- deduction register** A report listing the miscellaneous voluntary deductions for each employee.
- deep packet inspection** When the firewall examines the data in the body of an IP packet rather than looking only at the information in the IP header.
- default value** A control that helps preserve the integrity of data processing and stored data by leaving a field blank if a standard value is to be used.
- defense-in-depth** Employing multiple layers of controls to avoid a single point-of-failure. Overlapping, complementary, and redundant controls buy time for the organization to detect and react to attacks. It also increases effectiveness because if one procedure fails or is circumvented, another may function as planned.
- delete anomaly** When deleting a row from a table results in the loss of all information about an entity. For example, if customer addresses are stored only in the sales invoice table, then deleting the row representing the only sale to a particular customer results in the loss of all information about that customer.
- demand reports** Reports that have a prespecified content and format but are prepared only in response to a request from a manager or other employee.
- demilitarized zone (DMZ)** Placing the organization's Web servers and e-mail servers in a separate network that sits outside the corporate network but is accessible from the Internet.
- denial-of-service attack** A computer attack in which the attacker sends so many e-mail bombs (thousands per second), often from randomly generated false addresses, that the Internet service provider's e-mail server is overloaded and shuts down. Another denial-of-service attack involves sending so many requests for Web pages that the Web server crashes.
- detection risk** The risk that auditors and their procedures will not detect a material misstatement.
- detective controls** Controls designed to discover control problems when they arise.
- diagnostic control system** A performance measurement system that compares actual performance to planned performance.
- dictionary attack** Using special software to guess company addresses and send them blank e-mail messages. Unreturned messages are usually valid e-mail addresses that can be added to spammer e-mail lists.
- differential backup** Copying all changes made since the last full backup. Thus, each new differential backup file contains the cumulative effects of all activity since the last full backup.
- digital certificate** An electronic document, created and digitally signed by a trusted third party, that certifies the identity of the owner of a particular public key. The digital certificate contains that party's public key. Thus, digital certificates provide an automated method for obtaining an organization's or an individual's public key.
- digital fingerprint** A hash number that identifies and validates a digital certificate.
- digital signature** (1) A piece of data signed on a document by a computer. A digital signature cannot be forged and is useful in tracing authorization. (2) Information encrypted with the creator's private key.
- digital watermark** Code embedded in documents that enables an organization to identify confidential information that has been disclosed. A digital watermark is a detective control and organizations should investigate how a compromise occurred and take appropriate corrective action.
- direct access** An access method that allows the computer to access a particular record without reading other records. Because each storage location on a direct access storage device has a unique address, the computer can find the record needed as long as it has the record's address.
- direct access storage device (DASD)** A storage device (such as a disk drive) that can directly access individual storage locations to store or retrieve data.
- direct conversion** An approach to converting from one system to another in which the old system is discontinued, after which the new system is started (also known as "burning the bridges" or "crash conversion").
- disaster recovery plan** A plan to recover data processing capacity as smoothly and quickly as possible in the event of an emergency that disables the computer system.
- disbursement voucher** A document that identifies the vendor, lists the outstanding invoices, and indicates the net amount to be paid after deducting any applicable discounts and allowances.
- distributed data processing (DDP)** A system in which computers are set up at remote locations and then linked to a centralized mainframe computer.
- DNS spoofing** Sniffing the ID of a Domain Name System (server that converts a Web site name to an IP address) request and replying before the real DNS server.
- documentation** The narratives, flowcharts, diagrams, and other written materials that explain how a system works. It covers the who, what, when, where, why, and how of data entry, processing, storage, information output, and system controls.
- document flowchart** Flowchart that traces a document from its cradle to its grave. They show where each document originates, its distribution, the purposes for which it is used, its ultimate disposition, and everything that happens as it flows through the system. They illustrate the flow of documents and information among areas of responsibility within an organization.
- documents** Records of transaction or other company data such as checks, invoices, receiving reports, and purchase requisitions.
- dumpster diving** See *scavenging*.
- earnings statement** A report listing the amount of gross pay, deductions, and net pay for the current period and the year-to-date totals for each category.

- eavesdropping** Observing data transmissions intended for someone else. One way unauthorized individuals can intercept signals is by setting up a wiretap.
- e-business** All uses of advances in information technology, particularly networking and communications technology, to improve the ways an organization performs its business processes.
- echo check** A hardware control that verifies transmitted data by having the receiving device send the message back to the sending device so that the message received can be compared with the message sent.
- economic espionage** The theft of information and intellectual property.
- economic exchange** An event in which one agent gives a resource to another agent in exchange for some other resource.
- economic feasibility** The dimension of feasibility concerned with whether the benefits of a proposed system will exceed the costs.
- economic order quantity (EOQ)** The optimal order size to minimize the sum of ordering, carrying, and stockout costs. Ordering costs are expenses associated with processing purchase transactions. Carrying costs are the costs associated with holding inventory. Stockout costs, such as lost sales or production delays, result from inventory shortages.
- edit checks** Accuracy checks performed by an edit program.
- edit programs** Computer programs that verify the validity and accuracy of input data.
- electronic data interchange (EDI)** The use of computerized communications and a standard coding scheme to submit business documents electronically in a format that can be automatically processed by the recipient's information system.
- electronic data processing (EDP)** Processing data utilizing a computer system.
- electronic funds transfer (EFT)** The transfer of funds between two or more organizations or individuals using computers and other automated technology. This eliminates the delay associated with the time the remittance is in the mail.
- electronic lockbox** A lockbox arrangement (see *lockbox*) in which the bank electronically sends the company information about the customer account number and the amount remitted as soon as it receives payments. This enables the company to begin applying remittances to customer accounts before the photocopies of the checks arrive.
- electronic vaulting** Electronically transmitting backup copies of data to a physically different location. Electronic vaulting permits online access to backup data when necessary.
- element** A specific data item in an XBRL instance document, such as a financial statement line item.
- e-mail bomb** A denial-of-service attack in which the receiver's e-mail server is bombarded with hundreds of e-mail messages per second.
- e-mail spoofing (forgery)** Making a sender address and other parts of an e-mail header appear as though the e-mail originated from a different source.
- e-mail threats** Threats sent to victims by e-mail. The threats usually require some follow-up action, often at great expense to the victim.
- embedded audit modules** Special portions of application programs that track items of interest to auditors, such as unauthorized attempts to access the data files.
- embezzlement** The fraudulent appropriation of business property by an employee to whom it has been entrusted. It is often accompanied by falsification of records.
- encryption** The process of transforming normal text, called *plaintext*, into unreadable gibberish, called *ciphertext*. Encryption is particularly important when confidential data is being transmitted from remote terminals because data transmission lines can be electronically monitored without the user's knowledge.
- endpoints** Collective term for the workstations, servers, printers, and other devices that comprise an organization's network. Supplementing preventive controls on the network perimeter with additional preventive controls on the endpoints enhances the security of information systems.
- end-user computing (EUC)** The creation, control, and implementation by end users of their own information system.
- end-user system (EUS)** A system developed by users, rather than information systems professionals, to meet their information needs. An EUS often draws upon the information in existing corporate databases to meet users' information needs.
- enterprise resource planning (ERP) system** A system that integrates all aspects of an organization's activities into one accounting information system.
- Enterprise Risk Management—Integrated Framework (ERM)** A COSO-developed internal framework that expands on the elements of COSO's Internal Control Integrated Framework and provides an all-encompassing focus on the broader subject of enterprise risk management.
- entity** The item about which information is stored in a record. Examples include an employee, an inventory item, and a customer.
- entity integrity rule** A design constraint in a relational database, requiring that the primary key have a non-null value. This ensures that a specific object exists in the world and can be identified by reference to its primary key value.
- entity-relationship (E-R) diagram** A graphical depiction of a database's contents showing the various entities being modeled and the important relationships among them. An entity is any class of objects about which data are collected, such as the resources, events, and agents that comprise the REA data model. An E-R diagram represents entities as rectangles; lines and diamonds represent relationships between entities.
- error log** The record of data input and data processing errors.
- error message** A message indicating that the computer encountered a mistake or malfunction.
- error report** A report summarizing errors by record type, error type, and cause.
- evaluated receipt settlement (ERS)** An invoiceless approach to accounts payable that replaces the three-way matching process (vendor invoice, receiving report, and purchase order) with a two-way match of the purchase order and receiving report. ERS saves time and money by reducing the number of mismatches and the time and expense of generating and tracking invoices.
- event** (1) In the REA data model, a business activity about which management wants to collect information for planning or control purposes. (2) An incident or occurrence from internal or external sources that affects the implementation of strategy or the achievement of objectives.
- expected loss** The mathematical product of the potential dollar loss that would occur should a threat become a reality (called *exposure*) and the risk or probability that the threat will occur (called *likelihood*).

expenditure cycle A recurring set of business activities and related data processing operations associated with the purchase of and payment for goods and services.

exploit The set of instructions for taking advantage of a vulnerability.

exposure The potential dollar loss should a particular threat become a reality.

extension taxonomy A set of custom XBRL tags to define elements unique to the reporting organization that are not part of the standard generally accepted taxonomies for that industry.

external label A label on the outside of a storage medium that identifies the data it contains.

external-level schema An individual user's or application program's view of a subset of the organization's database. Each of these individual user views is also referred to as a subschema. Contrast with *conceptual-level schema* and *internal-level schema*.

F

fault tolerance The capability of a system to continue performing when there is a hardware failure.

feasibility study An investigation to determine whether the development of a new application or system is practical. One of the first steps in the systems evaluation and selection process.

field The part of a data record that contains the data value for a particular attribute. For example, fields in all accounts receivable records would include customer account number, customer address, and balance due.

field check An edit check in which the characters in a field are examined to ensure they are of the correct field type (e.g., numeric data in numeric fields).

file A set of logically related records, such as the payroll records of all employees.

file maintenance The periodic processing of transaction data, which is the most common task in data processing systems. It includes creating, reading, updating, and deleting records. After file maintenance, the master file will contain all current information.

file organization The way data are stored on physical storage media. File organization may be either sequential or direct (random) access.

financial audit A review of the reliability and integrity of financial and operating information and the means used to identify, measure, classify, and report such information.

financial electronic data interchange (FEDI) The combination of EFT and EDI that enables both remittance data and funds transfer instructions to be included in one electronic package.

financial total The total of a dollar field, such as total sales, in a set of records. It is usually generated manually from source documents prior to input and compared with machine-generated totals at each subsequent processing step. A discrepancy may indicate a loss of records or errors in data transcription or processing.

financial value-added network (FVAN) An independent organization that offers specialized hardware and software to link various EDI networks with the banking system for EFT.

financing cycle The business activities and data processing operations associated with obtaining funds to operate, repay creditors, and distribute profits to investors.

firewall A combination of security algorithms and router communications protocols that prevent outsiders from tapping into corporate databases and e-mail systems.

flexible benefits plan A plan under which each employee receives some minimum coverage in medical insurance and pension contributions, plus additional benefit "credits" that can be used to acquire extra vacation time or additional health insurance. These plans are sometimes called *cafeteria-style benefit plans* because they offer a menu of options.

flexible budget A budget in which the amounts are stated in terms of formulas based upon actual level of activity.

flowchart An analytical technique used to describe some aspect of an information system in a clear, concise, and logical manner. Flowcharts use a standard set of symbols to describe pictorially transaction processing procedures and the flow of data through a system.

flowcharting symbols A set of objects that are used in flowcharts to show how and where data move. Each symbol has a special meaning that is easily conveyed by its shape.

flowcharting template A piece of hard, flexible plastic on which the shapes of flowcharting symbols have been die cut.

Foreign Corrupt Practices Act (1977) Legislation that, among other things, requires all publicly owned corporations subject to the Securities Exchange Act of 1934 to keep reasonably detailed records and maintain a system of internal accounting controls.

foreign key An attribute appearing in one table that is itself the primary key of another table. Foreign keys are used to link tables.

forensic accountants Accountants who specialize in fraud auditing and investigation. Upon qualification, forensic accountants may receive a Certified Fraud Examiner (CFE) certificate.

fraud Any and all means a person uses to gain an unfair advantage over another person.

fraud hot line A phone number employees can call to anonymously report fraud and abuse.

fraudulent financial reporting Intentional or reckless conduct, whether by act or omission, that results in materially misleading financial statements.

G

Gantt chart A bar graph used for project planning and control. Project activities are shown on the left and units of time across the top. The time period each activity is expected to take is represented with a horizontal bar on the graph.

general authorization The authorization given to regular employees to handle routine transactions without special approval.

general controls Controls designed to make sure an organization's information system and control environment is stable and well managed. Contrast with *application controls*.

generalized audit software (GAS) A software package that can be used to perform audit tests on the data files of a company.

general journal A journal used to record infrequent or nonroutine transactions, such as loan payments and end-of-period adjusting and closing entries.

general journal listing A report showing the details (account number, source reference code, description, and amount debited or credited) of each entry posted to the general ledger. This report

indicates whether the total debits equal the total credits posted to the general ledger.

general ledger Ledger that contains summary-level data for every asset, liability, equity, revenue, and expense account of the organization.

general ledger and reporting system The information-processing operations involved in updating the general ledger and preparing reports that summarize organizational activities.

give-get exchange An event in which two entities exchange items, such as cash for goods or services.

goal conflict Occurs when a decision or action of a subsystem is inconsistent with another subsystem or the system as a whole.

goal congruence Achieved when a subsystem achieves its goals while contributing to the organization's overall goal.

grandfather-father-son concept Retaining the three most current copies of the master files (the son is the most recent) and transaction files. If a master file is destroyed, it can be recreated using a prior master file and the appropriate transaction file.

group codes Two or more subgroups of digits that are used to code an item. A group code is often used in conjunction with a block code.

H

hacking Unauthorized access and use of computer systems, usually by means of a personal computer and telecommunications networks.

hardening The process of turning off unnecessary program features.

hash Plaintext that has been transformed into short code.

hashing Transforming plaintext of any length into a short code called a hash.

hash total A total generated from values for a field that would not usually be totaled, such as customer account numbers. It is usually generated manually from source documents prior to input and compared with machine-generated totals at each subsequent processing step. Any discrepancy may indicate a loss of records or errors in data transcription or processing.

header label/record Type of internal label that appears at the beginning of each file and contains the file name, expiration date, and other file identification information.

help desk An in-house group of analysts and technicians who answer employees' questions with the purpose of encouraging, supporting, coordinating, and controlling end-user activity.

hijacking Gaining control of someone else's computer to carry out illicit activities, such as sending spam without the computer user's knowledge.

home page A "storefront" or site on the Internet set up by individuals and firms to provide useful and interesting information.

hot site Completely operational data processing facility configured to meet the user's requirement that can be made available to a disaster-stricken organization on short notice.

human resources management (HRM)/payroll cycle The recurring set of business activities and data processing operations associated with effectively managing the employee workforce.

identity theft Assuming someone's identity, usually for economic gain, by illegally obtaining confidential information such as a social security number.

impact See *exposure*.

impersonation See *masquerading*.

implementation The process of installing a computer system. It includes selecting and installing equipment, training personnel, establishing operating and control policies and procedures, testing and documenting the system, installing software, and getting the system to function properly.

implementation and conversion phase The capstone phase in the systems development life cycle where the elements and activities of the system come together.

implementation plan A written plan that outlines how the new system will be implemented. The plan includes a timetable for completion, the employee who is responsible for each activity, cost estimates, and task milestones.

imprest fund A cash account with two characteristics: (1) It is set at a fixed amount, such as \$100; and (2) vouchers are required for every disbursement. At all times, the sum of cash plus vouchers should equal the preset fund balance.

incremental backup Copying data items that have changed since the last backup. This produces a set of incremental backup files, each containing the results of one day's transactions.

information Data that have been organized and processed to provide meaning to a user.

information overload The state in which additional information cannot be used efficiently and has no marginal value.

information processing The process of turning data into information. This process has four stages: data input, data processing, data storage, and information output.

information rights management (IRM) Software that offers the capability not only to limit access to specific files or documents, but also to specify the actions (read, copy, print, download, etc.) that individuals who are granted access to that resource can perform. Some IRM software even has the capability to limit access privileges to a specific period of time and to remotely erase protected files.

information system An organized way of collecting, processing, managing, and reporting information so that an organization can achieve its objectives and goals. Formal information systems have an explicit responsibility to produce information. An informal information system meets a need that is not satisfied by a formal channel and operates without formal designation of responsibility.

information system library A collection of corporate databases, files, and programs stored in a separate storage area.

information systems audit Reviews the general and application controls of an AIS to assess its compliance with internal control policies and procedures and its effectiveness in safeguarding assets.

information systems steering committee Plans and oversees the information systems function. The committee often consists of high-level management people, such as the controller and systems and user-department management. The steering committee sets policies that govern the AIS and ensures top-management participation, guidance, and control.

inherent risk The susceptibility of a set of accounts or transactions to significant control problems in the absence of internal control.

initial investigation A preliminary investigation to determine whether a proposed new system is both needed and possible.

input Data entered into the computer system either from an external storage device or from the keyboard of the computer.

input controls Controls that ensure that only accurate, valid, and authorized data are entered into the system.

input controls matrix A matrix that shows the control procedures applied to each field of an input record.

input validation routines Computer programs or routines designed to check the validity or accuracy of input data.

inquiry processing Processing user information queries by searching databases for the desired information and then organizing the information into an appropriate response.

insert anomaly A problem that arises when attributes that are not characteristics of the primary key are stored in a table. The problem arises because new information about those attributes cannot be entered in the database without violating integrity rules. For example, assume that information about vendors is stored only as part of the purchases table. Data about potential new vendors, or about alternative suppliers, could not be added until a purchase from them was made. Otherwise, the purchase order number column, the primary key of the purchases table, would have a null value, violating the entity integrity rule.

instance document An XBRL report that contains tagged data.

integrated test facility A testing technique in which a dummy company or division is introduced into the company's computer system. Test transactions may then be conducted on these fictitious records without affecting the real records. Test transactions may be processed along with real transactions, and the employees of the computer facility need not be aware that testing is being done.

integration Eliminating duplicate recording, storage, reporting, and other processing activities in an organization. For example, companies that used to have separate programs to prepare customer statements, collect cash, and maintain accounts receivable records now combine these functions into a single application.

integrity Protecting data from unauthorized tampering.

interactive control system Helps top-level managers with high-level activities that demand frequent and regular attention, such as developing company strategy, setting company objectives, understanding and assessing threats and risks, monitoring changes in competitive conditions and emerging technologies, and developing responses and action plans to proactively deal with these high-level issues.

internal auditing An independent, objective assurance and consulting activity designed to add value and improve organizational effectiveness and efficiency. Internal auditing helps an organization accomplish its objectives by using a systematic, disciplined approach to evaluate and improve the effectiveness of the risk management, control, and governance processes.

internal control flowchart A document flowchart that describes and evaluates internal controls. Often used by auditors in the planning stage of an audit.

Internal Control Integrated Framework A framework developed by COSO to define internal controls as well as to provide guidance for evaluating and enhancing internal control systems. It is widely accepted as the authority on internal controls.

internal controls Controls within a business organization that ensure information is processed correctly.

internal control system The plan of organization and the methods and measures adopted within a business to safeguard its assets, maintain records that accurately and fairly reflect company assets, check the accuracy and reliability of its accounting data, provide assurance that financial reporting is prepared in accordance with GAAP, promote operational efficiency, comply with applicable

laws and regulations, and encourage adherence to prescribed managerial policies.

internal environment The tone or culture of a company that helps determine the risk consciousness of employees. It is the foundation for all other ERM components, providing discipline and structure. It is essentially the same thing as the control environment in the internal control framework.

internal labels Labels written in machine-readable form on a magnetic storage medium that identify the data contained on the storage medium. Internal labels include volume, header, and trailer labels.

internal-level schema A low-level view of the entire database describing how the data are actually stored and accessed. It includes information about record layouts, definitions, addresses, indexes, and so forth. Contrast with *external-level schemas* and *conceptual-level schemas*.

internal rate of return (IRR) The effective interest rate that equates the present value of total costs to the present value of total savings.

Internet auction fraud Using an Internet auction site to defraud another.

Internet misinformation Using the Internet to spread false or misleading information. This can be done in a number of ways, including inflammatory messages in online chats, setting up Web sites, and spreading urban legends.

Internet Protocol (IP) Protocol that specifies the structure of the TCP packets and how to route them to the proper destination.

Internet pump-and-dump fraud Using the Internet to pump up the price of a stock and then sell it.

Internet service providers (ISPs) Companies that provide connections to the Internet for individuals and other companies.

Internet terrorism Hackers using the Internet to disrupt electronic commerce and destroy company or individual communications.

intranet An internal network that can connect to the main Internet and be navigated with browser software. It is usually closed off from the general public.

intrusion detection systems (IDS) A system that creates logs of all network traffic that was permitted to pass the firewall and then analyzes those logs for signs of attempted or successful intrusions.

intrusion prevention systems (IPS) A new type of filter designed to identify and drop packets that are part of an attack.

inventory control The function of determining what, when, and how much inventory to purchase.

investigative audit Examines incidents of possible fraud, misappropriation of assets, waste and abuse, or improper governmental activities, looking for evidence of impropriety.

IP address spoofing Creating Internet Protocol packets with a forged IP address to hide the sender's identity or to impersonate another computing system.

J

job-order costing A cost system that assigns costs to specific production batches or jobs; it is used when the product or service being produced can be distinctly identified.

job-time ticket A document used to collect data about labor activity by recording the amount of time a worker spent on each specific job task.

journal voucher A form used to document one or more journal entries such as those made to update the general ledger.

journal voucher file A file that stores all journal entries used to update the general ledger.

just-in-time (JIT) inventory system A system that minimizes or virtually eliminates manufacturing inventories by scheduling inventory deliveries at the precise times and locations needed. Instead of making infrequent bulk deliveries to a central receiving and storage facility, suppliers deliver materials in small lots at frequent intervals to the specific locations that require them.

just-in-time (JIT) manufacturing Manufacturing systems with short planning horizons whose goal is to minimize or eliminate inventories of raw materials, work in process, and finished goods. JIT is often referred to as *pull manufacturing* because goods are produced in response to customer demand. Theoretically, JIT manufacturing systems produce only in response to customer orders. In practice, however, most JIT manufacturing systems develop short-run production plans.

K

key A unique identification code assigned to each data record within a system.

key escrow The process of storing a copy of an encryption key in a secure location.

key logger Spyware that records a user's keystrokes, e-mails sent and received, Web sites visited, and chat session participation.

key-to-disk encoder Several keying stations linked to a computer. Data may be entered simultaneously from each of the key stations and pooled on a disk file.

key-to-tape encoder A device for keying in data and recording the data on magnetic tape.

key verification Checking the accuracy of data entry by having two people enter the same data using a key-operated device. The computer then compares the two sets of keystrokes to determine whether the data were entered correctly.

kickbacks Gifts given by vendors to purchasing agents for the purpose of influencing their choice of suppliers.

kiting A fraud scheme where the perpetrator conceals a theft of cash by creating cash through the transfer of money between banks. For example, suppose a fraud perpetrator opens checking accounts in banks A, B, and C. Then the perpetrator "creates" cash by depositing a \$1,000 check from bank A into bank B and then withdraws the \$1,000 from bank B. Since there are insufficient funds in bank A to cover the \$1,000 check, the perpetrator deposits a \$1,000 check from bank C to bank A before his check to bank B clears bank A. Since bank C also has insufficient funds, \$1,000 must be deposited to bank C before the check to bank A clears. The check to bank C is written from bank B, which also has insufficient funds. The scheme continues, with checks and deposits occurring as needed to keep the checks from bouncing.

L

LAN See *local area network*.

lapping Concealing the theft of cash by means of a series of delays in posting collections to accounts. For example, a perpetrator steals customer A's accounts receivable payment. Funds received at a later date from customer B are used to pay off customer A's balance. Funds from customer C are used to pay off B's balance, and so forth.

lean manufacturing The goal of lean manufacturing is to minimize or eliminate inventories of raw materials, work in process, and finished goods. Lean manufacturing is often referred to as *pull manufacturing* because goods are produced in response to customer demand.

Lebanese looping Inserting a sleeve into an ATM that will not eject a card, pretending help for the purpose of obtaining a PIN, and then using the card and PIN to drain the account.

legal feasibility The dimension of feasibility that determines whether there will be any conflicts between the system under consideration and the organization's ability to discharge its legal obligations.

likelihood The probability that a threat to an AIS will come to pass.

limit check An edit check to ensure that a numerical amount in a record does not exceed some predetermined limit.

line count Total number of lines entered during a data processing session.

Linkbases One or more XBRL files that define the relationships among elements found in a specific instance document.

local area network (LAN) A network that links computers, printers, and other electronic equipment located within a limited geographical area, such as a single building.

lockbox A postal address to which customers send their remittances. This Post Office box is maintained by the participating bank, which picks up the checks each day and deposits them to the company's account. The bank sends the remittance advices, an electronic list of all remittances, and digital copies of all checks to the company.

log analysis The process of examining logs to monitor security.

logical access The ability to use computer equipment to access company data.

logical models Descriptions of a system that focus on the essential activities and flow of information in the system irrespective of how the flow is actually accomplished.

logical view The manner in which a user or programmer conceptually organizes, views, and understands the relationships among data items. Contrast with *physical view*.

logic errors Errors that occur when the instructions given to the computer do not accomplish the desired objective. Contrast with *syntax errors*.

logic time bomb A program that lies idle until some specified circumstance or a particular time triggers it. Once triggered, the program sabotages the system by destroying programs or data.

M

MAC address A Media Access Control address is a hardware address that uniquely identifies each node on a network.

magnetic disks Magnetic storage media consisting of one or more flat, round disks with a magnetic surface on which data can be written.

magnetic ink character recognition (MICR) The recognition of characters printed by a machine that uses special magnetic ink.

magnetic tape A secondary storage medium that is about 1/2 inch in width and that has a magnetic surface on which data can be stored. The most popular types are seven-track and nine-track tapes.

mainframe computers Large digital computers, typically with a separate stand-alone CPU.

management audit A review of how well management is utilizing company resources and how well company operations and programs follow established objectives.

management by exception A method for interpreting variances displayed on performance reports. If the performance report shows actual performance to be at or near budgeted figures, a manager can assume that the item is under control and that no action needs to be taken. Significant deviations from budgeted amounts, in *either* direction, signal the need to investigate the cause of the discrepancy and take appropriate action to correct the problem.

management information system The set of human and capital resources that are dedicated to collecting and processing data so that all levels of management have the information they need to plan and control the activities of the organization.

man-in-the-middle (MITM) attack A hacker placing himself between a client and a host to intercept network traffic; also called *session hijacking*.

manual information system Information system in which most data processing is completed by people without the use of computers.

manufacturing overhead All manufacturing costs that are not economically feasible to trace directly to specific jobs or processes.

manufacturing resource planning (MRP-II) An extension of materials resource planning that seeks to balance existing production capacity and raw materials needs to meet forecasted sales demands. Also referred to as *push manufacturing* because goods are produced in expectation of customer demand.

many-to-many (M:N) relationship A relationship between two entities where each entity can be associated with many instances of the other entity. For example, each inventory item can be sold to many different customers and each customer can order many different inventory items.

mapping programs Programs that provide information as to which portions of an application program are not executed.

masquerading Gaining access to a system by pretending to be an authorized user. This approach requires that the perpetrator know the legitimate user's identification numbers and passwords.

master file A permanent file of records that stores cumulative information about an organization's resources and the agents with whom it interacts. As transactions take place, individual records within a master file are updated to keep them current.

master plan A long-range planning document that specifies the overall information system plan of an organization. It shows what the system will consist of, how it will be developed, who will develop it, how needed resources will be acquired, and where the AIS is headed.

master production schedule (MPS) Specifies how much of each product is to be produced during the planning period and when that production should occur.

materiality The concept that an auditor should focus on detecting and reporting only those errors, deficiencies, and omissions that could possibly have a significant impact on decisions.

materials requirements planning (MRP) An approach to inventory management that seeks to reduce required inventory levels by improving the accuracy of forecasting techniques to better schedule purchases to satisfy production needs.

materials requisition Authorizes the removal of the necessary quantity of raw materials from the storeroom to the factory location where production operations are to begin.

maximum cardinality The maximum number of instances that an entity can be linked to the other entity in the relationship.

message The data transmitted over a data communication system.

message acknowledgment techniques Techniques that let the sender of an electronic message know that a message was received. They include echo checks, trailer records, and numbered batches.

minimum cardinality The minimum number of instances that an entity can be linked to the other entity in the relationship.

misappropriation of assets See *employee fraud*.

mnemonic code Letters and numbers that are interspersed to identify an item. The mnemonic code is derived from the description of the item and is usually easy to memorize. For example, Dry300W05 could represent a low end (300), white (W) dryer (Dry) made by Whirlpool (05).

modular conversion An approach for converting from an old system to a new system in which parts of the old system are gradually replaced by the new until the old system has been entirely replaced.

monthly statement A document summarizing all transactions that occurred during the past month and informing customers of their current account balance.

move tickets Documents that identify the internal transfer of parts, the location to which they are transferred, and the time of the transfer.

multifactor authentication The use of two or more authentication methods (passwords, ID badges, biometrics, etc.) in conjunction to achieve a greater level of security.

multimodal authentication The use of multiple authentication credentials of the same type to achieve a greater level of security.

mutual authentication scheme A routing verification procedure that requires both computers to exchange their passwords before communication takes place.

N

narrative description Written, step-by-step explanation of system components and how the components interact.

net present value (NPV) A value determined by discounting all estimated future cash flows back to the present, using a discount rate that reflects the time value of money.

network A group of interconnected computers and terminals; a series of locations tied together by communications channels.

network administrator One who installs, manages, and supports a network. The network administrator also controls access to the network and maintains the shared software and data.

network interface card (NIC) The device needed to connect a computer or peripheral to a data communications network.

network managers The people responsible for ensuring that all applicable devices are linked to the organization's internal and external networks and that the networks operate continuously and properly.

neural networks Computing systems that imitate the brain's learning process by using a network of interconnected processors that perform multiple operations simultaneously and interact dynamically. Neural networks recognize and understand voice, face, and word patterns much more successfully than do regular computers and humans.

nonoperational (or throwaway) prototypes Prototypes that are discarded, but the system requirements identified from the prototypes are used to develop a new system.

nonrepudiation Creating legally binding agreements that cannot be unilaterally repudiated by either party. This is done by signing

documents and giving both parties copies. In today's digital world, the same level of nonrepudiation is accomplished by using hashing and asymmetric encryption to create a digital signature.

nonvoucher system A method for processing accounts payable in which each approved invoice is posted to individual vendor records in the accounts payable file and is then stored in an open invoice file. When a check is written to pay for an invoice, the invoice is removed from the open invoice file, marked paid, and stored in the paid invoice file. Contrast with *voucher system*.

normalization The process of following the guidelines for properly designing a relational database that is free from delete, insert, and update anomalies.

O

off-line devices Devices that are not connected to or controlled by a computer or network. Off-line devices are used to prepare data for entry into the computer system (e.g., key-to-tape encoder, key-punch/verification equipment). Contrast with *online devices*.

one-to-many (1:N) relationship A relationship between two entities where one entity in the relationship can be associated with many instances of the other entity in that relationship.

one-to-one (1:1) relationship A relationship between two entities where one entity in the relationship is associated with only one instance of the other entity in the relationship.

online analytical processing (OLAP) Tools that provide access to information stored in a data warehouse by using queries to investigate hypothesized relationships.

online batch processing Processing in which the computer captures data electronically and stores it so that it can be processed later.

online devices Hardware devices that are connected directly to the CPU by a cable or telephone line.

online processing Processing individual transactions as they occur and from their point of origin rather than accumulating them to be processed in batches. Online processing requires the use of online data entry devices and direct access file storage media so that each master record can be accessed directly.

online, real-time processing The computer system processes data immediately after capture and provides updated information to the user on a timely basis.

open-invoice method Method for maintaining accounts receivable in which customers typically pay according to each invoice. Usually, two copies of the invoice are mailed to the customer, who is requested to return one copy with the payment.

operating budget A report that projects an organization's revenues and expenses for a given time period, usually a month or a year.

operating system A software program that controls the overall operation of a computer system. Its functions include controlling the execution of computer programs, scheduling, debugging, assigning storage areas, managing data, and controlling input and output.

operational audit See *management audit*.

operational feasibility The dimension of feasibility concerned with whether a proposed system will be used by the people in an organization. It also is concerned with how useful the system will be within the operating environment of the organization.

operational prototypes Prototypes that are further developed into fully functional systems.

operations and maintenance The last phase of the system development life cycle where follow-up studies are conducted to detect and correct design deficiencies. Minor modifications will be made as problems arise in the new system.

operations list A document that specifies the labor and machine requirements needed to manufacture a product. It indicates how a product moves through the factory, specifying what is done at each step and how much time each operation should take.

operations objectives Objectives that deal with the effectiveness and efficiency of company operations, such as performance and profitability goals and safeguarding assets.

opportunity The condition or situation that allows a person or organization to commit and conceal a dishonest act and convert it to personal gain.

Optical Character Recognition (OCR) The use of light-sensitive hardware devices to convert characters readable by humans into computer input. Because OCR readers can read only certain items, a special machine-readable font must be used.

ordering costs All expenses associated with processing purchase transactions.

output The information produced by a system. Output is typically produced for the use of a particular individual or group of users.

output controls Controls that regulate system output.

outsourcing Hiring an outside company to handle all or part of the data processing activities.

P

packet sniffers Programs that capture data from information packets as they travel over the Internet or company networks. Captured data is sifted to find confidential or proprietary information that can be sold or otherwise used.

packing slip A document listing the quantity and description of each item included in a shipment.

parallel conversion A systems conversion approach in which the new and old systems are run simultaneously until the organization is assured that the new system is functioning correctly.

parallel simulation An approach auditors use to detect unauthorized program changes and data processing accuracy. The auditor writes his or her own version of a program and then reprocesses data. The output of the auditor's program and the client's program are compared to verify that they are the same.

parity bit An extra bit added to a byte and magnetized as needed to ensure that there is always an odd (or even) number of magnetized bits. The computer uses the odd (or even) parity scheme to check the accuracy of each item of data.

parity checking Process in which a computer, as it reads or receives a set of characters, verifies that the proper number of magnetized bits is in each character received. If not, the corresponding character may contain an error.

password A series of letters, numbers, or both that must be entered to access and use system resources. Password use helps prevent unauthorized tampering with hardware, software, and the organization's data.

password cracking Occurs when an intruder penetrates a system's defenses, steals the file containing valid passwords, decrypts them, and uses them to gain access to system resources such as programs, files, and data.

- patch** Code released by software developers that fixes a particular vulnerability.
- patch management** The process of regularly applying patches and updates to software.
- payback period** The number of years required for the net savings to equal the initial cost of an investment.
- payroll clearing account** A general ledger account used to check the accuracy and completeness of recording payroll costs and their subsequent allocation to appropriate cost centers.
- payroll register** A listing of payroll data for each employee for a payroll period.
- payroll service bureau** An organization that maintains the payroll master file for each of its clients and performs their payroll processing activities for a fee.
- penetration test** An authorized attempt to break into the organization's information system.
- performance evaluations** A project development control that requires evaluating each module or task as it is completed.
- performance objectives** The overall performance goals that an entity wishes to achieve.
- performance report** A report that compares standard, or expected, performances with actual performance and also shows the variances, or differences, between the two. Used for financial control. Contrast with *budget*.
- peripherals** The hardware devices (input, output, processing, and data communications) that are connected to a CPU.
- personal identification number (PIN)** A confidential code that allows an individual to gain access to a system and the data or resources stored in that system.
- phase-in conversion** See *modular conversion*.
- phishing** Sending an e-mail pretending to be a legitimate company, usually a financial institution, and requesting information. The recipient is asked to either respond to the e-mail request or visit a Web page and submit data. The request is bogus, and the information gathered is used to commit identity theft or to steal funds from the victim's account.
- phreaker** A hacker who attacks phone systems.
- physical access** Ability to physically use computer equipment.
- physical design** A phase of the system development life cycle where the broad, user-oriented requirements of the conceptual design are implemented by creating a detailed set of specifications that are used to code and test the computer programs.
- physical model** The description of how a system functions by describing the flow of documents, the computer processes performed and the people performing them, the equipment used, and other physical elements of the system.
- physical systems design** The phase of the systems development life cycle in which the designer specifies the hardware, software, and procedures for delivering the conceptual systems design.
- physical systems design report** A report prepared at the end of the physical design phase that describes the system and summarizes what was accomplished. Management uses this report to decide whether or not to proceed to the implementation phase.
- physical view** The way data are physically arranged and stored in the computer system. Contrast with *logical view*.
- picking ticket** A document authorizing the inventory control function to release merchandise to the shipping department. The picking ticket is often printed so that the item numbers and quantities are listed in the sequence in which they can be most efficiently retrieved from the warehouse.
- piggybacking** When a perpetrator latches onto a user who is logging in to a system. The legitimate user unknowingly carries the perpetrator with him into the system.
- pilot conversion** The implementation of a system in part of the organization, such as a branch location. This localizes conversion problems and allows training in a live environment. Disadvantages are the long conversion times and the need to interface the old system with the new system.
- plaintext** Normal text that has not been encrypted.
- podslurping** Using a small device with storage capacity (iPod, flash drive) to download unauthorized data from a computer.
- point-of-sale (POS) devices** Electronic devices used to record sales information at the time of the sale and to perform other data processing functions.
- point scoring** An objective procedure in which weighted selection criteria are used to evaluate the overall merits of vendor proposals.
- policies** The rules that provide a formal direction for achieving performance objectives and that enable performance.
- policy and procedures manual** A management tool for assigning authority and responsibility. It explains proper business practices, describes the knowledge and experience needed by key personnel, spells out management policy for handling specific transactions, and documents the systems and procedures employed to process those transactions.
- post-implementation review** Review made after a new system has been operating for a brief period. The purpose is to ensure that the new system is meeting its planned objectives, to identify the adequacy of system standards, and to review system controls.
- post-implementation review report** A report that analyzes a newly delivered system to determine if the system achieved its intended purpose and was completed within budget.
- preformatting** An online data entry control in which the computer displays a form on the screen and the user fills in the blanks on the form as needed.
- pressure** A person's incentive or motivation for committing fraud.
- preventive controls** Controls that deter problems before they arise. Effective preventive controls include hiring qualified accounting personnel; appropriately segregating employee duties; and effectively controlling physical access to assets, facilities, and information.
- preventive maintenance** A program of regularly examining the hardware components of a computer and replacing any that are found to be weak.
- primary activities** Activities in the value chain that are performed to create, market, and deliver products and services to customers and provide post-delivery service and support. Primary activities include production, shipping and receiving, and marketing.
- primary key** The attribute, or combination of attributes, that uniquely identifies a row in a database table. The primary key is used to distinguish, order, and reference records in a database.
- private key system** An encryption system in which both the sender and the receiver have access to the key but do not allow others access to the same key.

process A set of actions, automated or manual, that transform data into other data or information.

process costing A cost system that assigns costs to each process, or work center, in the production cycle, and then calculates the average cost for all units produced. Process costing is used when masses of similar goods or services are produced or sold.

processing controls Controls that ensure that all transactions are processed accurately and completely and that all files and records are properly updated.

processing test transactions Running hypothetical transactions through a new system to test for processing errors.

procurement card A corporate credit card that employees can use to purchase specific kinds of items.

production cycle The recurring set of business activities and related data processing operations associated with the manufacture of products.

production order A document authorizing the manufacture of a specified quantity of a particular product. It lists the operations to be performed, the quantity to be produced, and the location to which the finished product is to be delivered.

professional employer organization (PEO) An organization that processes payroll and also provides human resource management services such as employee benefit design and administration.

program A set of instructions that can be executed by a computer.

program evaluation and review technique (PERT) A commonly used technique for planning, coordinating, controlling, and scheduling complex projects such as systems implementation.

program flowchart A diagrammatical representation of the sequence of logical operations performed by a computer in executing a program. A program flowchart describes the specific logic to perform a process shown on a system flowchart.

program maintenance The revision of a computer program to meet new program instructions, satisfy system demands such as the need for a new report, correct an error, or make changes in file content.

programmer The person who takes the design provided by systems analysts and creates an information system by writing the computer programs.

programming The process of writing software programs to accomplish a specific task or set of tasks.

program tracing A technique used to obtain detailed knowledge of the logic of an application program as well as to test the program's compliance with its control specifications.

project development plan A document that shows how a project will be completed, including the modules or tasks to be performed and who will perform them, the dates they should be completed, and project costs.

project development team A group of people consisting of specialists, management, and users that develop a project's plan and direct the steps of the systems development life cycle. The team monitors costs, progress, and employees, and also gives status reports to top management and to the steering committee.

projection A way of resisting change by blaming anything and everything on the new system. The system becomes the scapegoat for all real and imagined problems and errors.

project milestones Significant points in a development effort where a formal review of progress is made.

prompting An online data entry control that uses the computer to control the data entry process. The system requests each required item of input data and then waits for an acceptable response before requesting the next required item.

proposal to conduct systems analysis A document calling for the analysis of either an existing or a proposed system. This document is prepared by a user or department and requests the information systems function to analyze the feasibility of developing a system to perform a specific function.

protocol The set of rules governing the exchange of data between two systems or components of a system.

prototype A simplified working model of an information system.

prototyping An approach to systems design in which a simplified-working model, or prototype, of an information system is developed. The users experiment with the prototype to determine what they like and do not like about the system. The developers make modifications until the users are satisfied with the system.

Public Company Accounting Oversight Board (PCAOB) A five-member board that regulates the auditing profession. The PCAOB was created as part of the Sarbanes-Oxley Act, and its members are appointed and overseen by the SEC.

public key infrastructure (PKI) An approach to encryption that uses two keys: a public key that is publicly available and a private key that is kept secret and known only by the owner of that pair of keys. With PKI, either key (the public or private) can be used to encode a message, but only the other key in that public-private pair can be used to decode that message.

purchase order A document that formally requests a vendor to sell and deliver specified products at designated prices. It is also a promise to pay and becomes a contract once the vendor accepts it.

purchase requisition A document or electronic form that identifies the requisitioner; specifies the delivery location and date needed; identifies the item numbers, descriptions, quantity, and price of each item requested; and may suggest a vendor.

Q

query A request for specific information from a computer. When the information is found, it is retrieved, displayed, or analyzed as requested. Queries are often used with a database management system to extract data from the database.

query-by-example (QBE) languages Graphical query languages for retrieving information from a relational database.

query languages Languages used to process data files and to obtain quick responses to questions about those files.

R

random access memory (RAM) A temporary storage location for computer instructions and data.

range check An edit check designed to verify that a data item falls within a certain predetermined range of acceptable values.

ransomware Software that encrypts programs and data until a ransom is paid to remove it.

rationalization The excuse that fraud perpetrators use to justify their illegal behavior.

- REA data model** A data model used to design AIS databases. It contains information about three fundamental objects: resources, events, and agents. Resources represent identifiable objects that have economic value to the organization. Events represent an organization's business activities. Agents represent the people or organizations about which data are collected.
- real-time notification** A variation of the embedded audit module in which the auditor is notified of each transaction as it occurs by means of a message printed on the auditor's terminal.
- real-time system** A system that is able to respond to an inquiry or provide data fast enough to make the information meaningful to the user. Real-time systems are usually designed for very fast response.
- reasonable assurance** The concept that an auditor cannot obtain complete assurance that information is correct, because to do so would be prohibitively expensive. Instead, the auditor accepts a reasonable degree of risk that the audit conclusion is incorrect.
- reasonableness test** An edit check of the logical correctness of relationships among data items. For example, a journal entry that debits inventory and credits wages payable is not reasonable.
- receiving report** A document that records details about each delivery, including the date received, shipper, vendor, quantity received.
- record** A set of logically related data items that describe specific attributes of an entity, such as all payroll data relating to a single employee.
- record count** A total of the number of input documents in a process or the number of records processed at a given time.
- record layout** A document that illustrates the arrangement of items of data in input, output, and file records.
- recovery point objective (RPO)** The length of time between the last backup and the time that an incident occurred. The RPO represents the period of time for which management is willing to have to reenter data about past transactions.
- recovery procedures** A set of procedures that is followed if the computer quits during data processing. The procedures allow the user to recover from hardware or software failures.
- recovery time objective (RTO)** The time by which the organization's information system must be available again following a disaster.
- redundant arrays of independent drives (RAID)** Writing data to multiple disk drives simultaneously so that if one disk drive fails the data can be readily accessed from another.
- redundant data check** An edit check that requires the inclusion of two identifiers in each input record (e.g., the customer's account number and the first five letters of the customer's name). If these input values do not match those on the record, the record will not be updated.
- reengineering** See *business process reengineering*.
- referential integrity rule** A constraint in relational database design requiring that any non-null value of a foreign key must correspond to a primary key in the referenced table. For example, if vendor number is a foreign key in the inventory table, to indicate the preferred source of that item, then any vendor number appearing in that table must appear as a primary key value in the vendor table. This constraint ensures consistency in the database. Note, however, that the foreign key can be null, if there is no existing relationship between the two tables. For example, a null value for vendor number in any row in the inventory table would indicate that there is no preferred vendor for that inventory item.
- relational data model** A database model in which all data elements are logically viewed as being stored in two-dimensional tables called *relations*. In these tables each row represents a unique entity or record. Each column represents a field where the record's attributes are stored. The tables serve as the building blocks from which data relationships can be created.
- relational database** A database management system that uses the relational data model developed by Dr. E. F. Codd in 1970.
- remittance advice** An enclosure included with a customer's payment that indicates the invoices, statements, or other items paid.
- remittance list** A document listing all checks received in the mail.
- Remote Authentication Dial-In User Service (RADIUS)** A standard method for verifying the identity of users attempting to connect via dial-in access. Users connect to a remote access server and submit their login credentials. The remote access server passes those credentials to the RADIUS server, which performs compatibility tests to authenticate the identity of that user.
- remote batch processing** Accumulating transaction records in batches at some remote location and then transmitting them electronically to a central location for processing.
- reorder point** The level to which the inventory balance of an item must fall before an order to replenish stock is initiated.
- report** System output organized in a meaningful fashion. Used by employees to control operational activities, by managers to make decisions and design strategies, and by investors and creditors to gather information about a company's business activities. Prepared for both internal and external use.
- reporting objectives** Objectives to help ensure the accuracy, completeness, and reliability of internal and external company reports, of both a financial and nonfinancial nature. They also improve decision making and monitor company activities and performance more efficiently.
- report writers** A language that simplifies report creation. Typically, users need specify only which data elements they want printed and how the report should be formatted. The report writer searches the database, extracts the specified data items, and prints them according to the user-specified format.
- reprocessing** An approach auditors use to detect unauthorized program changes. The auditor verifies the integrity of an application program and then saves it for future use. At subsequent intervals, and on a surprise basis, the auditor uses the previously verified version of the program to reprocess transaction data. The output of the two runs is compared and discrepancies are investigated.
- request for proposal (RFP)** A request by an organization or department for vendors to bid on hardware, software, or services.
- request for systems development** A written request for a new or improved system. The request describes the current system's problems, why the change is needed, and the proposed system's goals and objectives as well as its anticipated benefits and costs.
- requirements costing** A system evaluation method in which a list is made of all required features. If a proposed system does not have a desired feature, the cost of developing or purchasing that feature is added to the basic cost of the system. This method allows different systems to be compared and evaluated based on the costs of providing the required features.
- residual risk** The risk that remains after management implements internal controls or some other form of response to risk.
- resources** Those things that have economic value to an organization such as cash, inventory, supplies, factories, and land.

response time The amount of time that elapses between making a query and receiving a response.

responsibility accounting A system of reporting financial results on the basis of managerial responsibilities within an organization.

restoration The process of installing the backup copy of a database or file for use in data processing.

revenue cycle The recurring set of business activities and data processing operations associated with providing goods and services to customers and collecting cash in payment for those sales.

risk The likelihood that a threat or hazard will actually come to pass.

risk appetite The amount of risk a company is willing to accept to achieve its goals and objectives.

rollback A process whereby a log of all pre-update values is prepared for each record that is updated within a particular interval. If there is a system failure, the records can be restored to the pre-update values and the processing restarted.

round-down technique A fraud technique used in financial institutions that pay interest. The programmer instructs the computer to round down all interest calculations to two decimal places. The fraction of a cent rounded down on each calculation is put into the programmer's own account.

routers Special purpose devices that are designed to read the destination address fields in IP packet headers to decide where to send (route) the packet next.

routing verification procedures Controls to ensure that messages are not routed to the wrong system address. Examples are header labels, mutual authentication schemes, and dial-back.

run-to-run totals Comparison of the new balance of an updated general ledger account to its prior balance plus the sum of all current period debits and credits.

S

sabotage An intentional act where the intent is to destroy a system or some of its components.

salami technique A fraud technique in which tiny slices of money are stolen from many different accounts.

sales invoice A document notifying customers of the amount of a sale and where to send payment.

sales order The document created during sales order entry listing the item numbers, quantities, prices, and terms of the sale.

Sarbanes-Oxley Act (SOX) A law passed by Congress in 2002. SOX applies to publicly held companies and their auditors and is intended to prevent financial statement fraud, make financial reports more transparent, provide protection to investors, strengthen the internal controls at public companies, and punish executives who perpetrate fraud.

scanning routines Software routines that search a program for the occurrence of a particular variable name or other combinations of characters.

scareware Malicious software of no benefit that is sold using scare tactics.

scavenging Searching for corporate or personal records to gain unauthorized access to confidential information. Scavenging methods include searching garbage cans, communal trash bins, and city dumps to find documents with confidential information.

scheduled reports Reports that are generated by a system at specified time intervals.

scheduling feasibility The dimension of feasibility that determines if the system being developed can be implemented in the time allotted.

schema (1) A description of the data elements in a database, the relationships among the data elements, and the structure or overall logical model used to organize and describe the data. (2) An XBRL file that defines every element that appears in a specific instance document.

secondary key A field that can be used to identify records in a file. Unlike the primary key, it does not provide a unique identification.

security management Ensures that all aspects of the system are secure and protected from all internal and external threats.

segregation of accounting duties Separating the accounting functions of authorization, custody, and recording so as to minimize an employee's ability to commit fraud.

segregation of duties The separation of assigned duties and responsibilities in such a way that no single employee can both perpetrate and conceal errors or irregularities.

segregation of systems duties Implementing control procedures to clearly divide authority and responsibility within the information system function to prevent employees from perpetrating and concealing fraud.

sequence check An edit check that determines if a batch of input data is in the proper numerical or alphabetical sequence.

sequence codes Documents are numbered consecutively to account for them. Gaps in the sequence code indicate missing documents that should be investigated. Examples of documents that are given sequence codes include prenumbered checks, invoices, and purchase orders.

sequential access An access method that requires data items to be accessed in the same order in which they were written.

sequential file A way of storing numeric or alphabetical records according to a key (e.g., customer numbers from 00001 to 99999). To access a sequential file record, the system starts at the beginning of the file and reads each record until the desired record is located.

sequential file processing Processing a master file sequentially from beginning to end. The master and transaction files are processed in the same predetermined order, such as alphabetically.

server High-capacity computer that contains the network software to handle communications, storage, and resource-sharing needs of other computers in the network. The server also contains the application software and data common to all users.

sexting Exchanging sexually explicit text messages and pictures with other people by means of a phone.

shoulder surfing Watching people enter telephone calling card or credit card numbers or listening as they give credit card numbers over the telephone or to a clerk.

sign check An edit check that verifies that the data in a field have the appropriate arithmetic sign.

size check An edit check that ensures the input data will fit into the assigned field.

smart cards Plastic cards containing a microprocessor, memory chips, and software that can store up to three pages of text. Used in Europe as a credit or ATM card.

SMS spoofing Using short message service (SMS) to change the name or number a text message appears to come from.

- snapshot technique** An audit technique that records the content of both a transaction record and a related master file record before and after each processing step.
- social engineering** Using deception to obtain unauthorized access to information resources. Access is usually obtained by fooling an employee.
- software agents** Computer programs that learn how to do often-performed, tedious, time consuming, or complex tasks.
- software piracy** The unauthorized copying of software.
- source code (or source program)** A computer program written in a programming language that is translated into the object (machine language) program by a translation program such as a compiler or assembler.
- source code comparison program** Compares the current version of a program with the source code of the program. If no changes were authorized, the two versions should be identical and any differences should be investigated. If the difference is an authorized change, auditors examine program change specifications to ensure that the changes were authorized and correctly incorporated.
- source data automation (SDA)** The collection of transaction data in machine-readable form at the time and place of origin. Examples of SDA devices are optical scanners and ATMs.
- source documents** Contain the initial record of a transaction that takes place. Examples of source documents, which are usually recorded on preprinted forms, include sales invoices, purchase orders, and employee time cards. Contrast with *operational document*.
- spamming** Simultaneously e-mailing the same unsolicited message to many people, often in an attempt to sell them some product.
- special-purpose analysis reports** Reports that have no prespecified content or format and are not prepared according to any regular schedule; rather, they are generally prepared in response to a management request to investigate a specific problem or opportunity.
- specialized journals** Journals where large numbers of repetitive transactions—such as credit sales, cash receipts, purchases on account, and cash disbursements—are recorded.
- specific authorization** Special approval an employee needs in order to be allowed to handle a transaction.
- spoofing** Altering something, such as an e-mail message, to make it look as if someone else sent it.
- spyware** Software that monitors computing habits and sends the data to someone else, often without the computer user's permission.
- SQL injection (insertion)** Inserting a malicious SQL query in input in such a way that it is passed to and executed by an application program.
- standards** The required procedures implemented to meet the policies.
- stateful packet filtering** A technique employed by firewalls in which a table is maintained that lists all established connections between the organization's computers and the Internet. The firewall consults this table to determine whether an incoming packet is part of an ongoing communication initiated by an internal computer.
- static packet filtering** A process that screens individual IP packets based solely on the contents of the source and/or destination fields in the IP packet header.
- steering committee** An executive-level committee to plan and oversee the information systems function. The committee typically consists of management from the systems department, the controller, and other management affected by the information systems function.
- strategic master plan** An organization's multiple-year plan that serves as a technological road map and lays out the projects the company must complete to achieve its long-range goals.
- strategic objectives** High-level goals that are aligned with and support the company's mission.
- strategic planning** Decisions that establish the organization's objectives and policies for accomplishing those objectives.
- structured programming** A modular approach to programming in which each module performs a specific function and is coordinated by a control module.
- structured query language (SQL)** A text-based query language provided by most relational database management systems. Powerful queries can be built using basic keywords such as: SELECT, FROM, and WHERE.
- structured relationships** Relationships in program design in which every event entity is linked to a resource entity and two agent entities.
- structured walkthrough** A formal program design review process. One or more programmers walk through another programmer's logic and code to detect weaknesses and errors in program design.
- style sheet** An XBRL file that provides instructions on how to display (render) an instance document on either a computer screen or printed report.
- subschema** (1) A subset of the schema that includes only those data items used in a particular application program or by a particular user. (2) The way the user defines the data and the data relationships.
- subsidiary ledgers** Ledgers used to record the detailed data for any general ledger account that has many individual subaccounts. Subsidiary ledgers are commonly used for accounts receivable, inventory, fixed assets, and accounts payable.
- subsystems** Smaller systems that are a part of the entire information system. Each subsystem performs a specific function that is important to and that supports the system of which it is a part.
- superzapping** The unauthorized use of a special system program to bypass regular system controls and perform illegal acts. The superzap utility was originally written to handle emergencies, such as restoring a system that had crashed.
- supply chain** An extended system that includes an organization's value chain as well as its suppliers, distributors, and customers.
- support activities** Activities in the value chain that enable the primary activities to be performed efficiently and effectively. Examples include administration, purchasing, and human resources.
- symmetric encryption systems** Encryption systems that use the same key both to encrypt and to decrypt.
- synchronous transmission** Data transmission in which start and stop bits are required only at the beginning and end of a block of characters. Contrast with *asynchronous transmission*.
- syntax errors** Errors that result from using the programming language improperly or from incorrectly typing the source program.
- system** (1) An entity consisting of two or more components or subsystems that interact to achieve a goal. (2) The equipment and programs that comprise a complete computer installation. (3) The programs and related procedures that perform a single task on a computer.
- system control audit review file (SCARF)** A concurrent audit technique that embeds audit modules into application software to continuously monitor all transaction activity and collect data on transactions having special audit significance.

system flowchart A diagrammatical representation that shows the flow of data through a series of operations in an automated data processing system. It shows how data are captured and put into the system, the processes that operate on the data, and system outputs.

system performance measurements Measurements used to evaluate and assess a system. Common measurements include throughput (output per unit of time), utilization (percentage of time the system is being productively used), and response time (how long it takes the system to respond).

system review A step in internal control evaluation in which it is determined if the necessary control procedures have been prescribed.

systems administrator Ensures that an information system operates smoothly and efficiently.

systems analysis (1) A rigorous and systematic approach to decision making, characterized by a comprehensive definition of available alternatives and an exhaustive analysis of the merits of each alternative as a basis for choosing the best alternative. (2) Examination of user information requirements in an organization to establish objectives and specifications for the design of an information system.

systems analysis report Comprehensive report prepared at the end of the systems analysis and design phase that summarizes and documents the findings of analysis activities.

systems analysts The people who help users determine their information needs and then design an information system to meet those needs.

systems design The process of preparing detailed specifications for the development of a new information system.

systems development life cycle (SDLC) Five processes a company goes through when it decides to design and implement a new system. The five steps are systems analysis, conceptual design, physical design, implementation and conversion, and operation and maintenance.

systems documentation A complete description of all aspects of each systems application, including narrative material, charts, and program listings.

systems implementation The task of delivering a completed system to an organization for use in day-to-day operations.

systems integrator A vendor who uses common standards and manages a cooperative systems development effort involving its own development personnel and those of the client and other vendors.

systems software Software that interfaces between the hardware and the application program. Systems software includes operating systems, database management systems, utility programs, language translators, and communications software.

systems survey The systematic gathering of facts relating to the existing information system. A systems analyst generally carries out this task.

systems survey report The culmination of the systems survey. It contains documentation such as memos; interview and observation notes; questionnaire data; file and record layouts and descriptions; input and output descriptions; and copies of documents, flowcharts, and data flow diagrams.

T

tagging An audit procedure in which certain records are marked with a special code before processing. During processing, all data relating to the marked records are captured and saved so that the auditors can verify them later.

taxonomy A set of XBRL files that defines elements and the relationships among them.

technical feasibility The dimension of feasibility concerned with whether a proposed system can be developed given the available technology.

terminal An input/output device for entering or receiving data directly from the computer.

test data Data that have been specially developed to test the accuracy and completeness of a computer program. The results from the test data are compared with hand-calculated results to verify that the program operates properly.

test data generator program A program that takes the specifications describing the logic characteristics of the program to be tested and automatically generates a set of test data that can be used to check the logic of the program.

test of control A test whose objective it is to determine whether control procedures are being followed correctly.

threats Any potential adverse occurrence or unwanted event that could be injurious to either the AIS or the organization. Also referred to as an *event*.

throughput (1) The total amount of useful work performed by a computer system during a given period of time. (2) A measure of production efficiency representing the number of "good" units produced in a given period of time.

time-based model of security Implementing a set of preventive, detective, and corrective controls that enable an organization to recognize that an attack is occurring and take steps to thwart it before any assets have been compromised.

time card A document that records the employee's arrival and departure times for each work shift. The time card records the total hours worked by an employee during a pay period.

time sheet A data entry screen (or paper document) used by salaried professionals to record how much time was spent performing various tasks for specific clients.

trailer label (record) Type of internal label that appears at the end of each file and serves as an indicator that the end of the file has been reached. The trailer label contains the batch totals calculated during input.

transaction An agreement between two entities to exchange goods or services. Any exchange that can be measured in economic terms by an organization.

transaction cycles A group of related business activities (e.g., sales order entry, shipping, billing, and cash receipts constitutes the revenue cycle). The four transaction cycles covered in the text are revenue, expenditure, production, and human resource management/payroll.

transaction file File that contains the individual business transactions that occur during a specific fiscal period. A transaction file is conceptually similar to a journal in a manual AIS.

transaction log A detailed record of every transaction entered in a system.

transaction processing A process that begins with capturing transaction data and ends with an informational output.

transcription error An error in which a digit of a number is written incorrectly (e.g., a 4 in the tens position transcribed as a 9, which would cause an error of 50 in the value of the number).

Transmission Control Protocol/Internet Protocol (TCP/IP) The protocol enabling communications on the Internet. It creates what

is called a packet-switching network. When a message is ready to be sent over the Internet, the TCP breaks it up into small packets. Each packet is then given a header, which contains the destination address, and the packets are then sent individually over the Internet. The IP uses the information in the packet header to guide the packets so that they arrive at the proper destination. Once there, the TCP reassembles the packets into the original message.

transposition error An error that results when numbers in two adjacent columns are inadvertently exchanged (for example, 64 is written as 46).

trap door A set of computer instructions that allows a user to bypass the system's normal controls.

trial balance A report listing the balances of all general ledger accounts. It is so named because one of its purposes is to allow the accountant to verify that the total debit balances in various accounts equal the total credit balances in other accounts.

triggered exception reports Preformatted reports generated only when certain conditions exist (e.g., the amount of raw materials on hand falls below the safety stock amount). The reports bring the information about the existing conditions to the attention of a decision maker.

Trojan horse A set of unauthorized computer instructions in an authorized and otherwise properly functioning program. It performs some illegal act at a preappointed time or under a predetermined set of conditions.

tuple (rhymes with *couple*). A row in a relation. A tuple contains data about a specific occurrence in a database table. For example, each row in the inventory table contains all the pertinent data about a particular inventory item.

turnaround document Records of company data sent to an external party and then returned to the system as input. Turnaround documents are prepared in machine-readable form to facilitate their subsequent processing as input records. An example is a utility bill.

turnkey system A system that is delivered to customers ready (theoretically) to be turned on. A turnkey system supplier buys hardware, writes application software that is tailored both to that equipment and to the specific needs of its customers, and then markets the entire system.

U

uninterruptible power supply (UPS) An alternative power supply device that protects against the loss of power and fluctuations in the power level by using battery power to enable the system to operate long enough to back up critical data and safely shut down.

Universal Product Code (UPC) A machine-readable code that is read by optical scanners. The code consists of a series of bar codes and is printed on most products sold in grocery stores.

UNIX A flexible and widely used operating system for 16-bit machines.

update anomaly If attributes that are not characteristics of the primary key of a relation are stored in that table, then that data item is stored in many different rows. For example, if customer addresses are stored in the sales invoice table, then the address for a given customer is stored many times (once for each sale). Consequently, if the value of that data item is not changed in every row in which it is stored, inconsistencies in the database will result.

updating Changing stored data to reflect more recent events (e.g., changing the accounts receivable balance because of a recent sale or collection).

user ID A knowledge identifier, such as an employee number or account number, that users enter to identify themselves when signing on to a system.

user identification (ID) and authentication system A system that requires users to identify themselves by entering a unique user ID when they sign on to the system.

users People who interact with the system. Users are those who record data, manage the system, and control the system's security. Those who use information from the system are end users.

utility programs A set of prewritten programs that perform a variety of file and data-handling tasks (e.g., sorting or merging files) and other housekeeping chores.

utilization The percentage of time a system is being productively used.

V

validity check An edit test in which an identification number or transaction code is compared with a table of valid identification numbers or codes maintained in computer memory.

value-added network (VAN) A public network that adds value to the data communications process by handling the difficult task of interfacing with the multiple types of hardware and software used by different companies.

value chain The linking together of all the primary and support activities in a business. Value is added as a product passes through the chain.

value of information The benefit produced by the information minus the cost of producing it.

value system The combination of several value chains into one system. A value system includes the value chains of a company, its suppliers, its distributors, and its customers.

vendor-managed inventory (VMI) Practice in which manufacturers and distributors manage a retail customer's inventory using EDI. The supplier accesses its customer's point-of-sale system in order to monitor inventory and automatically replenish products when they fall to agreed-upon levels.

virtualization Taking advantage of the power and speed of modern computers to run multiple systems simultaneously on one physical computer. This reduces the number of servers needed and thereby reduces hardware, maintenance, and data center costs.

virtual private network (VPN) A network that controls access to an extranet using encryption and authentication technology.

virus A segment of executable code that attaches itself to an application program or some other executable system component. When the hidden program is triggered, it makes unauthorized alterations to the way a system operates.

voucher A document that summarizes the data relating to a disbursement and represents final authorization of payment.

voucher package The set of documents used to authorize payment to a vendor. It consists of a purchase order, receiving report, and vendor invoice.

voucher system A method for processing accounts payable in which a disbursement voucher is prepared instead of posting invoices directly to vendor records in the accounts payable subsidiary ledger. The disbursement voucher identifies the vendor, lists the outstanding invoices, and indicates the net amount to be paid after

deducting any applicable discounts and allowances. Contrast with *nonvoucher system*.

vulnerabilities Flaws in programs that can be exploited to either crash the system or take control of it.

vulnerability scans Automated tools designed to identify whether a given system possesses any well-known vulnerabilities. The scanning tool can also identify unused and unnecessary programs that represent potential security threats. The process of identifying and turning off unnecessary programs is called *hardening*.

W

walk-throughs Meetings, attended by those associated with a project, in which a detailed review of systems procedures and/or program logic is carried out in a step-by-step manner.

war dialing Searching for an idle modem by programming a computer to dial thousands of phone lines. Finding an idle modem often enables a hacker to gain access to the network to which it is connected.

war driving The practice of looking for unprotected home or corporate wireless networks.

Web cramming Developing a free and worthless trial-version Web site and charging the phone bill of the consumer for months even if the consumer cancels.

Web-page spoofing See *phishing*.

white-collar criminals Typically, businesspeople who commit fraud. White-collar criminals usually resort to trickery or cunning, and their crimes usually involve a violation of trust or confidence.

wide area network (WAN) A telecommunications network that covers a large geographic area anywhere in size from a few cities to the whole globe. A WAN uses telephone lines, cables, microwaves, or satellites to connect a wide variety of hardware devices in many different locations.

wiretap To listen in (eavesdrop) on an unprotected communications line.

worm Similar to a virus, except that it is a program rather than a code segment hidden in a host program. A worm also copies itself automatically and actively transmits itself directly to other systems.

X

XBRL eXtensible Business Reporting Language is a variant of XML (eXtensible Markup Language) specifically designed for use in communicating the content of financial data. It does this by creating tags for each data item that look much like the tags used by HTML.

Z

zero-balance check An internal check that requires the balance of an account to be zero after all entries to it have been made.