Chapter 7
Securing Information Systems

LEARNING TRACK 4: GENERAL AND APPLICATION CONTROLS FOR INFORMATION SYSTEMS

To minimize errors, disaster, computer crime, and breaches of security, special policies and procedures must be incorporated into the design and implementation of information systems. The combination of manual and automated measures that safeguard information systems and ensure that they perform according to management standards is termed controls. **Controls** consist of all the methods, policies, and organizational procedures that ensure the safety of the organization's assets, the accuracy and reliability of its accounting records, and operational adherence to management standards.

controls All the methods, policies, and procedures that ensure protection of the organization's assets, accuracy and reliability of its records, and operational adherence to management standards

In the past, the control of information systems was treated as an afterthought, addressed only toward the end of implementation, just before the system was installed. Today, however, organizations are so critically dependent on information systems that vulnerabilities and control issues must he identified as early as possible. The control of an information system must be an integral part of its design. Users and builders of systems must pay close attention to controls throughout the system's life span.

Computer systems are controlled by a combination of general controls and application controls.

General controls are those that control the design, security, and use of computer programs and the security of data files in general throughout the organization. On the whole, general controls apply to all computerized applications and consist of a combination of system software and manual procedures that create an overall control environment.

general controls Overall controls that establish a framework for controlling the design, security, and use of computer programs throughout an organization

Application controls are specific controls unique to each computerized application, such as payroll, accounts receivable, and order processing. They consist of both controls applied from the user functional area of a particular system and from programmed procedures.

application controls Specific controls unique to each computerized application

GENERAL CONTROLS

General controls are overall controls that ensure the effective operation of programmed procedures. They apply to all application areas. General controls include the following:

- Controls over the system implementation process
- Software controls
- Physical hardware controls
- Computer operations controls
- Data security controls
- Administrative controls

Implementation Controls

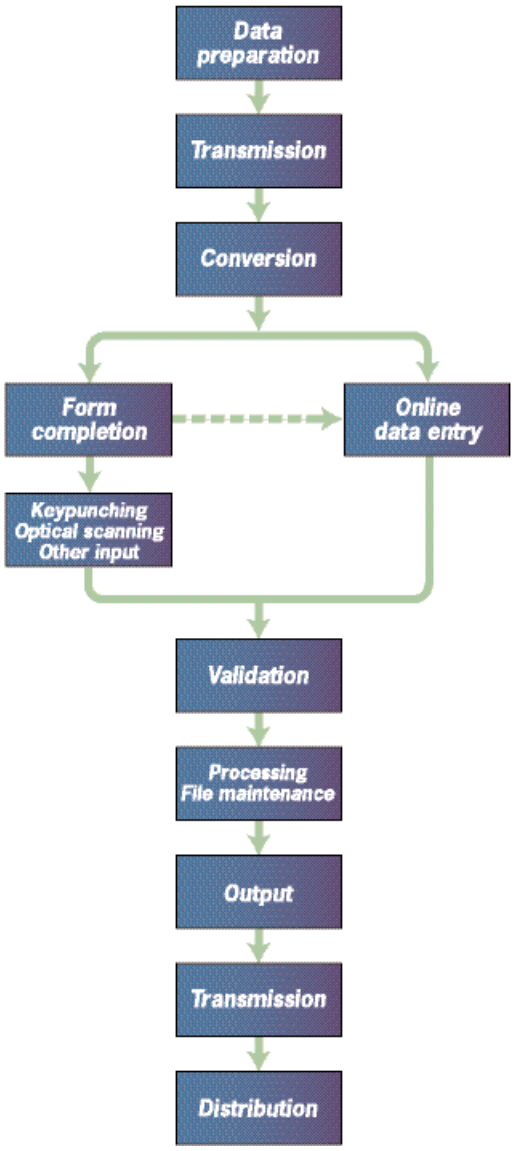
Implementation controls audit the systems development process at various points to ensure that the process is properly controlled and managed. The systems development audit should look for the presence of formal review points at various stages of development that enable users and management to approve or disapprove the implementation.

Implementation controls Audit of the systems development process at various points to make sure that it is properly controlled and managed

The systems development audit should also examine the level of user involvement at each stage of implementation and check for the use of a formal cost/benefit methodology in establishing system feasibility. The audit should also look for the use of controls and quality assurance techniques for program development, conversion, and testing.

FIGURE 1

Points in the processing cycle where errors can occur. Each of the points illustrated in this figure represents a control point where special automated and/or manual procedures should be established to reduce the risk of errors during processing.



An important though frequently neglected requirement of systems building is appropriate documentation. Without good documentation that shows how a system operates from both a technical and a user standpoint, an information system may be difficult, if not impossible, to operate, maintain, or use. Table 1 lists the various pieces of documentation that are normally required to run and maintain an information system. The systems development audit should look for system, user, and operations documentation that conforms to formal standards.

software controls Controls to ensure the security and reliability of software

program security controls Controls designed to prevent unauthorized changes to programs in systems that are already in production

Software Controls

Controls are essential for the various categories of software used in computer systems. **Software controls** monitor the use of system software and prevent unauthorized access of software programs, system software, and computer programs.

System software controls govern the software for the operating system, which regulates and manages computer resources to facilitate execution of application programs. System software controls are also used for compilers, utility programs, reporting of operations, file setup and handling, and library recordkeeping. System software is an important control area because it performs overall control functions for the programs that directly process data and data files. **Program security controls** are designed to prevent unautho-

TABLE 1 ESSENTIAL USER AND TECHNICAL DOCUMENTATION FOR AN INFORMATION SYSTEM

TECHNICAL DOCUMENTATION	*USER DOCUMENTATION*
Hardware/operation system requirements	*Sample reports/output layouts*
File layouts	*Sample input forms/screens*
Record layouts	*Data preparation instructions*
List of programs/modules	*Data input instructions*
Program structure charts	*Instructions for using reports*
Narrative program/module descriptions	*Security profiles*
Source program listings	*Functional description of system*
Module cross references	*Work flows*
Error conditions/actions	*Error correction procedures*
Abnormal termination	*Accountabilities*
Job setup requirements	*Processing procedure narrative*
Job run schedules	*List/description of controls*
Report-output distribution	*Responsible user contact*
Responsible programmer contact	
Job control language listings	
Backup/recovery procedures	
Run control procedures	
File access procedures	

rized changes to programs in systems that are already in production.

Hardware Controls

Hardware controls ensure that computer hardware is physically secure and check for equipment malfunction. Computer hardware should he physically secured so that it can be accessed only by authorized individuals. Access to rooms where computers operate should be restricted to computer operations personnel. Computer terminals in other areas or PCs can be kept in locked rooms. Computer equipment should he specially protected against fires and extremes of temperature and humidity. Organizations that are critically dependent on their computers must also make provisions for emergency backup in case of power failure.

hardware controls Controls to ensure the physical security and correct performance of computer hardware

Many kinds of computer hardware also contain mechanisms that check for equipment malfunction. Parity checks detect equipment malfunctions responsible for altering bits within bytes during processing. Validity checks monitor the structure of on-off hits within bytes to make sure that it is valid for the character set of a particular computer machine. Echo checks verify that a hardware device is performance ready.

Computer Operations Controls

Computer operations controls apply to the work of the computer department and help ensure that programmed procedures are consistently and correctly applied to the storage and processing of data. They include controls over the setup of computer processing jobs, operations software and computer operations, and backup and recovery procedures for processing that ends abnormally.

computer operations controls Procedures to ensure that programmed procedures are consistently and correctly applied to data storage and processing.

Instructions for running computer jobs should be fully documented, reviewed, and approved by a responsible official. Controls over operations software include manual procedures designed to both prevent and detect error. These are comprised of specified operating instructions for system software, restart and recovery procedures, and procedures for specific applications.

Human-operator error at a computer system at the Shell Pipeline Corporation caused the firm to ship 93,000 barrels of crude oil to the wrong trader. This one error cost Shell $2 million. A computer operator at Exxon Corporation headquarters inadvertently erased valuable records about the 1989 grounding of the Exxon Valdez and the Alaskan oil spill that were stored on magnetic tape. Such errors could have been avoided had the companies incorporated tighter operational safeguards.

System software can maintain a system log detailing all activity during processing. This log can he printed for review so that hardware malfunction, abnormal endings, and operator actions can be investigated. Specific instructions for backup and recovery can be developed so that in the event of a hardware or software failure, the recovery process for production programs, system software, and data files does not create erroneous changes in the system.

Data Security Controls

data security controls
Controls to ensure that data files on either disk or tape are not subject to unauthorized access, change or destruction

Data security controls ensure that valuable business data files are not subject to unauthorized access, change, or destruction. Such controls are required for data files when they are in use and when they are being held for storage. It is easier to control data files in batch systems, since access is limited to operators who run the batch jobs. However, on-line and real-time systems are vulnerable at several points. They can be accessed through terminals as well as by operators during production runs.

When data can be input online through a terminal, entry of unauthorized input must be prevented. For example, a credit note could be altered to match a sales invoice on file. In such situations, security can be developed on several levels:

- Terminals can be physically restricted so that they are available only to authorized individuals.

- System software can include the use of passwords assigned only to authorized individuals. No one can log on to the system without a valid password.

- Additional sets of passwords and security restrictions can be developed for specific systems and applications. For example, data security software can limit access to specific files, such as the files for the accounts receivable system. It can restrict the type of access so that only individuals authorized to update these specific files will have the ability to do so. All others will only be able to read the files or will be denied access altogether.

Systems that allow online inquiry and reporting must have data files secured. Figure 2 illustrates the security allowed for two sets of users of an online personnel database with sensitive information such as employees' salaries, benefits, and medical histories. One set of users consists of all employees who perform clerical functions such as inputting employee data into the system. All individuals with this type of profile can update the system but can neither read nor update sensitive fields such as salary, medical history, or earnings data. Another profile applies to a divisional manager, who cannot update the system but can read all employee data fields for his or her division, including medical history and salary. These profiles would be established and maintained by a data security system. A multilayered data security system is essential for ensuring that this information can he accessed only by authorized persons. The data security system illustrated in Figure 2 provides very fine-grained security restrictions, such as allowing authorized personnel users to inquire about all employee information except in confidential fields such as salary or medical history.

Although the security risk of files maintained offline is smaller, such data files on disk or tape can he removed for unauthorized purposes. 'These can he secured in lockable storage areas, with tight procedures so that they are released only for authorized processing. Usage logs and library records can be maintained for each removable storage device if it is labeled and assigned a unique identity number.

SECURITY PROFILE 1

User: Personnel Dept Clerk

Location: Division 1

Employee Identification Codes with This Profile:	00753, 27834, 37665, 44116
Data Field Restrictions	**Type of Access**
All employee data for Division 1 only	Read and Update
• Medical history data	None
• Salary	None
• Pensionable earnings	None

SECURITY PROFILE 2

User: Divisional Personnel Manager

Location: Division 1

Employee Identification Codes with This Profile:	27321
Data Field Restrictions	**Type of Access**
All employee data for Division 1 only	Read Only

FIGURE 2

Security profiles for a personnel system. These two examples represent two security profiles or data security patterns that might be found in a personnel system. Depending upon the security profile, a user would have certain restrictions on access to various systems, locations, or data in an organization.

Administrative Controls

Administrative controls are formalized standards, rules, procedures, and control disciplines to ensure that the organization's general and application controls are properly executed and enforced. The most important administrative controls are (1) segregation of functions, (2) written policies and procedures, and (3) supervision.

administrative controls
Formalized standards, rules, procedures, and disciplines to ensure that the organization's controls are properly executed and enforced

Segregation of functions is a fundamental principle of internal control in any organization. In essence, it means that job functions should be designed to minimize the risk of errors or fraudulent manipulation of the organization's assets. The individuals responsible for operating systems should not be the same ones who can initiate transactions that change the assets held in these systems. Responsibilities for input, processing, and output are usually divided among different people to restrict what each one can do with the system. For example, the individuals who operate the system should not have the authority to initiate payments or to sign checks. A typical arrangement is to have the organization's information systems department responsible for data and program files and end users responsible for initiating input transactions or correcting errors. Within the information systems department, the duties of programmers and analysts are segregated from those of computer equipment operators.

segregation of functions
Principle of internal control to divide responsibilities and assign tasks among people so that job functions do not overlap to minimize the risk of errors and fraudulent manipulation of the organization's assets

Written policies and procedures establish formal standards for controlling information system operations. Procedures must be formalized in writing and authorized by the appropriate level of management. Accountabilities and responsibilities must be clearly specified.

Supervision of personnel involved in control procedures ensures that the controls for an information system are performing as intended. With supervision, weaknesses can be spotted, errors corrected, and deviations from standard procedures identified. Without adequate supervision, the best-designed set of controls may be bypassed, short-circuited, or neglected.

Weakness in each of these general controls can have a widespread effect on programmed procedures and data throughout the organization. Table 2 summarizes the effect

TABLE 2 EFFECT OF WEAKNESS IN GENERAL CONTROLS

WEAKNESS AREA	IMPACT
Implementation controls	*New systems or systems that have been modified will have errors or fail to function as required*
Software controls (program security)	*Unauthorized changes can be made in processing. The organization may not be sure of which programs or systems have been changed.*
Software controls (system software)	*These controls may not have a direct effect on individual applications. Since other general controls depend heavily on system software, a weakness in this area impairs the other general controls*
Physical hardware controls	*Hardware may have serious malfunctions or may break down altogether, introducing numerous errors or destroying computerized records.*
Computer operations controls	*Random errors may occur in a system. (Most processing will be correct but occasionally it may not be.)*
Data file security controls	*Unauthorized changes can be made in data stored in computer systems or unauthorized individuals can access sensitive information.*
Administrative controls	*All of the other controls may not be properly executed or enforced.*

of weaknesses in major general control areas.

APPLICATION CONTROLS

Application controls are specific controls within each separate computer application, such as payroll or order processing. They include both automated and manual procedures that ensure that only authorized data are completely and accurately processed by that application. The controls for each application should take account of the whole sequence of processing, manual and computer, from the first steps taken to prepare transactions to the production and use of final output.

Not all of the application controls discussed here are used in every information system. Some systems require more of these controls than others, depending on the importance of the data and the nature of the application.

Application controls focus on the following objectives:

1. *Completeness of input and update*. All current transactions must reach the computer and be recorded on computer files.

2. *Accuracy of input and update*. Data must be accurately captured by the computer and correctly recorded on computer files.

3. *Validity*. Data must be authorized or otherwise checked with regard to the appropriateness of the transaction. (In other words, the transaction must reflect the right event in the external world. The validity of an address change, for example, refers to whether a transac-

TABLE 3 IMPORTANT EDIT TECHNIQUES

EDIT TECHNIQUE	DESCRIPTION	EXAMPLE
Reasonableness checks	*To be accepted, the data must fall within certain limits set in advance, or they will be rejected.*	*If an order transaction is for 20,000 units and the largest order on record was 50 units, the transaction will be rejected.*
Format checks	*Characteristics of the contents (letter/digit), length, and sign of individual data fields are checked by the system.*	*A nine-position Social Security number should not contain any alphabetic characters.*
Existence checks	*The computer compares input reference data to tables or master files to make sure that valid codes are being used.*	*An employee can have a Fair Labor Standards Act code of only 1, 2, 3, 4, or 5. All other values for this field will be rejected.*
Dependency checks	*The computer checks whether a logical relationship is maintained between the data for the same transaction. When it is not, the transaction is rejected.*	*A car loan initiation transaction should show a logical relationship between the size of the loan, the number of loan repayments, and the size of each installment.*
Check digit	*An extra reference number called a check digit follows an identification code and bears a mathematical relationship to the other digits. This extra digit is input with the data, recomputed by the computer, and the result compared with the one input.*	*A product code with the last position as a check digit, as developed by the Modulus 11 check digit system, can detect user error in transcription or transposition of product information.*

tion actually captured the right address for a specific individual.)

4. *Maintenance*. Data on computer files must continue to remain correct and current.

Application controls can be classified as (1) input controls, (2) processing controls, and (3) output controls.

Input Controls

Input controls check data for accuracy and completeness when they enter the system. There are specific input controls for input authorization, data conversion, data editing, and error handling.

input controls Procedures to check data for accuracy and completeness when they enter the system, including input authorization, data conversion, and edit checks

Input authorization. Input must be properly authorized, recorded, and monitored as source documents flow to the computer. For example, formal procedures can be set up to authorize only selected members of the sales department to prepare sales transactions for an order entry system. Sales input forms might he serially numbered, grouped into batches, and logged so that they can be tracked as they pass from sales units to the unit responsible for inputting them into the computer. The batches may require authorization signatures before they can be entered into the computer.

input authorization Proper authorization, recording, and monitoring of source documents as they enter the computer system

Data conversion. input must be properly converted into computer transactions, with no errors as it is transcribed from one form to another. Transcription errors can be eliminated or reduced by keying input transactions directly into computer terminals from their source documents. (Point-of-sale systems can capture sales and inventory transactions directly by scanning product bar codes.)

data conversion Process of properly transcribing data from one form into another form for computer transactions

batch control totals A type of input control that requires counting batches or any quantity fieldin a batch of transactions prior to processing for comparison and reconciliation after processing

Batch control totals can be established beforehand for transactions grouped in batches. These totals can range from a simple document count to totals for quantity fields such as total sales amount (for the batch). Computer programs count the batch totals from transactions input. Batches that do not balance are rejected. Online, real-time systems can also utilize batch controls by creating control totals to reconcile with hard copy documents that feed input.

edit checks Routines performed to verify input data and correct errors prior to processing

Edit checks. Various routines can he performed to edit input data for errors before they are processed. Transactions that do not meet edit criteria will be rejected. The edit routines can produce lists of errors to be corrected later. The most important types of edit techniques are summarized in Table 3.

An advantage of online, real-time systems is that editing can be performed up front. As each transaction is input and entered it can be edited, and the terminal operator can be notified immediately if an error is found. Alternatively, the operator may fail to correct the error on purpose or by accident. The system can he designed to reject additional input until the error is corrected or to print a hard copy error list that can be reviewed by others.

Processing Controls

processing controls Routines for establishing that data are complete and accurate during updating

Processing controls establish that data are complete and accurate during updating. The major processing controls are run control totals, computer matching, and programmed edit checks.

run control totals Procedures for controlling completeness of computer updating by generating control totals that reconcile totals before and after processing

Run control totals reconcile the input control totals with the totals of items that have updated the file. Updating can he controlled by generating control totals during processing. The totals, such as total transactions processed or totals for critical quantities, can be compared manually or by computer. Discrepancies are noted for investigation.

computer matching Processing control that matches input data with information held on master files

Computer matching matches the input data with information held on master or suspense files, with unmatched items noted for investigation. Most matching occurs during input, but under some circumstances it may be required to ensure completeness of updating. For example, a matching program might match employee time cards with a payroll master file and report missing or duplicate time cards.

Edit checks verify reasonableness or consistency of data. Most edit checking oc-curs at the time data are input. However, certain applications require some type of reasonableness or dependency check during updating as well. For example, consistency checks might be utilized by a utility company to compare a customer's electric bill with previous bills. If the bill were 500 percent higher this month compared to last month, the bill would not be processed until the meter was rechecked.

Output Controls

output controls Ensure that the results of computer processing are accurate, complete, and properly distributed

Output controls ensure that the results of computer processing are accurate, complete, and properly distributed. Typical output controls include the following:

- Balancing output totals with input and processing totals
- Reviews of the computer processing logs to determine that all of the correct computer jobs were executed properly for processing
- Audits of output reports to make sure that totals, formats, and critical details are correct and reconcilable with input
- Formal procedures and documentation specifying authorized recipients of output reports, checks, or other critical documents

DEVELOPING A CONTROL STRUCTURE: COSTS AND BENEFITS

Information systems can make exhaustive use of all of the control mechanisms previously discussed. But they may be so expensive to build and so complicated to use that the system is economically or operationally unfeasible. Some cost/benefit analysis must be performed to determine which control mechanisms provide the most effective safeguards without sacrificing operational efficiency or cost.

One of the criteria that determine how much control is built into a system is the importance of its data. Major financial and accounting systems, for example, such as a pay-

roll system or one that tracks purchases and sales on the stock exchange, must have higher standards of controls than a system to inventory employee training and skills or a "tickler" system to track dental patients and remind them that their six-month checkup is due. For instance, Swiss Bank invested in additional hardware and software to increase its network reliability because it was running critical financial trading and banking applications.

Standing data, the data that are permanent and that affect transactions flowing into and out of a system (e.g., codes for existing products or cost centers) require closer monitoring than individual transactions. A single error in transaction data will affect only that transaction, while a standing data error may affect many or all trans-actions each rime the file is processed.

The cost effectiveness of controls will also be influenced by the efficiency, complexity, and expense of each control technique. For example, complete one-for-one checking may be time-consuming and operationally impossible for a system that processes hundreds of thousands of utilities payments daily. But it might be possible to use this technique to verify only critical data such as dollar amounts and account numbers, while ignoring names and addresses.

A third consideration is the level of risk if a specific activity or process is not properly controlled. System builders can undertake a risk assessment, determining the likely frequency of a problem and the potential damage if it were to occur. For example, if an event is likely to occur no more than once a year, with a maximum of a $1000 loss to the organization, it would not be feasible to spend $20,000 on the design and maintenance of a control to protect against that event. However, if that same event could occur at least once a day, with a potential loss of over $300,000 a year, $100,000 spent on a control might be entirely appropriate.

Table 4 illustrates sample results of a risk assessment for an online order processing system that processes 30,000 orders per day. The probability of a power failure occurring in a one-year period is 30 percent. Loss of order transactions while power is down could range from $5000 to $200,000 for each occurrence, depending on how long processing was halted. The probabaility of embezzlement occurring over a yearly period is about 5 percent, with potential losses ranging from $1000 to $50,000 for each occurrence. User errors have a 98 percent chance of occurring over a yearly period, with losses ranging from $200 to $40,000 for each occurrence. The average loss for each event can be weighted by multiplying it by the probability of its occurrence annually to determine the expected annual loss. Once the risks have been assessed, system builders can concentrate on the control points with the greatest vulnerability and potential loss. In this case, controls should focus on ways to minimize the risk of power failures and user errors.

TABLE 4 ONLINE ORDER PROCESSING RISK MANAGEMENT

EXPOSURE	PROBABILITY OF OCCURRENCE	LOSS RANGE/ AVERAGE ($)	EXPECTED ANNUAL LOSS ($)
Power failure	*30*	*5000-200,000 (102,500)*	*30,750*
Embezzlement	*5*	*1000-50,000 (25,500)*	*1,275*
User Error	*98*	*200-40,000 (20,100)*	*19,698*

This chart shows the results of a risk assessment of three selected areas of an online order processing system. The likelihood of each exposure occurring over a one-year period is expressed as a percentage. The next column shows the highest and lowest possible loss that could be expected each time the exposure occurred and an "average" loss calculated by adding the highest and lowest figures together and dividing by 2. The expected annual loss for each exposure can be determined by multiplying the "average' loss by its probability of occurrence.

In some situations, organizations may not know the precise probability of threats occurring to their information systems, and they may not be able to quantify the impact of events that disrupt their information systems. In these instances, management may choose to describe risks and their likely impact in a qualitative manner.

To decide which controls to use, information system builders must examine various control techniques in relation to each other and to their relative cost effectiveness. A control weakness at one point may be offset by a strong control at another. It may not be cost effective to build tight controls at every point in the processing cycle if the areas of greatest risk are secure or if compensating controls exist elsewhere. The combination of all the controls developed for a particular application will determine its overall control structure.