Chapter 8
Securing Information Systems

LEARNING TRACK 1: GENERAL AND APPLICATION CONTROLS FOR INFORMATION SYSTEMS

Types of Information Systems Controls

Protection of information resources requires a well-designed set of controls. Computer systems are controlled by a combination of general controls and application controls. General controls govern the design, security, and use of computer programs and the security of data files in general throughout the organization's information technology infrastructure. On the whole, general controls apply to all computerized applications and consist of a combination of hardware, software, and manual procedures that create an overall control environment. Application controls are specific controls unique to each computerized application, such as payroll or order processing. They consist of controls applied from the business functional area of a particular system and from programmed procedures.

GENERAL CONTROLS

General controls include software controls, physical hardware controls, computer operations controls, data security controls, controls over the systems implementation process, and administrative controls. Table 1 describes the functions of each type of control.

TABLE 1 General Controls

TYPE OF GENERAL CONTROL	DESCRIPTION
Software controls	Monitor the use of system software and prevent unauthorized access of software programs, system software, and computer programs. System software is an important control area because it performs overall control functions for the programs that directly process data and data files.
Hardware controls	Ensure that computer hardware is physically secure and check for equipment malfunction. Computer equipment should be specially protected against fires and extremes of temperature and humidity. Organizations that are dependent on their computers also must make provisions for backup or continued operation to maintain constant service.
Computer operations controls	Oversee the work of the computer department to 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 and computer operations and backup and recovery procedures for processing that ends abnormally.
Data security controls	Ensure that valuable business data files on either disk or tape are not subject to unauthorized access, change, or destruction while they are in use or in storage.
Implementation controls	Audit the systems development process at various points to ensure that the process is properly controlled and managed. The systems development audit looks for the presence of formal reviews by users and management at various stages of development; the level of user involvement at each stage of implementation; and the use of a formal cost-benefit methodology in establishing system feasibility. The audit should look for the use of controls and quality assurance techniques for program development, conversion, and testing and for complete and thorough system, user, and operations documentation.
Administrative controls	Formalize standards, rules, procedures, and control disciplines to ensure that the organization's general and application controls are properly executed and enforced.

APPLICATION CONTROLS

Application controls include both automated and manual procedures that ensure that only authorized data are completely and accurately processed by that application. Application controls can be classified as (1) input controls, (2) processing controls, and (3) output 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. Processing controls establish that data are complete and accurate during updating. Run control totals, computer matching, and programmed edit checks are used as processing controls. Output controls ensure that the results of computer processing are accurate, complete, and properly distributed. Table 2 provides more detailed examples of each type of application control.

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.

TABLE 2 Application Controls

NAME OF CONTROL	TYPE OF APPLICATION CONTROL	DESCRIPTION
Control totals	Input, processing	Totals established beforehand for input and processing transactions. These totals can range from a simple document count to totals for quantity fields, such as total sales amount (for a batch of transactions). Computer programs count the totals from transactions input or processed.
Edit checks	Input	Programmed routines that can be performed to edit input data for errors before they are processed. Transactions that do not meet edit criteria are rejected. For example, data might be checked to make sure they are in the right format (for instance, a nine-digit social security number should not contain any alphabetic characters).
Computer matching	Input, processing	Matches input data with information held on master or suspense files and notes unmatched items for investigation. For example, a matching program might match employee time cards with a payroll master file and report missing or duplicate time cards.
Run control totals	Processing, output	Balance the total of transactions processed with total number of transactions input or output.
Report distribution logs	Output	Documentation specifying that authorized recipients have received their reports, checks, or other critical documents.