CIA   PDF

1. Client-server architecture may
potentially involve a variety of hardware, systems software, and
application software from many vendors. The best way to protect a
client-server system from unauthorized access is throughA A
combination of application and general access control techniquesB
Use of a commercially available authentication systemC Encryption
of all network trafficD Thorough testing and evaluation of remote
procedure calls.A correct Security is more difficult to achieve in a
client-server system than in a mainframe environment. The system
has numerous access points, and users have many chances to alter
data.Thus, application controls must be combined with general
access controls to protect the system.B incorrect Authentication
systems are only a part of the solution.C incorrect Encryption affects
only general access control techniques.D incorrect Testing and
evaluation of RPC's may be only a small part of an overall security
review. A company with several hundred stores has a network for the
stores to transmit sales data to headquarters.The network is also used
for 2 The information systems and audit directors also agreed that
maintaining the integrity of the system that kept inventory data was
crucial for distributing correct product quantities to stores. The best
way to ensure the integrity of the application software is throughA
Access controls for terminals in the receiving departmentB Audit
trails for items sold and received.C Change controls for inventory

software. D Monitoring software for the network. A incorrect Access controls for terminals in the receiving department ensure that only authorized receiving personnel have access to specific categories of information. However, they do not affect personnel in other functional areas. B Audit trails permit audits of transaction 0updates to date files but do not ensure the integrity of application software. C Change control is vital to the effectiveness of internal control. It is the set of procedures that ensure that only authorized, tested, and documented program changes are made. Such procedures include not only segregation of duties in the development and implementation processes, but also design and code walk-through, coordination of changes, review and approval by users and management, review of compliance with standards, minimum testing requirements, and backout procedures in the event of failure. D Monitoring software is designed to monitor performance (human or machine) for specified function such as capacity used or number of tasks performed. 3 The information systems director is concerned that someone might be able to enter fictitious orders from store terminals. Of the following, the best control for minimizing the likelihood of such an occurrence is to A no Encrypting transmissions from the stores would ensure the confidentiality of the transmissions but would not deter the entry of bogus transactions. B Change controls for programs ensure that only program changes are authorized, tested, and documented. Initial data input also needs to be restricted and available only to those who are authorized. C yes Password control procedures, which are type of access control,

prevent the improper use or manipulation of data files and programs. They ensure that only those persons with a bona fide purpose and authorization have access to data processing. The use of passwords is an effective control in an online system to prevent unauthorized access to computer files, especially if remote terminals are involved. List of authorized persons are maintained in the computer.D Encouraging store employees to report suspicious activity is a good practice, but suspicious activity often goes undetected or an employee does not feel comfortable reporting on a co-worker. 4 The information systems and audit directors agreed on the need to maintain security and integrity of transmissions and the data they represent. The best means of ensuring the confidentiality of satellite transmissions would be 1380A Encryption B Access controlC Monitoring softwareD Cyclic redundancy checks A yes Encryption encodes data before transmission over communication lines in order to prevent its use by unauthorized users but allow its recovery by authorized users. Encryption is the best means of ensuring the confidentiality of satellite transmissions. If an unauthorized individual records the transmissions, they will not be intelligible without proper decoding.B no Access control protests against unauthorized entry to the application systems but does not protect the transmission of data.C no Monitoring software is designed to monitor performance(human or machine) for specified functions such as number of tasks preformed or capacity used.D no Cyclic redundancy checks are complies computations performed with the data bits and the check bits in data transmissions to ensure the

integrity, not the confidentiality, of the data. 5 Controls that are designed to provide management with assurance of the realization of specified minimum gross margins on sales are A Directive controlsB Preventive controlsC Detective controls.D Output controls. A yes According to SIAS 1, " A control is any action taken by management to enhance the likelihood that established objectives and goals will be achieved" The objective of directive controls is to cause or encourage desirable events to occur, e.g., providing management with assurance of the realization of specified minimum gross margins on sales.B no Preventive controls deter undesirable events from occurring,.C no Detective controls detect and correct undesirable events.\D no Output controls relate to the accuracy and reasonableness of information processed by a system, not to operating controls. 100Test