Part 1 : 07/28/10 09:06:11

Question 1 - CIA 598 3-54 - Systems Controls and Security Measures

Which of the following statements regarding security of electronic mail is correct?

A. All messages on the Internet are encrypted thereby providing enhanced security.
B. Passwords are effective in preventing casual access to another's electronic mail.
C. Supervisory-level access to the file server containing electronic messages would not give access to the file containing electronic mail messages without first decrypting the security control log.
D. Passwords are not needed with discretionary access control.

A. Messages on the Internet are not encrypted. It is the sender and receiver's responsibility to encrypt confidential information.

B. Passwords are effective against the casual intruder.

C. If someone gains access to the server, they can download the file of messages and gain access to the messages without working with any security log.

D. Discretionary access does not completely eliminate the need for passwords.

Question 2 - CIA 1196 III-40 - Systems Controls and Security Measures

Which of the following is an indication that a computer virus is present?

A. Numerous copyright violations due to unauthorized use of purchased software.
B. Frequent power surges that harm computer equipment.
C. Inadequate backup, recovery, and contingency plans.
D. Unexplainable losses of or changes to data.

A. Numerous copyright violations are compliance problems.

B. Power surges are primarily caused by power supply problems.

C. Inadequate backup, recovery, and contingency plans are weaknesses of operational planning.

D. Unexplainable losses of, or changes to data are an indication of computer viruses.

Question 3 - CMA 1289 5-11 - Systems Controls and Security Measures

Most of today's computer systems have hardware controls that are built in by the computer manufacturer. Common hardware controls are

A. Duplicate circuitry, echo check, and internal header labels.
B. Duplicate circuitry, echo check, and dual reading.
C. Duplicate circuitry, echo check, tape file protection and internal header labels.
D. Tape file protection, cryptographic protection, and limit checks.

A. Hardware controls are controls installed in computers that can identify incorrect data handling or improper operation of the equipment. An internal header label is not a hardware control. A header label is a routing verification procedure that protects against transactions being routed to the wrong computer network system address. Any transaction transmitted over the network must have a header label identifying its destination. Before sending the transaction, the system verifies that the destination is valid and is authorized to receive data. After the transaction has been received, the system verifies that the message did go to the destination code in the header.

B. Duplicate circuitry, echo check, and dual reading are part of the error correction systems built into hardware to provide the system with fault tolerance. Duplicate circuitry is the double wiring of key hardware

elements to ensure that if one malfunctions, the other will take over. An echo check is the process of sending the received data back to the sending computer to compare with what was actually sent to make sure that it is the same. In a dual read check, data are read twice during input and compared.

C. Tape file protection is not a hardware control; it is a data storage control that provides security for computer data stored on tapes by protecting the data from being overwritten. An internal header label is not a hardware control; it is a routing verification procedure that protects against transactions being routed to the wrong computer network system address. Any transaction transmitted over the network must have a header label identifying its destination. Before sending the transaction, the system verifies that the destination is valid and is authorized to receive data. After the transaction has been received, the system verifies that the message did go to the destination code in the header.

D. Hardware controls are controls installed in computers that can identify incorrect data handling or improper operation of the equipment. None of these are hardware controls. Tape file protection is a data storage control that provides security for computer data stored on tapes by protecting the data from being overwritten. Cryptographic protection relates to the encryption of data sent over a network or the Internet to protect private or confidential data from being intercepted by unauthorized individuals. A limit check is an edit test that ensures that only data within predefined limits will be accepted by the system.

Question 4 - HOCK CMA P1D3 09 - Systems Controls and Security Measures

General controls are designed to ensure that a company's control environment is stable and well managed. Which of the following is **not** an example of general controls?

A. Access controls
B. Equipment controls
C. Segregation of duties within the data processing function.
D. Using reasonableness checks to detect if data is inconsistent with past transactions.

A. Access controls pertain to controlling access to both physical equipment and logical data, and are an important general control.

B. Equipment controls are general controls that can identify incorrect data handling or improper operation of the equipment.

C. General organization controls include segregation of duties.

D. Reasonableness checks are are example of input controls, which are application controls, not general controls.

Question 5 - CMA 1287 5-15 - Systems Controls and Security Measures

In an automated payroll processing environment, a department manager substituted the time card for a terminated employee with a time card for a fictitious employee. The fictitious employee had the same pay rate and hours worked as the terminated employee. The best control technique to detect this action using employee identification numbers would be a

A. Batch total.
B. Subsequent check.
C. Hash total.
D. Record count.

A. The question asks for the best control technique to detect this action using employee identification numbers. A batch total of the total payroll amount or the total hours worked would not utilize employee identification numbers.

B. While a subsequent check of the output from the payroll might detect the substitution, a hash total is a better control technique because it would detect the substitution more quickly and reliably.

C. A hash total is a meaningless sum of numbers in a batch, such as the sum of all the employee I.D. numbers. A hash total would detect a substituted employee time card, because the employee I.D. number of the substituted employee would be different from the employee I.D. number of the original employee.

D. A record count is a total of the number of records processed. Whereas a record count could detect that one additional employee had been paid, the question asks for the best control technique to detect the action using employee identification numbers. A record count would not include employee identification numbers.

Question 6 - CPA AUD R98-3 - Systems Controls and Security Measures

An entity has the following invoices in a batch:

Invoice #	Product	Quantity	Price
201	F10	150	$5.00
202	G15	200	$10.00
203	H20	250	$25.00
204	K35	300	$30.00

Which of the following numbers represents the record count?

A. 1
B. 810
C. 4
D. 900

A. 1 is the number of batches.

B. 810 is the total of invoices (201 + 201 + 203 + 204).

C. The record count is the number of records processed. Thus, the number of records processed is 4.

D. 900 is the total value of quantities (150 + 200 + 250 + 300).

Question 7 - CIA 597 I-19 - Systems Controls and Security Measures

Which of the following computerized control procedures would be most effective in ensuring that data uploaded from personal computers to a mainframe are complete and that no additional data is added?

A. Batch control totals, including control totals and hash totals.
B. Field-level edit controls that test each field for alphanumerical integrity.
C. Passwords that effectively limit access to only those authorized to upload the data to the mainframe computer.
D. Self-checking digits to ensure that only authorized part numbers are added to the database.

A. Batch control totals, including control totals with hash controls would be most effective in ensuring that data uploaded from personal computers to the mainframe are complete and that no additional data are added. These controls would provide the best information on the completion of the data transfer.

B. Field-level edit controls that test each field for alphanumerical integrity are input controls, but they would not ensure that the data transfer is complete.

C. Passwords are effective in limiting unauthorized personnel, but would not ensure that the data transfer is complete.

D. Self-checking digits would detect erroneous part numbers, but would not ensure that the data transfer is complete.

Question 8 - CIA 594 3-39 - Systems Controls and Security Measures

The Computer Center of a company processes its prior week's sales invoices, as well as its returns and allowances, at the end of the week. Cash receipts, however, are processed and deposited daily. Each morning the mail receipts clerk prepares the cash receipts prelist in duplicate. The original prelist goes to the head cashier together with the checks and an adding machine tape. The duplicate copy goes to the accounts receivable supervisor. The separate remittance advices are sent to the data input clerk. At midday, the head cashier prepares the bank deposit slip which is taken to the bank. After returning from the bank, the head cashier compares the original prelist to the validated bank deposit slip, initials the documents, and files them in chronological order.

The following morning the accounts receivable supervisor receives a summary processing list from the Computer Center with various control totals from the nightly accounts receivable update. The total on the prior day's duplicate cash receipts prelist is then compared with the total showing the difference between the prior day's beginning and ending accounts receivable subsidiary ledger totals. The amount shown on yesterday's duplicate cash receipts prelist was $35,532.32. This morning the difference between the beginning and ending subsidiary ledger totals was $35,541.32.

Which of the following is most likely not a true statement about the company?

A. The grandfather-father-son technique can be used as a file protection procedure in this system.
B. If the two control totals agree, the amount posted to each subsidiary ledger account is correct.
C. On the last day of the month, sales are understated.
D. If a customer is required to prepay for a custom order, the subsidiary ledger account will have a credit balance.

A. This is typically used for batch processing

B. The totals could agree, but individual payments could be posted to wrong accounts. This would not be caught by the above procedures.

C. See the correct answer for the explanation.

D. These derive from the logic of the narrative.

Question 9 - CMA 1287 5-16 - Systems Controls and Security Measures

An employee in the receiving department keyed in a shipment from a remote terminal and inadvertently omitted the purchase order number. The best systems control to detect this error would be

A. Batch total.
B. Reasonableness test.
C. Sequence check.
D. Completeness test.

A. Batch control totals are any type of control total or count applied to a specific group of transactions, such as total sales dollars in a batch of billings. Batch control totals are used to ensure that all input is processed correctly by the computer, but they will not detect missing input. If the purchase order number were omitted, a batch control total would not detect the omission.

B. A reasonableness test ensures that only data within predefined limits will be accepted by the system. If a purchase order number were omitted, a reasonableness test would not detect the omission.

C. A sequence check is a type of verification that is performed to help ensure that data is in the proper order. If a purchase order number were omitted, a sequence check would not detect the omission.

D. A completeness test is an input validation routine that checks and ensures that data is input into all required fields. If the purchase order number were omitted, a completeness test would detect the omission

and give the user a message that the input was missing.

Question 10 - HOCK CMA P1D3 11 - Systems Controls and Security Measures

Which of the following statements is **true** regarding source code and object code?

A. Source code is the machine language that a computer understands.
B. While source code and object code should correspond, the computer does not require them to correspond.
C. A compiler converts object code into source code.
D. Programs are written in object code, which is the language that a programmer uses for coding the program.

A. **Object code** is the language that the computer can understand.

B. This is a true statement. It is possible for a knowledgeable person to make a copy of the source code, rewrite some of the instructions, compile the modified source code into object code, replace the object code on the computer, and then destroy the modified source code. This results in a program running on the computer that does not correspond to the authorized source code. This weakness can be used to commit computer fraud if the controls over compiling and cataloging are not adequate.

C. A compiler converts the source code that a programmer writes into object code that the computer can understand.

D. Programs are written in **source code**.

Question 11 - HOCK CMA P1D3 05 - Systems Controls and Security Measures

Which of the following statements about Trojan horses is **false**?

A. A Trojan horse can be received from an email or the Internet.
B. A Trojan horse can appear as a desirable software program or utility.
C. A Trojan horse will immediately cause a computer to exhibit symptoms after it is infected.
D. A Trojan horse does not replicate itself.

A. This is a true statement. A Trojan horse can also be received via a USB drive, CD or DVD, Local Area Network, or virtually any other source connected to a computer or plugged into a computer.

B. This is a true statement. A Trojan horse gets its name because it appears to be useful, when in fact there is a danger hidden inside.

C. A computer infected with a Trojan horse may not exhibit any symptoms until the Trojan horse is activated by a particular event or command. Even after the Trojan horse is activated, the resulting behavior may not cause any abnormal symptoms, such as the Trojan collecting data and secretly sending it via the Internet to another computer.

D. This is a true statement. A Trojan horse must be actively transmitted and installed.

Question 12 - HOCK CMA P1D3 01 - Systems Controls and Security Measures

A disaster plan should specify all of the following **except**:

A. The priority of the services that need to be restored.
B. Where in the office the disaster recovery plan is stored.
C. The employees who will participate in disaster recovery.
D. What facilities will be used in the course of recovery.

A. This is part of a disaster recovery plan.

B. In the event of a disaster, the office may not be accessible, or may not even exist anymore. All members of the disaster recovery team should each keep a current copy of the plan at home.

C. This is a part of a disaster recovery plan. In addition to specifying who should participate, the plan should also outline each person's responsibilities and should designate a first and second in command.

D. This is part of a disaster recovery plan.

Question 13 - CIA 1190 I-34 - Systems Controls and Security Measures

All administrative and professional staff in a corporate legal department prepare documents on terminals connected to a file server on the LAN. The best control over unauthorized access to sensitive documents in the system is

A. Required entry of passwords for access to the system.
B. Periodic server backup and storage in a secure area.
C. Physical security for all disks containing document files.
D. Required entry of passwords for access to individual documents.

A. Requiring passwords for access to the system permits all departmental personnel to have access to all documents in the system.

B. Periodic server backup and storage in a secure area would not prevent unauthorized access to sensitive documents in the system.

C. The information is contained in the hard drive, not on disks.

D. The best control over unauthorized access to sensitive documents is to require entry of passwords for access to individual documents.

Question 14 - CIA 1194 3-22 - Systems Controls and Security Measures

Many organizations are critically dependent on information systems to support daily business operations. Consequently, an organization may incur significant loss of revenues or incur significant expenses if a disaster such as a hurricane or power outage causes information systems processing to be delayed or interrupted. A bank, for example, may incur significant penalties as a result of missed payments.

Which of the following management activities is essential to ensure continuity of operations in the event a disaster or catastrophe impairs information systems processing?

A. Contingency planning.
B. Electronic vaulting.
C. Review of insurance coverage.
D. Change control procedures.

A. Contingency planning is a management activity which is essential to ensure continuity of operations in the event a disaster impairs information systems processing.

B. Electronic vaulting is a technology that may be used to address contingency planning issues.

C. Review of insurance coverage is an aspect of risk analysis, and a much narrower concept than contingency planning.

D. Change control procedures do not ensure continuity of operations.

Question 15 - HOCK CMA P1D3 10 - Systems Controls and Security Measures

Which of the following exploits to Information Systems can occur over and over again without any direct action after the initial exploit?

A. Unauthorized modifications to software that skims transactions and diverts funds (e.g. rounding fractions into an expense account for reimbursement).
B. Data being stolen on removable storage devices (e.g. hard drive, USB memory).
C. Sabotaging the servers that run the data processing (e.g. unplugging the servers or removing their hard drives).
D. Data input manipulation (e.g. intentionally mis-entering information).

A. Once a skimming routine is inserted in the accounting system, it will run without any further intervention by the programmer.

B. Stealing data on removable storage requires direct action each time data is stolen and removed from the company premises.

C. Physically sabotaging a system requires direct action and cannot be carried out repeatedly without repeated sabotage efforts.

D. This cannot occur repeatedly without direct action by the person mis-entering the data.

Question 16 - CMA 690 3-27 - Systems Controls and Security Measures

One of the steps in assessing control risk in a computerized information control system is identifying necessary controls to prevent data from being lost, added, duplicated, or altered during processing. An example of this type of control is the

A. Authorization and approval of data in user departments and screening of data by data control groups.
B. Use of control totals, limit and reasonableness checks, and sequence tests.
C. Review of data output by data control groups.
D. Use of external and internal file labels.

A. While authorization of data, approval of data, and screening of data are controls, they are not controls that are used during the processing of the data.

B. Processing controls are controls designed to ensure that processing has occurred properly and that no transactions have been lost or incorrectly added. Control totals are of various kinds, but they all involve comparison of counts at various points with the correct count. A limit check, or a reasonableness check, tests a value to determine whether it falls within a prescribed range. A sequence test verifies that records are in the correct sequence.

C. While review of data output by data control groups is a control, it is not a control that is used during the processing of the data.

D. Labels, both external and internal, are used to identify a file. External labels are the gummed labels attached to the outside of a disk or other media that identify its contents. Internal labels identify the contents by means of an identification within the data file that can be read by the computer.

Question 17 - CPA 586 A-58 - Systems Controls and Security Measures

A small client recently put its cash disbursements system on a server. About which of the following internal control features would an auditor most likely be concerned?

A. There are restrictions on the amount of data that can be stored and on the length of time that data can be stored.
B. Programming of the applications are in BASIC, although COBOL is the dominant, standard language for business processing.
C. The server is operated by employees who have cash custody responsibilities.
D. Only one employee has the password to gain access to the cash disbursement system.

A. Limiting the amount of data that can be stored and the length it can be stored would not necessarily be considered a control weakness.

B. The systems programming language should have little effect on the internal controls.

C. The segregation of duties is the primary function of a control system. The segregation of duties means that authorizing a transaction, recording the transaction, physical custody of the related asset, and the periodic reconciliation of the physical asset are done by different people. If the server is operated by employees who have cash custody responsibilities then they have the ability to override controls in order to make changes the records to conceal the theft of cash.

D. Limiting access to the cash disbursement system would be considered a control strength.

Question 18 - CIA 596 3-48 - Systems Controls and Security Measures

A company with several hundred stores has a network for the stores to transmit sales data to headquarters. The network is also used for:

- vendors to submit reorders,
- stores to transmit special orders to headquarters,
- regional distribution centers to communicate delivery and out-of-stock information to the stores,
- the national office to distribute training materials,
- store, regional, and national personnel to share any information they think helpful.

In order to accommodate the large volume of transmissions, large stores have their own satellite receiving/transmitting stations. Small stores use leased lines.

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. Enforce password control procedures for users.
B. Encrypt outward bound transmissions from the stores.
C. Encourage employees to report suspicious activity.
D. Require change control procedures for programs.

A. Enforcing password control procedures would make it more difficult for an unauthorized person, such as a competitor intending to disrupt the distribution patterns, to gain prolonged entry.

B. Encrypting transmissions from the stores would increase the difficulty of eavesdropping on the transmissions but would not deter someone from entering bogus transactions.

C. Encouraging store employees to report suspicious activity is a good practice, but such activity might go undetected.

D. Requiring change control for programs ensures that program changes are authorized, tested, and documented.

Question 19 - CIA 594 3-14 - Systems Controls and Security Measures

Which of the following controls would assist in detecting an error when the data input clerk records a sales invoice as $12.99 when the actual amount is $122.99?

A. Sign check.
B. Echo check.
C. Limit check.
D. Batch control totals.

A. This control checks for positive or negative field restrictions.

B. This is a hardware control that checks for accuracy in data transmission; it is not an input control.

C. This would only work if the two amounts were reversed, and there was a dollar limit on invoices.

D. The other controls would not find this error.

Question 20 - CPA AUD R98-4 - Systems Controls and Security Measures

An entity has the following invoices in a batch:

Invoice Number	Product	Quantity	Unit Price
201	F10	150	$ 5.00
202	G15	200	$10.00
203	H20	250	$25.00
204	K35	300	$30.00

Which of the following most likely represents a hash total?

A. FGHK80
B. 810
C. 204
D. 4

A. FGHK80 is not a hash total.

B. Hash control is used to verify the completeness of the inputted data. Hash totals can be employee numbers, or invoice numbers. Thus, the hash total of invoice numbers is 810 (201 + 202 + 203 + 204).

C. 204 is a specific invoice number.

D. 4 is a record count.

Question 21 - CMA 691 4-25 - Systems Controls and Security Measures

Edit checks in a computerized accounting system

A. Must be installed for the system to be operational.
B. Should be performed on transactions prior to updating a master file.
C. Should be performed immediately prior to output distribution.
D. Are preventive controls.

A. Edit checks are controls that are built into a system, but they are not required for a system to be operational.

B. Edit checks are programs or routines that check the validity and accuracy of input data. Edit tests include completeness checks, limit checks, validity checks, overflow checks, check digits, and key verification.

C. Edit checks are programs or routines that check the validity and accuracy of input data. Just prior to output distribution is not the correct time to perform edit checks.

D. Preventive controls prevent errors and fraud before they occur. Edit checks are programs or routines that check the validity and accuracy of input data. Thus, edit checks are detective controls, because they detect errors.

Question 22 - CIA 596 1-8 - Systems Controls and Security Measures

An electric utility company records capital and maintenance expenditures through the use of a computerized project tracking system. Labor, material, and overhead are charged to the applicable project number. Monthly reports are produced which detail individual charges to each project, and expenditure totals are provided for the current month, fiscal year, and project life to date.

In order to prevent maintenance materials from being charged incorrectly to capital projects, the accounting information system should:

A. Verify that the project number being entered contains the required number of characters.
B. Use tables of project numbers and material requirements.
C. Authenticate the user identification and verify the input location.
D. Require internal file labels for inventory transactions.

A. Verifying the number of characters does not prevent incorrect charges, only incomplete ones.

B. Tables of predefined project numbers and material requirements would allow only acceptable jobs to be recorded.

C. System security does not address data accuracy.

D. Internal file labels address processing of data, not the prevention of data errors.

Question 23 - CMA 680 5-15 - Systems Controls and Security Measures

Omen Company is a manufacturer of men's shirts. It distributes weekly sales reports to each sales manager. The quantity 2R5 appeared in the quantity sold column for one of the items on the weekly sales report for one of the sales managers. The most likely explanation for what has occurred is that

A. The program did not contain a data checking routine for input data.
B. The output quantity has been stated in hexadecimal numbers.
C. The computer has malfunctioned during execution.
D. The printer has malfunctioned and the "R" should have been a decimal point.

A. The most likely explanation for the error is that the program did not contain a data checking routine for input data, e.g., field check. A field check would make sure that the input field contains that correct type of characters, e.g., quantity 250, etc.

B. R is not a hexadecimal character. Hexadecimal is usually written using the symbols 0-9, and A-F.

C. It is unlikely the computer malfunctioned during the printing of the quantity.

D. It is not possible that the quantity of shirts sold is 2.5. The quantity has to be a whole number.

Question 24 - CMA 1289 5-2 - Systems Controls and Security Measures

Payroll systems should have elaborate controls to prevent, detect, and correct errors and unauthorized tampering.

The best set of controls for a payroll system includes

A. Batch and hash totals, record counts of each run, proper separation of duties, special control over unclaimed checks, and backup copies of activity and master files.
B. Employee supervision, batch totals, record counts of each run, and payments by check.
C. Passwords and user codes, batch totals, employee supervision, and record counts of each run.
D. Sign tests, limit tests, passwords and user codes, online edit checks, and payments by check.

A. Batch totals for hours worked and dollar totals, hash totals of employee identification numbers, and record counts of each run should be utilized to check for accuracy and completeness. A system of control over unclaimed checks should be in place. Segregation of duties is essential, with the four functions of authorizing transactions, recording transactions, keeping custody of the assets, and reconciliation of the physical assets to the recorded amounts being performed by different people. Backup copies of all activity and master files are essential so that data will not be lost.

B. This is not the best answer because it is missing one more important controls.

C. This is not the best answer because it is missing one more important controls.

D. This is not the best answer because it is missing one more important controls.

Question 25 - CMA 686 5-14 - Systems Controls and Security Measures

Program documentation is a control designed primarily to ensure that

A. Data have been entered and processed.
B. Programs do not make mathematical errors.
C. Programmers have access to the tape library or information on disk files.
D. Programs are kept up to date and perform as intended.

A. Program documentation does not ensure that data has been entered and processed.

B. Program documentation will not ensure that programs do not have "bugs" in them.

C. After a program has been written, approved and documented, programmers should not have any further access to it.

D. Program documentation includes descriptions of the programs, program flowcharts, program listings of source code, input and output forms, change requests, operator instructions and controls. Documentation provides a basis for effective operation, use, audit, and future system enhancements. Program documentation is needed for diagnosing and correcting programming errors; and it provides a basis for reconstruction of the system in case of damage or destruction. Examining software documentation, such as system flowcharts, program flowcharts, data flow diagrams, and decision tables can also be a control, because it makes sure that the programs are complete in their data manipulation.

Question 26 - CIA 1190 III-23 - Systems Controls and Security Measures

In an order-entry system, in which manually prepared source documents are entered online for immediate processing, which of the following is an example of an appropriate input-output control?

A. Backup and recovery procedures.
B. Password authorization procedure.
C. Check-digit validation procedure.
D. Hash total verification.

A. Backup and recovery procedures are general controls.

B. Password authorization is a general control that controls access to the system.

C. Self-checking digits is used for error detection, e.g., incorrect identification numbers. It applies an algorithm to an input field and then applying the same algorithm to the code already entered to compare them. Thus, check digit is an appropriate input-output control.

D. Hash total is appropriate for batch processing, but not for online processing.

Question 27 - CIA 596 3-53 - Systems Controls and Security Measures

A department store company with stores in 11 cities is planning to install a network so that stores can transmit daily sales by item to headquarters and store salespeople can fill customer orders from merchandise held at the nearest store. Management believes that having daily sales statistics will permit better inventory management than is the case now with weekly deliveries of sales reports on paper. Salespeople have been asking about online inventory availability as a way to retain the customers that now go to another company's stores when merchandise is not available. The planning committee anticipates many more applications so that in a short time the network would be used at or near its capacity.

The planning committee identified several applications that would make the company's stores more competitive. One was an on-line gift registry system for customers such as those about to be married. The system would then allow other customers in any of the company's stores to view the information listed in the registry. Once purchased, an item would be deleted from the list. In order to maintain adequate security, the system should have the following restrictions on access:

A. Customers have read privileges; salespeople have update privileges.
B. Customers have update privileges; sales-people have read privileges.
C. Customers and salespeople have read privileges only.
D. Customers and salespeople have update privileges.

A. Customers with read privileges can examine the gift registry lists to make their selections, and salespeople can update the gift registry with actual purchases.

B. Customers should not have update privileges to prevent them from corrupting data files, intentionally or accidentally.

C. Reserving all system functions for salespeople would restrict access more than is required for adequate security and would hinder use of the system for maximum benefit.

D. Customers should not have update privileges to prevent them from corrupting data files, intentionally or accidentally.

Question 28 - CIA 1196 3-48 - Systems Controls and Security Measures

A company’s management is aware that it cannot foresee every contingency even with the best planning. Management believes, however, that a more thorough recovery plan increases the ability to resume operations quickly after an interruption and thus to:

A. Maintain the same level of employment.
B. Fulfill its obligations to customers.
C. Receive the maximum benefit from planning.
D. Minimize the cost of facility repair.

A. The company may or may not maintain the same level of employment after a disaster. For example, a disaster that destroys productive capacity in one plant may lead to layoffs.

B. The better the recovery plans, the more likely the company would be to resume operations quickly and fulfill its obligations to customers.

C. The maximum benefit from planning is that it prompts action to avoid the most likely or most devastating events with the potential to interrupt business. Management would be delighted if planning ensured that business was never interrupted and thus that the recovery plan was never invoked.

D. Thorough planning may or may not minimize the cost of facility repair. That is, the best approach may be to undergo more expensive repair sooner in order to resume operations sooner.

Question 29 - CIA 1189 II-25 - Systems Controls and Security Measures

Which of the following terms best describes the type of control practice evidenced by a segregation of duties between computer programmers and computer operators?

A. Applications control.
B. Hardware control.
C. Systems development control.
D. Organizational control.

A. Applications controls include input, processing and output controls.

B. Hardware controls are included in the equipment.

C. System development control includes items such as systems analysis, design, and implementation.

D. A basis of organizational controls is the segregation of duties. For example, there should be a segregation of duties between programmers and computer operators.

Question 30 - CIA 1195 III-63 - Systems Controls and Security Measures

A validation check used to determine if a quantity ordered field contains only numbers is an example of a(n)

A. Input control.
B. Processing control.
C. Audit trail control.
D. Data security control.

A. Validation checks are input controls. Input controls provide some reasonable assurance that the data inputted has the proper authorization, has been converted to machine-sensible form, and has been identified.

B. Processing control provide some reasonable assurance that processing has been properly completed, as intended.

C. Audit trail control is used to ensure that all relevant audit information has been recorded.

D. Data security control ensures that only identified and authorized personnel are permitted to access and use the computer system.

Question 31 - IIA, adapted CIA H30 - Systems Controls and Security Measures

Which of the following is a malicious program, the purpose of which is to reproduce itself throughout the network, and can possibly produce a denial of service attack by excessively utilizing system resources?

A. Virus.
B. Logic bomb.
C. Trojan horse.
D. Worm.

A. A virus is a program that alters the way another computer operates, but it is not an independent program that can reproduce itself throughout the network. A virus spreads by inserting copies of itself into the executable code or documents.

B. A logic bomb is a malicious program that is activated when some particular condition occurs (e.g., could be a date, or system operation).

C. A Trojan horse is an independent program that is disguised as legitimate software. They may look useful or interesting to an unsuspecting user, but are actually harmful when executed.

D. A worm is an independent program that replicates itself from system to system without the use of any host file. The difference between a worm and a virus is that the worm does not require the use of an infected host file, while the virus does require the spreading of an infected host file. Worms generally exist inside of other files, often Word or Excel documents. However, worms use the host file differently from viruses. Usually the worm releases a document that has the "worm" macro inside the document. The entire document spreads from computer to computer, so the entire document is, in essence, the worm.

Question 32 - CMA 696 4-14 - Systems Controls and Security Measures

A critical aspect of a disaster recovery plan is to be able to regain operational capability as soon as possible. In order to accomplish this, an organization can have an arrangement with its computer hardware vendor to have a fully operational facility available that is configured to the user's specific needs. This is best known as a(n)

A. Hot site.
B. Uninterruptible power system.
C. Cold site.
D. Parallel system.

A. A hot site is a backup facility that has a computer system that is similar to the one used regularly and is fully operational and thus immediately available.

B. An uninterruptible power system (UPS) is a backup power source that kicks in automatically in the event of a power outage to prevent loss of data.

C. A cold site is a facility that can be used to install computer equipment if needed, but it is not fully operational.

D. A parallel system is a system that is identical to the main system.

Question 33 - CIA 1196 III-75 - Systems Controls and Security Measures

In a database system, locking of data helps preserve data integrity by permitting transactions to have control of all the data needed to complete the transactions. However, implementing a locking procedure could lead to

A. Deadly embraces (retrieval contention).
B. Inconsistent processing.
C. Rollback failures.
D. Unrecoverable transactions.

A. A deadly embrace (also called a deadlock) occurs when two different applications or transactions each

have a lock on data that is needed by the other application or transaction. Neither process is able to proceed, because each is waiting for the other to do something. In these cases the system must have a method of determining which transaction goes first, and then it must let the second transaction be completed using the updated information after the first transaction.

B. Implementing a locking procedure does not lead to inconsistent processing. A locking procedure would, in fact, result in consistent processing, because each transaction has access to all the files and data that it needs in order to be processed.

C. Rollback processing is used to prevent any transactions being written to disk until they are complete. If there is a power failure or another fault during processing, at its first opportunity, the program automatically rolls itself back to its pre-fault state by undoing any partial posting that took place prior to the aborted processing. A rollback failure would be a failure to undo this partial posting.

D. Unrecoverable transactions occur if there is a power failure or another fault during processing, and a transaction or transactions are only partially processed. Rollback processing is used to prevent any transactions from being written to disk until they are complete. At its first opportunity, the program automatically rolls itself back to its pre-fault state by undoing any partial posting that took place prior to the aborted processing.

Question 34 - CMA 1290 4-21 - Systems Controls and Security Measures

Which one of the following represents a lack of internal control in a computer-based system?

A. Programmers have access to change programs and data files when an error is detected.
B. Provisions exist to protect data files from unauthorized access, modification, or destruction.
C. Any and all changes in applications programs have the authorization and approval of management.
D. Provisions exist to ensure the accuracy and integrity of computer processing of all files and reports.

A. Programmers are the individuals who write, test and document the systems. However, once a program has been written, tested and documented, the programmer should have no further access to the program or to the data files. If any change is necessary, management should authorize and approve the change.

B. g., passwords and restricted rights, represent good internal control, not a lack of internal control.

C. It is essential that any and all changes in applications programs have the authorization and approval of management.

D. Provisions exist to ensure the accuracy and integrity of computer processing of all files and reports.

Question 35 - HOCK CMA P1D3 02 - Systems Controls and Security Measures

Which of the following statements regarding encryption is **true**?

A. Secret key systems use two different keys, one for encryption and one for decryption.
B. A message encrypted with Company Q's public key can only be decrypted with Company Q's private key.
C. It is impossible to intercept encrypted data sent over the Internet.
D. Encryption is a 100% guarantee that data being transmitted cannot be read by an unintended third party.

A. A secret key system uses the same key for encryption and decryption. A public/private key system uses two different keys.

B. This is a true statement. Only the matching private key can decrypt a message encrypted with the public key. This is an essential part of the SSL system used on the Internet for secure web sites.

C. Quite to the contrary, it is very easy to intercept encrypted data. Encryption makes it difficult for transmitted data to be **read**, but it does nothing to prevent interception. There is a better answer among the choices here.

D. There are two problems with this answer. First and foremost, encryption is only as good as the secrecy of the encryption keys used in the encryption. If the encryption keys are lost, stolen or otherwise revealed to third parties, those third parties will be able to read the encrypted messages. Secondly, while encryption is mathematically very difficult to break, it is not impossible given enough time, skill and determination.

Question 36 - CMA 693 4-10 - Systems Controls and Security Measures

Online access controls are critical for the successful operation of today's computer systems. To assist in maintaining control over such access, many systems use tests that are maintained through an internal access control matrix consisting of

A. Authorized user code numbers, passwords, lists of all files and programs, and a record of the type of access each user is entitled to have to each file and program.
B. Authorized user code numbers and passwords.
C. A completeness test, closed loop verification, and a compatibility test.
D. A list of controls in the online system and a list of those individuals authorized to change and adjust these controls along with a complete list of files in the system.

A. These are all access controls.

B. Although these two items are access controls, this is not the most complete list of items that are access controls.

C. Completeness tests and closed loop verification are not access controls. A completeness test will not let processing proceed if a data item is not complete. Closed loop verification is an online data entry check which utilizes display and checking of data entry items.

D. A list of individuals authorized to change and adjust the controls is not an access control.

Question 37 - CPA 585 A-26 - Systems Controls and Security Measures

For control purposes, which of the following should be organizationally segregated from the computer operations function?

A. Systems development.
B. Surveillance of screen display messages.
C. Minor maintenance according to a schedule.
D. Data conversion.

A. Systems analysts are responsible for reviewing the current system to make sure that it is meeting the needs of the organization, and when it is not, they will provide the design specifications to the programmers of the new system. Systems analysts should not do programming, nor should they have access to hardware, software or data files. Therefore, the functions of computer operations and systems development should be segregated.

B. It is appropriate for the surveillance of screen display messages to be assigned to computer operators.

C. It is appropriate for minor maintenance according to schedule to be assigned to computer operators.

D. It is appropriate for data conversion to be assigned to computer operators.

Question 38 - CIA 1190 III-19 - Systems Controls and Security Measures

Six months after a disgruntled systems programmer was fired and passwords disabled, the company's mainframe was brought to a halt when it suddenly erased all of its own files and software. The most likely way the programmer accomplished this was by

A. Having an accomplice in the computer center.
B. Implanting a virus in the operating system and executing it via a backdoor.
C. Planting a computer virus through the use of telephone access.
D. Returning to the computer center after 6 months.

A. In these circumstances, it is not likely that there was collusion.

B. This is probably the best explanation of how the files and software were suddenly erased. A virus is a program that alters the way another computer operates. Viruses can damage programs, delete files or reformat the hard disk. A backdoor in a computer system is a method of bypassing normal authetication or securing remote access to a computer, while attempting to remain hidden from casual inspection.

C. The passwords were disabled, so the programmer would not know the new passwords.

D. The programmer was more than likely denied access to the computer center.

Question 39 - CMA 685 5-24 - Systems Controls and Security Measures

EDP accounting control procedures are referred to as general controls or application controls. The primary objective of application controls in a computer environment is to

A. Ensure the separation of incompatible functions in the data processing departments.
B. Plan for the protection of the facilities and backup for the systems.
C. Provide controls over the electronic functioning of the hardware.
D. Maintain the accuracy of the inputs, files, and outputs for specific applications.

A. General controls relate to the general environment within which transaction processing takes place. They are designed to ensure that the company's control environment is stable and well managed. Separation of incompatible functions in the data processing departments is a general control, not an application control.

B. General controls relate to the general environment within which transaction processing takes place. They are designed to ensure that the company's control environment is stable and well managed. Plans for the protection of the facilities and backup for the systems are general controls, not application controls.

C. General controls relate to the general environment within which transaction processing takes place. They are designed to ensure that the company's control environment is stable and well managed. Hardware controls are general controls, not application controls.

D. Application controls are controls that are specific to individual applications and are designed to prevent, detect, and correct errors and irregularities in transactions during the input, processing, and output stages.

Question 40 - HOCK CMA P1D3 06 - Systems Controls and Security Measures

Which of the following statements about a firewall is **false**?

A. A firewall can block port scans from finding computers on a company's network.
B. Firewalls act as a barrier between the internal and external network.
C. Firewalls can be either hardware-based or software-based.
D. Firewalls are an effective barrier from phishing attacks.

A. This is a true statement. Port scans would be unable to reach the computers on the company's network through the firewall.

B. This is the very basic definition of a firewall.

C. This is a true statement. Firewalls can either be a software program installed on a computer either as part of the operating system, or as a separate utility. Firewalls can also be a physical piece of equipment that is installed between the internal network and the Internet.

D. Firewalls are not an effective barrier against phishing attacks. A phishing attack involves tricking someone into divulging information, and a firewall cannot help prevent someone from releasing private information. A firewall's purpose is to prevent unauthorized access to the company internal network.

Question 41 - CMA 686 5-12 - Systems Controls and Security Measures

A control designed to catch errors at the point of data entry is

A. Checkpoints.
B. A record count.
C. A check digit.
D. A batch total.

A. A checkpoint is a control procedure that is performed several times per hour, and during that time, the network system will not accept posting. It stops and backs up all the data and other information needed to restart the system. This checkpoint is recorded on separate media.Then, if a hardware failure occurs, the company simply reverts to the last saved copy, and reprocesses only the transactions that were posted after that checkpoint. A checkpoint will not catch errors at the point of data entry.

B. A record count is a total of all the records processed. It is a control total, but it will not catch errors at the point of data entry.

C. A check digit is used for determining whether a number has been input properly. A check digit is a digit that is a function of the other digits within a set of numbers. If a typographical error is made in input, the check digit should recognize that something has been input incorrectly.

D. A batch total is a total of one field for all items in a batch. It is a control total, but it will not catch errors at the point of data entry.

Question 42 - HOCK CMA P1D3 08 - Systems Controls and Security Measures

Application controls are broken down into three categories. What are those three categories?

A. Edit tests, hash totals, and prenumbered forms.
B. Input, processing and output controls.
C. Access controls, equipment controls, and general operating procedures.
D. Data recording, data transcription and edit tests.

A. These are examples of application controls.

B. Application controls pertain to specific individual applications and are designed to prevent, detect and correct errors in transactions as they flow through the *input*, *processing*, and *output* stages of work.

C. These are all types of general controls that relate to the general transaction processing environment.

D. These are classifications of input controls.

Question 43 - CIA 1193 I-24 - Systems Controls and Security Measures

Your firm has recently converted its purchasing cycle from a manual process to an online computer system. Which of the following is a probable result associated with conversion to the new automatic system?

A. Processing errors are increased.
B. Processing time is increased.
C. Traditional duties are less segregated.
D. The firm’s risk exposures are reduced.

A. If the computer system is error free then processing errors will be decreased.

B. An advantage of converting to an online system is the reduction of processing time.

C. Manual systems usually have distinct segregation of duties, i.e., authorization, recording, physical custody of assets, and periodic reconciliation. However, in a computer system this distinction is not always as clear since the computer might print the checks, record the transaction and reconcile the account balances.

D. Converting to an online system does not reduce the firm's risk exposures.

Question 44 - CIA 594 3-12 - Systems Controls and Security Measures

Which of the following procedures would enhance the control structure of a computer operations department?

I. Periodic rotation of operators.

II. Mandatory vacations.

III. Controlled access to the facility.

IV. Segregation of personnel who are responsible for controlling input and output.

A. I, II, III.
B. III, IV.
C. I, II.
D. All of the choices would enhance the control structure.

A. See the correct answer for the explanation.

B. See the correct answer for the explanation.

C. This response is incomplete.

D. All of the above practices are effective control measures. Periodic rotation and mandatory vacations provide other personnel with the ability to detect operator problems. Controlled access and segregation of duties allow for the separation of incompatible functions.

Question 45 - CIA 597 1-51 - Systems Controls and Security Measures

Which of the following statements is most accurate regarding the data security of an on-line computer system protected by an internal user-to-data access control program?

A. Security will be dependent upon the controls over the issuance of user ID’s and user authentication.
B. Access to data is controlled by restricting specific applications to specific files.
C. Access to data is controlled by restricting specific terminals to specific applications.

D. The use of this type of access control software will eliminate any significant control weaknesses.

A. This effective administration of user ID’s and authentication procedures is the key to enforcing personal accountability, the basis for the user-to-data authorization technique.

B. This is a job-to-data authorization technique.

C. This is a terminal-to-data authorization technique.

D. The use of access software alone does not address all access security risks.

Question 46 - CIA 595 III-67 - Systems Controls and Security Measures

Managers at a consumer products company purchased personal computer software from only recognized vendors, and prohibited employees from installing nonauthorized software on their personal computers. To minimize the likelihood of computer viruses infecting any of its systems, the company should also

A. Test all new software on a stand-alone personal computer.
B. Institute program change control procedures.
C. Recompile infected programs from source code backups.
D. Restore infected systems with authorized versions.

A. This would be the best method to minimize the likelihood of computer viruses infecting any of its systems. The program should be quarantined since it's possible that even the vendor's software can be infected.

B. Instituting program change control procedures is a good control practice, but it does not minimize the likelihood of computer viruses inflecting the system.

C. The procedure of recompiling infected programs from source code backups does not minimize the likelihood of computer viruses infecting the system.

D. Restoring infected systems with authorized versions will be done when the system is already infected. Thus, it does not minimize the likelihood of computer viruses infecting the system.

Question 47 - CMA 693 4-6 - Systems Controls and Security Measures

Data processed by a computer system are usually transferred to some form of output medium for storage. However, the presence of computerized output does not, in and of itself, assure the output's accuracy, completeness, or authenticity. For this assurance, various controls are needed. The major types of controls for this area include

A. Activity listings, echo checks, and pre-numbered forms.
B. Input controls, tape and disk output controls, and printed output controls.
C. Tape and disk output controls and printed output controls.
D. Transaction controls, general controls, and printout controls.

A. Activity listings, echo checks, and pre-numbered forms do not assure the output's accuracy, completeness, or authenticity.

B. Input controls, such as data observation and recording controls, data transcription controls, and edit tests, are designed to ensure that the data are entered into the program correctly. They are important because if data are not input correctly, the output will not be correct. Output controls are used to check that input and processing has resulted in valid output. Their objective is to assure the output's validity, accuracy, and completeness. There are two types of output application controls: (1) Validating processing results, such as activity (proof) listings and reconciliations; and (2) Printed output controls, such as forms control and output distribution controls.

C. Although tape and disk output controls and printed output controls are major types of controls for output, these alone do not assure the accuracy, completeness, or authenticity of computer output.

D. Transaction controls, general controls, and printout controls do not assure the accuracy, completeness, or authenticity of computer output.

Question 48 - CMA 685 5-25 - Systems Controls and Security Measures

Which one of the following is the best reason for developing a computer security plan?

A. Recovery from the damage associated with any identified threats can be assured.
B. A company can select the set of control policies and procedures that optimize computer security relative to cost.
C. The user departments can be assured that control policies are in place and their data files are secure.
D. All possible threats associated with the data processing equipment are identified.

A. It is not possible to have complete assurance of recovery from damage associated with any identified threats.

B. Developing a computer security plan gives management the opportunity to select the set of control policies and procedures that will safeguard physical facilities and provide for the safety, privacy, and integrity of the data while balancing the costs against the benefits.

C. Just because a computer security plan has been developed, that does not mean it has been implemented or that user departments can be assured of anything.

D. It is not possible to identify all possible threats associated with data processing equipment.

Question 49 - CIA 594 3-13 - Systems Controls and Security Measures

Encryption is least likely to be used in which of the following situations:

A. When wire transfers are made between banks.
B. When transactions are transmitted over local area networks.
C. When confidential data are sent by satellite transmission.
D. When financial data are sent over dedicated, leased lines.

A. Encryption is often used in this situation.

B. Various factors need to be considered. Encoding is important when confidential data are transmitted between geographically separated locations that can be electronically monitored. Although LANs may need encryption protection, the type of data and the described communication media make the other options appear more vulnerable.

C. See the correct answer for the explanation.

D. See the correct answer for the explanation.

Question 50 - CPA AUD R98-5 - Systems Controls and Security Measures

A customer intended to order 100 units of product Z96014, but incorrectly ordered nonexistent product Z96015. Which of the following controls most likely would detect this error?

A. Hash total.

B. Check digit verification.
C. Redundant data check.
D. Record count.

A. Hash totals are used to verify the completeness of inputted data, e.g., number of employees, total of invoice numbers.

B. Self-checking digits are used for error detection, e.g., incorrect identification numbers. It applies an algorithm to an input field and then applying the same algorithm to the code already entered to compare them. Thus, check digit verification would detect the error in this situation.

C. A redundant data check searches for duplicate information.

D. A record count counts the number of transactions processed in a batch.

Question 51 - CIA 1194 1-63 **-** Systems Controls and Security Measures

A controller became aware that a competitor appeared to have access to the company's pricing information. The internal auditor determined that the "leak of information" was occurring during the electronic transmission of data from branch offices to the head office. Which of the following controls would be most effective in preventing the leak of information?

A. Use of fiber optic transmission lines.
B. Encryption.
C. Asynchronous transmission.
D. Use of passwords.

A. Fibre optic transmission lines will improve the quality of the transmission, but will not prevent theft of data.

B. Encryption is the conversion of data into a code. You may be able be able to access the data by "tapping into" the transmission line. However, you need an encryption "key" in order to understand the data being sent.

C. Asynchronous transmission does not prevent theft of data, it speeds up the transmission process.

D. Use of passwords will control access at the sending location, and will limit access to the head office computer. Passwords, however, will not prevent someone from "tapping into" the transmission line.

Question 52 - CIA 594 3-35 - Systems Controls and Security Measures

The Computer Center of a company processes its prior week's sales invoices, as well as its returns and allowances, at the end of the week. Cash receipts, however, are processed and deposited daily. Each morning the mail receipts clerk prepares the cash receipts prelist in duplicate. The original prelist goes to the head cashier together with the checks and an adding machine tape. The duplicate copy goes to the accounts receivable supervisor. The separate remittance advices are sent to the data input clerk. At midday, the head cashier prepares the bank deposit slip which is taken to the bank. After returning from the bank, the head cashier compares the original prelist to the validated bank deposit slip, initials the documents, and files them in chronological order.

The following morning the accounts receivable supervisor receives a summary processing list from the Computer Center with various control totals from the nightly accounts receivable update. The total on the prior day's duplicate cash receipts prelist is then compared with the total showing the difference between the prior day's beginning and ending accounts receivable subsidiary ledger totals. The amount shown on yesterday's duplicate cash receipts prelist was $35,532.32. This morning the difference between the beginning and ending subsidiary ledger totals was $35,541.32.

What is the most likely reason for the difference between the two amounts?

A. An irregularity occurred during data output.
B. A remittance advice was recorded twice.
C. A transposition error occurred.
D. The total on the cash receipts prelist was miscalculated.

A. If an error or irregularity had occurred, it would have been likely during data input, not output.

B. The nature of the discrepancy, a small number in an even dollar amount evenly divisible by 9, suggests that double recording is less likely than a transposition error.

C. The amount of a discrepancy between two batch totals often provides a clue about the error.When a difference can be divided evenly by 9, a transposition error may have occurred during data input where the column amounts in two adjacent columns are exchanged. Other possibilities to consider include: looking for transactions exactly equal to the amount of the discrepancy or transactions equal to half of the discrepancy. In the later case, a transaction may have been incorrectly debited or credited.

D. If the prior day's cash receipts prelist were wrong, the Head Cashier is likely to have discovered and reported this either when preparing the bank deposit or after agreeing the prelist to the validated bank deposit.

Question 53 - CIA 598 3-72 - Systems Controls and Security Measures

Which of the following application controls would offer reasonable assurance that inventory data were completely and accurately entered?

A. Check digits.
B. Limit checking.
C. Batch totals.
D. Sequence checking.

A. A check digit allows the computer to automatically reject incorrect entries. The cumber-some computation required to establish the check digit, however, tends to limit its use to a few key entries. Check digits are never used to test accuracy of input for an entire grouping of input.

B. Limit checks are useful to determine whether an entry is within acceptable limits only. Such limitation makes the limit check unusable to test the accuracy of input.

C. Batch total checks provide a reasonably good test for completeness and accuracy of input.

D. Sequence checking provides a reasonably good test for completeness of input but does not test accuracy.

Question 54 - CIA 594 3-37 - Systems Controls and Security Measures

The Computer Center of a company processes its prior week's sales invoices, as well as its returns and allowances, at the end of the week. Cash receipts, however, are processed and deposited daily. Each morning the mail receipts clerk prepares the cash receipts prelist in duplicate. The original prelist goes to the head cashier together with the checks and an adding machine tape. The duplicate copy goes to the accounts receivable supervisor. The separate remittance advices are sent to the data input clerk. At midday, the head cashier prepares the bank deposit slip which is taken to the bank. After returning from the bank, the head cashier compares the original prelist to the validated bank deposit slip, initials the documents, and files them in chronological order.

The following morning the accounts receivable supervisor receives a summary processing list from the Computer Center with various control totals from the nightly accounts receivable update. The total on the prior day's duplicate cash receipts prelist is then compared with the total showing the difference between the prior day's beginning and ending accounts receivable subsidiary ledger totals. The amount shown on yesterday's duplicate cash receipts prelist was $35,532.32. This morning the difference between the beginning and ending subsidiary ledger totals was

$35,541.32.

The company probably uses which of the following processing systems:

A. Batch processing for cash receipts and sales invoices.
B. Remote batch processing for cash receipts.
C. On-line credit check inquiries.
D. Real-time processing for cash receipts, batch processing for sales invoices.

A. Batch processing is probably used.

B. It's not a remote location.

C. This isn't discussed, nor is it likely considering the technological state of the described systems.

D. Cash receipts are not updated immediately as they occur.

Question 55 - CIA 596 3-49 - Systems Controls and Security Measures

A company with several hundred stores has a network for the stores to transmit sales data to headquarters. The network is also used for:

- vendors to submit reorders
- stores to transmit special orders to headquarters
- regional distribution centers to communicate delivery and out-of-stock information to the stores
- the national office to distribute training materials
- store, regional, and national personnel to share any information they think helpful.

In order to accommodate the large volume of transmissions, large stores have their own satellite receiving/transmitting stations. Small stores use leased lines.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 this application software is through:

A. Monitoring software for the network.
B. Audit trails for items sold and received.
C. Access controls for terminals in the receiving department.
D. Change controls for inventory software.

A. Monitoring software is designed to monitor performance (human or machine) for specified functions such as number of tasks performed or capacity utilized.

B. Audit trails permit audits of transaction updates to data files, not programs.

C. Access control ensures that only authorized persons have access to specific or categories of information resources, but is not enough by itself to ensure integrity of application software.

D. Change control is the set of procedures that ensure that only authorized, tested programs are run in production.

Question 56 - CIA 1195 3-38 - Systems Controls and Security Measures

A large property insurance company has regional centers that customers call to report claims. Although the regional centers are not located in areas known to be prone to natural disasters, the company needs a disaster recovery plan that would restore call answering capacity in the event of a disaster or other extended loss of service. The best plan for restoring capacity in the event of a disaster would be to reroute call traffic to:

A. A hot site that duplicates regional facilities.
B. A third-party service center.
C. Non-affected regional centers.
D. A cold site that duplicates regional facilities.

A.
Duplicating regional facilities in a hot site would provide space, equipment, and some software but would be overly expensive and would still not provide personnel.

B.
Rerouting call traffic to a third-party service center would be overly expensive because of personnel cost, and service center personnel would not be trained for the company's calls.

C. Rerouting call traffic to non-affected regional centers is the best approach because it minimizes cost, maximizes the company's control over the reconfiguration, and permits calls to be answered by the company's skilled personnel.

D. Duplicating regional facilities in a cold site would be overly expensive and would still not provide equipment, software, or personnel.

Question 57 - CIA 594 I-32 - Systems Controls and Security Measures

Passwords for personal computer software programs are designed to prevent

A. Unauthorized use of the software.
B. Incomplete updating of data files.
C. Inaccurate processing of data.
D. Unauthorized access to the computer.

A. Passwords are designed to prevent the unauthorized use of software.

B. Passwords are concerned with preventing the unauthorized use of software, not with preventing incomplete updating of data files.

C. Passwords are concerned with preventing the unauthorized use of software, not with the inaccurate processing of data.

D. Passwords do not prevent the unauthorized access to the computer.

Question 58 - CIA 594 3-38 - Systems Controls and Security Measures

The Computer Center of a company processes its prior week's sales invoices, as well as its returns and allowances, at the end of the week. Cash receipts, however, are processed and deposited daily. Each morning the mail receipts clerk prepares the cash receipts prelist in duplicate. The original prelist goes to the head cashier together with the checks and an adding machine tape. The duplicate copy goes to the accounts receivable supervisor. The separate remittance advices are sent to the data input clerk. At midday, the head cashier prepares the bank deposit slip which is taken to the bank. After returning from the bank, the head cashier compares the original prelist to the validated bank deposit slip, initials the documents, and files them in chronological order.

The following morning the accounts receivable supervisor receives a summary processing list from the Computer Center with various control totals from the nightly accounts receivable update. The total on the prior day's duplicate cash receipts prelist is then compared with the total showing the difference between the prior day's beginning and ending accounts receivable subsidiary ledger totals. The amount shown on yesterday's duplicate cash receipts prelist was $35,532.32. This morning the difference between the beginning and ending subsidiary ledger totals was $35,541.32.

Assume the difference occurred because the input clerk keyed in the wrong amount during data input. Which of the following would most likely detect such an error?

A. A sequence check.
B. A field check.
C. Check digit verification.
D. Batch total controls.

A. A sequence check looks for numerical or alphabetical sequence discrepancies.

B. A field check detects if the input characters are of the expected type (i.e., alpha, numeric, or A/N)

C. Check digit verification is used when a self-checking digit is included in an identification number. It can detect errors in fields, such as account or inventory numbers.

D. Computerized batch processing environments need batch total controls to detect errors that cannot be discovered through other input edit checks. The other listed controls would not detect an input error in a dollar amount, they are designed to detect other errors.

Question 59 - CIA 598 3-59 - Systems Controls and Security Measures

Preventing someone with sufficient technical skill from circumventing security procedures and making changes to production programs is best accomplished by

A. Comparing production programs with independently controlled copies.
B. Running test data periodically.
C. Reviewing reports of jobs completed.
D. Providing suitable segregation of duties.

A. Comparison of production programs and controlled copies will disclose changes, but will not prevent them.

B. Periodic running of test data will detect changes, but will not prevent them.

C. The reviews of jobs processed will disclose access, but will not prevent it.

D. When duties are separated, users cannot obtain a detailed knowledge of programs and computer operators cannot gain unsupervised access to production programs.

Question 60 - CIA 597 III-37 - Systems Controls and Security Measures

Output controls ensure that the results of computer processing are accurate, complete, and properly distributed. Which of the following is **not** a typical output control?

A. Periodically reconciling output reports to make sure that totals, formats, and critical details are correct and agree with input.
B. Reviewing the computer processing logs to determine that all of the correct computer jobs executed properly.
C. Matching input data with information on master files and placing unmatched items in a suspense file.
D. Maintaining formal procedures and documentation specifying authorized recipients of output reports, checks, or other critical documents.

A. Periodically reconciling output reports is an output control.

B. Reviewing the computer processing logs to determine that all of the correct computer jobs executed properly is an output control.

C. Matching input data with information on master files and placing unmatched items in a suspense file is a

processing control, not an output control. Output controls provide some reasonable assurance that the processing results (account listings or displays, reports, files, invoices, or disbursement checks) is accurate and that only authorized personnel receive the output.

D. Maintaining formal procedures and documentation is an output control.

Question 61 - CIA 1196 1-36 - Systems Controls and Security Measures

The automated system contains a table of pay rates which is matched to the employee job classifications. The best control to ensure that the table is updated correctly for only valid pay changes would be to:

A. Ensure that adequate edit and reasonableness checks are built into the automated system.
B. Limit access to the data table to management and line supervisors who have the authority to determine pay rates.
C. Require a supervisor in the department, who does not have the ability to change the table, to compare the changes to a signed management authorization.
D. Require that all pay changes be signed by the employee to verify that the change goes to a bona fide employee.

A. Edit checks will not detect invalid changes.

B. Access to the database (tables) of employee rates should be severely restricted to authorized personnel within the human resources department or payroll personnel. Proper supervisor personnel should approve the rates, but not have access to the tables.

C. This would be the most appropriate control because it (a) requires supervisory signed approval, (b) limits access to the tables to selected personnel within the payroll department, and (c) provides independent reconciliation of all changes.

D. The concern is not with bona fide employees. The concern is to gain assurance that all changes to the table are properly authorized and input into the system. Further, one pay rate will apply to more than one employee.

Question 62 - CMA Sample Q.4-10 - Systems Controls and Security Measures

An accounting system identification code that uses a sum-of-digits check digit will detect all of the following errors except

A. Validity errors.
B. Transcription errors.
C. Transposition errors.
D. Completeness errors.

A. Validity errors will be detected, because the sum of the digits will not check with the check digit.

B. Transcription errors will be detected, because the sum of the digits will not check with the check digit.

C. Transposition errors will not be detected. Even though the digits will be in the wrong sequence, the sum of the digits will be correct. Therefore, the sum of the digits will check with the check digit.

D. Completeness errors will be detected, because the sum of the digits will not check with the check digit.

Question 63 - CIA 1195 I-28 - Systems Controls and Security Measures

As organizations become more computer integrated, management is becoming increasingly concerned with the quality of access controls to the computer system. Which of the following provides the most accountability?

	Option I	Option II	Option III	Option IV
Restrict access by:	Individuals	Groups	Individuals	Departments
Identify computer data at:	Field level	Workstation	Workstation	Individual record level
Restrict access:	Need to know	Right to know	Normal processing by employee type	Items identified as processed by department
Identify users by:	Password	Password	Key access to workstation, or password on workstation	Departmental password
Limit ability to:	Delete, add,or modify data	Add or delete files	Add, delete, or modify data stored at workstation	Add, delete, or modify data normally processed by department

A. Option II.
B. Option IV.
C. Option I.
D. Option III

A. See the correct answer.

B. See the correct answer.

C. Access to a computer system should be restricted to individuals who have a need to know, and is consistent with their responsibility. The system should also be restricted at the field level, instead of at the workstation level. The problem with workstations is that they are connected to a larger network, and security may not be adequate. In addition, passwords should be required to identify the user and users should be limited to deleting, adding and modifying data.

D. See the correct answer.

Question 64 - CIA 579 II-5 - Systems Controls and Security Measures

Which of the following should the auditor recommend as the **most** economical point at which to correct input errors in an online system?

A. Output data are balanced with computer-produced control totals and delivered to the user.
B. Entry of data into each field of a record is completed.
C. Entry of data into each record is completed.
D. Input data are balanced with computer-produced control totals.

A. The most economical point at which to correct input errors in an online system is when the data is first entered into the system.

B. The most economical point at which to correct input errors in an online system is when the data is first entered into the system. Thus, the entry of data into each field of a record is the most economical point.

C. The most economical point at which to correct input errors in an online system is when the data is first entered into the system.

D. The most economical point at which to correct input errors in an online system is when the data is first entered into the system.

Question 65 - CIA 588 II-31 - Systems Controls and Security Measures

Which of the following represents an internal control weakness in a computer-based system?

A. The data control group is solely responsible for distributing reports and other output.
B. The computer librarian maintains custody and record keeping for computer application programs.
C. Computer operators have access to operator instructions and the authority to change programs.
D. Computer programmers write and revise programs designed by analysts.

A. Distributing computer reports is an appropriate function of the control group.

B. Maintaining custody and record keeping is an appropriate function for the computer librarian.

C. Computer operators should have access to operator instructions, but they cannot have the authority to change programs. Changing programs is the function for the computer programmer.

D. Programmers responsibility is to write, test and document the systems as designed by analysts.

Question 66 - CIA 591 III-24 - Systems Controls and Security Measures

The best **preventive** measure against a computer virus is to

A. Prepare and test a plan for recovering from the incidence of a virus.
B. Allow only authorized software from known sources to be used on the system.
C. Compare software in use with authorized versions of the software.
D. Execute virus exterminator programs periodically on the system.

A. Preparing and testing a plan for recovering from the incidence of a virus is a corrective measure, not a preventive measure.

B. The best preventive measure is to allow only authorized software from known sources to be on the system. It is expected that authorized software will be virus free.

C. Comparing software in use with authorized versions of the software is a detective measure, not a preventive measure.

D. Executing virus exterminator programs is a detective measure, not a preventive measure.

Question 67 - CIA 596 3-42 - Systems Controls and Security Measures

A mortgage broker prepared sample mortgage payment schedules on a personal computer to illustrate different payment plans to prospective loan customers. The schedules were especially helpful for loans with variable rates because the schedules illustrated how loan balances would fluctuate over multi-year horizons with different interest rate trends. The mortgage company's literature was not nearly as helpful, and the broker was convinced the schedules helped customers understand and appreciate the sophisticated loan types, which led to more loans.

The potential risk of erroneous logic in the schedules could best be minimized by:

A. Requiring adequate documentation for the schedules.
B. Adequate independent testing of the application.
C. Designing control procedures for sharing the schedules.
D. Ensuring adequate backup procedures for the application.

A. There should be adequate documentation for the schedules, but that would not detect or correct logic errors in the schedules.

B. Any potential risk of erroneous logic in the schedules could be minimized by adequate independent testing of the application to detect any errors that the broker could not recognize.

C. To the extent the schedules are shared with other brokers, there should be adequate control procedures, but that would not detect or correct logic errors in the schedules.

D. The application should have adequate backup procedures, but that would not detect or correct logic errors in the schedules.

Question 68 - CIA 1196 3-54 **-** Systems Controls and Security Measures

A company is very conscious of the sensitive nature of company information. Because company data is valuable, the most important thing that the security administrator should monitor is:

A. Access to operational data by privileged users.
B. Data owner specification of access privileges.
C. Multiple access to data by data owners.
D. Management authorization of modified access.

A. The security administrator should report access to data or resources by privileged users so that the access can be monitored for appropriate and authorized usage.

B. Data owner specification of access privileges is normal and is typically maintained by the system and need not be reported by the security administrator.

C. Multiple access to data by data owners, the individuals responsible for creating and maintaining specific data, is a normal occurrence.

D. Management authorization of modified access is expected as needs or conditions change and is not an event typically reported.

Question 69 - CPA 1195 A-14 **-** Systems Controls and Security Measures

Which of the following controls most likely could prevent computer personnel from modifying programs to bypass programmed controls?

A. Segregation of duties within computer for computer programming and computer operations.
B. Periodic management review of computer utilization reports and systems documentation.
C. Physical security of computer facilities in limiting access to computer equipment.
D. Participation of user department personnel in designing and approving new systems.

A. The segregation of duties is a primary function of a control system. The functions of programmer and computer operator should be segregated in order to prevent unauthorized modifications of the programs.

B. Management's review of computer utilization reports and systems documentation will not prevent unauthorized modifications of the programs.

C. Physical security does not prevent programmers from having access to data communications. Thus, physical security might not prevent unauthorized modifications.

D. The participation of user department personnel in designing and approving new systems will not prevent computer personnel from modifying an existing system.

Question 70 - CIA 1195 I-32 **-** Systems Controls and Security Measures

Most large-scale computer systems maintain at least three program libraries: production library (for running programs); source code library (maintains original source coding); and test library (for programs which are being changed). Which of the following statements is correct regarding the implementation of sound controls over computer program libraries?

A. Only the program librarian should be allowed to make changes to the production library.
B. Only programmers should have access to the production library.
C. The computer operator should have access to both the production library and the source code library to assist in diagnosing computer crashes.
D. Users should have access to the test library to determine whether all changes are properly made.

A. Program librarians are accountable for the programs in the production library. Thus, only the program librarian should be allowed to make changes.

B. Proper control states that programmers should not have access to the production library.

C. The computer operator should not have access to both the production library and the source code library. If computer operators did have access to both program libraries, they could make unauthorized changes to the computer programs.

D. Users should not have access to the test library. Users may not have the proper skills to make necessary changes.

Question 71 - CIA 598 3-49 **-** Systems Controls and Security Measures

Minimizing the likelihood of unauthorized editing of production programs, job control language, and operating system software can best be accomplished by:

A. Effective network security software.
B. Database access reviews.
C. Good change-control procedures.
D. Compliance reviews.

A. The purpose of network security software is to provide logical controls over the network.

B. Frequently, the purpose of database reviews is to determine if: (1) users have gained access to database areas for which they have no authorization, and (2) authorized users can access the database using programs that provide them with unauthorized privileges to view and/or change information.

C.

Change control is the process of strictly controlling changes to a system or program. All changes should require authorization by the appropriate personnel, and when a system or program is changed, the changes should not be made to the copy of the program that is being used, but rather to a copy. And any changes must also be properly reflected in all of the related documentation to ensure that changes have a minimal impact on processing and results in minimal risk to the system.

Program change control comprises: (1) maintaining records of change authorizations, code changes, and test results; (2) adhering to a systems development methodology (including documentation); (3) authorizing changeovers of subsidiary and headquarters' interfaces; and (4) restricting access to authorized source and executable codes.

D. The purpose of compliance reviews is to determine whether an organization has complied with applicable internal and external procedures and regulations.

Question 72 - CIA 594 3-31 - Systems Controls and Security Measures

A computer program will not generate month-end balances if transactions are missing. This is an example of a:

A. Detective control.
B. Corrective control.
C. Preventive control.
D. Discretionary control.

A.

See the correct answer for the explanation.

B.

See the correct answer for the explaantion.

C. A preventive control is designed to prevent errors from occurring.

D. See the correct answer for the explanation.

Question 73 - CIA 1193 I-29 - Systems Controls and Security Measures

A mail-order retailer of low-cost novelty items is receiving an increasing number of complaints from customers about the wrong merchandise being shipped. The order code for items has the format wwxxyyzz. The major category is ww, xx is the minor category, yy identifies the item, and zz identifies the catalog. In many cases, the wrong merchandise was sent because adjacent characters in the order code had been transposed. The best control for decreasing the number of orders with the wrong merchandise is to

A. Add check-digits to the order codes and verify them for each order.
B. Use a master file reference for all order codes to verify the existence of items.
C. Require customers to specify the name for each item they order.
D. Separate the parts of the order code with hyphens to make the characters easier to read.

A. The best control for decreasing the number of orders with the wrong merchandise is to add check-digits to the order codes and verify them for each order.

B. Using a master file reference for all order codes to verify the existence of items would not solve the problem of transposed characters.

C. Requiring customers to specify the name for each item they order would not allow the company to detect erroneous codes.

D. Separating the parts of the order code with hyphens would make the characters easier to read, but would not solve the problem of transposed characters.

Question 74 - HOCK CMA P1D3 07 - Systems Controls and Security Measures

Which of the following is not an example of a physical access control?

A. Having the computer center be protected from natural disasters as much as possible.
B. Shredding confidential documents when they are no longer needed.

C. Having access to the computer center be controlled by a security guard who can open the locked doors only by "buzzing in" authorized personnel.
D. Requiring scanning of magnetic ID cards to enter the computer center, with all access being logged automatically.

A. This is an example of a physical control because it pertains to keeping the computer equipment safe from damage or loss due to natural disasters.

B. While shredding sensitive documents when they are no longer needed is a very important output control, it does not pertain to the physical security of the computing equipment.

C. This is an example of a physical control because it pertains to controlling physical access to the computer equipment.

D. This is an example of a physical control because it pertains to controlling physical access to the computer equipment.

Question 75 - CIA 597 3-40 **-** Systems Controls and Security Measures

A department purchased one copy of a word processing software program for internal use. The manager of the department installed the program on the manager’s office computer and then made two complete copies of the original diskettes. Copy number 1 was solely for backup purposes. Copy number 2 was for use by another member of the department. In terms of software licenses and copyright law, which of the following is correct?

A. Neither copy is legal.
B. Only copy number 2 is legal.
C. Both copies are legal.
D. Only copy number 1 is legal.

A. One of the copies is indeed legal.

B. Any copy other than a backup copy is illegal and is a license violation.

C. Only copy number 1 is legal.

D. A backup copy is legal under the copyright law.

Question 76 - CIA 593 I-42 **-** Systems Controls and Security Measures

Contingency plans for information systems should include appropriate backup agreements. Which of the following arrangements would be considered too vendor-dependent when vital operations require almost immediate availability of computer resources?

A. A "cold site" arrangement.
B. A "hot site" arrangement.
C. A "cold and hot site" combination arrangement.
D. Using excess capacity at another data center within the organization.

A. A "cold site" is a facility where power and space are available to install processing equipment, but it is not immediately available. If an organization uses a cold site, its disaster recovery plan must include arrangements to get computer equipment installed there quickly. Thus, a "cold site" arrangement is too vendor-dependent because the company has to rely on the vendor for timely delivery of the equipment.

B. A "hot site" arrangement must be fully operational and immediately available. A "hot site" arrangement cannot be too vendor-dependent.

C. A "cold and hot site" combination arrangement is where the hot sit is first used until the cold site is prepared. Thus, it is not too vendor-dependent.

D. Using excess capacity at another data center within the organization ensures that assets needed for backup are available. Thus, it is not too vendor-dependent.

Question 77 - CMA 685 5-28 - Systems Controls and Security Measures

Routines that use the computer to check the validity and accuracy of transaction data during input are called

A. Edit programs.
B. Integrated test facilities.
C. Operating systems.
D. Compiler programs.

A. Edit programs or input validation routines are programs that check the validity and accuracy of input data. They perform edit tests by examining specific fields of data and rejecting transactions if their data fields do not meet data quality standards. Edit tests include completeness checks, which ensure that data is input into all required fields; limit checks, which ensure that only data within predefined limits will be accepted by the system; validity checks, which match the input data to an acceptable set of values or match the characteristics of input data to an acceptable set of characteristics; overflow checks, which make sure that the number of digits entered in a field is not greater than the capacity of the field; key verification, or the process of inputting the information again and comparing the two results; and check digits, which can be used for determining whether a number has been transcribed properly. A check digit is a digit that is a function of the other digits within a set of numbers. If a typographical error is made in input, the check digit will recognize that something has been input incorrectly.

B. An Integrated Test Facility (ITF) involves the use of test data and the creation of fictitious entities, such as fictitious employees, fictitious vendors, fictitious products, and fictitious accounts, within the master files of the computer system. Or alternatively, a separate, fictitious company may be used. The test data in an ITF are processed along with real data. No one knows that the data being processed includes these fictitious entries to fictitious records. An Integrated Test Facility is used by an auditor to check the operation of programs. By checking them this way, the auditor can be sure that the programs being checked are the same programs as those that are being used to process the real data. However, an Integrated Test Facility does not check the validity or accuracy of transaction data during input.

C. The operating system controls the operation of the system but it does not check the validity or accuracy of transaction data during input.

D. A compiler translates programs written in a higher level language into machine language. Computer programs are error tested by using a compiler, which checks for programming language errors. However, a compiler does not check the validity or accuracy of transaction data during input.

Question 78 - HOCK CMA P1D3 03 - Systems Controls and Security Measures

If Sarah Corp. wants to send an order over the Internet to Lee Inc. for raw materials, which of the following would be the **correct** methodology for encrypting the order so that only Lee Inc. will be able to decrypt and read the contents of the order?

A. Sarah Corp. would encrypt the message using Lee Inc's public key, and Lee Inc. would decrypt the message using their own private key.
B. Sarah Corp. would encrypt the message using Sarah Corp's private key, and Lee Inc. would decrypt the message using Sarah Corp's public key.
C. Sarah Corp. would request that Lee Inc. email their secret key so that Sarah Corp. could use it to encrypt the order for transmission.
D. Sarah Corp. would encrypt the message using Lee Inc's private key, and Lee Inc. would decrypt the message

using their own public key.

A. This is correct. Lee Inc's public key would be publicly available, and only Lee Inc., using their private key, would be able to decrypt any message encrypted with their public key.

B. Because Sarah Corp's public key is available publicly, any message encrypted with Sarah Corp's private key could be decrypted by anyone. Sarah Corp. may as well send the order without encryption.

C. Email cannot be trusted to be secure when sending via the Internet, and therefore the secret key could be intercepted and used by a third party to decrypt Sarah Corp's order details.

D. No one but Lee Inc. should have possession of their private key, so neither Sarah Corp. nor any other company would ever use Lee Inc's. private key.

Question 79 - CIA 596 3-52 - Systems Controls and Security Measures

A department store company with stores in 11 cities is planning to install a network so that stores can transmit daily sales by item to headquarters and store salespeople can fill customer orders from merchandise held at the nearest store. Management believes that having daily sales statistics will permit better inventory management than is the case now with weekly deliveries of sales reports on paper. Salespeople have been asking about online inventory availability as a way to retain the customers that now go to another company's stores when merchandise is not available. The planning committee anticipates many more applications so that in a short time the network would be used at or near its capacity.

As the planning committee identified the many applications that the proposed network could support, the committee realized that a significant risk could be:

A. Inability to obtain needed network compo¬nents from vendors as usage increases.
B. Lack of enthusiasm for installing and using the new network in the stores.
C. Incomplete, inadequately tested, or unauthorized application software.
D. Patent and trademark violations when using new application software.

A. Given the standard nature of the network, it is unlikely that the company would not be able to obtain needed components from vendors as usage increases.

B. On the contrary, management has stated its intention to install the network, salespeople have been asking for features that the network could provide, and the planning committee has identified many potential applications.

C. The pressure for the department store company to be competitive is so great that there may be a significant risk that application software could be incomplete, inadequately tested, or unauthorized.

D. These types of violations do not occur with in-house development.

Question 80 - CMA 695 4-22 - Systems Controls and Security Measures

In the organization of the information systems function, the most important separation of duties is

A. Having a separate information officer at the top level of the organization outside of the accounting function.
B. Not allowing the data librarian to assist in data processing operations.
C. Assuring that those responsible for programming the system do not have access to data processing operations.
D. Using different programming personnel to maintain utility programs from those who maintain the application programs.

A. Having a separate information officer at the top level of the organization outside of the accounting function is not as a critical separation of duty as between programmers and data processors.

B. Librarians maintain the documentation, programs and data files, but they should not have access to equipment. Furthermore, librarians can assist in data processing operations.

C. The separation of duties is critical in a IS control environment. Programmers and analysts are responsible for designing, writing, testing and documenting the system, but they should not have access to data processing operations.

D. Having a policy where different programmers would maintain different programs would not be an effective control function. Typically, programmers handle all kinds of different programs.

Question 81 - CIA 596 I-57 **-** Systems Controls and Security Measures

Which one of the following input controls or edit checks would catch certain types of errors within the payment amount field of a transaction?

A. Record count.
B. Check digit.
C. Echo check.
D. Limit check.

A. A record count counts the number of records processed.

B. Self-checking is the process of applying an algorithm to an input field and then applying the same algorithm to the code already entered to compare them.

C. Echo check is the process of sending the received data back to the sending computer to compare with what was actually sent to make sure that it is the same. For example, a CPU will send a signal to the printer, and the printer, prior to printing, will send a signal back to the CPU stating that the proper print position has been activated.

D. A limit and range checks is simply a maximum or minimum number for a record. For example, the number of days worked in a week cannot exceed 7.

Question 82 - CIA 1196 3-39 **-** Systems Controls and Security Measures

In one company, the application systems must be in service 24 hours a day. The company’s senior management and information systems management have worked hard to ensure that the information systems recovery plan supports the business disaster recovery plan. A crucial aspect of recovery planning for the company is ensuring that:

A. Management personnel can fill in for operations staff should the need arise.
B. Capacity planning procedures accurately predict workload changes.
C. Organizational and operational changes are reflected in the recovery plans.
D. Changes to systems are tested thoroughly before being placed into production.

A. A good recovery plan would specify how operational staff might be replaced should the need arise, but their replacements might not be management personnel.

B. Being able to predict workload changes accurately permits a company to minimize its information systems facility costs, but that is not a part of recovery planning.

C. A crucial aspect of recovery planning for the company is ensuring that organizational and operational changes are incorporated in the plans because such changes have the potential to make the recovery plans inapplicable.

D. It is vital that changes to systems be tested thoroughly before being placed into production, but that is not a part of recovery planning.

Question 83 - HOCK CMA P1D3 04 - Systems Controls and Security Measures

Which of the following is a technical computer crime that requires sophisticated knowledge of computers and/or networks?

A. Dumpster diving.
B. Denial of service.
C. Phising.
D. Social engineering.

A. Dumpster diving requires no computer knowledge whatsoever, only the willingness to get a little bit dirty.

B. A denial of service (DOS) attack involves overwhelming a server or cluster of servers to the point that they are unable to respond to legitimate requests, thereby making them unavailable for normal usage. A DOS attack certainly requires a reasonable amount of technical and network skills to successfully execute.

C. Phishing refers to deceiving others into revealing personal and/or sensitive information such as credit card numbers, social security numbers, passwords, etc., usually through an email message. This requires no sophisticated technical knowledge beyond being able to send an email.

D. Social engineering refers to using social tactics to gain information. For example, an employee from one company may call a competitor and pretend to be a coworker who forgot how to access certain files, hoping that the person who they are talking to will reveal that information. No technical skills are required; in fact, social skills would be the most essential when attempting to gain information through social engineering.

Question 84 - CIA 596 3-43 - Systems Controls and Security Measures

It is important to maintain proper segregation of duties in a computer environment. Which of the following access setups is appropriate for updating production data and modifying production programs?

A. Users can update production data and application programmers can modify production programs.
B. Users can modify production programs and application programmers can update production data.
C. Users can update production data.
D. Users can update production data and both users and application programmers can modify production programs.

A. Application programmers should not be able to directly change production programs. They should submit changes to the change control unit for placing into production.

B. Application programmers should never have update access to production data. Users have no need to change production programs.

C. Users need to update data through applications programs.

D. None of these access rights would be appropriate. Application programmers should not have access to production data and only the change control unit should be able to modify production programs.

Question 85 - CIA 590 I-20 - Systems Controls and Security Measures

The practice of maintaining a test program library separate from the production program library is an example of

A. Physical security.
B. An input control.
C. An organizational control.

D. A concurrency control.

A. Physical security is also an organizational control, but it refers to the restriction on physical access, not the separation of test program library from the production program library.

B. Input controls provide assurance that the data inputted has the proper authority, and has not be lost, added or changed.

C. Organizational control includes the proper segregation of duties. Thus, the practice of maintaining a test program library separate from the production program library is an example of an organizational control.

D. Concurrency controls is the process of managing the situation when two or more programs are trying to access the same information at the same time.

Question 86 - CIA 594 1-65 - Systems Controls and Security Measures

Backup and recovery controls are crucial to ensuring the reliability of a teleprocessing network. When reviewing the controls over backup and recovery, which of the following would not be included?

A. Adequacy of user data file backups on the LAN.
B. Controls over hardware and software failures.
C. Use and adequacy of encryption processes.
D. Adequacy of documents/manuals informing all personnel of their backup and recovery responsibilities.

A. Data file backups are critical and the auditor would review the adequacy to the backup files.

B. The controls over hardware and software failures are included in the review of backup and recovery.

C. Encryption is a communication control for security, and not related to backup and recovery.

D. Documented responsibilities for backup and recovery and personnel knowledge of their responsibilities is very important in the backup and recovery process. Auditors would review the documentation and knowledge of responsibilities.

Question 87 - CIA 594 3-36 - Systems Controls and Security Measures

The Computer Center of a company processes its prior week's sales invoices, as well as its returns and allowances, at the end of the week. Cash receipts, however, are processed and deposited daily. Each morning the mail receipts clerk prepares the cash receipts prelist in duplicate. The original prelist goes to the head cashier together with the checks and an adding machine tape. The duplicate copy goes to the accounts receivable supervisor. The separate remittance advices are sent to the data input clerk. At midday, the head cashier prepares the bank deposit slip which is taken to the bank. After returning from the bank, the head cashier compares the original prelist to the validated bank deposit slip, initials the documents, and files them in chronological order.

The following morning the accounts receivable supervisor receives a summary processing list from the Computer Center with various control totals from the nightly accounts receivable update. The total on the prior day's duplicate cash receipts prelist is then compared with the total showing the difference between the prior day's beginning and ending accounts receivable subsidiary ledger totals. The amount shown on yesterday's duplicate cash receipts prelist was $35,532.32. This morning the difference between the beginning and ending subsidiary ledger totals was $35,541.32.

What is the first thing that the accounts receivable supervisor should do to try to resolve the discrepancy in the two amounts?

A. Send a copy of the prelist and the Summary Processing List to the Internal Audit Department.
B. Manually recalculate the total on the cash receipts prelist.

C. Call the head cashier to determine the amount deposited.
D. Compare the accounts receivable subsidiary ledger total with the total in the accounts receivable general ledger account.

A. Minor errors should be investigated and corrected by operating personnel.

B. The external validation in A is better, as well as more efficient.

C. This takes a short period of time and includes external verification of the amount on the cash receipts prelist. This would prove that an error was made during data input suggesting that further investigative effort should be concentrated there.

D. The narrative implies that the AR General Ledger Account is updated when the AR subsidiary ledgers are updated. Thus, there would be no difference between these amounts.

Question 88 - CIA 598 3-70 - Systems Controls and Security Measures

Computer program libraries can best be kept secure by:

A. Monitoring physical access to program library media.
B. Installing a logging system for program access.
C. Denying access from remote terminals.
D. Restricting physical and logical access.

A. Monitoring physical access to program library media would control only unauthorized physical access.

B. Installing a logging system for program access would permit detection of unauthorized access but would not prevent it.

C. Denying all remote access via terminals would likely be inefficient and would not secure program libraries against physical access.

D. Restricting physical and logical access secures program libraries from unauthorized use, in person and remotely via terminals.

Question 89 - CIA 596 III-36 - Systems Controls and Security Measures

Change control typically includes procedures for separate libraries for production programs and for test versions of programs. The reason for this practice is to

A. Facilitate user input on proposed changes.
B. Segregate incompatible duties.
C. Promote efficiency of system development.
D. Permit unrestricted access to programs.

A. Separating production and test versions of programs will not facilitate user input on proposed changes.

B. Separating production and test versions of programs is the means of restricting access to production programs to individual users. Thus, the effect is a separation of incompatible duties, such as programmers and operators.

C. Separating libraries for production programs and for test versions of programs would require a specific policy or procedure. Thus, separating these functions may in fact decrease efficiency of system development.

D. Separating production and test versions of programs will not permit unrestricted access to programs.

Question 90 - CPA 594 A-16 - Systems Controls and Security Measures

Which of the following statements most likely represents a disadvantage for an entity that keeps data files on a server rather than on a manual system?

A. Attention is focused on the accuracy of the programming process rather than errors in individual transactions.
B. It is usually more difficult to compare recorded accountability with the physical count of assets.
C. It is usually easier for unauthorized persons to access and alter the files.
D. Random error associated with processing similar transactions in different ways is usually greater.

A. Focusing attention on the accuracy of the programming processes is an advantage of using a server, not a disadvantage.

B. It is neither more nor less difficult to compare recorded accountability with the physical count of assets.

C. Generally, in a manual system, one individual is usually assigned responsibility for maintaining and safeguarding the records. But, in a server environment, it is usually easier for unauthorized persons to access and alter the files.

D. Random error associated with processing similar transactions is a disadvantage of a manual system.