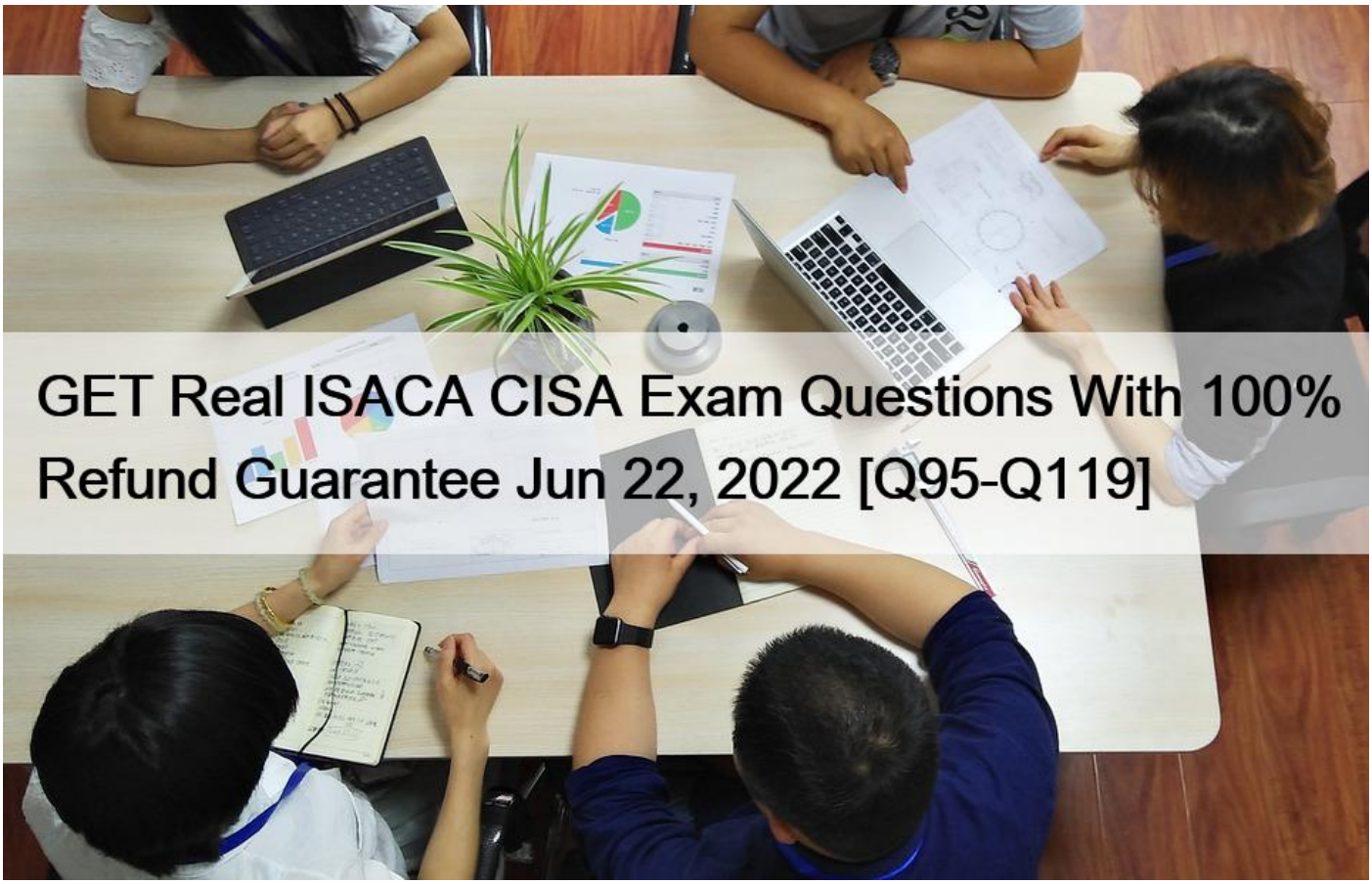
GET Real ISACA CISA Exam Questions With 100% Refund Guarantee Jun 22, 2022 [Q95-Q119



GET Real ISACA CISA Exam Questions With 100% Refund Guarantee Jun 22, 2022
Get Special Discount Offer on CISA Dumps PDF

What are the strengths of the candidate who wants to take the ISACA CISA Exam

There are qualified and knowledgeable instructors. They specialize in the subject matter and can teach it well. The facilities that the school has for learning purposes are extremely sophisticated and modern. The library is large and full of resources for students to enjoy and boost their learning abilities. The school has a good reputation in the community, which means students can find jobs easily with a degree from this university. An online program makes it possible for more people to enroll in the university even if they have family or work commitments. This is an excellent option for someone who is looking to get ahead in their career but doesn't have the time or money to go away from home anymore.

What are the options available for the registration of the ISACA CISA Certification Exam:

You can register in three ways- in person, through the phone, or via the Internet.
To register for the exam in person, you have to visit one of the testing centers in your area. You will have to carry an authentic ID proof with you. After filling out a form you have to pay a processing fee online or in the bank. Your payment needs to be made through a credit card or a check. You can also offer a cash payment to the Pearson VUE representative conducting the exam. If you want to take the exam and register for it, you need to retain a copy of your form and the payment receipt. You can get your card replaced if the store will not allow you to get a new one. Even though you have been issued a new card, it is wise to retain a copy of

both the old and new ones in case they are needed. If you are not prepared for the exam and want to take it in the future, you can add the certification exam to the cart.

What are the language, duration, and format of the ISACA CISA Certification Exam?

The Language, span, and format of the ISACA CISA Certification Exam are as follows:
Language: The CISA exam is being administered in 11 languages. Those languages are Chinese Traditional, Chinese Simplified, English, French, German, Hebrew, Italian, Japanese, Korean, Spanish, and Turkish.A number of questions: There will be 150 questions in the CISA exam. You have to answer all the questions. Questions of the CISA exam will be in the form of multiple choice.Time Duration: Candidates will have 240 min (04 hours) to attempt his/her CISA exam.

Q95. Which of the following statement is NOT true about smoke detector?
* The Smoke detectors should be above and below the ceiling tiles throughout the facilities and below the raised in the computer room floor
* The smoke detector should produce an audible alarm when activated and be linked to a monitored station
* The location of the smoke detector should be marked on the tiling for easy identification and access
* Smoke detector should replace fire suppression system

Explanation/Reference:

The word NOT is the keyword used in the question. You need to find out a statement which is not applicable to smoke detector. Smoke detector should supplement, not replace, fire suppression system.

For CISA exam you should know below information about smoke detector.

The Smoke detectors should be above and below the ceiling tiles throughout the facilities and below the raised computer room floor.

The smoke detector should produce an audible alarm when activated be linked to a monitored station The location of the smoke detector should be marked on the tiling for easy identification and access.

Smoke detector should supplement, not replace, fire suppression system

The following were incorrect answers:

The other presented options are valid statement about smoke detector.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number373

Q96. Communicating which of the following would BEST encourage management to initiate appropriate actions following the receipt of report findings?
* Risk implications of the observations
* Strict deadlines to close all observations
* Statistical sampling used to derive observations
* Recommendations that align with the business strategy

Section: Governance and Management of IT

Q97. Which of the following BEST describes the role of a directory server in a public key infrastructure (PKI)?
* Encrypts the information transmitted over the network
* Makes other users’ certificates available to applications

* Facilitates the implementation of a password policy
* Stores certificate revocation lists (CRLs)

Section: Protection of Information Assets

Explanation:

A directory server makes other users’ certificates available to applications. Encrypting the information

transmitted over the network and storing certificate revocation lists (CRLs) are roles performed by a

security server. Facilitating the implementation of a password policy is not relevant to public key

infrastructure (PKl).

Q98. An organization has suffered a number of incidents in which USB flash drives with sensitive data have been lost. Which of the following would be MOST effective in preventing loss of sensitive data?

* Modifying the disciplinary policy to be more stringent
* Implementing a check-in/check-out process for USB flash drives
* Issuing encrypted USB flash drives to staff
* Increasing the frequency of security awareness training

Section: Information System Operations, Maintenance and Support

Q99. What is the PRIMARY purpose of documenting objectives when preparing for an engagement?

* To help prioritize and schedule audite meetings
* To help ensure maximum use of audit resources during the engagement
* To identify areas with relatively high probability of material problems
* To address the overall risk associated with the activity under review

Q100. Total billing amounts on invoices are automatically transferred to an organization’s account ledger weekly.

During an IS audit, the auditor discovers that one week’s billing is missing from the ledger. Which of the following areas should the auditor examine FIRST?

* Module access rights
* Batch processing controls
* Change management
* Annual reconciliations

Q101. When reviewing an organization’s logical access security, which of the following should be of MOST concern to an IS auditor?

* Passwords are not shared.
* Password files are not encrypted.
* Redundant logon IDs are deleted.
* The allocation of logon IDs is controlled.

Section: Protection of Information Assets

Explanation:

When evaluating the technical aspects of logical security, unencrypted files represent the greatest risk. The sharing of passwords, checking for the redundancy of logon IDs and proper logon ID procedures are essential, but they are less important than ensuring that the password files are encrypted.

Q102. An organization having a number of offices across a wide geographical area has developed a disaster

recovery plan (DRP). Using actual resources, which of the following is the MOST cost-effective test of the

DRP?
* Full operational test
* Preparedness test
* Paper test
* Regression test

Section: Protection of Information Assets

Explanation:

A preparedness test is performed by each local office/area to test the adequacy of the preparedness of

local operations for the disaster recovery. A paper test is a structured walk- through of the disaster recovery

plan and should be conducted before a preparedness test. A full operational test is conducted after the

paper and preparedness test. A regression test is not a disaster recovery planning (DRP) test and is used

in software maintenance.

Q103. Which of the following exploit vulnerabilities to cause loss or damage to the organization and its assets?
* Exposures
* Threats
* Hazards
* Insufficient controls

Section: Protection of Information Assets

Explanation:

Threats exploit vulnerabilities to cause loss or damage to the organization and its assets.

Q104. If a database is restored from information backed up before the last system image, which of the following is recommended?
* The system should be restarted after the last transaction.
* The system should be restarted before the last transaction.
* The system should be restarted at the first transaction.
* The system should be restarted on the last transaction.

If a database is restored from information backed up before the last system image,

the system should be restarted before the last transaction because the final transaction must be

reprocessed.

Q105. Functional acknowledgements are used:
* as an audit trail for EDI transactions.
* to functionally describe the IS department.
* to document user roles and responsibilities.

* as a functional description of application software.
Explanation/Reference:

Explanation:

Functional acknowledgements are standard EDI transactions that tell trading partners that their electronic documents were received. Different types of functional acknowledgments provide various levels of detail and, therefore, can act as an audit trail for EDI transactions. The other choices are not relevant to the description of functional acknowledgements.

Q106. An organization plans to allow third parties to collect customer personal data from a retail loyalty platform via an application programming interface (API). Which of the following should be the PRIMARY consideration when designing this API?
* Data governance policies
* System resilience
* Regulatory compliance
* Data availability
Section: Governance and Management of IT

Q107. The selection of security controls is PRIMARILY linked to:
* risk appetite of the organization.
* regulatory requirements.
* business impact assessment.
* best practices of similar organizations.
Section: Protection of Information Assets

Q108. An IS auditor finds that, in accordance with IS policy, IDs of terminated users are deactivated within 90 days of termination. The IS auditor should:
* report that the control is operating effectively since deactivation happens within the time frame stated in the IS policy.
* verify that user access rights have been granted on a need-to-have basis.
* recommend changes to the IS policy to ensure deactivation of user IDs upon termination.
* recommend that activity logs of terminated users be reviewed on a regular basis.
Although a policy provides a reference for performing IS audit assignments, an IS auditor needs to review the adequacy and the appropriateness of the policy. If, in the opinion of the auditor, the time frame defined for deactivation is inappropriate,the auditor needs to communicate this to management and recommend changes to the policy. Though the deactivation happens as stated

in the policy, it cannot be concluded that the control is effective. Best practice would require that the ID of a terminated user be deactivated immediately. Verifying that user access rights have been granted on a need-to-have basis is necessary when permissions are granted. Recommending that activity logs of terminated users be reviewed on a regular basis is a good practice, but not as effective as deactivation upon termination.

Q109. What would be the major purpose of rootkit?
* to hide evidence from system administrators.
* to encrypt files for system administrators.
* to corrupt files for system administrators.
* to hijack system sessions.
* None of the choices.
Section: Protection of Information Assets

Explanation:

rootkit originally describes those recompiled Unix tools that would hide any trace of the intruder.

You can say that the only purpose of rootkit is to hide evidence from system administrators so there is no way to detect malicious special privilege access attempts.

Q110. Which of the following activities should an IS auditor perform FIRST during an external network security assessment?
* Enumeration
* Reconnaissance
* Exploitation
* Vulnerability scanning

Q111. .Mitigating the risk and impact of a disaster or business interruption usually takes priority over transference of risk to a third party such as an insurer. True or false?
* True
* False

Mitigating the risk and impact of a disaster or business interruption usually takes priority over transferring risk to a third party such as an insurer.

Q112. Which of the following would represent an acceptable test of an organization s business continuity plan?
* Full test of computer operations at an emergency site
* Paper test involving functional areas
* Benchmarking the plan against similar organizations
* Walk-through of the plan with technology suppliers

Q113. The waterfall life cycle model of software development is most appropriately used when:
* requirements are well understood and are expected to remain stable, as is the business environment in

which the system will operate.
* requirements are well understood and the project is subject to time pressures.
* the project intends to apply an object-oriented design and programming approach.
* the project will involve the use of new technology.

Section: Protection of Information Assets

Explanation:

Historically, the waterfall model has been best suited to the stable conditions described in choice

A. When the degree of uncertainty of the system to be delivered and the conditions in which it will be used

rises, the waterfall model has not been successful, in these circumstances, the various forms of iterative

development life cycle gives the advantage of breaking down the scope of the overall system to be

delivered, making the requirements gathering and design activities more manageable. The ability to deliver

working software earlier also acts to alleviate uncertainty and may allow an earlier realization of benefits.

The choice of a design and programming approach is not itself a determining factor of the type of software

development life cycle that is appropriate. The use of new technology in a project introduces a significant

element of risk. An iterative form of development, particularly one of the agile methods that focuses on

early development of actual working software, is likely to be the better option to manage this uncertainty.

Q114. A manager of a project was not able to implement all audit recommendations by the target date. The IS auditor should:
* recommend that the project be halted until the issues are resolved.
* recommend that compensating controls be implemented.
* evaluate risks associated with the unresolved issues.
* recommend that the project manager reallocate test resources to resolve the issues.

Explanation/Reference:

Explanation:

It is important to evaluate what the exposure would be when audit recommendations have not been completed by the target date. Based on the evaluation, management can accordingly consider compensating controls, risk acceptance, etc. All other choices might be appropriate only after the risks have been assessed.

Q115. Which of the following intrusion detection systems (IDSs) will MOST likely generate false alarms resulting from normal network activity?
* Statistical-based
* Signature-based
* Neural network
* Host-based

Section: Protection of Information Assets

Explanation:

A statistical-based IDS relies on a definition of known and expected behavior of systems. Since normal network activity may at times include unexpected behavior (e.g., a sudden massive download by multiple users), these activities will be flagged as suspicious. A signature-based IDS is limited to its predefined set of detection rules, just like a virus scanner. A neural network combines the previous two IDSs to create a hybrid and better system. Host-based is another classification of IDS. Any of the three IDSs above may be host- or network-based.

Q116. What is the first step in a business process re-engineering project?
* Identifying current business processes
* Forming a BPR steering committee
* Defining the scope of areas to be reviewed
* Reviewing the organizational strategic plan

Explanation/Reference:

Explanation: Defining the scope of areas to be reviewed is the first step in a business process re- engineering project.

Q117. An organization has implemented a quarterly job schedule to update database tables so prices are adjusted in line with a price index These changes do not go through the regular change management process Which of the following is the MOST important control to have in place?
* An overarching approval is obtained from the change advisory board
* Each production run is approved by an authorized individual
* User acceptance testing (UAT) is performed after the production run
* Exception reports are generated to identify anomalies

Q118. Which of the following layer of an OSI model responsible for routing and forwarding of a network packets?
* Transport Layer
* Network Layer
* Data Link Layer
* Physical Layer

Explanation/Reference:

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors.

For CISA exam you should know below information about OSI model:

The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal.OSI Model

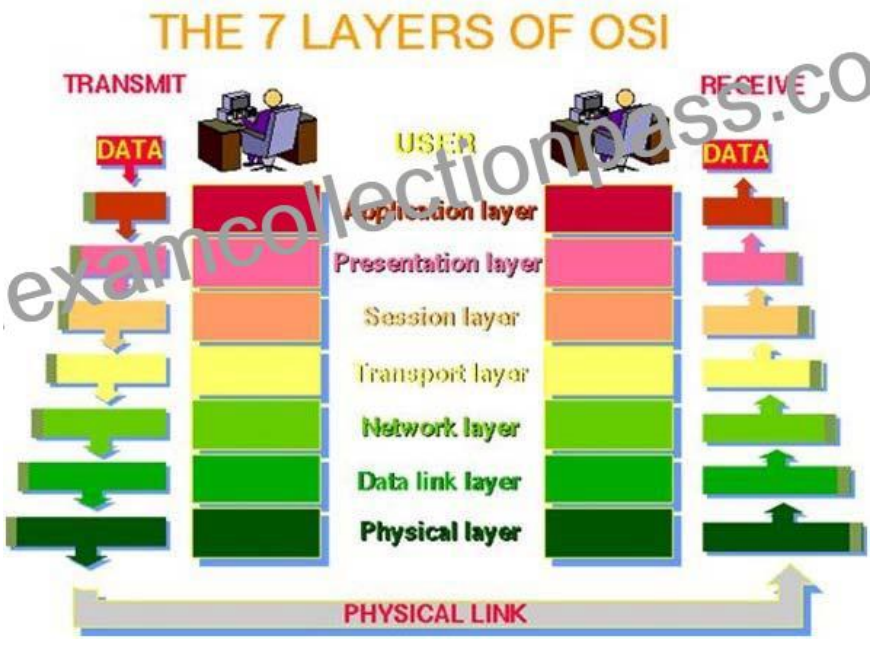


Image source: http://www.petri.co.il/images/osi_model.JPG

PHYSICAL LAYER

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:

What signal state represents a binary 1

How the receiving station knows when a “bit-time” starts

How the receiving station delimits a frame

DATA LINK LAYER

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

Link establishment and termination: establishes and terminates the logical link between two nodes.

Frame traffic control: tells the transmitting node to “back-off” when no frame buffers are available.

Frame sequencing: transmits/receives frames sequentially.

Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.

Frame delimiting: creates and recognizes frame boundaries.

Frame error checking: checks received frames for integrity.

Media access management: determines when the node “has the right” to use the physical medium.

NETWORK LAYER

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:

Routing: routes frames among networks.

Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to

“throttle back” its frame transmission when the router’s buffer fills up.

Frame fragmentation: if it determines that a downstream router’s maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.

Logical-physical address mapping: translates logical addresses, or names, into physical addresses.

Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet

The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagram’s, the transport protocol should include extensive error detection and recovery.

The transport layer provides:

Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.

Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.

Message traffic control: tells the transmitting station to “back-off” when no message buffers are available.

Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, pretending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers

Unlike the lower “subnet” layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true “source to destination” or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER

The session layer allows session establishment between processes running on different stations. It provides:

Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.

Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

PRESENTATION LAYER

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:

Character code translation: for example, ASCII to EBCDIC.

Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.

Data compression: reduces the number of bits that need to be transmitted on the network.

Data encryption: encrypt data for security purposes. For example, password encryption.

APPLICATION LAYER

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

Resource sharing and device redirection

Remote file access

Remote printer access

Inter-process communication

Network management

Directory services

Electronic messaging (such as mail)

Network virtual terminals

The following were incorrect answers:

Transport layer – The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

Data link layer – The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link.

Physical Layer – The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 260

Q119. .Which of the following is a guiding best practice for implementing logical access controls?
* Implementing theBiba Integrity Model
* Access is granted on a least-privilege basis, per the organization’s data owners
* Implementing the Take-Grant access control model
* Classifying data according to the subject’s requirements

Logical access controls should be reviewed to ensure that access is granted on a least-privilege basis, per the organization’s data owners.