CISA Q&As

Certified Information Systems Auditor

Pass Isaca CISA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/CISA.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Isaca Official Exam Center

QUESTION 1

Which of the following activities performed by a database administrator (DBA) should be performed by a different person?

A. Deleting database activity logs

B. Implementing database optimization tools

C. Monitoring database usage

D. Defining backup and recovery procedures

Correct Answer: A

Explanation

Explanation: Since database activity logs record activities performed by the database administrator (DBA), deleting them should be performed by an individual other than the DBA. This is a compensating control to aid in ensuring an appropriate segregation of duties and is associated with the DBA\\'s role. A DBA should perform the other activities as part of the normal operations.

QUESTION 2

An organization has contracted with a vendor for a turnkey solution for their electronic toll collection system (ETCS). The vendor has provided its proprietary application software as part of the solution. The contract should require that:

A. a backup server be available to run ETCS operations with up-to-date data.

B. a backup server be loaded with all the relevant software and data.

C. the systems staff of the organization be trained to handle any event.

D. source code of the ETCS application be placed in escrow.

Correct Answer: D

Explanation

Whenever proprietary application software is purchased, the contract should provide for a source code agreement. This will ensure that the purchasing company will have the opportunity to modify the software should the vendor cease to be in business.Having a backup server with current data and staff training is critical but not as critical as ensuring the availability of the source code.

QUESTION 3

Which of the following provides the MOST relevant information for proactively strengthening security settings?

A. Bastion host

B. Intrusion detection system

C. Honeypot

D. Intrusion prevention system

Correct Answer: C

Explanation

The design of a honeypot is such that it lures the hacker and provides clues as to the hacker\\'s methods and strategies and the resources required to address such attacks. A bastion host does not provide information about an attack. Intrusion detection systems and intrusion prevention systems are designed to detect and address an attack in progress and stop it as soon as possible. A honeypot allows the attack to continue, so as to obtain information about the hacker\\'s strategy and methods.

QUESTION 4

During the requirements definition phase for a database application, performance is listed as a top priority. To access the DBMS files, which of the following technologies should be recommended for optimal I/O performance?

A. Storage area network (SAN)

B. Network Attached Storage (NAS)

C. Network file system (NFS v2)

D. Common Internet File System (CIFS)

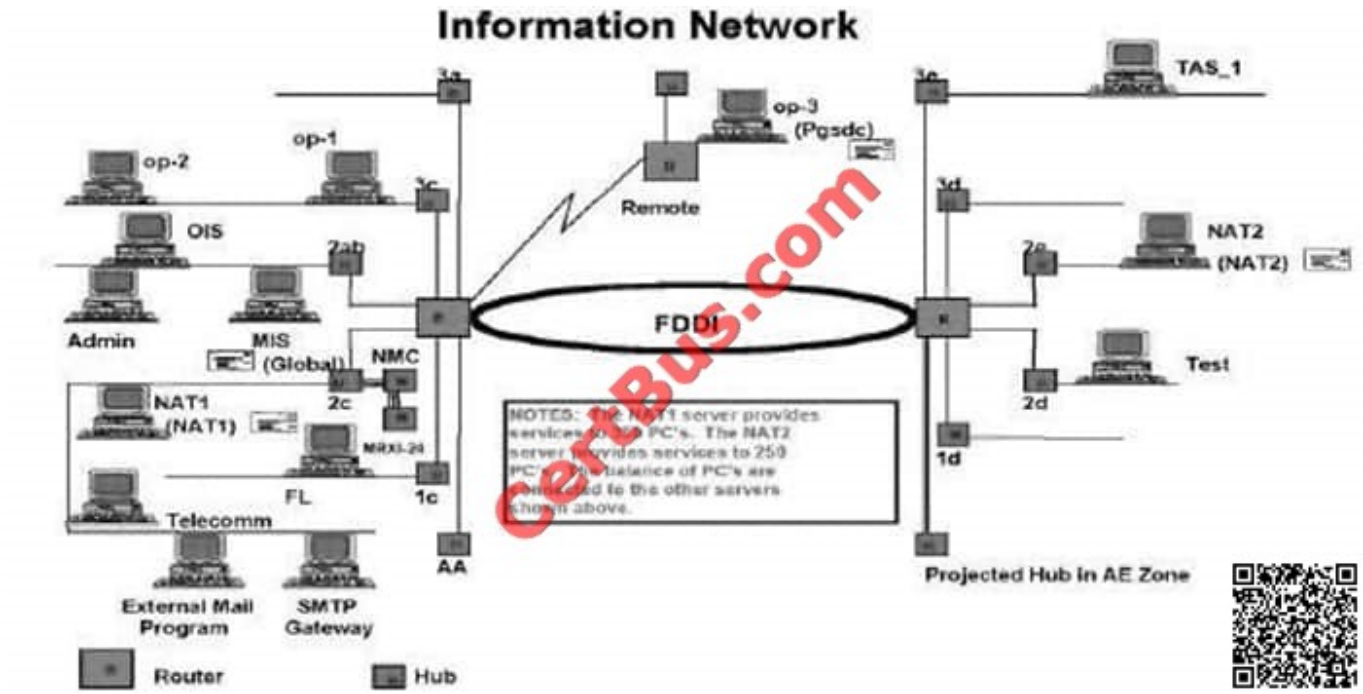
Correct Answer: A

Explanation

In contrast to the other options, in a SAN comprised of computers, FC switches or routers and storage devices, there is no computer system hosting and exporting its mounted file system for remote access, aside from special file systems. Access to information stored on the storage devices in a SAN is comparable to direct attached storage, which means that each block of data on a disk can be addressed directly, since the volumes of the storage device are handled as though they are local, thus providing optimal performance. The other options describe technologies in which a computer (or appliance) shares its information with other systems. To access the information, the complete file has to be read.

QUESTION 5

In the 2c area of the diagram, there are three hubs connected to each other. What potential risk might this indicate?



A. Virus attack

B. Performance degradation

C. Poor management controls

D. Vulnerability to external hackers

Correct Answer: B

Explanation

Hubs are internal devices that usually have no direct external connectivity, and thus are not prone to hackers. There are no known viruses that are specific to hub attacks. While this situation may be an indicator of poor management controls, choiceB is more likely when the practice of stacking hubs and creating more terminal connections is used.

QUESTION 6

Which of the following is the PRIMARY safeguard for securing software and data within an information processing facility?

A. Security awareness

B. Reading the security policy

C. Security committee

D. Logical access controls

Correct Answer: D

Explanation

To retain a competitive advantage and meet basic business requirements, organizations must ensure that the integrity of the information stored on their computer systems preserve the confidentiality of sensitive data and ensure the continued availability of their information systems. To meet these goals, logical access controls must be in place. Awareness (choice A) itself does not protect against unauthorized access or disclosure of information. Knowledge of an information systems security policy (choice B), which should be known by the organization\\'s employees, would help to protect information, but would not prevent the unauthorized access of information. A security committee (choice C) is key to the protection of information assets, butwould address security issues within a broader perspective.

QUESTION 7

An organization has outsourced its help desk. Which of the following indicators would be the best to include in the SLA?

A. Overall number of users supported

B. Percentage of incidents solved in the first call

C. Number of incidents reported to the help desk

D. Number of agents answering the phones

Correct Answer: B

Explanation

Since it is about service level (performance) indicators, the percentage of incidents solved on the first call is the only option that is relevant. Choices A, C and D are not quality measures of the help

desk service.

QUESTION 8

A legacy payroll application is migrated to a new application. Which of the following stakeholders should be PRIMARILY responsible for reviewing and signing-off on the accuracy and completeness of the data before going live?

A. IS auditor

B. Database administrator

C. Project manager

D. Data owner

Correct Answer: D

Explanation

Explanation:

During the data conversion stage of a project, the data owner is primarily responsible for

reviewing and signing-off that the data are migrated completely, accurately and are valid.

An IS auditor is not responsible for reviewing and signing-off on the accuracy of the

converted datA. However, an IS auditor should ensure that there is a review and sign-off

by the data owner during the data conversion stage of the project. A database

administrator\\'s primary responsibility is to maintain the integrity of the database and

make the database available to users. A database administrator is not responsible for reviewing migrated

datA. A project manager provides day-to-day management and

leadership of the project, but is not responsible for the accuracy and integrity of the data.

QUESTION 9

Which of the following provides the framework for designing and developing logical access controls?

A. Information systems security policy

B. Access control lists

C. Password management

D. System configuration files

Correct Answer: A

Explanation

The information systems security policy developed and approved by an organization\\'s top management is the basis upon which logical access control is designed and developed. Access control lists, password management and systems configuration files aretools for implementing the

access controls.

QUESTION 10

Which of the following is the MOST important objective of data protection?

A. identifying persons who need access to information

B. Ensuring the integrity of information

C. Denying or authorizing access to the IS system

D. Monitoring logical accesses

Correct Answer: B

Explanation

Maintaining data integrity is the most important objective of data security. This is a necessity if an organization is to

continue as a viable and successful enterprise. The other choices are important techniques for achieving the objective of data integrity.

QUESTION 11

Data flow diagrams are used by IS auditors to:

A. order data hierarchically.

B. highlight high-level data definitions.

C. graphically summarize data paths and storage.

D. portray step-by-step details of data generation.

Correct Answer: C

Explanation

Explanation: Data flow diagrams are used as aids to graph or chart data flow and storage. They trace the data from its origination to destination, highlighting the paths and storage of datA. They do not order

data in any hierarchy. The flow of the data will not necessarily match any hierarchy or data generation order.

QUESTION 12

In an organization, the responsibilities for IT security are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed. This represents which level of ranking in the information security governance maturity model?

A. Optimized

B. Managed

C. Defined

D. Repeatable

Correct Answer: B

Explanation

Explanation: Boards of directors and executive management can use the information security governance maturity model to establish rankings for security in their organizations. The ranks are nonexistent, initial, repeatable, defined, managed and optimized. When the responsibilities for IT security in an organization are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed, it is said to be \\'managed and measurable.\\'

QUESTION 13

To prevent unauthorized entry to the data maintained in a dial-up, fast response system, an IS auditor should recommend:

A. online terminals are placed in restricted areas.

B. online terminals are equipped with key locks.

C. ID cards are required to gain access to online terminals.

D. online access is terminated after a specified number of unsuccessful attempts.

Correct Answer: D

Explanation

The most appropriate control to prevent unauthorized entry is to terminate connection after a specified number of attempts. This will deter access through the guessing of IDs and passwords. The other choices are physical controls, which are not effective in deterring unauthorized accesses via telephone lines.

QUESTION 14

.

When are benchmarking partners identified within the benchmarking process?

A. In the design stage

B. In the testing stage

C. In the research stage

D. In the development stage

Correct Answer: C

Explanation

Benchmarking partners are identified in the research stage of the benchmarking process.

QUESTION 15

A company has implemented a new client-server enterprise resource planning (ERP)

system. Local branches transmit customer orders to a central manufacturing facility.

Which of the following would BEST ensure that the orders are entered accurately and the corresponding products are produced?

A. Verifying production to customer orders

B. Logging all customer orders in the ERP system

C. Using hash totals in the order transmitting process

D. Approving (production supervisor) orders prior to production

Correct Answer: A

Explanation

Explanation: Verification will ensure that production orders match customer orders. Logging can be

used to detect inaccuracies, but does not in itself guarantee accurate processing. Hash totals will ensure accurate order transmission, but not accurate processingcentrally. Production supervisory approval is a time consuming, manual process that does not guarantee proper control.

QUESTION 16

Which of the following intrusion detection systems (IDSs) will MOST likely generate false alarms resulting from normal network activity?

A. Statistical-based

B. Signature-based

C. Neural network

D. Host-based

Correct Answer: A

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.

QUESTION 17

An organization is using an enterprise resource management (ERP) application. Which of the following would be an effective access control?

A. User-level permissions

B. Role-based

C. Fine-grained

D. Discretionary

Correct Answer: B

Explanation

Role-based access controls the system access by defining roles for a group of users. Users are assigned to the various roles and the access is granted based on the user\\'s role. User-level permissions for an ERP system would create a

larger administrative overhead. Fine-grained access control is very difficult to implement and maintain in the context of a large enterprise. Discretionary access control may be configured or modified by the users or data owners, and therefore may create inconsistencies in the access control management.

QUESTION 18

The PRIMARY reason an IS auditor performs a functional walkthrough during the preliminary phase of an audit assignment is to:

A. understand the business process.

B. comply with auditing standards.

C. identify control weakness.

D. plan substantive testing.

Correct Answer: A

Explanation

Explanation:

Understanding the business process is the first step an IS auditor needs to perform.

Standards do not require an IS auditor to perform a process walkthrough. Identifying control weaknesses is not the primary reason for the walkthrough and typically occurs at a later stage in the audit, while planning for substantive testing is performed at a later stage in the audit.

QUESTION 19

Which of the following exposures could be caused by a line grabbing technique?

A. Unauthorized data access

B. Excessive CPU cycle usage

C. Lockout of terminal polling

D. Multiplexor control dysfunction

Correct Answer: A

Explanation

Line grabbing will enable eavesdropping, thus allowing unauthorized data access, it will not necessarily cause multiplexor dysfunction, excessive CPU usage or lockout of terminal polling.

QUESTION 20

Which of the following is by far the most common prevention system from a network security perspective?

A. Firewall

B. IDS

C. IPS

D. Hardened OS

E. Tripwire

F. None of the choices.

Correct Answer: A

User account access controls and cryptography can protect systems files and data, respectively. On the other hand, firewalls are by far the most common prevention systems from a network security perspective as they can shield access to internal network services, and block certain kinds of attacks through packet filtering.

QUESTION 21

When using an integrated test facility (ITF), an IS auditor should ensure that:

A. production data are used for testing.

B. test data are isolated from production data.

C. a test data generator is used.

D. master files are updated with the test data.

Correct Answer: B

An integrated test facility (ITF) creates a fictitious file in the database, allowing for test transactions to be processed simultaneously with live datA. While this ensures that periodic testing does not require a separate test process, there is a need to isolate test data from production datA. An IS auditor is not required to use production data or a test data generator. Production master files should not be updated with test data.

QUESTION 22

Which audit technique provides the BEST evidence of the segregation of duties in an IS department?

A. Discussion with management

B. Review of the organization chart

C. Observation and interviews

D. Testing of user access rights

Correct Answer: C

Explanation

Explanation: By observing the IS staff performing their tasks, an IS auditor can identify whether they are performing any incompatible operations, and by interviewing the IS staff, the auditor can get an overview of the tasks performed. Based on the observationsand interviews the auditor can evaluate the segregation of duties. Management may not be aware of the detailed functions of each employee in the IS department; therefore, discussion with the management would provide only limited information regardingsegregation of duties. An organization chart would not provide details of the functions of the employees. Testing of user rights would provide information about the rights they have within the IS systems, but would not provide complete information about the functions they perform.

QUESTION 23

As compared to understanding an organization\\'s IT process from evidence directly collected, how valuable are prior audit reports as evidence?

A. The same value.

B. Greater value.

C. Lesser value.

D. Prior audit reports are not relevant.

Correct Answer: C

Explanation

Prior audit reports are considered of lesser value to an IS auditor attempting to gain an understanding of an organization\\'s IT process than evidence directly collected.

QUESTION 24

The PRIMARY objective of a logical access control review is to:

A. review access controls provided through software.

B. ensure access is granted per the organization\\'s authorities.

C. walk through and assess the access provided in the IT environment.

D. provide assurance that computer hardware is adequately protected against abuse.

Correct Answer: B

Explanation

The scope of a logical access control review is primarily to determine whether or not access is granted per the organization\\'s authorizations. Choices A and C relate to procedures of a logical access control review, rather than objectives. Choice D is relevant to a physical access control review.

QUESTION 25

The Federal Information Processing Standards (FIPS) are primarily for use by (choose all that apply):

A. all non-military government agencies

B. US government contractors

C. all military government agencies

D. all private and public colleges in the US

E. None of the choices.

Correct Answer: AB

Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States Federal government for use by all nonmilitary government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community.

QUESTION 26

The MOST likely

for a successful social engineering attack is:

A. that computers make logic errors.

B. that people make judgment errors.

C. the computer knowledge of the attackers.

D. the technological sophistication of the attack method.

Correct Answer: B

Explanation

Humans make errors in judging others; they may trust someone when, in fact, the person is untrustworthy. Driven by logic, computers make the same error every time they execute the erroneous logic; however, this is not the basic argument in designing a social engineering attack. Generally, social engineering attacks do not require technological expertise; often, the attacker is not proficient in information technology or systems. Social engineering attacks are human-based and generally do not involve complicated technology.

QUESTION 27

.

What should IS auditors always check when auditing password files?

A. That deleting password files is protected

B. That password files are encrypted

C. That password files are not accessible over the network

D. That password files are archived

Correct Answer: B

Explanation

IS auditors should always check to ensure that password files are encrypted.

QUESTION 28

As part of the IEEE 802.11 standard ratified in September 1999, WEP uses the CRC- 32 checksum for:

A. integrity.

B. validity.

C. accuracy.

D. confidentiality.

E. None of the choices.

Correct Answer: A

As part of the IEEE 802.11 standard ratified in September 1999, WEP uses the stream cipher RC4 for

confidentiality and the CRC-32 checksum for integrity.

Many WEP systems require a key in hexadecimal format. If one chooses keys that spell words in the

limited 0-9, A-F hex character set, these keys can be easily guessed.

QUESTION 29

Which of the following findings should an IS auditor be MOST concerned about when performing an audit of backup and recovery and the offsite storage vault?

A. There are three individuals with a key to enter the area.

B. Paper documents are also stored in the offsite vault.

C. Data files that are stored in the vault are synchronized.

D. The offsite vault is located in a separate facility.

Correct Answer: C

Explanation

Choice A is incorrect because more than one person would typically need to have a key to the vault to ensure that individuals responsible for the offsite vault can take vacations and rotate duties.

Choice B is not correct because an IS auditor would not be concerned with whether paper documents are stored in the offsite vault. In fact, paper documents, such as procedural documents and a copy of the contingency plan, would most likely be stored in the

offsite vault, and the location of the vault is important, but not as important as the files being synchronized.

QUESTION 30

Information for detecting unauthorized input from a terminal would be BEST provided by the:

A. console log printout.

B. transaction journal.

C. automated suspense file listing.

D. user error report.

Correct Answer: B

Explanation

Explanation: The transaction journal would record all transaction activity, which then could be compared to the authorized source documents to identify any unauthorized input. A console log printout is not the best, because it would not record activity from a specific terminal. An automated suspense file listing would only list transaction activity where an edit error occurred, while the user error report would only list input that resulted in an edit error.

QUESTION 31

Which of the following terms generally refers to small programs designed to take advantage of a software flaw that has been discovered?

A. exploit

B. patch

C. quick fix

D. service pack

E. malware

F. None of the choices.

Correct Answer: A

"The term ""exploit"" generally refers to small programs designed to take advantage of a software flaw that has been discovered, either remote or local. The code from the exploit program is frequently reused in trojan horses and computer viruses. In some cases, a vulnerability can lie in a certain programs processing of a specific file type, such as a non-executable media file."

QUESTION 32

You should keep all computer rooms at reasonable temperatures, which is in between (choose all that apply):

A. 60 - 75 degrees Fahrenheit

B. 10 - 25 degrees Celsius

C. 30 - 45 degrees Fahrenheit

D. 1 - 15 degrees Celsius

E. 20 - 35 degrees Fahrenheit

F. 0 - 5 degrees Celsius

Correct Answer: AB

You should keep all computer rooms at reasonable temperatures, which is in between 60 - 75 degrees

Fahrenheit or 10 - 25 degrees Celsius.

You should also

keep humidity levels at 20 - 70 percent.

QUESTION 33

Which of the following is an oft-cited cause of vulnerability of networks?

A. software monoculture

B. software diversification

C. single line of defense

D. multiple DMZ

E. None of the choices.

Correct Answer: A

An oft-cited cause of vulnerability of networks is homogeneity or software monoculture. In particular, Microsoft Windows has such a large share of the market that concentrating on it will enable a cracker to subvert a large number of systems. Introducing inhomogeneity purely for the sake of robustness would however bring high costs in terms of training and maintenance.

QUESTION 34

Properly planned risk-based audit programs are often capable of offering which of the following benefits?

A. audit efficiency and effectiveness.

B. audit efficiency only.

C. audit effectiveness only.

D. audit transparency only.

E. audit transparency and effectiveness.

F. None of the choices.

Correct Answer: A

Properly planned risk-based audit programs shall increase audit efficiency and effectiveness. The sophistication and formality of this kind of audit do vary a lot depending on the target\\'s size and complexity.

QUESTION 35

Host Based ILDandP primarily addresses the issue of:

A. information integrity

B. information accuracy

C. information validity

D. information leakage

E. None of the choices.

Correct Answer: D

Information Leakage Detection and Prevention (ILDandP) is a computer security term referring to systems designed to detect and prevent the unauthorized transmission of information from the computer systems of an organization to outsiders. Network ILDandP are gateway-based systems installed on the organization\\'s internet network connection and analyze network traffic to search for unauthorized information transmissions. Host Based ILDandP systems run on end-user workstations to monitor and control access to physical devices and access information before it has been encrypted.

QUESTION 36

An IS auditor notes that patches for the operating system used by an organization are deployed by the IT department as advised by the vendor. The MOST significant concern

an IS auditor should have with this practice is the nonconsideration bylT of:

A. the training needs for users after applying the patch.

B. any beneficial impact of the patch on the operational systems.

C. delaying deployment until testing the impact of the patch.

D. the necessity of advising end users of new patches.

Correct Answer: C

Explanation

Explanation:

Deploying patches without testing exposes an organization to the risk of system disruption or failure. Normally, there is no need for training or advising users when a new operating system patch has been installed. Any beneficial impact is less important than the risk of unavailability that could be avoided with proper testing.

QUESTION 37

.

What determines the strength of a secret key within a symmetric key cryptosystem?

A. A combination of key length, degree of permutation, and the complexity of the data- encryption algorithm that uses the key

B. A combination of key length, initial input vectors, and the complexity of the data- encryption algorithm that uses the key

C. A combination of key length and the complexity of the data-encryption algorithm that uses the key

D. Initial input vectors and the complexity of the data-encryption algorithm that uses the key

Correct Answer: B

Explanation

The strength of a secret key within a symmetric key cryptosystem is determined by a combination of key length, initial input vectors, and the complexity of the data-encryption algorithm that uses the key.

QUESTION 38

Which of the following insurance types provide for a loss arising from fraudulent acts by employees?

A. Business interruption

B. Fidelity coverage

C. Errors and omissions

D. Extra expense

Correct Answer: B

Explanation

Fidelity insurance covers the loss arising from dishonest or fraudulent acts by employees. Business interruption insurance covers the loss of profit due to the disruption in the operations of an organization. Errors and omissions insurance provides legal liability protection in the event that the professional practitioner commits an act that results in financial loss to a client. Extra expense insurance is designed to cover the extra costs of continuing operations following a disaster/disruption within an organization.

QUESTION 39

Which of the following is an advantage of an integrated test facility (ITF)?

A. It uses actual master files or dummies and the IS auditor does not have to review the source of the transaction.

B. Periodic testing does not require separate test processes.

C. It validates application systems and tests the ongoing operation of the system.

D. The need to prepare test data is eliminated.

Correct Answer: B

Explanation

Explanation: An integrated test facility creates a fictitious entity in the database to process test transactions simultaneously with live input. Its advantage is that periodic testing does not require separate test processes. However, careful planning is necessary, and test data must be isolated from production data.

QUESTION 40

Which of the following encryption methods uses a matching pair of key-codes, securely distributed, which are used once-and-only-once to encode and decode a single message?

A. Blowfish

B. Tripwire

C. certificate

D. DES

E. one-time pad

F. None of the choices.

Correct Answer: E

It\\'s possible to protect messages in transit by means of cryptography. One method of encryption --the onetime pad --has been proven to be unbreakable when correctly used. This method uses a matching pair of key- codes, securely distributed, which are used once-and-only-once to encode and decode a single message. Note that this method is difficult to use securely, and is highly inconvenient as well.

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.certbus.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: