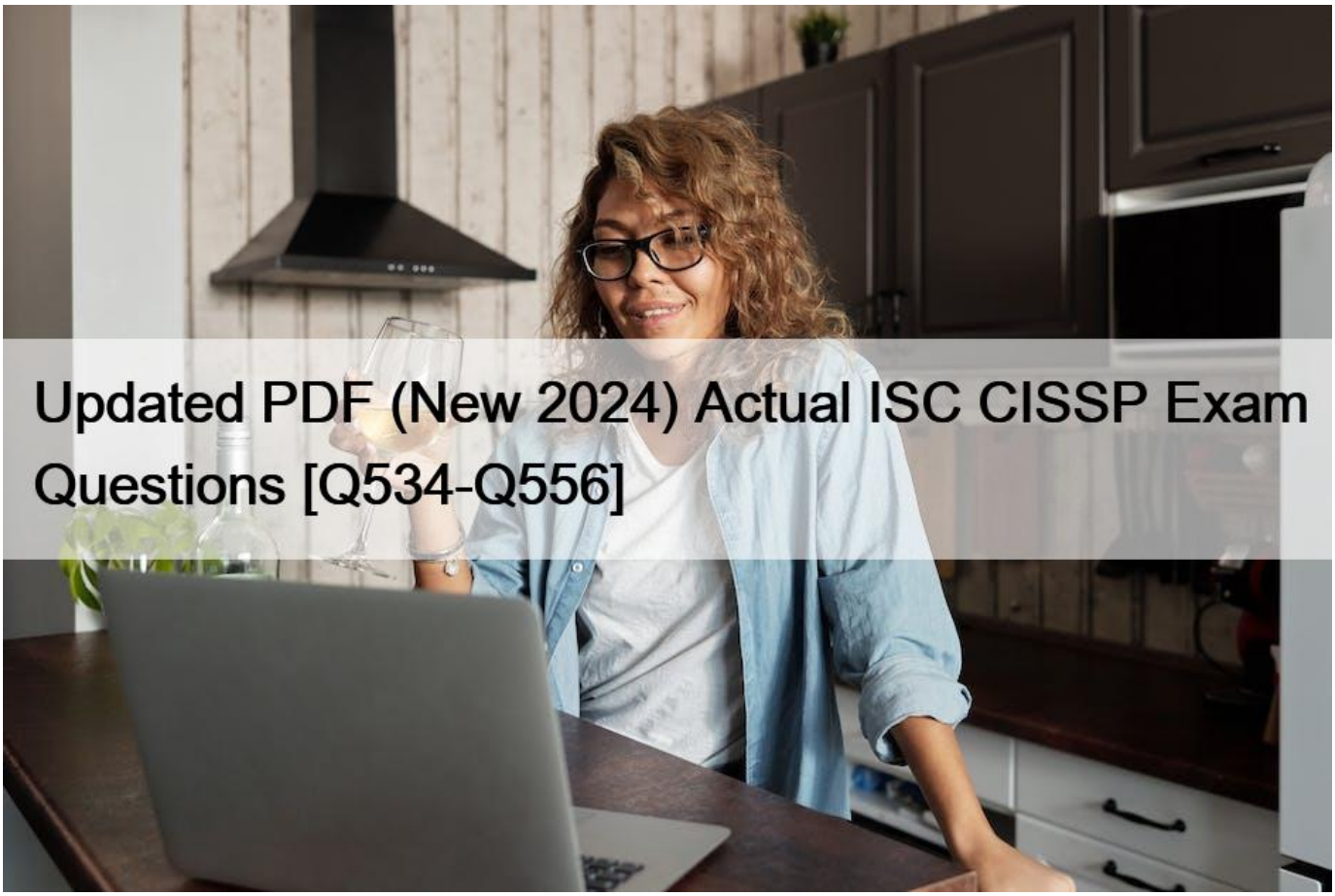
Updated PDF (New 2024) Actual ISC CISSP Exam Questions [Q534-Q556



Updated PDF (New 2024) Actual ISC CISSP Exam Questions
Verified CISSP Exam Dumps PDF [2024] Access using DumpsMaterials

NO.534 A chain of custody shows who _____ _____ and _____.(Choose three)
* Who controlled the evidence
* Who transcribed the evidence
* Who validated the evidence
* Who presented the evidence
* Secured the evidence
* Obtained the evidence

The chain of evidence shows who obtained the evidence, who secured the evidence, and who controlled the evidence.

NO.535 What does an Exposure Factor (EF) describe?
* The annual expected financial loss to an organization from a threat
* The percentage of loss that a realized threat event would have on a

specific asset
* Anumber that represents the estimated frequency of the occurrence of an expected threat

* Adollar figure that is assigned to a single event
The correct answer is “The percentage of loss that a realized threat event would have on a specific asset”. Answer “Adollar figure that is assigned to a single event” is an SLE,

“Anumber that represents the estimated frequency of the occurrence of

an expected threat” is an ARO, and “The annual expected financial loss to an organization from a threat” is an ALE.

NO.536 Following project initiation, which of the following items represent the linear progression of Disaster Recovery (DR) phases?
* Risk analysis, strategy development, plan implementation, support and maintenance
* Risk analysis, off-site storage strategy development, recovery team selection and training, plan testing and maintenance
* Disaster avoidance, system identification, develop user recovery plan, develop backup systems, select and train recovery teams
* Data collection, network recovery planning, team selection and training, plan test and maintenance

NO.537 Which of the following is NOT a media viability control used to protect the viability of data storage media?
* clearing
* marking
* handling
* storage
Explanation/Reference:

Explanation:

Clearing is not an example of a media viability control used to protect the viability of data storage media.

Media viability controls are implemented to preserve the proper working state of the media, particularly to facilitate the timely and accurate restoration of the system after a failure.

Many physical controls should be used to protect the viability of the data storage media. The goal is to protect the media from damage during handling and transportation, or during short-term or long-term storage. Proper marking and labeling of the media is required in the event of a system recovery process:

Marking. All data storage media should be accurately marked or labeled. The labels can be used to

▪

identify media with special handling instructions, or to log serial numbers or bar codes for retrieval during a system recovery.

Handling. Proper handling of the media is important. Some issues with the handling of media include

▪

cleanliness of the media and the protection from physical damage to the media during transportation to the archive sites.

Storage. Storage of the media is very important for both security and environmental reasons. A proper

▪

heat- and humidity-free, clean storage environment should be provided for the media. Data media is sensitive to temperature, liquids, magnetism, smoke, and dust.

Incorrect Answers:

B: Marking is a media viability control used to protect the viability of data storage media.

C: Handling is a media viability control used to protect the viability of data storage media.

D: Storage is a media viability control used to protect the viability of data storage media.

References:

Krutz, Ronald L. and Russell Dean Vines, The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 324

NO.538 Review of which of the following would be MOST preferred in measuring the effectiveness of a newly adopted security administration process?
* Access control infrastructure and procedures
* Security Operational Metrics
* System access logs for unusual activities
* Security administrator’s productivity

NO.539 Which of the following questions should any user not be able to answer regarding their organization information security policy?
* Who is involved in establishing the security policy?
* Where is the organization security policy defined?
* What are the actions that need to be performed in case of a disaster?
* Who is responsible for monitoring compliance to the organization security policy?

According to CISSP documentation, the actual definition and procedures defined inside an organization disaster recovery policy are of private nature. Only people working in the company and with a role inside it should know about those procedures. Its not a good practice to be divulgating Disaster recovery procedures to external people. Many times external people need to know who is involved in it, and who is responsible. This could be the case of a vendor providing replacement equipment in case of disaster.

NO.540 What should an auditor do when conducting a periodic audit on media retention?
* Check electronic storage media to ensure records are not retained past their destruction date.
* Ensure authorized personnel are in possession of paper copies containing Personally Identifiable Information….
* Check that hard disks containing backup data that are still within a retention cycle are being destroyed….
* Ensure that data shared with outside organizations is no longer on a retention schedule.

NO.541 Which of the following is the MAIN reason that system re-certification and re-accreditation are needed?
* To assist data owners in making future sensitivity and criticality determinations
* To assure the software development team that all security issues have been addressed
* To verify that security protection remains acceptable to the organizational security policy
* To help the security team accept or reject new systems for implementation and production

The main reason that system re-certification and re-accreditation are needed is to verify that the security protection of the system remains acceptable to the organizational security policy, especially after significant changes or updates to the system.
Re-certification is the process of reviewing and testing the security controls of the system to ensure that they are still effective and compliant with the security policy. Re-accreditation is the process of authorizing the system to operate based on the results of the re-certification. The other options are not the main reason for system re-certification and re-accreditation, as they either do not relate

to the security protection of the system (A and D), or do not involve re-certification and re-accreditation (B). References: CISSP All-in-One Exam Guide, Eighth Edition, Chapter 10, page 633; Official (ISC)2 CISSP CBK Reference, Fifth Edition, Chapter 10, page 695.

NO.542 The Bell-LaPadula model addresses which one of the following items?
* Covert channels
* Definition of a secure state transition
* Information flow from high to low
* The creation and destruction of subjects and objects
Information flow from high to low is addressed by the * -property

of the Bell0LaPadula model, which states that a subject cannot write

data from a higher level of classification to a lower level of

classification. This property is also known as the confinement property or the no write down property.

* In answer “Covert channels”, covert channels are not addressed by the model. The Bell-

LaPadula model deals with information flow through normal channels and does not address the covert passing of information through unintended paths.

The creation and destruction of subjects and objects, answer “The creation and destruction of subjects and objects”, is not addressed by the model.

* Answer “Definition of a secure state transition” refers to the fact that the model discusses a secure transition from one secure state to another, but it never provides a definition of a secure transition.

NO.543 Phreakers are hackers who specialize in telephone fraud. What type of telephone fraud/attack makes use of a device that generates tones to simulate inserting coins in pay phones, thus fooling the system into completing free calls?
* Red Boxes
* Blue Boxes
* White Boxes
* Black Boxes
Explanation/Reference:

Explanation:

A red box is a phreaking device that generates tones to simulate inserting coins in pay phones, thus fooling the system into completing free calls. In the US, a dime is represented by two tones, a nickel by one, and a quarter by a set of 5 tones. Any device capable of playing back recorded sounds can potentially be used as a red box.

Commonly used devices include modified Radio Shack tone dialers, personal MP3 players, and audio- recording greeting cards. BLUE BOX An early phreaking tool, the blue box is an electronic device that simulates a telephone operator’s dialing console. It functions by replicating the tones used to switch long- distance calls and using them to route the user’s own call, bypassing the normal switching mechanism.

The most typical use of a blue box was to place free telephone calls – inversely, the Black Box enabled one to receive calls which were free to the caller. The blue box no longer works in most western nations, as modern switching systems are now digital and no longer use the inband signaling which the blue box emulates. Instead, signaling occurs on an out-of-band channel which

cannot be accessed from the line the caller is using (called Common Channel Interoffice Signaling (CCIS)). BLACK BOX The black box (as distinguished from blue boxes and red boxes), sometimes called an Agnew (see Spiro (device) for the origin of the nickname), was a device built by phone phreaks during the 1960s and 1970s in order to defeat long distance phone call toll charges, and specifically to block the supervision signal sent by the receiving telephone handset when the call was answered at the receiving end of the call. The act of picking up the handset of a telephone causes a load to be put on the telephone line, so that the DC voltage on the line drops below the approximately 45 volts present when the phone is disconnected.

The black box consisted of a large capacitor which was inserted in series with the telephone, thereby blocking DC current but allowing AC current (i.e., ringing signal and also audio signal) to pass. When the black box was switched into the telephone line, the handset could be picked up without the telephone system knowing and starting the billing process. In other words, the box fooled the phone company into thinking no one had answered at the receiving end, and therefore billing was never started on the call.

WHITE BOX The white box is simply a portable Touch-Tone Keypad.

References:

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2001, Page 654.

http://en.wikipedia.org/wiki/Red_box_(phreaking)

http://en.wikipedia.org/wiki/Blue_box

http://www.bombshock.com/archive/Phreaking_and_Phone_Systems/Box_Plans/

NO.544 Which of the following benefits does Role Based Access Control (RBAC) provide for the access review process?
* Lowers the amount of access requests after review
* Gives more control into the revocation phase
* Gives more fine-grained access analysis to accesses
* Lowers the number of items to be reviewed

NO.545 What are suitable protocols for securing VPN connections?
* S/MIME and SSH
* TLS and SSL
* IPsec and L2TP
* PKCS# and X.509

Both of them can be used to create and secure VPN’s. The Layer 2 Tunnel Protocol (L2TP) is an emerging Internet Engineering Task Force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco’s Layer 2 Forwarding (L2F) and Microsoft’s Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for VPNs. VPNs allow users and telecommuters to connect to their corporate intranets or extranets. IPSec is a series of guidelines for the protection of Internet Protocol (IP) communications. It specifies ways for securing private information transmitted over public networks. Services supported by IPSec include confidentiality (encryption), authenticity (proof of sender), integrity (detection of data tampering) and replay protection (defense against unauthorized re-sending of data). It work on layer 3 of the OSI model and is the most common protocols used to create VPNs.

NO.546 What is the appropriate role of the security analyst in the application system development or acquisition project?
* policeman
* control evaluator & consultant
* data owner
* application user

The correct answer is “control evaluator & consultant”. During any system development or acquisition, the security

staff should evaluate security controls and advise (or consult) on the strengths and weaknesses with those responsible for making the final decisions on the project.

The other answers are not correct because:

policeman – It is never a good idea for the security staff to be placed into this type of role

(though it is sometimes unavoidable). During system development or acquisition, there should be no need of anyone filling the role of policeman.

data owner – In this case, the data owner would be the person asking for the new system to manage, control, and secure information they are responsible for. While it is possible the security staff could also be the data owner for such a project if they happen to have responsibility for the information, it is also possible someone else would fill this role.

Therefore, the best answer remains “control evaluator & consultant”.

application user – Again, it is possible this could be the security staff, but it could also be many other people or groups. So this is not the best answer.

Reference:

Official ISC2 Guide page: 555 – 560

All in One Third Edition page: 832 – 846

NO.547 Which of the following is the most important consideration in locating an alternate computing facility during the development of a disaster recovery plan?
* It is unlikely to be affected by the same disaster.
* It is close enough to become operational quickly.
* It is close enough to serve its users.
* It is convenient to airports and hotels.

Explanation/Reference:

Explanation:

When choosing a backup facility, it should be far enough away from the original site so that one disaster does not take out both locations. In other words, it is not logical to have the backup site only a few miles away if the company is concerned about, for example, tornado damage, because the backup site could also be affected or destroyed.

Incorrect Answers:

B: The alternate site should be too close so that one disaster does not take out both locations.

C: The alternate site should be too close so that one disaster does not take out both locations.

D: That the alternate city is convenient to airports and hotels is A major factor when considering an alternate site.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 924

NO.548 Which layer of the Open System Interconnection (OSI) model is reliant on other layers and is concerned with the structure, interpretation and handling of information?
* Presentation Layer
* Session Layer
* Application Layer
* Transport Layer
Section: Mixed questions

Explanation/Reference:

NO.549 What is called the act of a user professing an identity to a system, usually in the form of a log-on ID?
* Authentication
* Identification
* Integrity
* Confidentiality
“Identification is the act of a user professing an identity to a system, usually in the form of a logon ID to the system.” Pg 49 Krutz The CISSP Prep Guide.

“Identification describes a method of ensuring that a subject (user, program, or process) is the entity it claims to be. Identification can be provided with the use of a username or account number. To be properly authenticated, the subject is usually required to provide a second piece to the credential set. This piece could be a password, passphrase, cryptographic key, personal identification number (PIN), anatomical attribute, or token.” Pg 110 Shon Harris: All-in-One CISSP Certification

NO.550 It is MOST important to perform which of the following to minimize potential impact when implementing a new vulnerability scanning tool in a production environment?
* Negotiate schedule with the Information Technology (IT) operation’s team
* Log vulnerability summary reports to a secured server
* Enable scanning during off-peak hours
* Establish access for Information Technology (IT) management

NO.551 An Architecture where there are more than two execution domains or privilege levels is called:
* Ring Layering
* Network Environment.
* Security Models
In computer science, hierarchical protection domains, often called protection rings, are a mechanism to protect data and functionality from faults (fault tolerance) and malicious behavior (computer security). This approach is diametrically opposite to that of capability-based security.

Computer operating systems provide different levels of access to resources. A protection ring is one of two or more hierarchical levels or layers of privilege within the architecture of a computer system. This is generally hardware-enforced by some CPU architectures that provide different CPU modes at the hardware or microcode level. Rings are arranged in a hierarchy from most privileged (most trusted, usually numbered zero) to least privileged

(least trusted, usually with the highest ring number). On most operating systems, Ring 0 is the level with the most privileges and interacts most directly with the physical hardware such as the CPU and memory.

Special gates between rings are provided to allow an outer ring to access an inner ring’s resources in a predefined manner, as opposed to allowing arbitrary usage. Correctly gating access between rings can improve security by preventing programs from one ring or privilege level from misusing resources intended for programs in another. For example, spyware running as a user program in

Ring 3 should be prevented from turning on a web camera without informing the user, since hardware access should be a Ring 1 function reserved for device drivers. Programs such as web browsers running in higher numbered rings must request access to the network, a resource restricted to a lower numbered ring.

Ring Architecture

All of the other answers are incorrect because they are detractors.

References:

OIG CBK Security Architecture and Models (page 311)

and

https://en.wikipedia.org/wiki/Ring_%28computer_security%29

NO.552 Covert Channel Analysis is first introduced at what level of the TCSEC rating?
* C2 and above.
* B1 and above.
* B2 and above.
* B3 and above.

The Orange Book first introduce a requirement for Covert Channel Analysis at level B2 and all levels above B2 would also require this.

The AIO defines a Covert Channel as a communications path that enables a process to transmit information in a way that violates the system’s security policy. It is a communication channel that allows two cooperating processes to transfer information in such a way that it violates the system’s security policy. Even though there are protection mechanisms in place, if unauthorized information can be transferred using a signaling mechanism via entities or objects not normally considered to be able to communicate, then a covert channel may exist.

The following answers are incorrect:

C2 and above. Is incorrect because, the Orange book requires Covert Channel Analysis only starting at level B2 and above, level C2 is lower than B2 and it would not require covert channel analysis.

B1 and above. Is incorrect because, the Orange book requires Covert Channel Analysis only at level B2 and above, level B1 is lower than B2 and it would not require covert channel analysis.

B3 and above. Is incorrect because, the Orange book first requires Covert Channel

Analysis at level B2.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third

Edition ((ISC)2 Press) (Kindle Locations 13347-13350). Auerbach Publications. Kindle

Edition.

and

NIST http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt

NO.553 Knowledge-based Intrusion Detection Systems (IDS) are more common than:
* Network-based IDS
* Host-based IDS
* Behavior-based IDS
* Application-Based IDS

Knowledge-based IDS are more common than behavior-based ID systems. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 63. Application-Based IDS – “a subset of HIDS that analyze what’s going on in an application using the transaction log files of the application.” Source: Official ISC2 CISSP CBK Review Seminar Student Manual Version 7.0 p. 87 Host-Based IDS – “an implementation of IDS capabilities at the host level. Its most significant difference from NIDS is intrusion detection analysis, and related processes are limited to the boundaries of the host.” Source: Official ISC2 Guide to the CISSP CBK – p. 197 Network-Based IDS – “a network device, or dedicated system attached to the network, that monitors traffic traversing the network segment for which it is integrated.” Source: Official ISC2 Guide to the CISSP CBK – p. 196 CISSP for dummies a book that we recommend for a quick overview of the 10 domains has nice and concise coverage of the subject: Intrusion detection is defined as real-time monitoring and analysis of network activity and data for potential vulnerabilities and attacks in progress. One major limitation of current intrusion detection system (IDS) technologies is the requirement to filter false alarms lest the operator (system or security administrator) be overwhelmed with data. IDSes are classified in many different ways, including active and passive, network-based and host-based, and knowledge-based and behavior-based: Active and passive IDS An active IDS (now more commonly known as an intrusion prevention system – IPS) is a system

that’s configured to automatically block suspected attacks in progress without any intervention

required by an operator. IPS has the advantage of providing real-time corrective action in

response to an attack but has many disadvantages as well. An IPS must be placed in-line along a

network boundary; thus, the IPS itself is susceptible to attack. Also, if false alarms and legitimate

traffic haven’t been properly identified and filtered, authorized users and applications may be

improperly denied access. Finally, the IPS itself may be used to effect a Denial of Service (DoS)

attack by intentionally flooding the system with alarms that cause it to block connections until no

connections or bandwidth are available.

A passive IDS is a system that’s configured only to monitor and analyze network traffic activity and

alert an operator to potential vulnerabilities and attacks. It isn’t capable of performing any

protective or corrective functions on its own. The major advantages of passive IDSes are that

these systems can be easily and rapidly deployed and are not normally susceptible to attack

themselves.

Network-based and host-based IDS

A network-based IDS usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface. The IDS is placed along a network segment or boundary and monitors all traffic on that segment.

A host-based IDS requires small programs (or agents) to be installed on individual systems to be monitored. The agents monitor the operating system and write data to log files and/or trigger alarms. A host-based IDS can only monitor the individual host systems on which the agents are installed; it doesn’t monitor the entire network.

Knowledge-based and behavior-based IDS

A knowledge-based (or signature-based) IDS references a database of previous attack profiles and known system vulnerabilities to identify active intrusion attempts. Knowledge-based IDS is currently more common than behavior-based IDS.

Advantages of knowledge-based systems include the following:

It has lower false alarm rates than behavior-based IDS.

Alarms are more standardized and more easily understood than behavior-based IDS.

Disadvantages of knowledge-based systems include these:

Signature database must be continually updated and maintained.

New, unique, or original attacks may not be detected or may be improperly classified.

A behavior-based (or statistical anomaly-based) IDS references a baseline or learned pattern of normal system activity to identify active intrusion attempts. Deviations from this baseline or pattern cause an alarm to be triggered.

Advantages of behavior-based systems include that they

Dynamically adapt to new, unique, or original attacks.

Are less dependent on identifying specific operating system vulnerabilities.

Disadvantages of behavior-based systems include

Higher false alarm rates than knowledge-based IDSes.

Usage patterns that may change often and may not be static enough to implement an effective

behavior-based IDS.

NO.554 What is called the act of a user professing an identity to a system, usually in the form of a log-on ID?
* Authentication
* Identification
* Authorization
* Confidentiality

Identification is the act of a user professing an identity to a system, usually in the form of a log-on ID to the system.

Identification is nothing more than claiming you are somebody. You identify yourself when you speak to someone on the phone that you don’t know, and they ask you who they’re speaking to. When you say, “I’m Jason.”, you’ve just identified yourself.

In the information security world, this is analogous to entering a username. It’s not analogous to entering a password. Entering a password is a method for verifying that you are who you identified yourself as.

NOTE: The word “professing” used above means: “to say that you are, do, or feel something when other people doubt what you say”. This is exactly what happen when you provide your identifier (identification), you claim to be someone but the system cannot take your word for it, you must further Authenticate to the system to prove who you claim to be.

The following are incorrect answers:

Authentication: is how one proves that they are who they say they are. When you claim to be Jane Smith by logging into a computer system as “jsmith”, it’s most likely going to ask you for a password. You’ve claimed to be that person by entering the name into the username field (that’s the identification part), but now you have to prove that you are really that person.

Many systems use a password for this, which is based on “something you know”, i.e. a secret between you and the system.

Another form of authentication is presenting something you have, such as a driver’s license, an RSA token, or a smart card.

You can also authenticate via something you are. This is the foundation for biometrics. When you do this, you first identify yourself and then submit a thumb print, a retina scan, or another form of bio-based authentication.

Once you’ve successfully authenticated, you have now done two things: you’ve claimed to be someone, and you’ve proven that you are that person. The only thing that’s left is for the system to determine what you’re allowed to do.

Authorization: is what takes place after a person has been both identified and authenticated; it’s the step determines what a person can then do on the system.

An example in people terms would be someone knocking on your door at night. You say, “Who is it?”, and wait for a response. They say, “It’s John.” in order to identify themselves. You ask them to back up into the light so you can see them through the peephole. They do so, and you authenticate them based on what they look like (biometric). At that point you decide they can come inside the house.

If they had said they were someone you didn’t want in your house (identification), and you then verified that it was that person (authentication), the authorization phase would not include access to the inside of the house.

Confidentiality: Is one part of the CIA triad. It prevents sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. A good example is a credit card number while shopping online, the merchant needs it to clear the transaction but you do not want your informaiton exposed over the network, you would use a secure link such as SSL, TLS, or some tunneling tool to protect the information from prying eyes between point A and point B. Data encryption is a common method of ensuring confidentiality.

The other parts of the CIA triad are listed below:

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). In addition, some means must be in place to detect any changes in data that might occur as a result of non-humancaused events such as an electromagnetic pulse (EMP) or server crash. If an unexpected change occurs, a backup copy must be available to restore the affected data to its correct state.

Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed, providing a certain measure of redundancy and failover, providing adequate communications bandwidth and preventing the occurrence of bottlenecks, implementing emergency backup power systems, keeping current with all necessary system upgrades, and guarding against malicious actions such as denial-of-service (DoS) attacks.

Reference used for this question:

http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

http://www.danielmiessler.com/blog/security-identification-authentication-and-authorization

http://www.merriam-webster.com/dictionary/profess

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36

NO.555 Which of the following is the most reliable, secure means of removing data from magnetic storage media such as a magnetic tape, or a cassette?
* Degaussing
* Parity Bit Manipulation
* Zeroization
* Buffer overflow

A “Degausser (Otherwise known as a Bulk Eraser) has the main function of

reducing to near zero the magnetic flux stored in the magnetized medium. Flux density is

measured in Gauss or Tesla. The operation is speedier than overwriting and done in one short

operation. This is achieved by subjecting the subject in bulk to a series of fields of alternating

polarity and gradually decreasing strength.

The following answers are incorrect:Parity Bit Manipulation. Parity has to do with disk lerror detection, not data removal. A bit or series of bits appended to a character or block of characters to ensure that the information received is the same as the infromation that was sent.

Zeroization. Zeroization involves overwrting data to sanitize it. It is time-consuming and not foolproof. The potential of restoration of data does exist with this method.

Buffer overflow. This is a detractor. Although many Operating Systems use a disk buffer to temporarily hold data read from disk, its primary purpose has no connection to data removal. An overflow goes outside the constraints defined for the buffer and is a method used by an attacker to attempt access to a system.

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

Shon Harris AIO v3. pg 908

Reference: What is degaussing.

NO.556 Which of the following is the BEST way to protect against Structured Query language (SQL) injection?
* Enforce boundary checking.
* Ratfrict um of SELECT command.
* Restrict HyperText Markup Language (HTML) source code
* Use stored procedures.