method is implemented as a mirror. If vaulting updates are recorded in real-time, then it will be necessary to perform regular backups at the off-site location to provide recovery services due to inadvertent or malicious alterations to user or system data.

The following are incorrect answers:
Remote journaling refers to the parallel processing of transactions to an alternate site (as opposed to a batch dump process). Journaling is a technique used by database management systems to provide redundancy for their transactions. When a transaction is completed, the database management system duplicates the journal entry at a remote location. The journal provides sufficient detail for the transaction to be replayed on the remote system. This provides for database recovery in the event that the database becomes corrupted or unavailable.

Database shadowing uses the live processing of remote journaling, but creates even more redundancy by duplicating the database sets to multiple servers. There are also additional redundancy options available within application and database software platforms. For example, database shadowing may be used where a database management system updates records in multiple locations. This technique updates an entire copy of the database at a remote location.

Data clustering refers to the classification of data into groups (clusters). Clustering may also be used, although it should not be confused with redundancy. In clustering, two or more "partners" are joined into the cluster and may all provide service at the same time. For example, in an active 瓊ctive pair, both systems may provide services at any time. In the case of a failure, the remaining partners may continue to provide service but at a decreased capacity.

The following resource(s) were 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 20403-20407 and 20411-20414 and 20375-20377 and 20280-20283). Auerbach Publications. Kindle Edition.

QUESTION 651
Which of the following is covered under Crime Insurance Policy Coverage?

A. Inscribed, printed and Written documents
B. Manuscripts
C. Accounts Receivable
D. Money and Securities

Correct Answer: D
Explanation:
Source: TIPTON, Harold F.& KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Property Insurance overview, Page 589.

QUESTION 652
Which of the following computer recovery sites is only partially equipped with processing equipment?

A. hot site
B. rolling hot site
C. warm site
D. cold site

Correct Answer: C

Explanation:
A warm site has some basic equipment or in some case almost all of the equipment but it is not sufficient to be operational without bringing in the last backup and in some cases more computers and other equipment.

The following answers are incorrect:

hot site. Is incorrect because a hot-site is fully configured with all the required hardware. The only thing missing is the last backup and you are up and running.

Rolling hot site. Is incorrect because a rolling hot-site is fully configured with all the required hardware.

cold site. Is incorrect because a cold site has basically power, HVAC, basic cabling, but no or little as far as processing equipment is concerned. All other equipment must be brought to this site. It might take a week or two to reconstruct.

References:
OIG CBK Business Continuity and Disaster Recovery Planning (pages 368 - 369)

QUESTION 653
What is called the probability that a threat to an information system will materialize?

A. Threat
B. Risk
C. Vulnerability
D. Hole

Correct Answer: B
Explanation:
The Correct Answer: Risk: The potential for harm or loss to an information system or network; the probability that a threat will materialize.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 16, 32.

QUESTION 654
To be admissible in court, computer evidence must be which of the following?

A. Relevant
B. Decrypted
C. Edited
D. Incriminating

Correct Answer: A
Explanation:
Before any evidence can be admissible in court, the evidence has to be relevant, material to the issue, and it must be presented in compliance with the rules of evidence. This holds true for computer evidence as well.
While there are no absolute means to ensure that evidence will be allowed and helpful in a court of law, information security professionals should understand the basic rules of evidence.
Evidence should be relevant, authentic, accurate, complete, and convincing. Evidence gathering should emphasize these criteria.

As stated in CISSP for Dummies:

Because computer-generated evidence can sometimes be easily manipulated, altered , or tampered with, and because it's not easily and commonly understood, this type of evidence is usually considered suspect in a court of law. In order to be admissible, evidence must be

Relevant: It must tend to prove or disprove facts that are relevant and material to the case.

Reliable: It must be reasonably proven that what is presented as evidence is what was originally collected and that the evidence itself is reliable. This is accomplished, in part, through proper evidence handling and the chain of custody. (We discuss this in the upcoming section "Chain of custody and the evidence life cycle.")

Legally permissible: It must be obtained through legal means. Evidence that's not legally permissible may include evidence obtained through the following means:

Illegal search and seizure: Law enforcement personnel must obtain a prior court order; however, non-law enforcement personnel, such as a supervisor or system administrator, may be able to conduct an authorized search under some circumstances.

Illegal wiretaps or phone taps: Anyone conducting wiretaps or phone taps must obtain a prior court order.

Entrapment or enticement: Entrapment encourages someone to commit a crime that the individual may have had no intention of committing. Conversely, enticement lures someone toward certain evidence (a honey pot, if you will) after that individual has already committed a crime. Enticement is not necessarily illegal but does raise certain ethical arguments and may not be admissible in court.

Coercion: Coerced testimony or confessions are not legally permissible.

Unauthorized or improper monitoring: Active monitoring must be properly authorized and conducted in a standard manner; users must be notified that they may be subject to monitoring.

The following answers are incorrect:

decrypted. Is incorrect because evidence has to be relevant, material to the issue, and it must be presented in compliance with the rules of evidence.

edited. Is incorrect because evidence has to be relevant, material to the issue, and it must be presented in compliance with the rules of evidence. Edited evidence violates the rules of evidence.

incriminating. Is incorrect because evidence has to be relevant, material to the issue, and it must be presented in compliance with the rules of evidence.

Reference(s) used for this question:

CISSP STudy Guide (Conrad, Misenar, Feldman) Elsevier. 2012. Page 423
Mc Graw Hill, Shon Harris CISSP All In One (AIO), 6th Edition , Pages 1051-1056
CISSP for Dummies , Peter Gregory

QUESTION 655

In which of the following phases of system development life cycle (SDLC) is contingency planning most important?

A. Initiation
B. Development/acquisition
C. Implementation
D. Operation/maintenance

Correct Answer: A
Explanation:
Contingency planning requirements should be considered at every phase of SDLC, but most importantly when a new IT system is being conceived. In the initiation phase, system requirements are identified and matched to their related operational processes, allowing determination of the system's appropriate recovery priority.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 12).
And The Official ISC2 Guide to the CBK, Second Edition, Application Security, page 180-185

QUESTION 656
Which of the following questions is less likely to help in assessing an organization's contingency planning controls?

A. Is damaged media stored and/or destroyed?
B. Are the backup storage site and alternate site geographically far enough from the primary site?
C. Is there an up-to-date copy of the plan stored securely off-site?
D. Is the location of stored backups identified?

Correct Answer: A
Explanation:
Contingency planning involves more than planning for a move offsite after a disaster destroys a facility.
It also addresses how to keep an organization's critical functions operating in the event of disruptions, large and small.
Handling of damaged media is an operational task related to regular production and is not specific to contingency planning.
Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self- Assessment Guide for Information Technology Systems, November 2001 (Pages A-27 to A-28).

QUESTION 657
A contingency plan should address:

A. Potential risks.
B. Residual risks.
C. Identified risks.
D. All answers are correct.

Correct Answer: D
Explanation:
Because it is rarely possible or cost effective to eliminate all risks, an attempt is made to reduce risks to an acceptable level through the risk assessment process. This process allows, from a set of potential risks (whether likely or not), to come up with a set of identified, possible risks.
The implementation of security controls allows reducing the identified risks to a smaller set of residual risks. Because these residual risks represent the complete set of situations that could affect system performance, the scope of the contingency plan may be reduced to address only this decreased risk set.

As a result, the contingency plan can be narrowly focused, conserving resources while ensuring an effective system recovery capability.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 7).

QUESTION 658
Under the Business Exemption Rule to the hearsay evidence, which of the following exceptions would have no bearing on the inadmissibility of audit logs and audit trails in a court of law?

A. Records are collected during the regular conduct of business.
B. Records are collected by senior or executive management.
C. Records are collected at or near the time of occurrence of the act being investigated to generate automated reports.
D. You can prove no one could have changed the records/data/logs that were collected.

Correct Answer: B
Explanation:
Hearsay evidence is not normally admissible in court unless it has firsthand evidence that can be used to prove the evidence's accuracy, trustworthiness, and reliability like a business person who generated the computer logs and collected them.

It is important that this person generates and collects logs as a normal part of his business and not just this one time for court. It has to be a documented process that is carried out daily.

The value of evidence depends upon the genuineness and competence of the source; therefore, since record collection is not an activity likely to be performed by senior or executive management, records collected by senior or executive management are not likely to be admissible in court.

Hearsay evidence is usually not admissible in court unless it meets the Business Records Exemption rule to the Hearsay evidence.

In certain instances computer records fall outside of the hearsay rule (e.g., business records exemption)
Information relates to regular business activities
Automatically computer generated data
No human intervention
Prove system was operating correctly
Prove no one changed the data

If you have a documented business process and you make use of intrusion detection tools, log analysis tools, and you produce daily reports of activities, then the computer generated data might be admissible in court and would not be considered Hearsay Evidence.

Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 10: Law, Investigation, and Ethics (page 676).

QUESTION 659
Which of the following statements pertaining to the maintenance of an IT contingency plan is incorrect?

A. The plan should be reviewed at least once a year for accuracy and completeness.