required hardware and software provided by the service provider. A hot site in the context of the CBK is always a RENTAL place. If you have your own site fully equipped that you make use of in case of disaster that would be called a redundant site or an alternate site.

Wikipedia: "A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data."

References:
OIG CBK, Business Continuity and Disaster Recovery Planning (pages 367 - 368) AIO, 3rd Edition, Business Continuity Planning (pages 709 - 714) AIO, 4th Edition, Business Continuity Planning , p 790. Wikipedia - http://en.wikipedia.org/wiki/Hot_site#Hot_Sites

QUESTION 496
A deviation from an organization-wide security policy requires which of the following?

A. Risk Acceptance
B. Risk Assignment
C. Risk Reduction
D. Risk Containment

Correct Answer: A
Explanation:
A deviation from an organization-wide security policy requires you to manage the risk. If you deviate from the security policy then you are required to accept the risks that might occur.

In some cases, it may be prudent for an organization to simply accept the risk that is presented in certain scenarios. Risk acceptance is the practice of accepting certain risk(s), typically based on a business decision that may also weigh the cost versus the benefit of dealing with the risk in another way.

The OIG defines Risk Management as: This term characterizes the overall process.

The first phase of risk assessment includes identifying risks, risk-reducing measures, and the budgetary impact of implementing decisions related to the acceptance, avoidance, or transfer of risk.

The second phase of risk management includes the process of assigning priority to, budgeting, implementing, and maintaining appropriate risk-reducing measures.

Risk management is a continuous process of ever-increasing complexity. It is how we evaluate the impact of exposures and respond to them. Risk management minimizes loss to information assets due to undesirable events through identification, measurement, and control. It encompasses the overall security review, risk analysis, selection and evaluation of safeguards, cost璪enefit analysis, management decision, and safeguard identification and implementation, along with ongoing effectiveness review.

Risk management provides a mechanism to the organization to ensure that executive management knows current risks, and informed decisions can be made to use one of the risk management principles: risk avoidance, risk transfer, risk mitigation, or risk acceptance.

The 4 ways of dealing with risks are: Avoidance, Transfer, Mitigation, Acceptance

The following answers are incorrect:

Risk assignment. Is incorrect because it is a distractor, assignment is not one of the ways to manage risk.
Risk reduction. Is incorrect because there was a deviation of the security policy. You could have some additional exposure by the fact that you deviated from the policy.

Risk containment. Is incorrect because it is a distractor, containment is not one of the ways to manage risk.

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 8882-8886). Auerbach Publications. Kindle Edition.
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10206-10208). Auerbach Publications. Kindle Edition.

QUESTION 497
A business continuity plan is an example of which of the following?

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

Correct Answer: A
Explanation:
Business Continuity Plans are designed to minimize the damage done by the event, and facilitate rapid restoration of the organization to its full operational capacity. They are for use "after the fact", thus are examples of corrective controls.

Reference(s) used for this question:

KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 273).
Conrad, Eric; Misenar, Seth; Feldman, Joshua (2012-09-01). CISSP Study Guide (Kindle Location 8069). Elsevier Science (reference). Kindle Edition.

QUESTION 498
All of the following can be considered essential business functions that should be identified when creating a Business Impact Analysis (BIA) except one. Which of the following would not be considered an essential element of the BIA but an important TOPIC to include within the BCP plan:

A. IT Network Support
B. Accounting
C. Public Relations
D. Purchasing

Correct Answer: C
Explanation:
Public Relations, although important to a company, is not listed as an essential business function that should be identified and have loss criteria developed for.
All other entries are considered essential and should be identified and have loss criteria

developed.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 598).

QUESTION 499
Which of the following would be MOST important to guarantee that the computer evidence will be admissible in court?

A. It must prove a fact that is immaterial to the case.
B. Its reliability must be proven.
C. The process for producing it must be documented and repeatable.
D. The chain of custody of the evidence must show who collected, secured, controlled, handled, transported the evidence, and that it was not tampered with.

Correct Answer: D
Explanation:
It has to be material, relevant and reliable, and the chain of custody must be maintained, it is unlikely that it will be admissible in court if it has been tampered with.

The following answers are incorrect:

It must prove a fact that is immaterial to the case. Is incorrect because evidence must be relevant. If it is immaterial then it is not relevant.

Its reliability must be proven. Is incorrect because it is not the best answer. While evidence must be relevant if the chain of custody cannot be verified, then the evidence could lose it's credibility because there is no proof that the evidence was not tampered with. So, the correct answer above is the BEST answer.

The process for producing it must be documented and repeatable. Is incorrect because just because the process is documented and repeatable does not mean that it will be the same. This amounts to Corroborative Evidence that may help to support a case.

QUESTION 500
What can be described as a measure of the magnitude of loss or impact on the value of an asset?

A. Probability
B. Exposure factor
C. Vulnerability
D. Threat

Correct Answer: B
Explanation:
The exposure factor is a measure of the magnitude of loss or impact on the value of an asset.
The probability is the chance or likelihood, in a finite sample, that an event will occur or that a specific loss value may be attained should the event occur.
A vulnerability is the absence or weakness of a risk-reducing safeguard. A threat is event, the occurrence of which could have an undesired impact.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 3, August 1999.

QUESTION 501
Most access violations are:

A. Accidental
B. Caused by internal hackers
C. Caused by external hackers
D. Related to Internet

Correct Answer: A
Explanation:
The most likely source of exposure is from the uninformed, accidental or unknowing person, although the greatest impact may be from those with malicious or fraudulent intent.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 4: Protection of Information Assets (page 192).

QUESTION 502
What is the MOST critical piece to disaster recovery and continuity planning?

A. Security policy
B. Management support
C. Availability of backup information processing facilities
D. Staff training

Correct Answer: B
Explanation:
The keyword is ' MOST CRITICAL ' and the correct answer is ' Management Support ' as the management must be convinced of its necessity and that's why a business case must be made. The decision of how a company should recover from any disaster is purely a business decision and should be treated as so.

The other answers are incorrect because:

Security policy is incorrect as it is not the MOST CRITICAL piece.
Availability of backup information processing facilities is incorrect as this comes once the organization has BCP Plans in place and for a BCP Plan , management support must be there.
Staff training comes after the plans are in place with the support from management.

Reference:
Shon Harris , AIO v3 , Chapter-9: Business Continuity Planning , Page: 697.

QUESTION 503
Which of the following best describes remote journaling?

A. Send hourly tapes containing transactions off-site.
B. Send daily tapes containing transactions off-site.
C. Real-time capture of transactions to multiple storage devices.
D. Real time transmission of copies of the entries in the journal of transactions to an alternate site.

Correct Answer: D
Explanation:
Remote Journaling is a technology to facilitate sending copies of the journal of transaction entries

from a production system to a secondary system in realtime. The remote nature of such a connection is predicated upon having local journaling already established. Local journaling on the production side allows each change that ensues for a journal-eligible object e.g., database physical file, SQL table, data area, data queue, byte stream file residing within the IFS) to be recorded and logged. It's these local images that flow to the remote system. Once there, the journal entries serve a variety of purposes, from feeding a high availability software replay program or data warehouse to offering an offline, realtime vault of the most recent database changes.

Reference(s) used for this question:

The Essential Guide to Remote Journaling by IBM
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 286).

QUESTION 504
What is a hot-site facility?

A. A site with pre-installed computers, raised flooring, air conditioning, telecommunications and networking equipment, and UPS.
B. A site in which space is reserved with pre-installed wiring and raised floors.
C. A site with raised flooring, air conditioning, telecommunications, and networking equipment, and UPS.
D. A site with ready made work space with telecommunications equipment, LANs, PCs, and terminals for work groups.

Correct Answer: A
Explanation:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 505
Which backup method usually resets the archive bit on the files after they have been backed up?

A. Incremental backup method.
B. Differential backup method.
C. Partial backup method.
D. Tape backup method.

Correct Answer: A
Explanation:
The incremental backup method usually resets the archive bit on the files after they have been backed up.

An Incremental Backup will backup all the files that have changed since the last Full Backup (the first time it is run after a full backup was previously completed) or after an Incremental Backup (for the second backup and subsequent backups) and sets the archive bit to 0. This type of backup take less time during the backup phase but it will take more time to restore.

The other answers are all incorrect choices.

The following backup types also exists: