D. cold site

Correct Answer: D
Explanation:
Is the least expensive because it is basically a structure with power and would be the most difficult to test because you would have to install all of the hardware infrastructure in order for it to be operational for the test.

The following answers are incorrect:

non-mobile hot site. Is incorrect because it is more expensive then a cold site and easier to test because all of the infrastructure is in place.
mobile hot site. Is incorrect because it is more expensive then a cold site and easier to test because all of the infrastructure is in place.
warm site. Is incorrect because it is more expensive then a cold site and easier to test because more of the infrastructure is in place.

QUESTION 641
The typical computer fraudsters are usually persons with which of the following characteristics?

A. They have had previous contact with law enforcement
B. They conspire with others
C. They hold a position of trust
D. They deviate from the accepted norms of society

Correct Answer: C
Explanation:
These people, as employees, are trusted to perform their duties honestly and not take advantage of the trust placed in them.

The following answers are incorrect:

They have had previous contact with law enforcement. Is incorrect because most often it is a person that holds a position of trust and this answer implies they have a criminal background. This type of individual is typically not in a position of trust within an organization.
They conspire with others. Is incorrect because they typically work alone, often as a form of retribution over a percieved injustice done to them.
They deviate from the accepted norms of society. Is incorrect because while the nature of fraudsters deviate from the norm, the fraudsters often hold a position of trust within the organization.

QUESTION 642
This type of backup management provides a continuous on-line backup by using optical or tape "jukeboxes," similar to WORMs (Write Once, Read Many):

A. Hierarchical Storage Management (HSM).
B. Hierarchical Resource Management (HRM).
C. Hierarchical Access Management (HAM).
D. Hierarchical Instance Management (HIM).

Correct Answer: A
Explanation:
Hierarchical Storage Management (HSM) provides a continuous on-line backup by using optical

or tape "jukeboxes," similar to WORMs.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 71.

QUESTION 643
A prolonged complete loss of electric power is a:

A. brownout
B. blackout
C. surge
D. fault

Correct Answer: B
Explanation:
A prolonged power outage is a blackout. From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw- Hill/Osborne, 2005, page 368.

QUESTION 644
A momentary power outage is a:

A. spike
B. blackout
C. surge
D. fault

Correct Answer: D
Explanation:
A momentary power outage is a fault.

Power Excess
Spike --> Too much voltage for a short period of time. Surge --> Too much voltage for a long period of time.

Power Loss
Fault --> A momentary power outage.
Blackout --> A long power interruption.

Power Degradation
Sag or Dip --> A momentary low voltage.
Brownout --> A prolonged power supply that is below normal voltage.

Reference(s) used for this question:

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw- Hill/Osborne, 2005, page 368.
https://en.wikipedia.org/wiki/Power_quality

QUESTION 645
Physically securing backup tapes from unauthorized access is obviously a security concern and is considered a function of the:

A. Operations Security Domain.
B. Operations Security Domain Analysis.
C. Telecommunications and Network Security Domain.
D. Business Continuity Planning and Disater Recovery Planning.

Correct Answer: A
Explanation:
Physically securing the tapes from unauthorized access is obviously a security concern and is considered a function of the Operations Security Domain.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 71.

QUESTION 646
The scope and focus of the Business continuity plan development depends most on:

A. Directives of Senior Management
B. Business Impact Analysis (BIA)
C. Scope and Plan Initiation
D. Skills of BCP committee

Correct Answer: B
Explanation:
SearchStorage.com Definitions mentions "As part of a disaster recovery plan, BIA is likely to identify costs linked to failures, such as loss of cash flow, replacement of equipment, salaries paid to catch up with a backlog of work, loss of profits, and so on.

A BIA report quantifies the importance of business components and suggests appropriate fund allocation for measures to protect them. The possibilities of failures are likely to be assessed in terms of their impacts on safety, finances, marketing, legal compliance, and quality assurance.

Where possible, impact is expressed monetarily for purposes of comparison. For example, a business may spend three times as much on marketing in the wake of a disaster to rebuild customer confidence."

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 278.

QUESTION 647
Another example of Computer Incident Response Team (CIRT) activities is:

A. Management of the netware logs, including collection, retention, review, and analysis of data
B. Management of the network logs, including collection and analysis of data
C. Management of the network logs, including review and analysis of data
D. Management of the network logs, including collection, retention, review, and analysis of data

Correct Answer: D
Explanation:
Additional examples of CIRT activities are:
Management of the network logs, including collection, retention, review, and analysis of data
Management of the resolution of an incident, management of the remediation of a vulnerability, and post-event reporting to the appropriate parties.

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 64.

QUESTION 648
When you update records in multiple locations or you make a copy of the whole database at a remote location as a way to achieve the proper level of fault-tolerance and redundancy, it is knows as?

A. Shadowing
B. Data mirroring
C. Backup
D. Archiving

Correct Answer: A
Explanation:
Updating records in multiple locations or copying an entire database to a remote location as a means to ensure the appropriate levels of fault-tolerance and redundancy is known as Database shadowing. Shadowing is the technique in which updates are shadowed in multiple locations. It is like copying the entire database on to a remote location.

Shadow files are an exact live copy of the original active database, allowing you to maintain live duplicates of your production database, which can be brought into production in the event of a hardware failure. They are used for security reasons: should the original database be damaged or incapacitated by hardware problems, the shadow can immediately take over as the primary database. It is therefore important that shadow files do not run on the same server or at least on the same drive as the primary database files.

The following are incorrect answers:

Data mirroring In data storage, disk mirroring is the replication of logical disk volumes onto separate physical hard disks in real time to ensure continuous availability. It is most commonly used in RAID 1. A mirrored volume is a complete logical representation of separate volume copies.

Backups In computing the phrase backup means to copy files to a second medium (a disk or tape) as a precaution in case the first medium fails. One of the cardinal rules in using computers is back up your files regularly. Backups are useful in recovering information or a system in the event of a disaster, else you may be very sorry :-(

Archiving is the storage of data that is not in continual use for historical purposes. It is the process of copying files to a long-term storage medium for backup.

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 27614-27626). Auerbach Publications. Kindle Edition.
http://en.wikipedia.org/wiki/Disk_mirroring
http://www.webopedia.com/TERM/A/archive.html
http://ibexpert.net/ibe/index.php?n=Doc.DatabaseShadow

QUESTION 649
Which of the following is defined as the most recent point in time to which data must be synchronized without adversely affecting the organization (financial or operational impacts)?

A. Recovery Point Objective
B. Recovery Time Objective
C. Point of Time Objective
D. Critical Time Objective

Correct Answer: A
Explanation:
The recovery point objective (RPO) is the maximum acceptable level of data loss following an unplanned "event", like a disaster (natural or man-made), act of crime or terrorism, or any other business or technical disruption that could cause such data loss. The RPO represents the point in time, prior to such an event or incident, to which lost data can be recovered (given the most recent backup copy of the data).

The recovery time objective (RTO) is a period of time within which business and / or technology capabilities must be restored following an unplanned event or disaster. The RTO is a function of the extent to which the interruption disrupts normal operations and the amount of revenue lost per unit of time as a result of the disaster.

These factors in turn depend on the affected equipment and application(s). Both of these numbers represent key targets that are set by key businesses during business continuity and disaster recovery planning; these targets in turn drive the technology and implementation choices for business resumption services, backup / recovery / archival services, and recovery facilities and procedures.

Many organizations put the cart before the horse in selecting and deploying technologies before understanding the business needs as expressed in RPO and RTO; IT departments later bear the brunt of user complaints that their service expectations are not being met. Defining the RPO and RTO can avoid that pitfall, and in doing so can also make for a compelling business case for recovery technology spending and staffing.

For the CISSP candidate studying for the exam, there are no such objectives for "point of time," and "critical time." Those two answers are simply detracters.

Reference:
http://www.wikibon.org/Recovery_point_objective_/_recovery_time_objective_strategy

QUESTION 650
What can be defined as a batch process dumping backup data through communications lines to a server at an alternate location?

A. Remote journaling
B. Electronic vaulting
C. Data clustering
D. Database shadowing

Correct Answer: B
Explanation:
Electronic vaulting refers to the transfer of backup data to an off-site location. This is primarily a batch process of dumping backup data through communications lines to a server at an alternate location.
Electronic vaulting is accomplished by backing up system data over a network. The backup location is usually at a separate geographical location known as the vault site. Vaulting can be used as a mirror or a backup mechanism using the standard incremental or differential backup cycle. Changes to the host system are sent to the vault server in real-time when the backup