TCP has the value of 6
UDP has the value of 17
ICMP has the value of 1

Reference:
SANS http://www.sans.org/resources/tcpip.pdf?ref=3871

QUESTION 537
Which of the following backup sites is the most effective for disaster recovery?

A. Time brokers
B. Hot sites
C. Cold sites
D. Reciprocal Agreement

Correct Answer: B
Explanation:
A hot site has the equipment, software and communications capabilities to facilitate a recovery within a few minutes or hours following the notification of a disaster to the organization's primary site. With the exception of providing your own hot site, commercial hot sites provide the greatest protection. Most will allow you up to six weeks to restore your sites if you declare a disaster. They also permit an annual amount of time to test the Disaster Plan.

The following answers are incorrect:

Cold sites. Cold sites are empty computer rooms consisting only of environmental systems, such as air conditioning and raised floors, etc. They do not meet the requirements of most regulators and boards of directors that the disaster plan be tested at least annually.

Reciprocal Agreement. Reciprocal agreements are not contracts and cannot be enforced. You cannot force someone you have such an agreement with to provide processing to you.

Government regulators do not accept reciprocal agreements as valid disaster recovery backup sites.

Time Brokers. Time Brokers promise to deliver processing time on other systems. They charge a fee, but cannot guaranty that processing will always be available, especially in areas that experienced multiple disasters.

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

ISC2 OIG, 2007 p368
Shon Harris AIO v3. p.710

QUESTION 538
What is the PRIMARY reason to maintain the chain of custody on evidence that has been collected?

A. To ensure that no evidence is lost.
B. To ensure that all possible evidence is gathered.
C. To ensure that it will be admissible in court
D. To ensure that incidents were handled with due care and due diligence.

Correct Answer: C
Explanation:
This is the PRIMARY reason for the chain of custody of evidence. Evidence must be controlled every step of the way. If it is not, the evidence can be tampered with and ruled inadmissable. The Chain of Custody will include a detailed record of:

Who obtained the evidence
What was the evidence
Where and when the evidence was obtained
Who secured the evidence
Who had control or possession of the evidence

The following answers are incorrect because :

To ensure that no evidence is lost is incorrect as it is not the PRIMARY reason.
To ensure that all possible evidence is gathered is also incorrect as it is not the PRIMARY reason.
To ensure that incidents were handled with due care and due diligence is also incorrect as it is also not the PRIMARY reason.

The chain of custody is a history that shows how evidence was collected, analyzed, transported, and preserved in order to establish that it is sufficiently trustworthy to be presented as evidence in court. Because electronic evidence can be easily modified, a clearly defined chain of custody demonstrates that the evidence is trustworthy which would make it admissible in court.

Reference:
Shon Harris AIO v3 , Chapter-10: Law, Investigation, and Ethics , Page: 727

QUESTION 539
Which backup method copies only files that have changed since the last full backup, but does not clear the archive bit?

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

Correct Answer: A
Explanation:
One of the key item to understand regarding backup is the archive bit. The archive bit is used to determine what files have been backuped already. The archive bit is set if a file is modified or a new file is created, this indicates to the backup program that it has to be saved on the next backup. When a full backup is performed the archive bit will be cleared indicating that the files were backup. This allows backup programs to do an incremental or differential backup that only backs up the changes to the filesystem since the last time the bit was cleared
Full Backup (or Reference Backup)
A Full backup will backup all the files and folders on the drive every time you run the full backup. The archive bit is cleared on all files indicating they were all backuped.

Advantages:
All files from the selected drives and folders are backed up to one backup set.
In the event you need to restore files, they are easily restored from the single backup set.

Disadvantages:

A full backup is more time consuming than other backup options. Full backups require more disk, tape, or network drive space.
Incremental Backup
An incremental backup provides a backup of files that have changed or are new since the last incremental backup.

For the first incremental backup, all files in the file set are backed up (just as in a full backup). If you use the same file set to perform a incremental backup later, only the files that have changed are backed up. If you use the same file set for a third backup, only the files that have changed since the second backup are backed up, and so on.

Incremental backup will clear the archive bit.
Advantages:
Backup time is faster than full backups.
Incremental backups require less disk, tape, or network drive space. You can keep several versions of the same files on different backup sets.
Disadvantages:
In order to restore all the files, you must have all of the incremental backups available. It may take longer to restore a specific file since you must search more than one backup set to find the latest version of a file.
Differential Backup

A differential backup provides a backup of files that have changed since a full backup was performed. A differential backup typically saves only the files that are different or new since the last full backup. Together, a full backup and a differential backup include all the files on your computer, changed and unchanged.

Differential backup do not clear the archive bits.

Advantages:
Differential backups require even less disk, tape, or network drive space than incremental backups.
Backup time is faster than full or incremental backups.
Disadvantages:
Restoring all your files may take considerably longer since you may have to restore both the last differential and full backup.
Restoring an individual file may take longer since you have to locate the file on either the differential or full backup.

For more info see:
http://support.microsoft.com/kb/136621 Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

QUESTION 540
Which of the following items is NOT a benefit of cold sites?

A. No resource contention with other organisation
B. Quick Recovery
C. A secondary location is available to reconstruct the environment
D. Low Cost

Correct Answer: B
Explanation:

A cold site is a permanent location that provide you with your own space that you can move into in case of a disaster or catastrophe. It is one of the cheapest solution available as a rental place but it is also the one that would take the most time to recover. A cold site usually takes one to two weeks for recoverey.

Although major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. The plan should include a trategy to recover and perform system operations at an alternate facility for an extended period. In general, three types of alternate sites are available:

Dedicated site owned or operated by the organization. Also called redundant or alternate sites;
Reciprocal agreement or memorandum of agreement with an internal or external entity; and
Commercially leased facility.

Regardless of the type of alternate site chosen, the facility must be able to support system operations as defined in the contingency plan. The three alternate site types commonly categorized in terms of their operational readiness are cold sites, warm sites, or hot sites. Other variations or combinations of these can be found, but generally all variations retain similar core features found in one of these three site types.

Progressing from basic to advanced, the sites are described below:

Cold Sites are typically facilities with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support information system recovery activities.

Warm Sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources.

Hot Sites are facilities appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel.

As discussed above, these three alternate site types are the most common. There are also variations, and hybrid mixtures of features from any one of the three. Each organization should evaluate its core requirements in order to establish the most effective solution.

Two examples of variations to the site types are:

Mobile Sites are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements.

Mirrored Sites are fully redundant facilities with automated real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.

There are obvious cost and ready-time differences among the options. In these examples, the mirrored site is the most expensive choice, but it ensures virtually 100 percent availability. Cold sites are the least expensive to maintain, although they may require substantial time to acquire and install necessary equipment. Partially equipped sites, such as warm sites, fall in the middle of the spectrum. In many cases, mobile sites may be delivered to the desired location within 24 hours, but the time necessary for equipment installation and setup can increase this response time. The selection of fixed-site locations should account for the time and mode of transportation necessary to move personnel and/or equipment there. In addition, the fixed site should be in a geographic area that is unlikely to be negatively affected by the same hazard as the organization's primary site.

The following reference(s) were used for this question:
http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11- 2010.pdf

QUESTION 541
Which of the following statements do not apply to a hot site?

A. It is expensive.
B. There are cases of common overselling of processing capabilities by the service provider.
C. It provides a false sense of security.
D. It is accessible on a first come first serve basis. In case of large disaster it might not be accessible.

Correct Answer: C
Explanation:
Remember this is a NOT question. Hot sites do not provide a false sense of security since they are the best disaster recovery alternate for backup site that you rent.

A Cold, Warm, and Hot site is always a rental place in the context of the CBK. This is definivily the best choices out of the rental options that exists. It is fully configured and can be activated in a very short period of time.

Cold and Warm sites, not hot sites, provide a false sense of security because you can never fully test your plan.

In reality, using a cold site will most likely make effective recovery impossible or could lead to business closure if it takes more than two weeks for recovery.

Source: 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 284).

QUESTION 542
Of the following, which is NOT a specific loss criteria that should be considered while developing a BIA?

A. Loss of skilled workers knowledge
B. Loss in revenue
C. Loss in profits
D. Loss in reputation

Correct Answer: A
Explanation:
Although a loss of skilled workers knowledge would cause the company a great loss, it is not identified as a specific loss criteria. It would fall under one of the three other criteria listed as distracters.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 598).

QUESTION 543
What assesses potential loss that could be caused by a disaster?

A. The Business Assessment (BA)