QUESTION 607
Which of the following should be emphasized during the Business Impact Analysis (BIA) considering that the BIA focus is on business processes?

A. Composition
B. Priorities
C. Dependencies
D. Service levels

Correct Answer: C
Explanation:
The Business Impact Analysis (BIA) identifies time-critical aspects of the critical business processes, and determines their maximum tolerable downtime. The BIA helps to Identify organization functions, the capabilities of each organization unit to handle outages, and the priority and sequence of functions and applications to be recovered, identify resources required for recovery of those areas and interdependencies

In performing the Business Impact Analysis (BIA) it is very important to consider what the dependencies are. You cannot bring a system up if it depends on another system to be operational. You need to look at not only internal dependencies but external as well. You might not be able to get the raw materials for your business so dependencies are very important aspect of a BIA.

The BIA committee will not truly understand all business processes, the steps that must take place, or the resources and supplies these processes require. So the committee must gather this information from the people who do know-- department managers and specific employees throughout the organization. The committee starts by identifying the people who will be part of the BIA data-gathering sessions. The committee needs to identify how it will collect the data from the selected employees, be it through surveys, interviews, or workshops. Next, the team needs to collect the information by actually conducting surveys, interviews, and workshops. Data points obtained as part of the information gathering will be used later during analysis. It is important that the team members ask about how different tasks-- whether processes, transactions, or services, along with any relevant dependencies-- get accomplished within the organization.

The following answers are incorrect:
composition This is incorrect because it is not the best answer. While the make up of business may be important, if you have not determined the dependencies first you may not be able to bring the critical business processes to a ready state or have the materials on hand that are needed.

priorities This is incorrect because it is not the best answer. While the priorities of processes are important, if you have not determined the dependencies first you may not be able to bring the critical business processes to a ready state or have the materials on hand that are needed.

service levels This is incorrect because it is not the best answer. Service levels are not as important as dependencies.

Reference(s) used for this question:

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition. Business Continuity and Disaster Recovery Planning (Kindle Locations 188-191). . Kindle Edition. And Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 18562-18568). McGraw-Hill. Kindle Edition.

QUESTION 608
Which backup method only copies files that have been recently added or changed and also leaves the archive bit unchanged?

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

Correct Answer: D
Explanation:
A differential backup is a partial backup that copies a selected file to tape only if the archive bit for that file is turned on, indicating that it has changed since the last full backup. A differential backup leaves the archive bits unchanged on the files it copies.

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 69).

Also see: http://e-articles.info/e/a/title/Backup-Types/

Backup software can use or ignore the archive bit in determining which files to back up, and can either turn the archive bit off or leave it unchanged when the backup is complete. How the archive bit is used and manipulated determines what type of backup is done, as follows

Full backup
A full backup, which Microsoft calls a normal backup, backs up every selected file, regardless of the status of the archive bit. When the backup completes, the backup software turns off the archive bit for every file that was backed up. Note that "full" is a misnomer because a full backup backs up only the files you have selected, which may be as little as one directory or even a single file, so in that sense Microsoft's terminology is actually more accurate. Given the choice, full backup is the method to use because all files are on one tape, which makes it much easier to retrieve files from tape when necessary. Relative to partial backups, full backups also increase redundancy because all files are on all tapes. That means that if one tape fails, you may still be able to retrieve a given file from another tape.

Differential backup
A differential backup is a partial backup that copies a selected file to tape only if the archive bit for that file is turned on, indicating that it has changed since the last full backup. A differential backup leaves the archive bits unchanged on the files it copies. Accordingly, any differential backup set contains all files that have changed since the last full backup. A differential backup set run soon after a full backup will contain relatively few files. One run soon before the next full backup is due will contain many files, including those contained on all previous differential backup sets since the last full backup. When you use differential backup, a complete backup set comprises only two tapes or tape sets: the tape that contains the last full backup and the tape that contains the most recent differential backup.

Incremental backup
An incremental backup is another form of partial backup. Like differential backups, Incremental Backups copy a selected file to tape only if the archive bit for that file is turned on. Unlike the differential backup, however, the incremental backup clears the archive bits for the files it backs up. An incremental backup set therefore contains only files that have changed since the last full backup or the last incremental backup. If you run an incremental backup daily, files changed on Monday are on the Monday tape, files changed on Tuesday are on the Tuesday tape, and so forth. When you use an incremental backup scheme, a complete backup set comprises the tape

that contains the last full backup and all of the tapes that contain every incremental backup done since the last normal backup. The only advantages of incremental backups are that they minimize backup time and keep multiple versions of files that change frequently. The disadvantages are that backed-up files are scattered across multiple tapes, making it difficult to locate any particular file you need to restore, and that there is no redundancy. That is, each file is stored only on one tape.

Full copy backup
A full copy backup (which Microsoft calls a copy backup) is identical to a full backup except for the last step. The full backup finishes by turning off the archive bit on all files that have been backed up. The full copy backup instead leaves the archive bits unchanged. The full copy backup is useful only if you are using a combination of full backups and incremental or differential partial backups. The full copy backup allows you to make a duplicate "full" backup--e.g., for storage offsite, without altering the state of the hard drive you are backing up, which would destroy the integrity of the partial backup rotation. Some Microsoft backup software provides a bizarre backup method Microsoft calls a daily copy backup. This method ignores the archive bit entirely and instead depends on the date and timestamp of files to determine which files should be backed up. The problem is, it's quite possible for software to change a file without changing the date- and timestamp, or to change the date- and timestamp without changing the contents of the file. For this reason, we regard the daily copy backup as entirely unreliable and recommend you avoid using it.

QUESTION 609
A prolonged power supply that is below normal voltage is a:

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

Correct Answer: A
Explanation:
A prolonged power supply that is below normal voltage is a brownout.
From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw-Hill/Osborne, 2005, page 368.

QUESTION 610
What does "residual risk" mean?

A. The security risk that remains after controls have been implemented
B. Weakness of an assets which can be exploited by a threat
C. Risk that remains after risk assessment has has been performed
D. A security risk intrinsic to an asset being audited, where no mitigation has taken place.

Correct Answer: A
Explanation:
Residual risk is "The security risk that remains after controls have been implemented" ISO/IEC TR 13335-1 Guidelines for the Management of IT Security (GMITS), Part 1: Concepts and Models for IT Security, 1996. "Weakness of an assets which can be exploited by a threat" is vulnerability. "The result of unwanted incident" is impact. Risk that remains after risk analysis has been performed is a distracter.
Risk can never be eliminated nor avoided, but it can be mitigated, transferred or accpeted. Even after applying a countermeasure like for example putiing up an Antivirus. But still it is not 100%

that systems will be protected by antivirus.

QUESTION 611
What can be defined as an event that could cause harm to the information systems?

A. A risk
B. A threat
C. A vulnerability
D. A weakness

Correct Answer: B
Explanation:
A threat is an event or activity that has the potential to cause harm to the information systems. A risk is the probability that a threat will materialize. A vulnerability, or weakness, is a lack of a safeguard, which may be exploited by a threat, causing harm to the information systems.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 1: Access Control Systems (page 32).

QUESTION 612
Which of the following statements pertaining to a Criticality Survey is incorrect?

A. It is implemented to gather input from all personnel that is going to be part of the recovery teams.
B. The purpose of the survey must be clearly stated.
C. Management's approval should be obtained before distributing the survey.
D. Its intent is to find out what services and systems are critical to keeping the organization in business.

Correct Answer: A
Explanation:
The Criticality Survey is implemented through a standard questionnaire to gather input from the most knowledgeable people. Not all personnel that is going to be part of recovery teams is necessarily able to help in identifying critical functions of the organization.
The intent of such a survey is to identify the services and systems that are critical to the organization.
Having a clearly stated purpose for the survey helps in avoiding misinterpretations.
Management's approval of the survey should be obtained before distributing it.
Source: HARE, Chris, CISSP Study Guide: Business Continuity Planning Domain,

QUESTION 613
What can be defined as the maximum acceptable length of time that elapses before the unavailability of the system severely affects the organization?

A. Recovery Point Objectives (RPO)
B. Recovery Time Objectives (RTO)
C. Recovery Time Period (RTP)
D. Critical Recovery Time (CRT)

Correct Answer: B
Explanation:
One of the results of a Business Impact Analysis is a determination of each business function's Recovery Time Objectives (RTO). The RTO is the amount of time allowed for the recovery of a

business function. If the RTO is exceeded, then severe damage to the organization would result. The Recovery Point Objectives (RPO) is the point in time in which data must be restored in order to resume processing.

Reference(s) used for this question:
BARNES, James C.& ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 68).
And: 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 47).

QUESTION 614
Which of the following is the most important consideration in locating an alternate computing facility during the development of a disaster recovery plan?

A. It is unlikely to be affected by the same disaster.
B. It is close enough to become operational quickly.
C. It is close enough to serve its users.
D. It is convenient to airports and hotels.

Correct Answer: A
Explanation:
You do not want the alternate or recovery site located in close proximity to the original site because the same event that create the situation in the first place might very well impact that site also.

From NIST: "The fixed site should be in a geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure) as the organization's primary site.

The following answers are incorrect:

It is close enough to become operational quickly. Is incorrect because it is not the best answer. You'd want the alternate site to be close but if it is too close the same event could impact that site as well.

It is close enough to serve its users. Is incorrect because it is not the best answer. You'd want the alternate site to be close to users if applicable, but if it is too close the same event could impact that site as well

It is convenient to airports and hotels. Is incorrect because it is not the best answer, it is more important that the same event does not impact the alternate site then convenience.

References:
OIG CBK Business Continuity and Disaster Recovery Planning (pages 368 - 369) NIST document 800-34 pg 21

QUESTION 615
How is Annualized Loss Expectancy (ALE) derived from a threat?

A. ARO x (SLE - EF)
B. SLE x ARO
C. SLE/EF