Many elements of a BCP will address senior management, such as the statement of importance and priorities, the statement of organizational responsibility, and the statement of urgency and timing. Executive management staff initiates the project, gives final approval and gives ongoing support. The BCP committee directs the planning, implementation, and tests processes whereas functional business units participate in implementation and testing.
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 275).

QUESTION 529
Which of the following is a large hardware/software backup system that uses the RAID technology?

A. Tape Array.
B. Scale Array.
C. Crimson Array
D. Table Array.

Correct Answer: A
Explanation:
A Tape Array is a large hardware/software backup system based on the RAID technology.

There is a misconception that RAID can only be used with Disks. All large storage vendor from HP, to EMC, to Compaq have Tape Array based on RAID technology they offer.

This is a VERY common type of storage at an affordable price as well.

So RAID is not exclusively for DISKS. Often time this is referred to as Tape Librairies or simply RAIT.
RAIT (redundant array of independent tapes) is similar to RAID, but uses tape drives instead of disk drives. Tape storage is the lowest-cost option for very large amounts of data, but is very slow compared to disk storage. As in RAID 1 striping, in RAIT, data are striped in parallel to multiple tape drives, with or without a redundant parity drive. This provides the high capacity at low cost typical of tape storage, with higher-than-usual tape data transfer rates and optional data integrity.

References:
KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 70.
And Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 1271). McGraw-Hill. Kindle Edition.

QUESTION 530
Which of the following is the best reason for the use of an automated risk analysis tool?

A. Much of the data gathered during the review cannot be reused for subsequent analysis.
B. Automated methodologies require minimal training and knowledge of risk analysis.
C. Most software tools have user interfaces that are easy to use and does not require any training.
D. Information gathering would be minimized and expedited due to the amount of information already built into the tool.

Correct Answer: D
Explanation:
The use of tools simplifies this process. Not only do they usually have a database of assests,

threats, and vulnerabilities but they also speed up the entire process.

Using Automated tools for performing a risk assessment can reduce the time it takes to perform them and can simplify the process as well. The better types of these tools include a well-researched threat population and associated statistics. Using one of these tools virtually ensures that no relevant threat is overlooked, and associated risks are accepted as a consequence of the threat being overlooked.

In most situations, the assessor will turn to the use of a variety of automated tools to assist in the vulnerability assessment process. These tools contain extensive databases of specific known vulnerabilities as well as the ability to analyze system and network configuration information to predict where a particular system might be vulnerable to different types of attacks. There are many different types of tools currently available to address a wide variety of vulnerability assessment needs. Some tools will examine a system from the viewpoint of the network, seeking to determine if a system can be compromised by a remote attacker exploiting available services on a particular host system. These tools will test for open ports listening for connections, known vulnerabilities in common services, and known operating system exploits.

Michael Gregg says:
Automated tools are available that minimize the effort of the manual process. These programs enable users to rerun the analysis with different parameters to answer "what-ifs." They perform calculations quickly and can be used to estimate future expected losses easier than performing the calculations manually.

Shon Harris in her latest book says:
The gathered data can be reused, greatly reducing the time required to perform subsequent analyses. The risk analysis team can also print reports and comprehensive graphs to present to management.

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 4655-4661). Auerbach Publications. Kindle Edition.
CISSP Exam Cram 2 by Michael Gregg
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 2333-2335). McGraw-Hill. Kindle Edition.

The following answers are incorrect:

Much of the data gathered during the review cannot be reused for subsequent analysis. Is incorrect because the data can be reused for later analysis.

Automated methodologies require minimal training and knowledge of risk analysis. Is incorrect because it is not the best answer. While a minimal amount of training and knowledge is needed, the analysis should still be performed by skilled professionals.

Most software tools have user interfaces that are easy to use and does not require any training. Is incorrect because it is not the best answer. While many of the user interfaces are easy to use it is better if the tool already has information built into it. There is always a training curve when any product is being used for the first time.

QUESTION 531
Which of the following tape formats can be used to backup data systems in addition to its original intended audio uses?

A. Digital Video Tape (DVT).
B. Digital Analog Tape (DAT).
C. Digital Voice Tape (DVT).
D. Digital Audio Tape (DAT).

Correct Answer: D
Explanation:
Digital Audio Tape (DAT) can be used to backup data systems in addition to its original intended audio uses.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 70.

QUESTION 532
Out of the steps listed below, which one is not one of the steps conducted during the Business Impact Analysis (BIA)?

A. Alternate site selection
B. Create data-gathering techniques
C. Identify the company's critical business functions
D. Select individuals to interview for data gathering

Correct Answer: A
Explanation:
Selecting and Alternate Site would not be done within the initial BIA. It would be done at a later stage of the BCP and DRP recovery effort. All of the other choices were steps that would be conducted during the BIA. See below the list of steps that would be done during the BIA.

A BIA (business impact analysis) is considered a functional analysis, in which a team collects data through interviews and documentary sources; documents business functions, activities, and transactions ; develops a hierarchy of business functions; and finally applies a classification scheme to indicate each individual function's criticality level.

BIA Steps
1. Select individuals to interview for data gathering.
2. Create data-gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3. Identify the company's critical business functions.
4. Identify the resources these functions depend upon.
5. Calculate how long these functions can survive without these resources.
6. Identify vulnerabilities and threats to these functions.
7. Calculate the risk for each different business function.
8. Document findings and report them to management.

Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 905-909). McGraw-Hill. Kindle Edition.

QUESTION 533
Risk mitigation and risk reduction controls for providing information security are classified within three main categories, which of the following are being used?

A. preventive, corrective, and administrative
B. detective, corrective, and physical

C. Physical, technical, and administrative
D. Administrative, operational, and logical

Correct Answer: C
Explanation:
Security is generally defined as the freedom from danger or as the condition of safety. Computer security, specifically, is the protection of data in a system against unauthorized disclosure, modification, or destruction and protection of the computer system itself against unauthorized use, modification, or denial of service. Because certain computer security controls inhibit productivity, security is typically a compromise toward which security practitioners, system users, and system operations and administrative personnel work to achieve a satisfactory balance between security and productivity.

Controls for providing information security can be physical, technical, or administrative. These three categories of controls can be further classified as either preventive or detective. Preventive controls attempt to avoid the occurrence of unwanted events, whereas detective controls attempt to identify unwanted events after they have occurred. Preventive controls inhibit the free use of computing resources and therefore can be applied only to the degree that the users are willing to accept. Effective security awareness programs can help increase users' level of tolerance for preventive controls by helping them understand how such controls enable them to trust their computing systems. Common detective controls include audit trails, intrusion detection methods, and checksums.

Three other types of controls supplement preventive and detective controls. They are usually described as deterrent, corrective, and recovery.

Deterrent controls are intended to discourage individuals from intentionally violating information security policies or procedures. These usually take the form of constraints that make it difficult or undesirable to perform unauthorized activities or threats of consequences that influence a potential intruder to not violate security (e.g., threats ranging from embarrassment to severe punishment).
Corrective controls either remedy the circumstances that allowed the unauthorized activity or return conditions to what they were before the violation. Execution of corrective controls could result in changes to existing physical, technical, and administrative controls. Recovery controls restore lost computing resources or capabilities and help the organization recover monetary losses caused by a security violation.

Deterrent, corrective, and recovery controls are considered to be special cases within the major categories of physical, technical, and administrative controls; they do not clearly belong in either preventive or detective categories. For example, it could be argued that deterrence is a form of prevention because it can cause an intruder to turn away; however, deterrence also involves detecting violations, which may be what the intruder fears most. Corrective controls, on the other hand, are not preventive or detective, but they are clearly linked with technical controls when antiviral software eradicates a virus or with administrative controls when backup procedures enable restoring a damaged data base. Finally, recovery controls are neither preventive nor detective but are included in administrative controls as disaster recovery or contingency plans.

Reference(s) used for this question:
Handbook of Information Security Management, Hal Tipton

QUESTION 534
Which of the following is the most critical item from a disaster recovery point of view?

A. Data

B. Hardware/Software
C. Communication Links
D. Software Applications

Correct Answer: A
Explanation:
The most important point is ALWAYS the data. Everything else can be replaced or repaired.

Data MUST be backed up, backups must be regularly tested, because once it is truly lost, it is lost forever.

The goal of disaster recovery is to minimize the effects of a disaster or disruption. It means taking the necessary steps to ensure that the resources, personnel, and business processes are able to resume operation in a timely manner . This is different from continuity planning, which provides methods and procedures for dealing with longer-term outages and disasters.

The goal of a disaster recovery plan is to handle the disaster and its ramifications right after the disaster hits; the disaster recovery plan is usually very information technology (IT)?focused. A disaster recovery plan (DRP) is carried out when everything is still in emergency mode, and everyone is scrambling to get all critical systems back online.

Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 887). McGraw- Hill. Kindle Edition.
And Veritas eLearning CD - Introducing Disaster Recovery Planning, Chapter 1.

QUESTION 535
Which of the following is NOT a common backup method?

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

Correct Answer: B
Explanation:
A daily backup is not a backup method, but defines periodicity at which backups are made. There can be daily full, incremental or differential backups.
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).

QUESTION 536
The IP header contains a protocol field. If this field contains the value of 51, what type of data is contained within the ip datagram?

A. Transmission Control Protocol (TCP)
B. Authentication Header (AH)
C. User datagram protocol (UDP)
D. Internet Control Message Protocol (ICMP)

Correct Answer: B
Explanation: