Too much voltage for a long period of time is a surge.
Not enough voltage for a short period of time is a sag or dip.
Not enough voltage for a long period of time is brownout.
A short power interruption is a fault.
A long power interruption is a blackout.
You MUST know all of the power issues above for the purpose of the exam. From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw- Hill/Osborne, 2005, page 368.

QUESTION 631
During the testing of the business continuity plan (BCP), which of the following methods of results analysis provides the BEST assurance that the plan is workable?

A. Measurement of accuracy
B. Elapsed time for completion of critical tasks
C. Quantitatively measuring the results of the test
D. Evaluation of the observed test results

Correct Answer: C
Explanation:
It is important to have ways to measure the success of the plan and tests against the stated objectives. Therefore, results must be quantitatively gauged as opposed to an evaluation based only on observation. Quantitatively measuring the results of the test involves a generic statement measuring all the activities performed during BCP, which gives the best assurance of an effective plan. Although choices A and B are also quantitative, they relate to specific areas, or an analysis of results from one viewpoint, namely the accuracy of the results and the elapsed time.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 5: Disaster Recovery and Business Continuity (page 269).

QUESTION 632
In the statement below, fill in the blank:

Law enforcement agencies must get a warrant to search and seize an individual's property, as stated in the _____ Amendment.

A. First.
B. Second.
C. Third.
D. Fourth.

Correct Answer: D
Explanation:
The Fourth Amendment does not apply to a seizure or an arrest by private citizens.

Search and seizure activities can get tricky depending on what is being searched for and where. For example, American citizens are protected by the Fourth Amendment against unlawful search and seizure, so law enforcement agencies must have probable cause and request a search warrant from a judge or court before conducting such a search.

The actual search can only take place in the areas outlined by the warrant. The Fourth Amendment does not apply to actions by private citizens unless they are acting as police agents. So, for example, if Kristy's boss warned all employees that the management could remove files from their computers at any time, and her boss was not a police officer or acting as a police

agent, she could not successfully claim that her Fourth Amendment rights were violated. Kristy's boss may have violated some specific privacy laws, but he did not violate Kristy's Fourth Amendment rights.

In some circumstances, a law enforcement agent may seize evidence that is not included in the warrant, such as if the suspect tries to destroy the evidence. In other words, if there is an impending possibility that evidence might be destroyed, law enforcement may quickly seize the evidence to prevent its destruction. This is referred to as exigent circumstances, and a judge will later decide whether the seizure was proper and legal before allowing the evidence to be admitted. For example, if a police officer had a search warrant that allowed him to search a suspect's living room but no other rooms, and then he saw the suspect dumping cocaine down the toilet, the police officer could seize the cocaine even though it was in a room not covered under his search warrant. After evidence is gathered, the chain of custody needs to be enacted and enforced to make sure the evidence's integrity is not compromised.

All other choices were only detractors.

Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 1057). McGraw- Hill. Kindle Edition.

QUESTION 633
Of the reasons why a Disaster Recovery plan gets outdated, which of the following is not true?

A. Personnel turnover
B. Large plans can take a lot of work to maintain
C. Continous auditing makes a Disaster Recovery plan irrelevant
D. Infrastructure and environment changes

Correct Answer: C
Explanation:
Although a auditing is a part of corporate security, it in no way supercedes the requirments for a disaster recovery plan. All others can be blamed for a plan going out of date.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 609).

QUESTION 634
Which of the following statements pertaining to quantitative risk analysis is false?

A. Portion of it can be automated
B. It involves complex calculations
C. It requires a high volume of information
D. It requires little experience to apply

Correct Answer: D
Explanation:
Assigning the values for the inputs to a purely quantitative risk assessment requires both a lot of time and significant experience on the part of the assessors. The most experienced employees or representatives from each of the departments would be involved in the process. It is NOT an easy task if you wish to come up with accurate values.

"It can be automated" is incorrect. There are a number of tools on the market that automate the process of conducting a quantitative risk assessment.

"It involves complex calculations" is incorrect. The calculations are simple for basic scenarios but could become fairly complex for large cases. The formulas have to be applied correctly.

"It requires a high volume of information" is incorrect. Large amounts of information are required in order to develop reasonable and defensible values for the inputs to the quantitative risk assessment.

References:
CBK, pp. 60-61
AIO3, p. 73, 78
The Cissp Prep Guide - Mastering The Ten Domains Of Computer Security - 2001, page 24

QUESTION 635
Under the principle of culpable negligence, executives can be held liable for losses that result from computer system breaches if:

A. The company is not a multi-national company.
B. They have not exercised due care protecting computing resources.
C. They have failed to properly insure computer resources against loss.
D. The company does not prosecute the hacker that caused the breach.

Correct Answer: B
Explanation:
Culpable negligence is defined as: Recklessly acting without reasonable caution and putting another person at risk of injury or death (or failing to do something with the same consequences)

Where a suspected security breach has been caused (through wilful intent or culpable negligence) disciplinary action may be sought in line with the appropriate misconduct guidelines for internal employees.

By not exercising Due Care and taking the proper actions, the executives would be liable for losses a company has suffered.

Reference(s) used for this question:

TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
http://www.thefreedictionary.com/culpable+negligence

QUESTION 636
The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations or confusing an intruder about which flaws to exploit is called:

A. alteration
B. investigation
C. entrapment
D. enticement.

Correct Answer: D
Explanation:
Enticement deals with someone that is breaking the law. Entrapment encourages someone to commit a crime that the individual may or many have had no intention of committing. Enticement is not necessarily illegal but does raise ethical arguments and may not be admissible in court.

Enticement lures someone toward some evidence (a honeypot would be a great example) after that individual has already committed a crime.

Entrapment is when you persuade someone to commit a crime when the person otherwise had no intention to commit a crime. Entrapment is committed by a law enforcement player where you get tricked into committing a crime for which you woud later on get arrested without knowing you rare committing such a scrime. It is illegal and unethical as well.

All other choices were not applicable and only detractors.

References:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
CISSP Study Guide (Conrad, Misenar, Feldman). Elsevier. 2010. p. 428
http://www.dummies.com/how-to/content/security-certification-computer-forensics-and- inci.html

QUESTION 637
What is the highest amount a company should spend annually on countermeasures for protecting an asset valued at $1,000,000 from a threat that has an annualized rate of occurrence (ARO) of once every five years and an exposure factor (EF) of 30%?

A. $300,000
B. $150,000
C. $60,000
D. $1,500

Correct Answer: C
Explanation:
The cost of a countermeasure should not be greater in cost than the risk it mitigates (ALE). For a quantitative risk assessment, the equation is ALE = ARO x SLE where the SLE is calculated as the product of asset value x exposure factor. An event that happen once every five years would have an ARO of .2 (1 divided by 5).

SLE = Asset Value (AV) x Exposure Fact (EF)
SLE = 1,000,000 x .30 = 300,000

ALE = SLE x Annualized Rate of Occurance (ARO)
ALE = 300,000 x .2 = 60,000

Know your acronyms:
ALE -- Annual loss expectancy
ARO -- Annual rate of occurrence
SLE -- Single loss expectancy

The following are incorrect answers:

$300,000 is incorrect. See the explanation of the correct answer for the correct calculation.
$150,000 is incorrect. See the explanation of the correct answer for the correct calculation.
$1,500 is incorrect. See the explanation of the correct answer for the correct calculation.

Reference(s) used for this question:

Mc Graw Hill, Shon Harris, CISSP All In One (AIO) book, Sixth Edition , Pages 87-88 and Official ISC2 Guide to the CISSP Exam, (OIG), Pages 60-61
QUESTION 638

When should a post-mortem review meeting be held after an intrusion has been properly taken care of?

A. Within the first three months after the investigation of the intrusion is completed.
B. Within the first week after prosecution of intruders have taken place, whether successful or not.
C. Within the first month after the investigation of the intrusion is completed.
D. Within the first week of completing the investigation of the intrusion.

Correct Answer: D
Explanation:
A post-mortem review meeting should be held with all involved parties within three to five working days of completing the investigation of the intrusion. Otherwise, participants are likely to forget critical information. Even if it enabled an organization to validate the correctness of its chain of custody of evidence, it would not make sense to wait until prosecution is complete because it would take too much time and many cases of intrusion never get to court anyway.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Chapter 7: Responding to Intrusions (page 297).

QUESTION 639
Which of the following statements regarding an off-site information processing facility is TRUE?

A. It should have the same amount of physical access restrictions as the primary processing site.
B. It should be located in proximity to the originating site so that it can quickly be made operational.
C. It should be easily identified from the outside so in the event of an emergency it can be easily found.
D. Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive.

Correct Answer: A
Explanation:
It is very important that the offsite has the same restrictions in order to avoide misuse.

The following answers are incorrect because:

It should be located in proximity to the originating site so that it can quickly be made operational is incorrect as the offsite is also subject to the same disaster as of the primary site.

It should be easily identified from the outside so in the event of an emergency it can be easily found is also incorrect as it should not be easily identified to prevent intentional sabotage.
Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive is also incorrect as it should be like its primary site.

Reference:
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 5: Disaster Recovery and Business Continuity (page 265).

QUESTION 640
Which of the following computer recovery sites is the least expensive and the most difficult to test?

A. non-mobile hot site
B. mobile hot site
C. warm site