D. AV x EF

Correct Answer: B
Explanation:
Three steps are undertaken in a quantitative risk assessment:

Initial management approval
Construction of a risk assessment team, and
The review of information currently available within the organization.

There are a few formulas that you MUST understand for the exam. See them below:

SLE (Single Loss Expectancy)
Single loss expectancy (SLE) must be calculated to provide an estimate of loss. SLE is defined as the difference between the original value and the remaining value of an asset after a single exploit.

The formula for calculating SLE is as follows: SLE = asset value (in $) ?exposure factor (loss due to successful threat exploit, as a %)

Losses can include lack of availability of data assets due to data loss, theft, alteration, or denial of service (perhaps due to business continuity or security issues).

ALE (Annualized Loss Expectancy)
Next, the organization would calculate the annualized rate of occurrence (ARO).

This is done to provide an accurate calculation of annualized loss expectancy (ALE).

ARO is an estimate of how often a threat will be successful in exploiting a vulnerability over the period of a year.

When this is completed, the organization calculates the annualized loss expectancy (ALE). The ALE is a product of the yearly estimate for the exploit (ARO) and the loss in value of an asset after an SLE.

The calculation follows ALE = SLE x ARO

Note that this calculation can be adjusted for geographical distances using the local annual frequency estimate (LAFE) or the standard annual frequency estimate (SAFE). Given that there is now a value for SLE, it is possible to determine what the organization should spend, if anything, to apply a countermeasure for the risk in question.

Remember that no countermeasure should be greater in cost than the risk it mitigates, transfers, or avoids.
Countermeasure cost per year is easy and straightforward to calculate. It is simply the cost of the countermeasure divided by the years of its life (i.e., use within the organization). Finally, the organization is able to compare the cost of the risk versus the cost of the countermeasure and make some objective decisions regarding its countermeasure selection.

The following were incorrect answers:

All of the other choices were incorrect.

The following reference(s) were used for this quesiton:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition

((ISC)2 Press) (Kindle Locations 10048-10069). Auerbach Publications. Kindle Edition.

QUESTION 616
What would be the Annualized Rate of Occurrence (ARO) of the threat "user input error", in the case where a company employs 100 data entry clerks and every one of them makes one input error each month?

A. 100
B. 120
C. 1
D. 1200

Correct Answer: D
Explanation:
If every one of the 100 clerks makes 1 error 12 times per year, it makes a total of 1200 errors. The Annnualized Rate of Occurence (ARO) is a value that represents the estimated frequency in which a threat is expected to occur. The range can be from 0.0 to a large number. Having an average of 1200 errors per year means an ARO of 1200

QUESTION 617
Which one of the following represents an ALE calculation?

A. single loss expectancy x annualized rate of occurrence.
B. gross loss expectancy x loss frequency.
C. actual replacement cost - proceeds of salvage.
D. asset value x loss expectancy.

Correct Answer: A
Explanation:
Single Loss Expectancy (SLE) is the dollar amount that would be lost if there was a loss of an asset. Annualized Rate of Occurrence (ARO) is an estimated possibility of a threat to an asset taking place in one year (for example if there is a change of a flood occuring once in 10 years the ARO would be .1, and if there was a chance of a flood occuring once in 100 years then the ARO would be .01).

The following answers are incorrect:

gross loss expectancy x loss frequency. Is incorrect because this is a distractor.
actual replacement cost - proceeds of salvage. Is incorrect because this is a distractor.
asset value x loss expectancy. Is incorrect because this is a distractor.

QUESTION 618
Which of the following is a problem regarding computer investigation issues?

A. Information is tangible.
B. Evidence is easy to gather.
C. Computer-generated records are only considered secondary evidence, thus are not as reliable as best evidence.
D. In many instances, an expert or specialist is not required.

Correct Answer: C
Explanation:

Because computer-generated records normally fall under the category of hearsay evidence because they cannot be proven accurate and reliable this can be a problem.

Under the U.S. Federal Rules of Evidence, hearsay evidence is generally not admissible in court. This inadmissibility is known as the hearsay rule, although there are some exceptions for how, when, by whom and in what circumstances data was collected.

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 9: Law, Investigation, and Ethics (page 310).

IMPORTANT NOTE:
For the purpose of the exam it is very important to remember the Business Record exemption to the Hearsay Rule. For example: if you create log files and review them on a regular basis as part of a business process, such files would be admissable in court and they would not be considered hearsay because they were made in the course of regular business and it is part of regular course of business to create such record.

Here is another quote from the HISM book:

Business Record Exemption to the Hearsay Rule
Federal Rules of Evidence 803(6) allow a court to admit a report or other business document made at or near the time by or from information transmitted by a person with knowledge, if kept in the course of regularly conducted business activity, and if it was the regular practice of that business activity to make the [report or document], all as shown by testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness.

To meet Rule 803(6) the witness must:

Have custody of the records in question on a regular basis.
Rely on those records in the regular course of business.
Know that they were prepared in the regular course of business.

Audit trails meet the criteria if they are produced in the normal course of business. The process to produce the output will have to be proven to be reliable. If computer-generated evidence is used and admissible, the court may order disclosure of the details of the computer, logs, and maintenance records in respect to the system generating the printout, and then the defense may use that material to attack the reliability of the evidence. If the audit trails are not used or reviewed -- at least the exceptions (e.g., failed log-on attempts) -- in the regular course of business, they do not meet the criteria for admissibility.

Federal Rules of Evidence 1001(3) provide another exception to the hearsay rule. This rule allows a memory or disk dump to be admitted as evidence, even though it is not done in the regular course of business. This dump merely acts as statement of fact. System dumps (in binary or hexadecimal) are not hearsay because they are not being offered to prove the truth of the contents, but only the state of the computer.

BUSINESS RECORDS LAW EXAMPLE:
The business records law was enacted in 1931 (PA No. 56). For a document to be admissible under the statute, the proponent must show: (1) the document was made in the regular course of business; (2) it was the regular course of business to make the record; and (3) the record was made when the act, transaction, or event occurred, or shortly thereafter (State v. Vennard, 159 Conn. 385, 397 (1970); Mucci v. LeMonte, 157 Conn. 566, 570 (1969). The failure to establish any one of these essential elements renders the document inadmissible under the statute

(McCahill v. Town and Country Associates, Ltd. , 185 Conn. 37 (1981); State v. Peary, 176 Conn. 170 (1978); Welles v. Fish Transport Co. , , 123 Conn. 49 (1937).

The statute expressly provides that the person who made the business entry does not have to be unavailable as a witness and the proponent does not have to call as a witness the person who made the record or show the person to be unavailable (State v. Jeustiniano, 172 Conn. 275 (1977).

The person offering the business records as evidence does not have to independently prove the trustworthiness of the record. But, there is no presumption that the record is accurate; the record's accuracy and weight are issues for the trier of fact (State v. Waterman, 7 Conn. App. 326 (1986); Handbook of Connecticut Evidence, Second Edition, § 11. 14. 3).

Reference:
http://search.cga.state.ct.us/dtsearch_lpa.asp?cmd=getdoc&DocId=16833&Index=I%3A%5Czindex%5C1995&HitCount=0&hits=&hc=0&req=&Item=712

QUESTION 619
If your property Insurance has Replacement Cost Valuation (RCV) clause your damaged property will be compensated:

A. Based on the value of item on the date of loss
B. Based on new, comparable, or identical item for old regardless of condition of lost item
C. Based on value of item one month before the loss
D. Based on the value listed on the Ebay auction web site

Correct Answer: B
Explanation:
RCV is the maximum amount your insurance company will pay you for damage to covered property before deducting for depreciation. The RCV payment is based on the current cost to replace your property with new, identical or comparable property.

The other choices were detractor:

Application and definition of the insurance terms Replacement Cost Value (RCV), Actual Cash Value (ACV) and depreciation can be confusing. It's important that you understand the terms to help settle your claim fairly.

An easy way to understand RCV and ACV is to think in terms of "new" and "used." Replacement cost is the item's current price, new. "What will it cost when I replace it?" Actual cash is the item's used price, old. "How much money is it worth since I used it for five years?"

Hold Back
Most policies only pay the Actual Cash Value upfront, and then they pay you the "held back" depreciation after you incur the expense to repair or replace your personal property items.

NOTE:
You must remember to send documentation to the insurance company proving you've incurred the additional expense you will be reimbursed.

Actual Cash Value (ACV)
ACV is the amount your insurance company will pay you for damage to covered property after deducting for depreciation. ACV is the replacement cost of a new item, minus depreciation. If stated as a simple equation, ACV could be defined as follows: ACV=RCV- Depreciation

Unfortunately, ACV is not always as easy to agree upon as a simple math equation. The ACV can also be calculated as the price a willing buyer would pay for your used item.

Depreciation
Depreciation (sometimes called "hold back") is defined as the "loss in value from all causes, including age, and wear and tear." Although the definition seems to be clear, in our experience, value" as a real-world application is clearly subjective and varies widely. We have seen the same adjuster apply NO depreciation (100 percent value) on one claim and 40 percent depreciation almost half value) on an almost identical claim.

This shows that the process of applying depreciation is subjective and clearly negotiable.

Excessive Depreciation
When the insurance company depreciates more than they should, it is called "Excessive depreciation." Although not ethical, it is very common. Note any items that have excessive depreciation and write a letter to your insurance company.

References:
http://carehelp.org/downloads/category/1-insurance-handouts.html?download=17%3Ahandout08-rcv-and-acv
http://www.schirickinsurance.com/resources/value2005.pdf
TIPTON, Harold F.& KRAUSE, MICKI, information Security Management Handbook, 4th Edition, Volume 1 Property Insurance overview, Page 587.

QUESTION 620
Which common backup method is the fastest on a daily basis?

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

Correct Answer: B
Explanation:
The incremental backup method only copies files that have been recently changed or added. Only files with their archive bit set are backed up. This method is fast and uses less tape space but has some inherent vulnerabilities, one being that all incremental backups need to be available and restored from the date of the last full backup to the desired date should a restore be needed.
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 621
Which of the following enables the person responsible for contingency planning to focus risk management efforts and resources in a prioritized manner only on the identified risks?

A. Risk assessment
B. Residual risks
C. Security controls
D. Business units

Correct Answer: A
Explanation: