The risk assessment is critical because it enables the person responsible for contingency planning to focus risk management efforts and resources in a prioritized manner only on the identified risks. The risk management process includes the risk assessment and determination of suitable technical, management, and operational security controls based on the level of threat the risk imposes. Business units should be included in this process.
Source: 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 7).

QUESTION 622
Computer security should be first and foremost which of the following:

A. Cover all identified risks
B. Be cost-effective.
C. Be examined in both monetary and non-monetary terms.
D. Be proportionate to the value of IT systems.

Correct Answer: B
Explanation:
Computer security should be first and foremost cost-effective.

As for any organization, there is a need to measure their cost-effectiveness, to justify budget usage and provide supportive arguments for their next budget claim. But organizations often have difficulties to accurately measure the effectiveness and the cost of their information security activities.

The classical financial approach for ROI calculation is not particularly appropriate for measuring security-related initiatives: Security is not generally an investment that results in a profit. Security is more about loss prevention. In other terms, when you invest in security, you don't expect benefits; you expect to reduce the risks threatening your assets.

The concept of the ROI calculation applies to every investment. Security is no exception. Executive decision-makers want to know the impact security is having on the bottom line. In order to know how much they should spend on security, they need to know how much is the lack of security costing to the business and what are the most cost-effective solutions.

Applied to security, a Return On Security Investment (ROSI) calculation can provide quantitative answers to essential financial questions:

Is an organization paying too much for its security?
What financial impact on productivity could have lack of security?
When is the security investment enough?
Is this security product/organisation beneficial?

The following are other concerns about computer security but not the first and foremost:
The costs and benefits of security should be carefully examined in both monetary and non-monetary terms to ensure that the cost of controls does not exceed expected benefits.

Security should be appropriate and proportionate to the value of and degree of reliance on the IT systems and to the severity, probability, and extent of potential harm.

Requirements for security vary, depending upon the particular IT system. Therefore it does not make sense for computer security to cover all identified risks when the cost of the measures exceeds the value of the systems they are protecting.

Reference(s) used for this question:
SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 6).
http://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment

QUESTION 623
Because ordinary cable introduces a toxic hazard in the event of fire, special cabling is required in a separate area provided for air circulation for heating, ventilation, and air- conditioning (sometimes referred to as HVAC) and typically provided in the space between the structural ceiling and a drop-down ceiling. This area is referred to as the:

A. smoke boundry area
B. fire detection area
C. Plenum area
D. Intergen area

Correct Answer: C
Explanation:
In building construction, a plenum (pronounced PLEH-nuhm, from Latin meaning full) is a separate space provided for air circulation for heating, ventilation, and air- conditioning (sometimes referred to as HVAC) and typically provided in the space between the structural ceiling and a drop-down ceiling. A plenum may also be under a raised floor. In buildings with computer installations, the plenum space is often used to house connecting communication cables. Because ordinary cable introduces a toxic hazard in the event of fire, special plenum cabling is required in plenum areas.
Source: http://searchdatacenter.techtarget.com/sDefinition/0,,sid80_gci213716,00.html

QUESTION 624
Which approach to a security program ensures people responsible for protecting the company's assets are DRIVING the program?

A. The Delphi approach
B. The top-down approach
C. The bottom-up approach
D. The technology approach

Correct Answer: B
Explanation:
A security program should use a top-down approach, meaning that the initiation, support, and direction come from top management; work their way through middle management; and then reach staff members.

In contrast, a bottom-up approach refers to a situation in which staff members (usually IT) try to develop a security program without getting proper management support and direction. A bottom-up approach is commonly less effective, not broad enough to address all security risks, and doomed to fail.

A top-down approach makes sure the people actually responsible for protecting the company's assets (senior management) are driving the program.

The following are incorrect answers:

The Delphi approach is incorrect as this is for a brainstorming technique.
The bottom-up approach is also incorrect as this approach would be if the IT department tried to develop a security program without proper support from upper management.
The technology approach is also incorrect as it does not fit into the category of best answer.

Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 63). McGraw-Hill. Kindle Edition.

QUESTION 625
During the salvage of the Local Area Network and Servers, which of the following steps would normally be performed first?

A. Damage mitigation
B. Install LAN communications network and servers
C. Assess damage to LAN and servers
D. Recover equipment

Correct Answer: C
Explanation:
The first activity in every recovery plan is damage assessment, immediately followed by damage mitigation.
This first activity would typically include assessing the damage to all network and server components (including cables, boards, file servers, workstations, printers, network equipment), making a list of all items to be repaired or replaced, selecting appropriate vendors and relaying findings to Emergency Management Team.
Following damage mitigation, equipment can be recovered and LAN communications network and servers can be reinstalled.
Source: BARNES, James C.& ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 135).

QUESTION 626
Which of the following server contingency solutions offers the highest availability?

A. System backups
B. Electronic vaulting/remote journaling
C. Redundant arrays of independent disks (RAID)
D. Load balancing/disk replication

Correct Answer: D
Explanation:
Of the offered technologies, load balancing/disk replication offers the highest availability, measured in terms of minutes of lost data or server downtime. A Network-Attached Storage (NAS) or a Storage Area Network (SAN) solution combined with virtualization would offer an even higher availability.
Source: 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 49).

QUESTION 627
Computer-generated evidence is considered:

A. Best evidence
B. Second hand evidence
C. Demonstrative evidence
D. Direct evidence

Correct Answer: B
Explanation:
Computer-generated evidence normally falls under the category of hearsay evidence, or second-hand evidence, because it cannot be proven accurate and reliable. Under the U.S. Federal Rules of Evidence, hearsay evidence is generally not admissible in court. Best evidence is original or primary evidence rather than a copy or duplicate of the evidence. It does not apply to computer-generated evidence. Direct evidence is oral testimony by witness. Demonstrative evidence are used to aid the jury (models, illustrations, charts).
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).
And: ROTHKE, Ben, CISSP CBK Review presentation on domain 9.

QUESTION 628
Which of the following will a Business Impact Analysis NOT identify?

A. Areas that would suffer the greatest financial or operational loss in the event of a disaster.
B. Systems critical to the survival of the enterprise.
C. The names of individuals to be contacted during a disaster.
D. The outage time that can be tolerated by the enterprise as a result of a disaster.

Correct Answer: C
Explanation:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 629
If an employee's computer has been used by a fraudulent employee to commit a crime, the hard disk may be seized as evidence and once the investigation is complete it would follow the normal steps of the Evidence Life Cycle. In such case, the Evidence life cycle would not include which of the following steps listed below?

A. Acquisition collection and identification
B. Analysis
C. Storage, preservation, and transportation
D. Destruction

Correct Answer: D
Explanation:
Unless the evidence is illegal then it should be returned to owner, not destroyed.

The Evidence Life Cycle starts with the discovery and collection of the evidence. It progresses through the following series of states until it is finally returned to the victim or owner:

Acquisition collection and identification
Analysis

Storage, preservation, and transportation
Presented in court
Returned to victim (owner)

The Second edition of the ISC2 book says on page 529-530:

Identifying evidence: Correctly identifying the crime scene, evidence, and potential containers of evidence.
Collecting or acquiring evidence: Adhering to the criminalistic principles and ensuring that the contamination and the destruction of the scene are kept to a minimum. Using sound, repeatable, collection techniques that allow for the demonstration of the accuracy and integrity of evidence, or copies of evidence.
Examining or analyzing the evidence: Using sound scientific methods to determine the characteristics of the evidence, conducting comparison for individuation of evidence, and conducting event reconstruction.
Presentation of findings: Interpreting the output from the examination and analysis based on findings of fact and articulating these in a format appropriate for the intended audience (e.g., court brief, executive memo, report).

Note on returning the evidence to the Owner/Victim

The final destination of most types of evidence is back with its original owner. Some types of evidence, such as drugs or drug paraphernalia (i.e., contraband), are destroyed after the trial.

Any evidence gathered during a search, although maintained by law enforcement, is legally under the control of the courts. And although a seized item may be yours and may even have your name on it, it might not be returned to you unless the suspect signs a release or after a hearing by the court. Unfortunately, many victims do not want to go to trial; they just want to get their property back.

Many investigations merely need the information on a disk to prove or disprove a fact in question; thus, there is no need to seize the entire system. Once a schematic of the system is drawn or photographed, the hard disk can be removed and then transported to a forensic lab for copying.

Mirror copies of the suspect disk are obtained using forensic software and then one of those copies can be returned to the victim so that business operations can resume.

Reference(s) used for this question:
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 309).
And The Official Study Book, Second Edition, Page 529-230

QUESTION 630
A momentary high voltage is a:

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

Correct Answer: A
Explanation:
Too much voltage for a short period of time is a spike.