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 121).

**QUESTION 246**
The three classic ways of authenticating yourself to the computer security software are: something you know, something you have, and something:

A. you need.
B. you read.
C. you are.
D. you do.

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

**QUESTION 247**
Which of the following questions is less likely to help in assessing physical and environmental protection?

A. Are entry codes changed periodically?
B. Are appropriate fire suppression and prevention devices installed and working?
C. Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?
D. Is physical access to data transmission lines controlled?

**Correct Answer:** C
**Explanation:**
Physical security and environmental security are part of operational controls, and are measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. All the questions above are useful in assessing physical and environmental protection except for the one regarding processes that ensuring that unauthorized individuals cannot access information, which is more a production control.
Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self- Assessment Guide for Information Technology Systems, November 2001 (Pages A-21 to A-24).

**QUESTION 248**
This baseline sets certain thresholds for specific errors or mistakes allowed and the amount of these occurrences that can take place before it is considered suspicious?

A. Checkpoint level
B. Ceiling level
C. Clipping level
D. Threshold level

**Correct Answer:** C
**Explanation:**
Organizations usually forgive a particular type, number, or pattern of violations, thus permitting a predetermined number of user errors before gathering this data for analysis. An organization attempting to track all violations, without sophisticated statistical computing ability, would be unable to manage the sheer quantity of such data. To make a violation listing effective, a clipping

level must be established.

The clipping level establishes a baseline for violation activities that may be normal user errors. Only after this baseline is exceeded is a violation record produced. This solution is particularly effective for small- to medium-sized installations. Organizations with large-scale computing facilities often track all violations and use statistical routines to cull out the minor infractions (e.g., forgetting a password or mistyping it several times).

If the number of violations being tracked becomes unmanageable, the first step in correcting the problems should be to analyze why the condition has occurred. Do users understand how they are to interact with the computer resource? Are the rules too difficult to follow? Violation tracking and analysis can be valuable tools in assisting an organization to develop thorough but useable controls. Once these are in place and records are produced that accurately reflect serious violations, tracking and analysis become the first line of defense. With this procedure, intrusions are discovered before major damage occurs and sometimes early enough to catch the perpetrator. In addition, business protection and preservation are strengthened.

The following answers are incorrect:
All of the other choices presented were simply detractors.

The following reference(s) were used for this question:
Handbook of Information Security Management

**QUESTION 249**
Which of the following floors would be most appropriate to locate information processing facilities in a 6-stories building?

A. Basement
B. Ground floor
C. Third floor
D. Sixth floor

**Correct Answer:** C
**Explanation:**
You data center should be located in the middle of the facility or the core of a building to provide protection from natural disasters or bombs and provide easier access to emergency crewmembers if necessary. By being at the core of the facility the external wall would act as a secondary layer of protection as well.

Information processing facilities should not be located on the top floors of buildings in case of a fire or flooding coming from the roof. Many crimes and theft have also been conducted by simply cutting a large hole on the roof.

They should not be in the basement because of flooding where water has a natural tendancy to flow down :-) Even a little amount of water would affect your operation considering the quantity of electrical cabling sitting directly on the cement floor under under your raise floor.

The data center should not be located on the first floor due to the presence of the main entrance where people are coming in and out. You have a lot of high traffic areas such as the elevators, the loading docks, cafeteria, coffee shopt, etc.. Really a bad location for a data center.

So it was easy to come up with the answer by using the process of elimination where the top, the bottom, and the basement are all bad choices. That left you with only one possible answer which is the third floor.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 5th Edition, Page 425.

**QUESTION 250**
Which of the following is related to physical security and is not considered a technical control?

A. Access control Mechanisms
B. Intrusion Detection Systems
C. Firewalls
D. Locks

**Correct Answer:** D
**Explanation:**
All of the above are considered technical controls except for locks, which are physical controls.

Administrative, Technical, and Physical Security Controls

Administrative security controls are primarily policies and procedures put into place to define and guide employee actions in dealing with the organization's sensitive information. For example, policy might dictate (and procedures indicate how) that human resources conduct background checks on employees with access to sensitive information. Requiring that information be classified and the process to classify and review information classifications is another example of an administrative control. The organization security awareness program is an administrative control used to make employees cognizant of their security roles and responsibilities. Note that administrative security controls in the form of a policy can be enforced or verified with technical or physical security controls. For instance, security policy may state that computers without antivirus software cannot connect to the network, but a technical control, such as network access control software, will check for antivirus software when a computer tries to attach to the network.

Technical security controls (also called logical controls) are devices, processes, protocols, and other measures used to protect the C.I.
A.of sensitive information. Examples include logical access systems, encryptions systems, antivirus systems, firewalls, and intrusion detection systems.

Physical security controls are devices and means to control physical access to sensitive information and to protect the availability of the information. Examples are physical access systems (fences, mantraps, guards), physical intrusion detection systems (motion detector, alarm system), and physical protection systems (sprinklers, backup generator). Administrative and technical controls depend on proper physical security controls being in place. An administrative policy allowing only authorized employees access to the data center do little good without some kind of physical access control.
From the GIAC.ORG website

**QUESTION 251**
According to private sector data classification levels, how would salary levels and medical information be classified?

A. Public.
B. Internal Use Only.
C. Restricted.
D. Confidential.

**Correct Answer:** D

**Explanation:**
Typically there are three to four levels of information classification used by most organizations: Confidential: Information that, if released or disclosed outside of the organization, would create severe problems for the organization. For example, information that provides a competitive advantage is important to the technical or financial success (like trade secrets, intellectual property, or research designs), or protects the privacy of individuals would be considered confidential. Information may include payroll information, health records, credit information, formulas, technical designs, restricted regulatory information, senior management internal correspondence, or business strategies or plans. These may also be called top secret, privileged, personal, sensitive, or highly confidential. In other words this information is ok within a defined group in the company such as marketing or sales, but is not suited for release to anyone else in the company without permission.

The following answers are incorrect:

Public: Information that may be disclosed to the general public without concern for harming the company, employees, or business partners. No special protections are required, and information in this category is sometimes referred to as unclassified. For example, information that is posted to a company's public Internet site, publicly released announcements, marketing materials, cafeteria menus, and any internal documents that would not present harm to the company if they were disclosed would be classified as public. While there is little concern for confidentiality, integrity and availability should be considered.

Internal Use Only: Information that could be disclosed within the company, but could harm the company if disclosed externally. Information such as customer lists, vendor pricing, organizational policies, standards and procedures, and internal organization announcements would need baseline security protections, but do not rise to the level of protection as confidential information. In other words, the information may be used freely within the company but any unapproved use outside the company can pose a chance of harm.

Restricted: Information that requires the utmost protection or, if discovered by unauthorized personnel, would cause irreparable harm to the organization would have the highest level of classification. There may be very few pieces of information like this within an organization, but data classified at this level requires all the access control and protection mechanisms available to the organization. Even when information classified at this level exists, there will be few copies of it

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 952-976). Auerbach Publications. Kindle Edition.

**QUESTION 252**
Which of the following phases of a software development life cycle normally addresses Due Care and Due Diligence?

A. Implementation
B. System feasibility
C. Product design
D. Software plans and requirements

**Correct Answer:** D
**Explanation:**
The software plans and requirements phase addresses threats, vulnerabilities, security requirements, reasonable care, due diligence, legal liabilities, cost/benefit analysis, level of protection desired, test plans.

Implementation is incorrect because it deals with Installing security software, running the system, acceptance testing, security software testing, and complete documentation certification and accreditation (where necessary).

System Feasibility is incorrect because it deals with information security policy, standards, legal issues, and the early validation of concepts.

Product design is incorrect because it deals with incorporating security specifications, adjusting test plans and data,
determining access controls, design documentation, evaluating encryption options, and verification.

Sources:
KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 252).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Security Life Cycle Components, Figure 7.5 (page 346).

**QUESTION 253**
Which of the following rules is least likely to support the concept of least privilege?

A. The number of administrative accounts should be kept to a minimum.
B. Administrators should use regular accounts when performing routine operations like reading mail.
C. Permissions on tools that are likely to be used by hackers should be as restrictive as possible.
D. Only data to and from critical systems and applications should be allowed through the firewall.

**Correct Answer:** D
**Explanation:**
Only data to and from critical systems and applications should be allowed through the firewall is a detractor. Critical systems or applications do not necessarily need to have traffic go through a firewall. Even if they did, only the minimum required services should be allowed. Systems that are not deemed critical may also need to have traffic go through the firewall.

Least privilege is a basic tenet of computer security that means users should be given only those rights required to do their jobs or tasks. Least privilege is ensuring that you have the minimum privileges necessary to do a task. An admin NOT using his admin account to check email is a clear example of this.

Reference(s) used for this question:
National Security Agency, Systems and Network Attack Center (SNAC), The 60 Minute Network Security Guide, February 2002, page 9.

**QUESTION 254**
Which of the following is commonly used for retrofitting multilevel security to a database management system?

A. trusted front-end.
B. trusted back-end.
C. controller.
D. kernel.