D. multitasking

Correct Answer: A
Explanation:
Pipelining is a natural concept in everyday life, e.g. on an assembly line. Consider the assembly of a car: assume that certain steps in the assembly line are to install the engine, install the hood, and install the wheels (in that order, with arbitrary interstitial steps). A car on the assembly line can have only one of the three steps done at once. After the car has its engine installed, it moves on to having its hood installed, leaving the engine installation facilities available for the next car. The first car then moves on to wheel installation, the second car to hood installation, and a third car begins to have its engine installed. If engine installation takes 20 minutes, hood installation takes 5 minutes, and wheel installation takes 10 minutes, then finishing all three cars when only one car can be assembled at once would take 105 minutes. On the other hand, using the assembly line, the total time to complete all three is 75 minutes. At this point, additional cars will come off the assembly line at 20 minute increments.

In computing, a pipeline is a set of data processing elements connected in series, so that the output of one element is the input of the next one. The elements of a pipeline are often executed in parallel or in time-sliced fashion; in that case, some amount of buffer storage is often inserted between elements. Pipelining is used in processors to allow overlapping execution of multiple instructions within the same circuitry. The circuitry is usually divided into stages, including instruction decoding, arithmetic, and register fetching stages, wherein each stage processes one instruction at a time.

The following were not correct answers:

CISC: is a CPU design where single instructions execute several low-level operations (such as a load from memory, an arithmetic operation, and a memory store) within a single instruction.

RISC: is a CPU design based on simplified instructions that can provide higher performance as the simplicity enables much faster execution of each instruction.

Multitasking: is a method where multiple tasks share common processing resources, such as a CPU, through a method of fast scheduling that gives the appearance of parallelism, but in reality only one task is being performed at any one time.

Reference:
KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, pages 188-189.

Also see
http://en.wikipedia.org/wiki/Pipeline_(computing)

QUESTION 403
Which of the following statements pertaining to a security policy is incorrect?

A. Its main purpose is to inform the users, administrators and managers of their obligatory requirements for protecting technology and information assets.
B. It specifies how hardware and software should be used throughout the organization.
C. It needs to have the acceptance and support of all levels of employees within the organization in order for it to be appropriate and effective.
D. It must be flexible to the changing environment.

Correct Answer: B

Explanation:
A security policy would NOT define how hardware and software should be used throughout the organization. A standard or a procedure would provide such details but not a policy.
A security policy is a formal statement of the rules that people who are given access to anorganization's technology and information assets must abide. The policy communicates the security goals to all of the users, the administrators, and the managers. The goals will be largely determined by the following key tradeoffs: services offered versus security provided, ease of use versus security, and cost of security versus risk of loss.

The main purpose of a security policy is to inform the users, the administrators and the managers of their obligatory requirements for protecting technology and information assets.

The policy should specify the mechanisms through which these requirements can be met. Another purpose is to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy. In order for a security policy to be appropriate and effective, it needs to have the acceptance and support of all levels of employees within the organization. A good security policy must:

Be able to be implemented through system administration procedures, publishing of acceptable use guidelines, or other appropriate methods
Be able to be enforced with security tools, where appropriate, and with sanctions, where actual prevention is not technically feasible
Clearly define the areas of responsibility for the users, the administrators, and the managers
Be communicated to all once it is established
Be flexible to the changing environment of a computer network since it is a living document

Reference(s) used for this question:

National Security Agency, Systems and Network Attack Center (SNAC),The 60 Minute Network Security Guide, February 2002, page 7.
or
A local copy is kept at:
https://www.freepracticetests.org/documents/The%2060%20Minute%20Network%20Security%20Guide.pdf

QUESTION 404
Which property ensures that only the intended recipient can access the data and nobody else?

A. Confidentiality
B. Capability
C. Integrity
D. Availability

Correct Answer: A
Explanation:
Confidentiality is defined as the property that ensures that only the intended recipient can access the data and nobody else. It is usually achieve using cryptogrphic methods, tools, and protocols.

Confidentiality supports the principle of "least privilege" by providing that only authorized individuals, processes, or systems should have access to information on a need-to-know basis. The level of access that an authorized individual should have is at the level necessary for them to do their job. In recent years, much press has been dedicated to the privacy of information and the need to protect it from individuals, who may be able to commit crimes by viewing the information. Identity theft is the act of assuming one's identity through knowledge of confidential information

obtained from various sources.

The following are incorrect answers:
Capability is incorrect. Capability is relevant to access control. Capability-based security is a concept in the design of secure computing systems, one of the existing security models. A capability (known in some systems as a key) is a communicable, unforgeable token of authority. It refers to a value that references an object along with an associated set of access rights. A user program on a capability-based operating system must use a capability to access an object. Capability-based security refers to the principle of designing user programs such that they directly share capabilities with each other according to the principle of least privilege, and to the operating system infrastructure necessary to make such transactions efficient and secure.

Integrity is incorrect. Integrity protects information from unauthorized modification or loss.
Availability is incorrect. Availability assures that information and services are available for use by authorized entities according to the service level objective.

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 9345-9349). Auerbach Publications. Kindle Edition.
http://en.wikipedia.org/wiki/Capability-based_security

QUESTION 405
What prevents a process from accessing another process' data?

A. Memory segmentation
B. Process isolation
C. The reference monitor
D. Data hiding

Correct Answer: B
Explanation:
Process isolation is where each process has its own distinct address space for its application code and data. In this way, it is possible to prevent each process from accessing another process' data. This prevents data leakage, or modification to the data while it is in memory. Memory segmentation is a virtual memory management mechanism. The reference monitor is an abstract machine that mediates all accesses to objects by subjects. Data hiding, also known as information hiding, is a mechanism that makes information available at one processing level is not available at another level.
Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

QUESTION 406
Which of the following security mode of operation does NOT require all users to have the clearance for all information processed on the system?

A. Compartmented security mode
B. Multilevel security mode
C. System-high security mode
D. Dedicated security mode

Correct Answer: B
Explanation:
The multilevel security mode permits two or more classification levels of information to be

processed at the same time when all the users do not have the clearance of formal approval to access all the information being processed by the system.

In dedicated security mode, all users have the clearance or authorization and need-to-know to all data processed within the system.

In system-high security mode, all users have a security clearance or authorization to access the information but not necessarily a need-to-know for all the information processed on the system (only some of the data).

In compartmented security mode, all users have the clearance to access all the information processed by the system, but might not have the need-to-know and formal access approval.

Generally, Security modes refer to information systems security modes of operations used in mandatory access control (MAC) systems. Often, these systems contain information at various levels of security classification.

The mode of operation is determined by:

The type of users who will be directly or indirectly accessing the system. The type of data, including classification levels, compartments, and categories, that are processed on the system. The type of levels of users, their need to know, and formal access approvals that the users will have.

Dedicated security mode
In this mode of operation, all users must have:

Signed NDA for ALL information on the system.
Proper clearance for ALL information on the system.
Formal access approval for ALL information on the system.
A valid need to know for ALL information on the system.

All users can access ALL data.
System high security mode

In this mode of operation, all users must have:

Signed NDA for ALL information on the system.
Proper clearance for ALL information on the system. Formal access approval for ALL information on the system. A valid need to know for SOME information on the system.

All users can access SOME data, based on their need to know.

Compartmented security mode
In this mode of operation, all users must have:

Signed NDA for ALL information on the system.
Proper clearance for ALL information on the system. Formal access approval for SOME information they will access on the system. A valid need to know for SOME information on the system.

All users can access SOME data, based on their need to know and formal access approval.

Multilevel security mode
In this mode of operation, all users must have:

Signed NDA for ALL information on the system.
Proper clearance for SOME information on the system. Formal access approval for SOME information on the system. A valid need to know for SOME information on the system.

All users can access SOME data, based on their need to know, clearance and formal access approval.

References:
WALLHOFF, John, CBK#6 Security Architecture and Models (CISSP Study Guide), April 2002 (page 6).
http://en.wikipedia.org/wiki/Security_Modes

QUESTION 407
It is a violation of the "separation of duties" principle when which of the following individuals access the software on systems implementing security?

A. security administrator
B. security analyst
C. systems auditor
D. systems programmer

Correct Answer: D
Explanation:
Reason: The security administrator, security analysis, and the system auditor need access to portions of the security systems to accomplish their jobs. The system programmer does not need access to the working (AKA: Production) security systems.

Programmers should not be allowed to have ongoing direct access to computers running production systems (systems used by the organization to operate its business). To maintain system integrity, any changes they make to production systems should be tracked by the organization's change management control system.

Because the security administrator's job is to perform security functions, the performance of non-security tasks must be strictly limited. This separation of duties reduces the likelihood of loss that results from users abusing their authority by taking actions outside of their assigned functional responsibilities.

References:
OFFICIAL (ISC)2?GUIDE TO THE CISSP?EXAM (2003), Hansche, S., Berti, J., Hare, H., Auerbach Publication, FL, Chapter 5 - Operations Security, section 5.3,"Security Technology and Tools," Personnel section (page 32).
KRUTZ, R. & VINES, R. The CISSP Prep Guide: Gold Edition (2003), Wiley Publishing Inc., Chapter 6: Operations Security, Separations of Duties (page 303).

QUESTION 408
Which of the following is an advantage in using a bottom-up versus a top-down approach to software testing?

A. Interface errors are detected earlier.
B. Errors in critical modules are detected earlier.
C. Confidence in the system is achieved earlier.
D. Major functions and processing are tested earlier.