C. guideline
D. procedure

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

QUESTION 284
Which of the following is not one of the three goals of Integrity addressed by the Clark-Wilson model?

A. Prevention of the modification of information by unauthorized users.
B. Prevention of the unauthorized or unintentional modification of information by authorized users.
C. Preservation of the internal and external consistency.
D. Prevention of the modification of information by authorized users.

Correct Answer: A
Explanation:
There is no need to prevent modification from authorized users. They are authorized and allowed to make the changes. On top of this, it is also NOT one of the goal of Integrity within Clark-Wilson.

As it turns out, the Biba model addresses only the first of the three integrity goals which is Prevention of the modification of information by unauthorized users. Clark-Wilson addresses all three goals of integrity.

The Clark璚ilson model improves on Biba by focusing on integrity at the transaction level and addressing three major goals of integrity in a commercial environment. In addition to preventing changes by unauthorized subjects, Clark and Wilson realized that high-integrity systems would also have to prevent undesirable changes by authorized subjects and to ensure that the system continued to behave consistently. It also recognized that it would need to ensure that there is constant mediation between every subject and every object if such integrity was going to be maintained.

Integrity is addressed through the following three goals:

1. Prevention of the modification of information by unauthorized users.
2. Prevention of the unauthorized or unintentional modification of information by authorized users.
3. Preservation of the internal and external consistency.

The following reference(s) were 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 17689-17694). Auerbach Publications. Kindle Edition.
KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 31.

QUESTION 285
Which of the following statements pertaining to protection rings is false?

A. They provide strict boundaries and definitions on what the processes that work within each ring can access.
B. Programs operating in inner rings are usually referred to as existing in a privileged mode.

C. They support the CIA triad requirements of multitasking operating systems.
D. They provide users with a direct access to peripherals

Correct Answer: D
Explanation:
In computer science, hierarchical protection domains, often called protection rings, are mechanisms to protect data and functionality from faults (fault tolerance) and malicious behaviour (computer security). This approach is diametrically opposite to that of capability-based security.

Computer operating systems provide different levels of access to resources. A protection ring is one of two or more hierarchical levels or layers of privilege within the architecture of a computer system. This is generally hardware-enforced by some CPU architectures that provide different CPU modes at the hardware or microcode level.

Rings are arranged in a hierarchy from most privileged (most trusted, usually numbered zero) to least privileged (least trusted, usually with the highest ring number). On most operating systems, Ring 0 is the level with the most privileges and interacts most directly with the physical hardware such as the CPU and memory.

Special gates between rings are provided to allow an outer ring to access an inner ring's resources in a predefined manner, as opposed to allowing arbitrary usage. Correctly gating access between rings can improve security by preventing programs from one ring or privilege level from misusing resources intended for programs in another. For example, spyware running as a user program in Ring 3 should be prevented from turning on a web camera without informing the user, since hardware access should be a Ring 1 function reserved for device drivers. Programs such as web browsers running in higher numbered rings must request access to the network, a resource restricted to a lower numbered ring.

"They provide strict boundaries and definitions on what the processes that work within each ring can access" is incorrect. This is in fact one of the characteristics of a ring protection system.

"Programs operating in inner rings are usually referred to as existing in a privileged mode" is incorrect. This is in fact one of the characteristics of a ring protection system.

"They support the CIA triad requirements of multitasking operating systems" is incorrect. This is in fact one of the characteristics of a ring protection system.

Reference(s) used for this question:

CBK, pp. 310-311
AIO3, pp. 253-256
AIOv4 Security Architecture and Design (pages 308 - 310) AIOv5 Security Architecture and Design (pages 309 - 312)

QUESTION 286
Which of the following describes a technique in which a number of processor units are employed in a single computer system to increase the performance of the system in its application environment above the performance of a single processor of the same kind?

A. Multitasking

B. Multiprogramming
C. Pipelining
D. Multiprocessing

Correct Answer: D
Explanation:
Multiprocessing is an organizational technique in which a number of processor units are employed in a single computer system to increase the performance of the system in its application environment above the performance of a single processor of the same kind. In order to cooperate on a single application or class of applications, the processors share a common resource. Usually this resource is primary memory, and the multiprocessor is called a primary memory multiprocessor. A system in which each processor has a private (local) main memory and shares secondary (global) memory with the others is a secondary memory multiprocessor, sometimes called a multicomputer system because of the looser coupling between processors. The more common multiprocessor systems incorporate only processors of the same type and performance and thus are called homogeneous multiprocessors; however, heterogeneous multiprocessors are also employed. A special case is the attached processor, in which a second processor module is attached to a first processor in a closely coupled fashion so that the first can perform input/output and operating system functions, enabling the attached processor to concentrate on the application workload.

The following were incorrect answers:

Multiprogramming: The interleaved execution of two or more programs by a computer, in which the central processing unit executes a few instructions from each program in succession.

Multitasking: The concurrent operation by one central processing unit of two or more processes.

Pipelining: A procedure for processing instructions in a computer program more rapidly, in which each instruction is divided into numerous small stages, and a population of instructions are in various stages at any given time. One instruction does not have to wait for the previous one to complete all of the stages before it gets into the pipeline. It would be similiar to an assembly chain in the real world.

References:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

http://www.answers.com/multiprocessing?cat=technology
http://www.answers.com/multitasking?cat=biz-fin
http://www.answers.com/pipelining?cat=technology

QUESTION 287
When two or more separate entities (usually persons) operating in concert to protect sensitive functions or information must combine their knowledge to gain access to an asset, this is known as?

A. Dual Control
B. Need to know
C. Separation of duties
D. Segragation of duties

Correct Answer: A
Explanation:
The question mentions clearly "operating together". Which means the BEST answer is Dual

Control.

Two mechanisms necessary to implement high integrity environments where separation of duties is paramount are dual control or split knowledge.

Dual control enforces the concept of keeping a duo responsible for an activity. It requires more than one employee available to perform a task. It utilizes two or more separate entities (usually persons), operating together, to protect sensitive functions or information.

Whenever the dual control feature is limited to something you know., it is often called split knowledge (such as part of the password, cryptographic keys etc.) Split knowledge is the unique "what each must bring" and joined together when implementing dual control.

To illustrate, let say you have a box containing petty cash is secured by one combination lock and one keyed lock. One employee is given the combination to the combo lock and another employee has possession of the correct key to the keyed lock. In order to get the cash out of the box both employees must be present at the cash box at the same time. One cannot open the box without the other. This is the aspect of dual control.

On the other hand, split knowledge is exemplified here by the different objects (the combination to the combo lock and the correct physical key), both of which are unique and necessary, that each brings to the meeting.

This is typically used in high value transactions / activities (as per the organizations risk appetite) such as:

Approving a high value transaction using a special user account, where the password of this user account is split into two and managed by two different staff. Both staff should be present to enter the password for a high value transaction. This is often combined with the separation of duties principle. In this case, the posting of the transaction would have been performed by another staff. This leads to a situation where collusion of at least 3 people are required to make a fraud transaction which is of high value.

Payment Card and PIN printing is separated by SOD principles. Now the organization can even enhance the control mechanism by implementing dual control / split knowledge. The card printing activity can be modified to require two staff to key in the passwords for initiating the printing process. Similarly, PIN printing authentication can also be made to be implemented with dual control. Many Host Security modules (HSM) comes with built in controls for dual controls where physical keys are required to initiate the PIN printing process.

Managing encryption keys is another key area where dual control / split knowledge to be implemented.

PCI DSS defines Dual Control as below. This is more from a cryptographic perspective, still useful:

Dual Control: Process of using two or more separate entities (usually persons) operating in concert to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person is permitted to access or use the materials (for example, the cryptographic key). For manual key generation, conveyance, loading, storage, and retrieval, dual control requires dividing knowledge of the key among the entities. (See also Split Knowledge).

Split knowledge: Condition in which two or more entities separately have key components that individually convey no knowledge of the resultant cryptographic key.

It is key for information security professionals to understand the differences between Dual Control and Separation of Duties. Both complement each other, but are not the same.

The following were incorrect answers:

Segregation of Duties address the splitting of various functions within a process to different users so that it will not create an opportunity for a single user to perform conflicting tasks.

For example, the participation of two or more persons in a transaction creates a system of checks and balances and reduces the possibility of fraud considerably. So it is important for an organization to ensure that all tasks within a process has adequate separation.

Let us look at some use cases of segregation of duties

A person handling cash should not post to the accounting records A loan officer should not disburse loan proceeds for loans they approved Those who have authority to sign cheques should not reconcile the bank accounts The credit card printing personal should not print the credit card PINs Customer address changes must be verified by a second employee before the change can be activated.

In situations where the separation of duties are not possible, because of lack of staff, the senior management should set up additional measure to offset the lack of adequate controls.

To summarise, Segregation of Duties is about Separating the conflicting duties to reduce fraud in an end to end function.

Need To Know (NTK):
The term "need to know", when used by government and other organizations (particularly those related to the military), describes the restriction of data which is considered very sensitive. Under need-to-know restrictions, even if one has all the necessary official approvals (such as a security clearance) to access certain information, one would not be given access to such information, unless one has a specific need to know; that is, access to the information must be necessary for the conduct of one's official duties. As with most security mechanisms, the aim is to make it difficult for unauthorized access to occur, without inconveniencing legitimate access. Need-to-know also aims to discourage "browsing" of sensitive material by limiting access to the smallest possible number of people.

EXAM TIP: HOW TO DECIPHER THIS QUESTION

First, you probably nototiced that both Separation of Duties and Segregation of Duties are synonymous with each others. This means they are not the BEST answers for sure. That was an easy first step.

For the exam remember:

Separation of Duties is synonymous with Segregation of Duties Dual Control is synonymous with Split Knowledge

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 16048-16078). Auerbach Publications. Kindle Edition.
http://www.ciso.in/dual-control-or-segregation-of-duties/