Correct Answer: B
Explanation:
The bottom-up approach to software testing begins with the testing of atomic units, such as programs and modules, and work upwards until a complete system testing has taken place. The advantages of using a bottom-up approach to software testing are the fact that there is no need for stubs or drivers and errors in critical modules are found earlier. The other choices refer to advantages of a top down approach which follows the opposite path.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 299).

QUESTION 409
Degaussing is used to clear data from all of the following medias except:

A. Floppy Disks
B. Read-Only Media
C. Video Tapes
D. Magnetic Hard Disks

Correct Answer: B
Explanation:
Atoms and Data
Shon Harris says: "A device that performs degaussing generates a coercive magnetic force that reduces the magnetic flux density of the storage media to zero. This magnetic force is what properly erases data from media. Data are stored on magnetic media by the representation of the polarization of the atoms. Degaussing changes"

The latest ISC2 book says:
"Degaussing can also be a form of media destruction. High-power degaussers are so strong in some cases that they can literally bend and warp the platters in a hard drive. Shredding and burning are effective destruction methods for non-rigid magnetic media. Indeed, some shredders are capable of shredding some rigid media such as an optical disk. This may be an effective alternative for any optical media containing nonsensitive information due to the residue size remaining after feeding the disk into the machine. However, the residue size might be too large for media containing sensitive information. Alternatively, grinding and pulverizing are acceptable choices for rigid and solid-state media. Specialized devices are available for grinding the face of optical media that either sufficiently scratches the surface to render the media unreadable or actually grinds off the data layer of the disk. Several services also exist which will collect drives, destroy them on site if requested and provide certification of completion. It will be the responsibility of the security professional to help, select, and maintain the most appropriate solutions for media cleansing and disposal."

Degaussing is achieved by passing the magnetic media through a powerful magnet field to rearrange the metallic particles, completely removing any resemblance of the previously recorded signal (from the "all about degaussers link below). Therefore, degaussing will work on any electronic based media such as floppy disks, or hard disks - all of these are examples of electronic storage. However, "read-only media" includes items such as paper printouts and CD-ROM wich do not store data in an electronic form or is not magnetic storage. Passing them through a magnet field has no effect on them.

Not all clearing/ purging methods are applicable to all media-- for example, optical media is not susceptible to degaussing, and overwriting may not be effective against Flash devices. The

degree to which information may be recoverable by a sufficiently motivated and capable adversary must not be underestimated or guessed at in ignorance. For the highest-value commercial data, and for all data regulated by government or military classification rules, read and follow the rules and standards.

I will admit that this is a bit of a trick question. Determining the difference between "read- only media" and "read-only memory" is difficult for the question taker. However, I believe it is representative of the type of question you might one day see on an exam.

The other answers are incorrect because:

Floppy Disks, Magnetic Tapes, and Magnetic Hard Disks are all examples of magnetic storage, and therefore are erased by degaussing.

A videotape is a recording of images and sounds on to magnetic tape as opposed to film stock used in filmmaking or random access digital media. Videotapes are also used for storing scientific or medical data, such as the data produced by an electrocardiogram. In most cases, a helical scan video head rotates against the moving tape to record the data in two dimensions, because video signals have a very high bandwidth, and static heads would require extremely high tape speeds. Videotape is used in both video tape recorders (VTRs) or, more commonly and more recently, videocassette recorder (VCR) and camcorders. A Tape use a linear method of storing information and since nearly all video recordings made nowadays are digital direct to disk recording (DDR), videotape is expected to gradually lose importance as non-linear/random-access methods of storing digital video data become more common.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 25627-25630). McGraw-Hill. Kindle Edition.
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition. Security Operations (Kindle Locations 580-588). . Kindle Edition.

All About Degaussers and Erasure of Magnetic Media:
http://www.degausser.co.uk/degauss/degabout.htm
http://www.degaussing.net/
http://www.cerberussystems.com/INFOSEC/stds/ncsctg25.htm

QUESTION 410
Which of the following is considered the weakest link in a security system?

A. People
B. Software
C. Communications
D. Hardware

Correct Answer: A
Explanation:
The Correct Answer: People. The other choices can be strengthened and counted on (For the most part) to remain consistent if properly protected. People are fallible and unpredictable. Most security intrusions are caused by employees. People get tired, careless, and greedy. They are not always reliable and may falter in following defined guidelines and best practices. Security professionals must install adequate prevention and detection controls and properly train all systems users Proper hiring and firing practices can eliminate certain risks. Security Awareness training is key to ensuring people are aware of risks and their responsibilities.

The following answers are incorrect:Software. Although software exploits are major threat and cause for concern, people are the weakest point in a security posture. Software can be removed, upgraded or patched to reduce risk.

Communications. Although many attacks from inside and outside an organization use communication methods such as the network infrastructure, this is not the weakest point in a security posture. Communications can be monitored, devices installed or upgraded to reduce risk and react to attack attempts.

Hardware. Hardware components can be a weakness in a security posture, but they are not the weakest link of the choices provided. Access to hardware can be minimized by such measures as installing locks and monitoring access in and out of certain areas.

The following reference(s) were/was used to create this question:

Shon Harris AIO v.3 P.19, 107-109
ISC2 OIG 2007, p.51-55

QUESTION 411
Why does compiled code pose more of a security risk than interpreted code?

A. Because malicious code can be embedded in compiled code and be difficult to detect.
B. If the executed compiled code fails, there is a chance it will fail insecurely.
C. Because compilers are not reliable.
D. There is no risk difference between interpreted code and compiled code.

Correct Answer: A
Explanation:
From a security standpoint, a compiled program is less desirable than an interpreted one because malicious code can be resident somewhere in the compiled code, and it is difficult to detect in a very large program.

QUESTION 412
At what stage of the applications development process should the security department become involved?

A. Prior to the implementation
B. Prior to systems testing
C. During unit testing
D. During requirements development

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

QUESTION 413
Configuration Management controls what?

A. Auditing of changes to the Trusted Computing Base.
B. Control of changes to the Trusted Computing Base.
C. Changes in the configuration access to the Trusted Computing Base.

D. Auditing and controlling any changes to the Trusted Computing Base.

Correct Answer: D
Explanation:
All of these are components of Configuration Management.

The following answers are incorrect:

Auditing of changes to the Trusted Computing Base. Is incorrect because it refers only to auditing the changes, but nothing about controlling them.
Control of changes to the Trusted Computing Base. Is incorrect because it refers only to controlling the changes, but nothing about ensuring the changes will not lead to a weakness or fault in the system.
Changes in the configuration access to the Trusted Computing Base. Is incorrect because this does not refer to controlling the changes or ensuring the changes will not lead to a weakness or fault in the system.

QUESTION 414
Which of the following describes a logical form of separation used by secure computing systems?

A. Processes use different levels of security for input and output devices.
B. Processes are constrained so that each cannot access objects outside its permitted domain.
C. Processes conceal data and computations to inhibit access by outside processes.
D. Processes are granted access based on granularity of controlled objects.

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

QUESTION 415
Which of the following security controls might force an operator into collusion with personnel assigned organizationally within a different function in order to gain access to unauthorized data?

A. Limiting the local access of operations personnel
B. Job rotation of operations personnel
C. Management monitoring of audit logs
D. Enforcing regular password changes

Correct Answer: A
Explanation:
The questions specifically said: "within a different function" which eliminate Job Rotation as a choice.

Management monitoring of audit logs is a detective control and it would not prevent collusion.
Changing passwords regularly would not prevent such attack.

This question validates if you understand the concept of separation of duties and least privilege. By having operators that have only the minimum access level they need and only what they need to do their duties within a company, the operations personnel would be force to use collusion to defeat those security mechanism.

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

QUESTION 416
Related to information security, availability is the opposite of which of the following?

A. delegation
B. distribution
C. documentation
D. destruction

Correct Answer: D
Explanation:
Availability is the opposite of "destruction."
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

QUESTION 417
Which of the following choices describe a condition when RAM and Secondary storage are used together?

A. Primary storage
B. Secondary storage
C. Virtual storage
D. Real storage

Correct Answer: C
Explanation:
Virtual storage a service provided by the operating system where it uses a combination of RAM and disk storage to simulate a much larger address space than is actually present. Infrequently used portions of memory are paged out by being written to secondary storage and paged back in when required by a running program.

Most OS's have the ability to simulate having more main memory than is physically available in the system. This is done by storing part of the data on secondary storage, such as a disk. This can be considered a virtual page. If the data requested by the system is not currently in main memory, a page fault is taken. This condition triggers the OS handler. If the virtual address is a valid one, the OS will locate the physical page, put the right information in that page, update the translation table, and then try the request again. Some other page might be swapped out to make room. Each process may have its own separate virtual address space along with its own mappings and protections.

The following are incorrect answers:
Primary storage is incorrect. Primary storage refers to the combination of RAM, cache and the processor registers. Primary Storage The data waits for processing by the processors, it sits in a staging area called primary storage. Whether implemented as memory, cache, or registers (part of the CPU), and regardless of its location, primary storage stores data that has a high probability of being requested by the CPU, so it is usually faster than long-term, secondary storage. The location where data is stored is denoted by its physical memory address. This memory register identifier remains constant and is independent of the value stored there. Some examples of primary storage devices include random-access memory (RAM), synchronous dynamic random-access memory (SDRAM), and read-only memory (ROM). RAM is volatile, that is, when the system shuts down, it flushes the data in RAM although recent research has shown that data may still be retrievable. Contrast this
Secondary storage is incorrect. Secondary storage holds data not currently being used by the CPU and is used when data must be stored for an extended period of time using high- capacity,