will be accomplished via username/password. But there is still nothing actually developed at this point to evaluate or accredit.

The "development & documentation phase" is where the system is created and documented. Part of the documentation includes specific evaluation and accreditation criteria. That is the criteria that will be used to evaluate and accredit the system during the "acceptance phase".

In other words - you cannot evaluate or accredit a system that has not been created yet. Of the four answers listed, only the acceptance phase is dealing with an existing system. The others deal with planning and creating the system, but the actual system isn't there yet.

Reference:
Official ISC2 Guide Page: 558 - 559
All in One Third Edition page: 832 - 833 (recommended reading)

QUESTION 264
Which of the following is less likely to be included in the change control sub-phase of the maintenance phase of a software product?

A. Estimating the cost of the changes requested
B. Recreating and analyzing the problem
C. Determining the interface that is presented to the user
D. Establishing the priorities of requests

Correct Answer: D
Explanation:
Change control sub-phase includes Recreating and analyzing the problem, Determining the interface that is presented to the user, and Establishing the priorities of requests.
Source: 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).

QUESTION 265
Which of the following should NOT be performed by an operator?

A. Implementing the initial program load
B. Monitoring execution of the system
C. Data entry
D. Controlling job flow

Correct Answer: C
Explanation:
Under the principle of separation of duties, an operator should not be performing data entry. This should be left to data entry personnel.

System operators represent a class of users typically found in data center environments where mainframe systems are used. They provide day-to-day operations of the mainframe environment, ensuring that scheduled jobs are running effectively and troubleshooting problems that may arise. They also act as the arms and legs of the mainframe environment, load and unloading tape and results of job print runs. Operators have elevated privileges, but less than those of system administrators. If misused, these privileges may be used to circumvent the system's security policy. As such, use of these privileges should be monitored through audit logs.

Some of the privileges and responsibilities assigned to operators include:

Implementing the initial program load: This is used to start the operating system. The boot process or initial program load of a system is a critical time for ensuring system security. Interruptions to this process may reduce the integrity of the system or cause the system to crash, precluding its availability.

Monitoring execution of the system: Operators respond to various events, to include errors, interruptions, and job completion messages.

Volume mounting: This allows the desired application access to the system and its data.

Controlling job flow: Operators can initiate, pause, or terminate programs. This may allow an operator to affect the scheduling of jobs. Controlling job flow involves the manipulation of configuration information needed by the system. Operators with the ability to control a job or application can cause output to be altered or diverted, which can threaten the confidentiality.

Bypass label processing: This allows the operator to bypass security label information to run foreign tapes (foreign tapes are those from a different data center that would not be using the same label format that the system could run). This privilege should be strictly controlled to prevent unauthorized access.

Renaming and relabeling resources: This is sometimes necessary in the mainframe environment to allow programs to properly execute. Use of this privilege should be monitored, as it can allow the unauthorized viewing of sensitive information.

Reassignment of ports and lines: Operators are allowed to reassign ports or lines. If misused, reassignment can cause program errors, such as sending sensitive output to an unsecured location. Furthermore, an incidental port may be opened, subjecting the system to an attack through the creation of a new entry point into the system.

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 19367-19395). Auerbach Publications. Kindle Edition.

QUESTION 266
Which of the following is not a responsibility of an information (data) owner?

A. Determine what level of classification the information requires.
B. Periodically review the classification assignments against business needs.
C. Delegate the responsibility of data protection to data custodians.
D. Running regular backups and periodically testing the validity of the backup data.

Correct Answer: D
Explanation:
This responsibility would be delegated to a data custodian rather than being performed directly by the information owner.

"Determine what level of classification the information requires" is incorrect. This is one of the major responsibilities of an information owner.

"Periodically review the classification assignments against business needs" is incorrect. This is one of the major responsibilities of an information owner.

"Delegates responsibility of maintenance of the data protection mechanisms to the data custodian" is incorrect. This is a responsibility of the information owner.

References:
CBK p. 105.
AIO3, p. 53-54, 960

QUESTION 267
Which of the following is an advantage of prototyping?

A. Prototype systems can provide significant time and cost savings.
B. Change control is often less complicated with prototype systems.
C. It ensures that functions or extras are not added to the intended system.
D. Strong internal controls are easier to implement.

Correct Answer: A
Explanation:
Prototype systems can provide significant time and cost savings, however they also have several disadvantages. They often have poor internal controls, change control becomes much more complicated and it often leads to functions or extras being added to the system that were not originally intended.

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 306).

QUESTION 268
Which of the following is not a component of a Operations Security "triples"?

A. Asset
B. Threat
C. Vulnerability
D. Risk

Correct Answer: D
Explanation:
The Operations Security domain is concerned with triples - threats, vulnerabilities and assets.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 216.

QUESTION 269
Which of the following BEST explains why computerized information systems frequently fail to meet the needs of users?

A. Inadequate quality assurance (QA) tools.
B. Constantly changing user needs.
C. Inadequate user participation in defining the system's requirements.
D. Inadequate project management.

Correct Answer: C
Explanation:
Inadequate user participation in defining the system's requirements. Most projects fail to meet the

needs of the users because there was inadequate input in the initial steps of the project from the user community and what their needs really are.

The other answers, while potentially valid, are incorrect because they do not represent the most common problem assosciated with information systems failing to meet the needs of users.

References:
All in One pg 834
Only users can define what their needs are and, therefore, what the system should accomplish. Lack of adequate user involvement, especially in the systems requirements phase, will usually result in a system that doesn't fully or adequately address the needs of the user.

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 296).

QUESTION 270
What can best be defined as the sum of protection mechanisms inside the computer, including hardware, firmware and software?

A. Trusted system
B. Security kernel
C. Trusted computing base
D. Security perimeter

Correct Answer: C
Explanation:
The Trusted Computing Base (TCB) is defined as the total combination of protection mechanisms within a computer system. The TCB includes hardware, software, and firmware. These are part of the TCB because the system is sure that these components will enforce the security policy and not violate it.

The security kernel is made up of hardware, software, and firmware components at fall within the TCB and implements and enforces the reference monitor concept.

Reference:
AIOv4 Security Models and Architecture pgs 268, 273

QUESTION 271
What can be defined as: It confirms that users' needs have been met by the supplied solution ?

A. Accreditation
B. Certification
C. Assurance
D. Acceptance

Correct Answer: D
Explanation:
Acceptance confirms that users' needs have been met by the supplied solution. Verification and Validation informs Acceptance by establishing the evidence ?set against acceptance criteria - to determine if the solution meets the users' needs. Acceptance should also explicitly address any integration or interoperability requirements involving other equipment or systems. To enable acceptance every user and system requirement must have a 'testable' characteristic.

Accreditation is the formal acceptance of security, adequacy, authorization for operation and acceptance of existing risk. Accreditation is the formal declaration by a Designated Approving Authority (DAA) that an IS is approved to operate in a particular security mode using a prescribed set of safeguards to an acceptable level of risk.

Certification is the formal testing of security safeguards and assurance is the degree of confidence that the implemented security measures work as intended. The certification is a Comprehensive evaluation of the technical and nontechnical security features of an IS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified ecurity requirements.

Assurance is the descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality. For example, an evaluation may require that all source code is kept in a change management system, or that full functional testing is performed. The Common Criteria provides a catalogue of these, and the requirements may vary from one evaluation to the next. The requirements for particular targets or types of products are documented in the Security Targets (ST) and Protection Profiles (PP), respectively.

Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 4, August 1999.
Official ISC2 Guide to the CISSP CBK, Second Edition, on page 211.
http://www.aof.mod.uk/aofcontent/tactical/randa/content/randaintroduction.htm

QUESTION 272
Who should DECIDE how a company should approach security and what security measures should be implemented?

A. Senior management
B. Data owner
C. Auditor
D. The information security specialist

Correct Answer: A
Explanation:
They are responsible for security of the organization and the protection of its assets.

The following answers are incorrect because :

Data owner is incorrect as data owners should not decide as to what security measures should be applied.

Auditor is also incorrect as auditor cannot decide as to what security measures should be applied.

The information security specialist is also incorrect as they may have the technical knowledge of how security measures should be implemented and configured , but they should not be in a position of deciding what measures should be applied.

Reference:
Shon Harris AIO v3 , Chapter-3: Security Management Practices , Page : 51.

QUESTION 273
A channel within a computer system or network that is designed for the authorized transfer of information is identified as a(n)?