C. System-High Security Mode
D. Dedicated Security Mode

Correct Answer: B
Explanation:
In multilevel mode, two or more classification levels of data exist, some people are not cleared for all the data on the system.
Risk is higher because sensitive data could be made available to someone not validated as being capable of maintaining secrecy of that data (i.e., not cleared for it).
In other security modes, all users have the necessary clearance for all data on the system.
Source: LaROSA, Jeanette (domain leader), Application and System Development Security CISSP Open Study Guide, version 3.0, January 2002.

QUESTION 299
Which of the following is the act of performing tests and evaluations to test a system's security level to see if it complies with the design specifications and security requirements?

A. Validation
B. Verification
C. Assessment
D. Accuracy

Correct Answer: B
Explanation:
Verification vs. Validation:
Verification determines if the product accurately represents and meets the specifications. A product can be developed that does not match the original specifications. This step ensures that the specifications are properly met.

Validation determines if the product provides the necessary solution intended real-world problem. In large projects, it is easy to lose sight of overall goal. This exercise ensures that the main goal of the project is met.

From DITSCAP:
6.3.2. Phase 2, Verification. The Verification phase shall include activities to verify compliance of the system with previously agreed security requirements. For each life-cycle development activity, DoD Directive 5000.1 (reference (i)), there is a corresponding set of security activities, enclosure 3, that shall verify compliance with the security requirements and evaluate vulnerabilities.

6.3.3. Phase 3, Validation. The Validation phase shall include activities to evaluate the fully integrated system to validate system operation in a specified computing environment with an acceptable level of residual risk. Validation shall culminate in an approval to operate.

You must also be familiar with Verification and Validation for the purpose of the exam. A simple definition for Verification would be whether or not the developers followed the design specifications along with the security requirements. A simple definition for Validation would be whether or not the final product meets the end user needs and can be use for a specific purpose.

Wikipedia has an informal description that is currently written as: Validation can be expressed by the query "Are you building the right thing?" and Verification by "Are you building it right?

NOTE:
DITSCAP was replaced by DIACAP some time ago (2007). While DITSCAP had defined both a verification and a validation phase, the DIACAP only has a validation phase. It may not make a

difference in the answer for the exam; however, DIACAP is the cornerstone policy of DOD C&A and IA efforts today. Be familiar with both terms just in case all of a sudden the exam becomes updated with the new term.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 1106). McGraw- Hill. Kindle Edition.
http://iase.disa.mil/ditscap/DITSCAP.html
https://en.wikipedia.org/wiki/Verification_and_validation
For the definition of "validation" in DIACAP, Click Here Further sources for the phases in DIACAP, Click Here.

QUESTION 300
What is the appropriate role of the security analyst in the application system development or acquisition project?

A. policeman
B. control evaluator & consultant
C. data owner
D. application user

Correct Answer: B
Explanation:
The correct answer is "control evaluator & consultant". During any system development or acquisition, the security staff should evaluate security controls and advise (or consult) on the strengths and weaknesses with those responsible for making the final decisions on the project.

The other answers are not correct because:

policeman - It is never a good idea for the security staff to be placed into this type of role (though it is sometimes unavoidable). During system development or acquisition, there should be no need of anyone filling the role of policeman.

data owner - In this case, the data owner would be the person asking for the new system to manage, control, and secure information they are responsible for. While it is possible the security staff could also be the data owner for such a project if they happen to have responsibility for the information, it is also possible someone else would fill this role. Therefore, the best answer remains "control evaluator & consultant".

application user - Again, it is possible this could be the security staff, but it could also be many other people or groups. So this is not the best answer.

Reference:
Official ISC2 Guide page: 555 - 560
All in One Third Edition page: 832 - 846

QUESTION 301
Which of the following can be defined as the process of rerunning a portion of the test scenario or test plan to ensure that changes or corrections have not introduced new errors?

A. Unit testing

B. Pilot testing
C. Regression testing
D. Parallel testing

Correct Answer: C
Explanation:
Regression testing is the process of rerunning a portion of the test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be the same as the data used in the original test. Unit testing refers to the testing of an individual program or module. Pilot testing is a preliminary test that focuses only on specific and predetermined aspects of a system. Parallel testing is the process of feeding test data into two systems and comparing the results.
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 300).

QUESTION 302
What is called the formal acceptance of the adequacy of a system's overall security by the management?

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

Correct Answer: C
Explanation:
Accreditation is the authorization by management to implement software or systems in a production environment. This authorization may be either provisional or full.

The following are incorrect answers:

Certification is incorrect. Certification is the process of evaluating the security stance of the software or system against a selected set of standards or policies. Certification is the technical evaluation of a product. This may precede accreditation but is not a required precursor.

Acceptance is incorrect. This term is sometimes used as the recognition that a piece of software or system has met a set of functional or service level criteria (the new payroll system has passed its acceptance test). Certification is the better tem in this context.

Evaluation is incorrect. Evaluation is certainly a part of the certification process but it is not the best answer to the question.

Reference(s) used for this question:
The Official Study Guide to the CBK from ISC2, pages 559-560

AIO3, pp. 314 - 317
AIOv4 Security Architecture and Design (pages 369 - 372) AIOv5 Security Architecture and Design (pages 370 - 372)
QUESTION 303
Which of the following determines that the product developed meets the projects goals?

A. verification
B. validation

C. concurrence
D. accuracy

Correct Answer: B
Explanation:
Software Development Verification vs. Validation:

Verification determines if the product accurately represents and meets the design specifications given to the developers. A product can be developed that does not match the original specifications. This step ensures that the specifications are properly met and closely followed by the development team.

Validation determines if the product provides the necessary solution intended real-world problem. It validates whether or not the final product is what the user expected in the first place and whether or not it solve the problem it intended to solve. In large projects, it is easy to lose sight of overall goal. This exercise ensures that the main goal of the project is met.

From DITSCAP:
6.3.2. Phase 2, Verification. The Verification phase shall include activities to verify compliance of the system with previously agreed security requirements. For each life-cycle development activity, DoD Directive 5000.1 (reference (i)), there is a corresponding set of security activities, enclosure 3, that shall verify compliance with the security requirements and evaluate vulnerabilities.

6.3.3. Phase 3, Validation. The Validation phase shall include activities to evaluate the fully integrated system to validate system operation in a specified computing environment with an acceptable level of residual risk. Validation shall culminate in an approval to operate.

NOTE:
DIACAP has replace DITSCAP but the definition above are still valid and applicable for the purpose of the exam.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 1106). McGraw- Hill. Kindle Edition.
http://iase.disa.mil/ditscap/DITSCAP.html

QUESTION 304
The major objective of system configuration management is which of the following?

A. system maintenance.
B. system stability.
C. system operations.
D. system tracking.

Correct Answer: B
Explanation:
A major objective with Configuration Management is stability. The changes to the system are controlled so that they don't lead to weaknesses or faults in th system.
The following answers are incorrect:

system maintenance. Is incorrect because it is not the best answer. Configuration Management does control the changes to the system but it is not as important as the overall stability of the system.

system operations. Is incorrect because it is not the best answer, the overall stability of the system is much more important.
system tracking. Is incorrect because while tracking changes is important, it is not the best answer. The overall stability of the system is much more important.

QUESTION 305
The security of a computer application is most effective and economical in which of the following cases?

A. The system is optimized prior to the addition of security.
B. The system is procured off-the-shelf.
C. The system is customized to meet the specific security threat.
D. The system is originally designed to provide the necessary security.

Correct Answer: D
Explanation:
The earlier in the process that security is planned for and implement the cheaper it is. It is also much more efficient if security is addressed in each phase of the development cycle rather than an add-on because it gets more complicated to add at the end. If security plan is developed at the beginning it ensures that security won't be overlooked.

The following answers are incorrect:

The system is optimized prior to the addition of security. Is incorrect because if you wait to implement security after a system is completed the cost of adding security increases dramtically and can become much more complex.
The system is procured off-the-shelf. Is incorrect because it is often difficult to add security to off-the shelf systems.
The system is customized to meet the specific security threat. Is incorrect because this is a distractor. This implies only a single threat.

QUESTION 306
Who is responsible for implementing user clearances in computer-based information systems at the B3 level of the TCSEC rating ?

A. Security administrators
B. Operators
C. Data owners
D. Data custodians

Correct Answer: A
Explanation:
Security administrator functions include user-oriented activities such as setting user clearances, setting initial password, setting other security characteristics for new users or changing security profiles for existing users. Data owners have the ultimate responsibility for protecting data, thus determining proper user access rights to data.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 307
Which of the following best corresponds to the type of memory addressing where the address location that is specified in the program instruction contains the address of the final desired location?