Correct Answer: A
Explanation:
If you are "retrofitting" that means you are adding to an existing database management system (DBMS). You could go back and redesign the entire DBMS but the cost of that could be expensive and there is no telling what the effect will be on existing applications, but that is redesigning and the question states retrofitting. The most cost effective way with the least effect on existing applications while adding a layer of security on top is through a trusted front-end.

Clark-Wilson is a synonym of that model as well. It was used to add more granular control or control to database that did not provide appropriate controls or no controls at all. It is one of the most popular model today. Any dynamic website with a back-end database is an example of this today.

Such a model would also introduce separation of duties by allowing the subject only specific rights on the objects they need to access.

The following answers are incorrect:

trusted back-end. Is incorrect because a trusted back-end would be the database management system (DBMS). Since the question stated "retrofitting" that eliminates this answer.
controller. Is incorrect because this is a distractor and has nothing to do with "retrofitting".
kernel. Is incorrect because this is a distractor and has nothing to do with "retrofitting". A security kernel would provide protection to devices and processes but would be inefficient in protecting rows or columns in a table.

QUESTION 255
The preliminary steps to security planning include all of the following EXCEPT which of the following?

A. Establish objectives.
B. List planning assumptions.
C. Establish a security audit function.
D. Determine alternate courses of action

Correct Answer: C
Explanation:
The keyword within the question is: preliminary

This means that you are starting your effort, you cannot audit if your infrastructure is not even in place.

Reference used for this question:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 256
What is defined as the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept?

A. The reference monitor
B. Protection rings
C. A security kernel
D. A protection domain

Correct Answer: C
Explanation:
A security kernel is defined as the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept. A reference monitor is a system component that enforces access controls on an object. A protection domain consists of the execution and memory space assigned to each process. The use of protection rings is a scheme that supports multiple protection domains.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 194).

QUESTION 257
External consistency ensures that the data stored in the database is:

A. in-consistent with the real world.
B. remains consistant when sent from one system to another.
C. consistent with the logical world.
D. consistent with the real world.

Correct Answer: D
Explanation:
External consistency ensures that the data stored in the database is consistent with the real world.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, page 33.

QUESTION 258
Which of the following does not address Database Management Systems (DBMS) Security?

A. Perturbation
B. Cell suppression
C. Padded cells
D. Partitioning

Correct Answer: C
Explanation:
Padded cells complement Intrusion Detection Systems (IDSs) and are not related to DBMS security. Padded cells are simulated environments to which IDSs seamlessly transfer detected attackers and are designed to convince an attacker that the attack is going according to the plan. Cell suppression is a technique used against inference attacks by not revealing information in the case where a statistical query produces a very small result set. Perturbation also addresses inference attacks but involves making minor modifications to the results to a query. Partitioning involves splitting a database into two or more physical or logical parts; especially relevant for multilevel secure databases.
Source: LaROSA, Jeanette (domain leader), Application and System Development Security CISSP Open Study Guide, version 3.0, January 2002.

QUESTION 259
Which of the following best describes the purpose of debugging programs?

A. To generate random data that can be used to test programs before implementing them.
B. To ensure that program coding flaws are detected and corrected.
C. To protect, during the programming phase, valid changes from being overwritten by other changes.
D. To compare source code versions before transferring to the test environment

Correct Answer: B
Explanation:
Debugging provides the basis for the programmer to correct the logic errors in a program under development before it goes into production.
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 298).

QUESTION 260
The Orange Book states that "Hardware and software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB [Trusted Computing Base]." This statement is the formal requirement for:

A. Security Testing.
B. Design Verification.
C. System Integrity.
D. System Architecture Specification.

Correct Answer: C
Explanation:
This is a requirement starting as low as C1 within the TCSEC rating.

The Orange book requires the following for System Integrity Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

NOTE FROM CLEMENT:
This is a question that confuses a lot of people because most people take for granted that the orange book with its associated Bell LaPadula model has nothing to do with integrity. However you have to be careful about the context in which the word integrity is being used. You can have Data Integrity and you can have System Integrity which are two completely different things.

Yes, the Orange Book does not specifically address the Integrity requirements, however it has to run on top of systems that must meet some integrity requirements.

This is part of what they call operational assurance which is defined as a level of confidence of a trusted system's architecture and implementation that enforces the system's security policy. It includes:

System architecture
Covert channel analysis
System integrity
Trusted recovery

DATA INTEGRITY

Data Integrity is very different from System Integrity. When you have integrity of the data, there are three goals:

1. Prevent authorized users from making unauthorized modifications
2. Preven unauthorized users from making modifications
3. Maintaining internal and external consistancy of the data

Bell LaPadula which is based on the Orange Book address does not address Integrity, it addresses only Confidentiality.
Biba address only the first goal of integrity.
Clark-Wilson addresses the three goals of integrity.

In the case of this question, there is a system integrity requirement within the TCB. As mentioned above here is an extract of the requirements: Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

The following answers are incorrect:

Security Testing. Is incorrect because Security Testing has no set of requirements in the Orange book.

Design Verification. Is incorrect because the Orange book's requirements for Design Verification include: A formal model of the security policy must be clearly identified and documented, including a mathematical proof that the model is consistent with its axioms and is sufficient to support the security policy.

System Architecture Specification. Is incorrect because there are no requirements for System Architecture Specification in the Orange book.

The following reference(s) were used for this question:

Trusted Computer Security Evaluation Criteria (TCSEC), DoD 5200.28-STD, page 15, 18, 25, 31, 40, 50.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Security Architecture and Design, Page 392-397, for users with the Kindle Version see Kindle Locations 28504-28505.
DOD TCSEC - http://www.cerberussystems.com/INFOSEC/stds/d520028.htm

QUESTION 261
Which of the following are the steps usually followed in the development of documents such as security policy, standards and procedures?

A. design, development, publication, coding, and testing.
B. design, evaluation, approval, publication, and implementation.
C. initiation, evaluation, development, approval, publication, implementation, and maintenance.
D. feasibility, development, approval, implementation, and integration.

Correct Answer: C
Explanation:
The common steps used the the development of security policy are initiation of the project, evaluation, development, approval, publication, implementation, and maintenance. The other choices listed are the phases of the software development life cycle and not the step used to develop ducuments such as Policies, Standards, etc...

Reference:
TIPTON, Harold F.& KRAUSE, MICKI, Information Security Management Handbook, 4th Edition,

Volume 3, 2002, Auerbach Publications.

QUESTION 262
Which of the following would be the best criterion to consider in determining the classification of an information asset?

A. Value
B. Age
C. Useful life
D. Personal association

Correct Answer: A
Explanation:
Information classification should be based on the value of the information to the organization and its sensitivity (reflection of how much damage would accrue due to disclosure).

Age is incorrect. While age might be a consideration in some cases, the guiding principles should be value and sensitivity.

Useful life. While useful lifetime is relevant to how long data protections should be applied, the classification is based on information value and sensitivity.

Personal association is incorrect. Information classification decisions should be based on value of the information and its sensitiviry.

References
CBK, pp. 101 - 102.

QUESTION 263
A security evaluation report and an accreditation statement are produced in which of the following phases of the system development life cycle?

A. project initiation and planning phase
B. system design specification phase
C. development & documentation phase
D. acceptance phase

Correct Answer: D
Explanation:
The Correct Answer: "acceptance phase". Note the question asks about an "evaluation report" - which details how the system evaluated, and an "accreditation statement" which describes the level the system is allowed to operate at. Because those two activities are a part of testing and testing is a part of the acceptance phase, the only answer above that can be correct is "acceptance phase".

The other answers are not correct because:

The "project initiation and planning phase" is just the idea phase. Nothing has been developed yet to be evaluated, tested, accredited, etc.

The "system design specification phase" is essentially where the initiation and planning phase is fleshed out. For example, in the initiation and planning phase, we might decide we want the system to have authentication. In the design specification phase, we decide that authentication