KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Database Security Issues (page 358).

QUESTION 325
Which of the following would provide the BEST stress testing environment taking under consideration and avoiding possible data exposure and leaks of sensitive data?

A. Test environment using test data.
B. Test environment using sanitized live workloads data.
C. Production environment using test data.
D. Production environment using sanitized live workloads data.

Correct Answer: B
Explanation:
The best way to properly verify an application or system during a stress test would be to expose it to "live" data that has been sanitized to avoid exposing any sensitive information or Personally Identifiable Data (PII) while in a testing environment. Fabricated test data may not be as varied, complex or computationally demanding as "live" data. A production environment should never be used to test a product, as a production environment is one where the application or system is being put to commercial or operational use. It is a best practice to perform testing in a non-production environment.
Stress testing is carried out to ensure a system can cope with production workloads, but as it may be tested to destruction, a test environment should always be used to avoid damaging the production environment. Hence, testing should never take place in a production environment. If only test data is used, there is no certainty that the system was adequately stress tested.

QUESTION 326
What can best be defined as high-level statements, beliefs, goals and objectives?

A. Standards
B. Policies
C. Guidelines
D. Procedures

Correct Answer: B
Explanation:
Policies are high-level statements, beliefs, goals and objectives and the general means for their attainment for a specific subject area. Standards are mandatory activities, action, rules or regulations designed to provide policies with the support structure and specific direction they require to be effective. Guidelines are more general statements of how to achieve the policies objectives by providing a framework within which to implement procedures. Procedures spell out the specific steps of how the policy and supporting standards and how guidelines will be implemented.
Source: HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.

QUESTION 327
Which expert system operating mode allows determining if a given hypothesis is valid?

A. Blackboard
B. Lateral chaining
C. Forward chaining
D. Backward chaining

Correct Answer: D
Explanation:
Backward-chaining mode - the expert system backtracks to determine if a given hypothesis is valid. Backward-chaining is generally used when there are a large number of possible solutions relative to the number of inputs.

Incorrect answers are:
In a forward-chaining mode, the expert system acquires information and comes to a conclusion based on that information. Forward-chaining is the reasoning approach that can be used when there is a small number of solutions relative to the number of inputs.

Blackboard is an expert system-reasoning methodology in which a solution is generated by the use of a virtual blackboard, wherein information or potential solutions are placed on the blackboard by a plurality of individuals or expert knowledge sources. As more information is placed on the blackboard in an iterative process, a solution is generated.

Lateral-chaining mode - No such expert system mode.

Sources:
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 259).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Expert Systems (page 354).

QUESTION 328
Risk reduction in a system development life-cycle should be applied:

A. Mostly to the initiation phase.
B. Mostly to the development phase.
C. Mostly to the disposal phase.
D. Equally to all phases.

Correct Answer: D
Explanation:
Risk is defined as the combination of the probability that a particular threat source will exploit, or trigger, a particular information system vulnerability and the resulting mission impact should this occur. Previously, risk avoidance was a common IT security goal. That changed as the nature of the risk became better understood. Today, it is recognized that elimination of all risk is not cost-effective. A cost-benefit analysis should be conducted for each proposed control. In some cases, the benefits of a more secure system may not justify the direct and indirect costs. Benefits include more than just prevention of monetary loss; for example, controls may be essential for maintaining public trust and confidence. Direct costs include the cost of purchasing and installing a given technology; indirect costs include decreased system performance and additional training. The goal is to enhance mission/business capabilities by managing mission/business risk to an acceptable level.
Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page 8).

QUESTION 329
Which of the following phases of a system development life-cycle is most concerned with

establishing a good security policy as the foundation for design?

A. Development/acquisition
B. Implementation
C. Initiation
D. Maintenance

Correct Answer: C
Explanation:
A security policy is an important document to develop while designing an information system. The security policy begins with the organization's basic commitment to information security formulated as a general policy statement.

The policy is then applied to all aspects of the system design or security solution. The policy identifies security goals (e.g., confidentiality, integrity, availability, accountability, and assurance) the system should support, and these goals guide the procedures, standards and controls used in the IT security architecture design.

The policy also should require definition of critical assets, the perceived threat, and security-related roles and responsibilities.

Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page 6).

QUESTION 330
A Security Kernel is defined as a strict implementation of a reference monitor mechanism responsible for enforcing a security policy. To be secure, the kernel must meet three basic conditions, what are they?

A. Confidentiality, Integrity, and Availability
B. Policy, mechanism, and assurance
C. Isolation, layering, and abstraction
D. Completeness, Isolation, and Verifiability

Correct Answer: D
Explanation:
A security kernel is responsible for enforcing a security policy. It is a strict implementation of a reference monitor mechanism. The architecture of a kernel operating system is typically layered, and the kernel should be at the lowest and most primitive level.

It is a small portion of the operating system through which all references to information and all changes to authorizations must pass. In theory, the kernel implements access control and information flow control between implemented objects according to the security policy.

To be secure, the kernel must meet three basic conditions:

completeness (all accesses to information must go through the kernel), isolation (the kernel itself must be protected from any type of unauthorized access), and verifiability (the kernel must be proven to meet design specifications).

The reference monitor, as noted previously, is an abstraction, but there may be a reference validator, which usually runs inside the security kernel and is responsible for performing security access checks on objects, manipulating privileges, and generating any resulting security audit

messages.

A term associated with security kernels and the reference monitor is the trusted computing base (TCB). The TCB is the portion of a computer system that contains all elements of the system responsible for supporting the security policy and the isolation of objects. The security capabilities of products for use in the TCB can be verified through various evaluation criteria, such as the earlier Trusted Computer System Evaluation Criteria (TCSEC) and the current Common Criteria standard.

Many of these security terms--reference monitor, security kernel, TCB--are defined loosely by vendors for purposes of marketing literature. Thus, it is necessary for security professionals to read the small print and between the lines to fully understand what the vendor is offering in regard to security features.

TIP FOR THE EXAM:
The terms Security Kernel and Reference monitor are synonymous but at different levels.
As it was explained by Diego:

While the Reference monitor is the concept, the Security kernel is the implementation of such concept (via hardware, software and firmware means).

The two terms are the same thing, but on different levels: one is conceptual, one is "technical"

The following are incorrect answers:
Confidentiality, Integrity, and Availability
Policy, mechanism, and assurance
Isolation, layering, and abstraction

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 13858-13875). Auerbach Publications. Kindle Edition.

QUESTION 331
Which of the following is used to interrupt the opportunity to use or perform collusion to subvert operation for fraudulent purposes?

A. Key escrow
B. Rotation of duties
C. Principle of need-to-know
D. Principle of least privilege

Correct Answer: B
Explanation:
Job rotations reduce the risk of collusion of activities between individuals. Companies with individuals working with sensitive information or systems where there might be the opportunity for personal gain through collusion can benefit by integrating job rotation with segregation of duties. Rotating the position may uncover activities that the individual is performing outside of the normal operating procedures, highlighting errors or fraudulent behavior.

Rotation of duties is a method of reducing the risk associated with a subject performing a (sensitive) task by limiting the amount of time the subject is assigned to perform the task before being moved to a different task.

The following are incorrect answers:

Key escrow is related to the protection of keys in storage by splitting the key in pieces that will be controlled by different departments. Key escrow is the process of ensuring a third party maintains a copy of a private key or key needed to decrypt information. Key escrow also should be considered mandatory for most organization's use of cryptography as encrypted information belongs to the organization and not the individual; however often an individual's key is used to encrypt the information.

Separation of duties is a basic control that prevents or detects errors and irregularities by assigning responsibility for different parts of critical tasks to separate individuals, thus limiting the effect a single person can have on a system. One individual should not have the capability to execute all of the steps of a particular process. This is especially important in critical business areas, where individuals may have greater access and capability to modify, delete, or add data to the system. Failure to separate duties could result in individuals embezzling money from the company without the involvement of others.

The need-to-know principle specifies that a person must not only be cleared to access classified or other sensitive information, but have requirement for such information to carry out assigned job duties. Ordinary or limited user accounts are what most users are assigned. They should be restricted only to those privileges that are strictly required, following the principle of least privilege. Access should be limited to specific objects following the principle of need-to-know.

The principle of least privilege requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. Least privilege refers to granting users only the accesses that are required to perform their job functions. Some employees will require greater access than others based upon their job functions. For example, an individual performing data entry on a mainframe system may have no need for Internet access or the ability to run reports regarding the information that they are entering into the system. Conversely, a supervisor may have the need to run reports, but should not be provided the capability to change information in the database.

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 10628-10631). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10635-10638). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10693-10697). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 16338-16341). Auerbach Publications. Kindle Edition.

QUESTION 332
Which of the following would be the MOST serious risk where a systems development life cycle methodology is inadequate?

A. The project will be completed late.
B. The project will exceed the cost estimates.