the vast majority of your security resides on a centrally managed server. In a decentralized (or distributed) environment, you have a collection of PC's each with their own operating systems to maintain, their own software to maintain, local data storage requiring protection and backup. You may also have PDA's and "smart phones", data watches, USB devices of all types able to store data... the list gets longer all the time.

It is entirely possible to reach a reasonable and acceptable level of security in a distributed environment. But doing so is significantly more difficult, requiring more effort, more money, and more time.

The other answers are not correct because:

scalability - A distributed computing environment is almost infinitely scalable. Much more so than a centralized environment. This is therefore a bad answer.

heterogeneity - Having products and systems from multiple vendors in a distributed environment is significantly easier than in a centralized environment. This would not be a "challenge of distributed computing solutions" and so is not a good answer.

usability - This is potentially a challenge in either environment, but whether or not this is a problem has very little to do with whether it is a centralized or distributed environment. Therefore, this would not be a good answer.

Reference:
Official ISC2 Guide page: 313-314
All in One Third Edition page: (unavailable at this time)

QUESTION 362
One purpose of a security awareness program is to modify:

A. employee's attitudes and behaviors towards enterprise's security posture
B. management's approach towards enterprise's security posture
C. attitudes of employees with sensitive data
D. corporate attitudes about safeguarding data

Correct Answer: A
Explanation:
The Correct Answer: security awareness training is to modify employees behaviour and attitude towards towards enterprise's security posture.

Security-awareness training is performed to modify employees' behavior and attitude toward security. This can best be achieved through a formalized process of security- awareness training.

It is used to increase the overall awareness of security throughout the company. It is targeted to every single employee and not only to one group of users.

Unfortunately you cannot apply a patch to a human being, the only thing you can do is to educate employees and make them more aware of security issues and threats. Never underestimate human stupidity.

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

also see:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 130). McGraw- Hill. Kindle Edition.

QUESTION 363
Making sure that only those who are supposed to access the data can access is which of the following?

A. confidentiality.
B. capability.
C. integrity.
D. availability.

Correct Answer: A
Explanation:
From the published (ISC)2 goals for the Certified Information Systems Security Professional candidate, domain definition. Confidentiality is making sure that only those who are supposed to access the data can access it.
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 364
Which of the following statements pertaining to software testing is incorrect?

A. Unit testing should be addressed and considered when the modules are being designed.
B. Test data should be part of the specifications.
C. Testing should be performed with live data to cover all possible situations.
D. Test data generators can be used to systematically generate random test data that can be used to test programs.

Correct Answer: C
Explanation:
Live or actual field data is not recommended for use in the testing procedures because both data types may not cover out of range situations and the correct outputs of the test are unknown. Live data would not be the best data to use because of the lack of anomalies and also because of the risk of exposure to your live data.

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 251).

QUESTION 365
The Reference Validation Mechanism that ensures the authorized access relationships between subjects and objects is implementing which of the following concept:

A. The reference monitor.
B. Discretionary Access Control.
C. The Security Kernel.
D. Mandatory Access Control.

Correct Answer: A
Explanation:
The reference monitor concept is an abstract machine that ensures that all subjects have the necessary access rights before accessing objects. Therefore, the kernel will mediates all

accesses to objects by subjects and will do so by validating through the reference monitor concept.
The kernel does not decide whether or not the access will be granted, it will be the Reference Monitor which is a subset of the kernel that will say YES or NO.

All access requests will be intercepted by the Kernel, validated through the reference monitor, and then access will either be denied or granted according to the request and the subject privileges within the system.

1. The reference monitor must be small enough to be full tested and valided
2. The Kernel must MEDIATE all access request from subjects to objects
3. The processes implementing the reference monitor must be protected
4. The reference monitor must be tamperproof

The following answers are incorrect:

The security kernel is the mechanism that actually enforces the rules of the reference monitor concept.

The other answers are distractors.

Shon Harris, All In One, 5th Edition, Security Architecture and Design, Page 330 also see http://en.wikipedia.org/wiki/Reference_monitor

QUESTION 366
Which of the following is best defined as an administrative declaration by a designated authority that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards?

A. Certification
B. Declaration
C. Audit
D. Accreditation

Correct Answer: D
Explanation:
Accreditation: is an administrative declaration by a designated authority that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards. It is usually based on a technical certification of the system's security mechanisms.

Certification: Technical evaluation (usually made in support of an accreditation action) of an information system\'s security features and other safeguards to establish the extent to which the system\'s design and implementation meet specified security requirements.

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 367
Ensuring least privilege does not require:

A. Identifying what the user's job is.
B. Ensuring that the user alone does not have sufficient rights to subvert an important process.
C. Determining the minimum set of privileges required for a user to perform their duties.
D. Restricting the user to required privileges and nothing more.

Correct Answer: B
Explanation:
Ensuring that the user alone does not have sufficient rights to subvert an important process is a concern of the separation of duties principle and it does not concern the least privilege principle.
Source: DUPUIS, Cl闈ent, Access Control Systems and Methodology CISSP Open Study Guide, version 1.0, march 2002 (page 33).

QUESTION 368
Which software development model is actually a meta-model that incorporates a number of the software development models?

A. The Waterfall model
B. The modified Waterfall model
C. The Spiral model
D. The Critical Path Model (CPM)

Correct Answer: C
Explanation:
The spiral model is actually a meta-model that incorporates a number of the software development models. This model depicts a spiral that incorporates the various phases of software development. The model states that each cycle of the spiral involves the same series of steps for each part of the project. CPM refers to the Critical Path Methodology.
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 246).

QUESTION 369
When considering an IT System Development Life-cycle, security should be:

A. Mostly considered during the initiation phase.
B. Mostly considered during the development phase.
C. Treated as an integral part of the overall system design.
D. Added once the design is completed.

Correct Answer: C
Explanation:
Security must be considered in information system design. Experience has shown it is very difficult to implement security measures properly and successfully after a system has been developed, so it should be integrated fully into the system life-cycle process. This includes establishing security policies, understanding the resulting security requirements, participating in the evaluation of security products, and finally in the engineering, design, implementation, and disposal of the system.

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 7).

QUESTION 370
Which of the following is best defined as a mode of system termination that automatically leaves system processes and components in a secure state when a failure occurs or is detected in a system?

A. Fail proof
B. Fail soft
C. Fail safe
D. Fail Over

Correct Answer: C
Explanation:
NOTE: This question is referring to a system which is Logical/Technical, so it is in the context of a system that you must choose the right answer. This is very important to read the question carefully and to identify the context whether it is in the Physical world or in the Technical/Logical world.

RFC 2828 (Internet Security Glossary) defines fail safe as a mode of system termination that automatically leaves system processes and components in a secure state when a failure occurs or is detected in the system.

A secure state means in the Logical/Technical world that no access would be granted or no packets would be allowed to flow through the system inspecting the packets such as a firewall for example.

If the question would have made reference to a building or something specific to the Physical world then the answer would have been different. In the Physical World everything becomes open and full access would be granted. See the valid choices below for the Physical context.

Fail-safe in the physical security world is when doors are unlocked automatically in case of emergency. Used in environment where humans work around. As human safety is prime concern during Fire or other hazards.

The following were all wrong choices:

Fail-secure in the physical security world is when doors are locked automatically in case of emergency. Can be in an area like Cash Locker Room provided there should be alternative manually operated exit door in case of emergency.

Fail soft is selective termination of affected non-essential system functions and processes when a failure occurs or is detected in the system.

Fail Over is a redundancy mechanism and does not apply to this question. There is a great post within the CCCure Forums on this specific QUESTION NO: :

saintrockz who is a long term contributor to the forums did outstanding research and you have the results below. The CCCure forum is a gold mine where thousands of QUESTION
NO: s related to the CBK have been discussed.

According to the Official ISC2 Study Guide (OIG):
Fault Tolerance is defined as built-in capability of a system to provide continued correct execution in the presence of a limited number of hardware or software faults. It means a system can operate in the presence of hardware component failures. A single component failure in a fault-tolerant system will not cause a system interruption because the alternate component will take