properly rolled out. The change control analyst needs to understand how various changes can affect security, interoperability, performance, and productivity. Or, a company can choose to just roll out the change and see what happens.
The following answers are incorrect:

Systems Administrator - A systems administrator (sysadmin/netadmin) configures network and server hardware and the operating systems to ensure that the information can be available and accessible. The administrator maintains the computing infrastructure using tools and utilities such as patch management and software distribution mechanisms to install updates and test patches on organization computers. The administrator tests and implements system upgrades to ensure the continued reliability of the servers and network devices. The administrator provides vulnerability management through either commercial off the shelf (COTS) and/or non-COTS solutions to test the computing environment and mitigate vulnerabilities appropriately.

End User - The end user is responsible for protecting information assets on a daily basis through adherence to the security policies that have been communicated.

Security Administrator - A security administrator manages the user access request process and ensures that privileges are provided to those individuals who have been authorized for access by application/system/data owners. This individual has elevated privileges and creates and deletes accounts and access permissions. The security administrator also terminates access privileges when individuals leave their jobs or transfer between company divisions. The security administrator maintains records of access request approvals and produces reports of access rights for the auditor during testing in an access controls audit to demonstrate compliance with the policies.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 109
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 108). McGraw- Hill. Kindle Edition.

QUESTION 357
What is called a system that is capable of detecting that a fault has occurred and has the ability to correct the fault or operate around it?

A. A fail safe system
B. A fail soft system
C. A fault-tolerant system
D. A failover system

Correct Answer: C
Explanation:
A fault-tolerant system is capable of detecting that a fault has occurred and has the ability to correct the fault or operate around it. In a fail-safe system, program execution is terminated, and the system is protected from being compromised when a hardware or software failure occurs and is detected. In a fail-soft system, when a hardware or software failure occurs and is detected, selected, non-critical processing is terminated. The term failover refers to switching to a duplicate "hot" backup component in real-time when a hardware or software failure occurs, enabling processing to continue.
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 196).

QUESTION 358
What can best be described as a domain of trust that shares a single security policy and single management?

A. The reference monitor
B. A security domain
C. The security kernel
D. The security perimeter

Correct Answer: B
Explanation:
A security domain is a domain of trust that shares a single security policy and single management.

The term security domain just builds upon the definition of domain by adding the fact that resources within this logical structure (domain) are working under the same security policy and managed by the same group.

So, a network administrator may put all of the accounting personnel, computers, and network resources in Domain 1 and all of the management personnel, computers, and network resources in Domain 2. These items fall into these individual containers because they not only carry out similar types of business functions, but also, and more importantly, have the same type of trust level. It is this common trust level that allows entities to be managed by one single security policy.

The different domains are separated by logical boundaries, such as firewalls with ACLs, directory services making access decisions, and objects that have their own ACLs indicating which individuals and groups can carry out operations on them.

All of these security mechanisms are examples of components that enforce the security policy for each domain. Domains can be architected in a hierarchical manner that dictates the relationship between the different domains and the ways in which subjects within the different domains can communicate. Subjects can access resources in domains of equal or lower trust levels.

The following are incorrect answers:

The reference monitor is an abstract machine which must mediate all access to subjects to objects, be protected from modification, be verifiable as correct, and is always invoked. Concept that defines a set of design requirements of a reference validation mechanism (security kernel), which enforces an access control policy over subjects' (processes, users) ability to perform operations (read, write, execute) on objects (files, resources) on a system. The reference monitor components must be small enough to test properly and be tamperproof.

The security kernel is the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept.

The security perimeter includes the security kernel as well as other security-related system functions that are within the boundary of the trusted computing base. System elements that are outside of the security perimeter need not be trusted. not every process and resource falls within the TCB, so some of these components fall outside of an imaginary boundary referred to as the security perimeter. A security perimeter is a boundary that divides the trusted from the untrusted. For the system to stay in a secure and trusted state, precise communication standards must be developed to ensure that when a component within the TCB needs to communicate with a

component outside the TCB, the communication cannot expose the system to unexpected security compromises. This type of communication is handled and controlled through interfaces.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 28548-28550). McGraw-Hill. Kindle Edition.

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 7873-7877). McGraw-Hill. Kindle Edition.

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition , Access Control, Page 214-217
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition. Security Architecture and Design (Kindle Locations 1280-1283). . Kindle Edition.

TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation. AIO 6th edition chapter 3 access control page 214-217 defines Security domains. Reference monitor, Security Kernel, and Security Parameter are defined in Chapter 4, Security Architecture and Design.

QUESTION 359
What can best be defined as the detailed examination and testing of the security features of an IT system or product to ensure that they work correctly and effectively and do not show any logical vulnerabilities, such as evaluation criteria?

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

Correct Answer: B
Explanation:
Evaluation as a general term is described as the process of independently assessing a system against a standard of comparison, such as evaluation criteria. Evaluation criterias are defined as a benchmark, standard, or yardstick against which accomplishment, conformance, performance, and suitability of an individual, hardware, software, product, or plan, as well as of risk-reward ratio is measured.

What is computer security evaluation?
Computer security evaluation is the detailed examination and testing of the security features of an IT system or product to ensure that they work correctly and effectively and do not show any logical vulnerabilities. The Security Target determines the scope of the evaluation. It includes a claimed level of Assurance that determines how rigorous the evaluation is.

Criteria
Criteria are the "standards" against which security evaluation is carried out. They define several degrees of rigour for the testing and the levels of assurance that each confers. They also define the formal requirements needed for a product (or system) to meet each Assurance level.

TCSEC
The US Department of Defense published the first criteria in 1983 as the Trusted Computer Security Evaluation Criteria (TCSEC), more popularly known as the "Orange Book". The current issue is dated 1985. The US Federal Criteria were drafted in the early 1990s as a possible replacement but were never formally adopted.

ITSEC
During the 1980s, the United Kingdom, Germany, France and the Netherlands produced versions of their own national criteria. These were harmonised and published as the Information Technology Security Evaluation Criteria (ITSEC). The current issue, Version 1.2, was published by the European Commission in June 1991. In September 1993, it was followed by the IT Security Evaluation Manual (ITSEM) which specifies the methodology to be followed when carrying out ITSEC evaluations.

Common Criteria
The Common Criteria represents the outcome of international efforts to align and develop the existing European and North American criteria. The Common Criteria project harmonises ITSEC, CTCPEC (Canadian Criteria) and US Federal Criteria (FC) into the Common Criteria for Information Technology Security Evaluation (CC) for use in evaluating products and systems and for stating security requirements in a standardised way. Increasingly it is replacing national and regional criteria with a worldwide set accepted by the International Standards Organisation (ISO15408).

The following answer were not applicable:

Certification is the process of performing a comprehensive analysis of the security features and safeguards of a system to establish the extent to which the security requirements are satisfied. Shon Harris states in her book that Certification is the comprehensive technical evaluation of the security components and their compliance for the purpose of accreditation.

Wikipedia describes it as: Certification is a comprehensive evaluation of the technical and non-technical security controls (safeguards) of an information system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements

Accreditation is the official management decision to operate a system. Accreditation is the formal declaration by a senior agency official (Designated Accrediting Authority (DAA) or Principal Accrediting Authority (PAA)) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural security controls (safeguards). Acceptance testing refers to user testing of a system before accepting delivery.

Reference(s) used for this question:

HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.
https://en.wikipedia.org/wiki/Certification_and_Accreditation
http://www.businessdictionary.com/definition/evaluation-criteria.html
http://www.cesg.gov.uk/products_services/iacs/cc_and_itsec/secevalcriteria.shtml

QUESTION 360
Which of the following describes a computer processing architecture in which a language compiler or pre-processor breaks program instructions down into basic operations that can be performed by the processor at the same time?

A. Very-Long Instruction-Word Processor (VLIW)
B. Complex-Instruction-Set-Computer (CISC)
C. Reduced-Instruction-Set-Computer (RISC)
D. Super Scalar Processor Architecture (SCPA)

Correct Answer: A
Explanation:
Very long instruction word (VLIW) describes a computer processing architecture in which a language compiler or pre-processor breaks program instruction down into basic operations that can be performed by the processor in parallel (that is, at the same time). These operations are put into a very long instruction word which the processor can then take apart without further analysis, handing each operation to an appropriate functional unit.

The following answer are incorrect:

The term "CISC" (complex instruction set computer or computing) refers to computers designed with a full set of computer instructions that were intended to provide needed capabilities in the most efficient way. Later, it was discovered that, by reducing the full set to only the most frequently used instructions, the computer would get more work done in a shorter amount of time for most applications. Intel's Pentium microprocessors are CISC microprocessors.

The PowerPC microprocessor, used in IBM's RISC System/6000 workstation and Macintosh computers, is a RISC microprocessor. RISC takes each of the longer, more complex instructions from a CISC design and reduces it to multiple instructions that are shorter and faster to process. RISC technology has been a staple of mobile devices for decades, but it is now finally poised to take on a serious role in data center servers and server virtualization. The latest RISC processors support virtualization and will change the way computing resources scale to meet workload demands.

A superscalar CPU architecture implements a form of parallelism called instruction level parallelism within a single processor. It therefore allows faster CPU throughput than would otherwise be possible at a given clock rate. A superscalar processor executes more than one instruction during a clock cycle by simultaneously dispatching multiple instructions to redundant functional units on the processor. Each functional unit is not a separate CPU core but an execution resource within a single CPU such as an arithmetic logic unit, a bit shifter, or a multiplier.

Reference(s) Used for this question:

http://whatis.techtarget.com/definition/0,,sid9_gci214395,00.html
http://searchcio-midmarket.techtarget.com/definition/CISC
http://en.wikipedia.org/wiki/Superscalar

QUESTION 361
Which of the following is often the greatest challenge of distributed computing solutions?

A. scalability
B. security
C. heterogeneity
D. usability

Correct Answer: B
Explanation:
The correct answer to this "security". It is a major factor in deciding if a centralized or decentralized environment is more appropriate.

Example:
In a centralized computing environment, you have a central server and workstations (often "dumb terminals") access applications, data, and everything else from that central servers. Therefore,