his or her opinion of a certain threat and turns it in to the team that is performing the analysis. The results are compiled and distributed to the group members, who then write down their comments anonymously and return them to the analysis group.

The comments are compiled and redistributed for more comments until a consensus is formed. This method is used to obtain an agreement on cost, loss values, and probabilities of occurrence without individuals having to agree verbally.

Here is the ISC2 book coverage of the subject:
One of the methods that uses consensus relative to valuation of information is the consensus/modified Delphi method. Participants in the valuation exercise are asked to comment anonymously on the task being discussed. This information is collected and disseminated to a participant other than the original author. This participant comments upon the observations of the original author. The information gathered is discussed in a public forum and the best course is agreed upon by the group (consensus).

EXAM TIP:
The DSS is what some of the books are referring to as the Delphi Method or Delphi Technique. Be familiar with both terms for the purpose of the exam.

The other answers are incorrect:

'DSS is aimed at solving highly structured problems' is incorrect because it is aimed at solving less structured problems.

'DSS supports only structured decision-making tasks' is also incorrect as it supports semi-structured decision-making tasks.

'DSS combines the use of models with non-traditional data access and retrieval functions' is also incorrect as it combines the use of models and analytic techniques with traditional data access and retrieval functions.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 91). McGraw-Hill.Kindle Edition.
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition. Information Security Governance and Risk Management ((ISC)2 Press) (Kindle Locations 1424-1426). Auerbach Publications. Kindle Edition.

QUESTION 381
Related to information security, integrity is the opposite of which of the following?

A. abstraction
B. alteration
C. accreditation
D. application

Correct Answer: B
Explanation:
Integrity is the opposite of "alteration."
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 382

Related to information security, the prevention of the intentional or unintentional unauthorized disclosure of contents is which of the following?

A. Confidentiality
B. Integrity
C. Availability
D. capability

Correct Answer: A
Explanation:
Confidentiality is the prevention of the intentional or unintentional unauthorized disclosure of contents.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 60.

QUESTION 383
When attempting to establish Liability, which of the following would be describe as performing the ongoing maintenance necessary to keep something in proper working order, updated, effective, or to abide by what is commonly expected in a situation?

A. Due care
B. Due concern
C. Due diligence
D. Due practice

Correct Answer: A
Explanation:
My friend JD Murray at Techexams.net has a nice definition of both, see his explanation below:

Oh, I hate these two. It's like describing the difference between "jealously" and "envy." Kinda the same thing but not exactly. Here it goes:

Due diligence is performing reasonable examination and research before committing to a course of action. Basically, "look before you leap." In law, you would perform due diligence by researching the terms of a contract before signing it. The opposite of due diligence might be "haphazard" or "not doing your homework."

Due care is performing the ongoing maintenance necessary to keep something in proper working order, or to abide by what is commonly expected in a situation. This is especially important if the due care situation exists because of a contract, regulation, or law. The opposite of due care is "negligence."

In summary, Due Diligence is Identifying threats and risks while Due Care is Acting upon findings to mitigate risks

EXAM TIP:
The Due Diligence refers to the steps taken to identify risks that exists within the environment. This is base on best practices, standards such as ISO 27001, ISO 17799, and other consensus. The first letter of the word Due and the word Diligence should remind you of this. The two letters are DD = Do Detect.

In the case of due care, it is the actions that you have taken (implementing, designing, enforcing, updating) to reduce the risks identified and keep them at an acceptable level. The same apply here, the first letters of the work Due and the work Care are DC. Which should remind you that

DC = Do correct.

The other answers are only detractors and not valid.

Reference(s) used for this question:
CISSP Study Guide, Syngress, By Eric Conrad, Page 419 HARRIS, Shon, All-In-One CISSP Certification Exam Guide Fifth Edition, McGraw-Hill, Page 49 and 110.
Corporate; (Isc)?(2010-04-20). Official (ISC)2 Guide to the CISSP CBK, Second Edition ((ISC)2 Press) (Kindle Locations 11494-11504). Taylor & Francis. Kindle Edition.
My friend JD Murray at Techexams.net

QUESTION 384
Which of the following is NOT an example of an operational control?

A. backup and recovery
B. Auditing
C. contingency planning
D. operations procedures

Correct Answer: B
Explanation:
Operational controls are controls over the hardware, the media used and the operators using these resources.
Operational controls are controls that are implemented and executed by people, they are most often procedures.
Backup and recovery, contingency planning and operations procedures are operational controls.
Auditing is considered an Administrative / detective control. However the actual auditing mechanisms in place on the systems would be consider operational controls.

QUESTION 385
What can be defined as an abstract machine that mediates all access to objects by subjects to ensure that subjects have the necessary access rights and to protect objects from unauthorized access?

A. The Reference Monitor
B. The Security Kernel
C. The Trusted Computing Base
D. The Security Domain

Correct Answer: A
Explanation:
The reference monitor refers to abstract machine that mediates all access to objects by subjects.

This question is asking for the concept that governs access by subjects to objects, thus the reference monitor is the best answer. While the security kernel is similar in nature, it is what actually enforces the concepts outlined in the reference monitor.

In operating systems architecture a reference monitor concept defines a set of design requirements on a reference validation mechanism, which enforces an access control policy over subjects' (e.g., processes and users) ability to perform operations (e.g., read and write) on objects (e.g., files and sockets) on a system. The properties of a reference monitor are:

The reference validation mechanism must always be invoked (complete mediation). Without this

property, it is possible for an attacker to bypass the mechanism and violate the security policy. The reference validation mechanism must be tamperproof (tamperproof). Without this property, an attacker can undermine the mechanism itself so that the security policy is not correctly enforced.
The reference validation mechanism must be small enough to be subject to analysis and tests, the completeness of which can be assured (verifiable). Without this property, the mechanism might be flawed in such a way that the policy is not enforced.

For example, Windows 3.x and 9x operating systems were not built with a reference monitor, whereas the Windows NT line, which also includes Windows 2000 and Windows XP, was designed to contain a reference monitor, although it is not clear that its properties (tamperproof, etc.) have ever been independently verified, or what level of computer security it was intended to provide.

The claim is that a reference validation mechanism that satisfies the reference monitor concept will correctly enforce a system's access control policy, as it must be invoked to mediate all security-sensitive operations, must not be tampered, and has undergone complete analysis and testing to verify correctness. The abstract model of a reference monitor has been widely applied to any type of system that needs to enforce access control, and is considered to express the necessary and sufficient properties for any system making this security claim.

According to Ross Anderson, the reference monitor concept was introduced by James Anderson in an influential 1972 paper.

Systems evaluated at B3 and above by the Trusted Computer System Evaluation Criteria (TCSEC) must enforce the reference monitor concept.

The reference monitor, as defined in AIO V5 (Harris) is: "an access control concept that refers to an abstract machine that mediates all access to objects by subjects."

The security kernel, as defined in AIO V5 (Harris) is: "the hardware, firmware, and software elements of a trusted computing based (TCB) that implement the reference monitor concept. The kernel must mediate all access between subjects and objects, be protected from modification, and be verifiable as correct."

The trusted computing based (TCB), as defined in AIO V5 (Harris) is: "all of the protection mechanisms within a computer system (software, hardware, and firmware) that are responsible for enforcing a security policy."

The security domain, "builds upon the definition of domain (a set of resources available to a subject) by adding the fact that resources withing this logical structure (domain) are working under the same security policy and managed by the same group."

The following answers are incorrect:

"The security kernel" is incorrect. One of the places a reference monitor could be implemented is in the security kernel but this is not the best answer.

"The trusted computing base" is incorrect. The reference monitor is an important concept in the TCB but this is not the best answer.

"The security domain is incorrect." The reference monitor is an important concept in the security domain but this is not the best answer.

Reference(s) used for this question:

Official ISC2 Guide to the CBK, page 324
AIO Version 3, pp. 272 - 274
AIOv4 Security Architecture and Design (pages 327 - 328) AIOv5 Security Architecture and Design (pages 330 - 331)
Wikipedia article at https://en.wikipedia.org/wiki/Reference_monitor

QUESTION 386
Which of the following phases of a software development life cycle normally incorporates the security specifications, determines access controls, and evaluates encryption options?

A. Detailed design
B. Implementation
C. Product design
D. Software plans and requirements

Correct Answer: C
Explanation:
The Product design phase deals with incorporating security specifications, adjusting test plans and data, determining access controls, design documentation, evaluating encryption options, and verification.

Implementation is incorrect because it deals with Installing security software, running the system, acceptance testing, security software testing, and complete documentation certification and accreditation (where necessary).

Detailed design is incorrect because it deals with information security policy, standards, legal issues, and the early validation of concepts. software plans and requirements is incorrect because it deals with addressesing threats, vulnerabilities, security requirements, reasonable care, due diligence, legal liabilities, cost/benefit analysis, level of protection desired, test plans.

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 252).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Security Life Cycle Components, Figure 7.5 (page 346).

QUESTION 387
An Architecture where there are more than two execution domains or privilege levels is called:

A. Ring Architecture.
B. Ring Layering
C. Network Environment.
D. Security Models

Correct Answer: A
Explanation:
In computer science, hierarchical protection domains, often called protection rings, are a mechanism to protect data and functionality from faults (fault tolerance) and malicious behavior (computer security). This approach is diametrically opposite to that of capability-based security.

Computer operating systems provide different levels of access to resources. A protection ring is one of two or more hierarchical levels or layers of privilege within the architecture of a computer