over the task transparently. As the cost of components continues to drop, and the demand for system availability increases, many non-fault-tolerant systems have redundancy built-in at the subsystem level. As a result, many non-fault-tolerant systems can tolerate hardware faults - consequently, the line between a fault-tolerant system and a non-fault-tolerant system becomes increasingly blurred.

According to Common Criteria:
Fail Secure - Failure with preservation of secure state, which requires that the TSF (TOE security functions) preserve a secure state in the face of the identified failures.

Acc. to The CISSP Prep Guide, Gold Ed.:
Fail over - When one system/application fails, operations will automatically switch to the backup system.
Fail safe - Pertaining to the automatic protection of programs and/or processing systems to maintain safety when a hardware or software failure is detected in a system. Fail secure - The system preserves a secure state during and after identified failures occur. Fail soft - Pertaining to the selective termination of affected non-essential processing when a hardware or software failure is detected in a system.

Acc. to CISSP for Dummies:
Fail closed - A control failure that results all accesses blocked. Fail open - A control failure that results in all accesses permitted. Failover - A failure mode where, if a hardware or software failure is detected, the system automatically transfers processing to a hot backup component, such as a clustered server. Fail-safe - A failure mode where, if a hardware or software failure is detected, program execution is terminated, and the system is protected from compromise. Fail-soft (or resilient) - A failure mode where, if a hardware or software failure is detected, certain, noncritical processing is terminated, and the computer or network continues to function in a degraded mode. Fault-tolerant - A system that continues to operate following failure of a computer or network component.

It's good to differentiate this concept in Physical Security as well:

Fail-safe
Door defaults to being unlocked
Dictated by fire codes

Fail-secure
Door defaults to being locked

Reference(s) used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 371
What would BEST define a covert channel?

A. An undocumented backdoor that has been left by a programmer in an operating system
B. An open system port that should be closed.
C. A communication channel that allows transfer of information in a manner that violates the system's security policy.
D. A trojan horse.

Correct Answer: C
Explanation:
The Correct Answer: A communication channel that allows transfer of information in a manner

that violates the system's security policy.
A covert channel is a way for an entity to receive information in an unauthorized manner. It is an information flow that is not controlled by a security mechanism. This type of information path was not developed for communication; thus, the system does not properly protect this path, because the developers never envisioned information being passed in this way.

Receiving information in this manner clearly violates the system's security policy. The channel to transfer this unauthorized data is the result of one of the following conditions:?Oversight in the development of the product

Improper implementation of access controls
Existence of a shared resource between the two entities
Installation of a Trojan horse

The following answers are incorrect:

An undocumented backdoor that has been left by a programmer in an operating system is incorrect because it is not a means by which unauthorized transfer of information takes place. Such backdoor is usually referred to as a Maintenance Hook.

An open system port that should be closed is incorrect as it does not define a covert channel.

A trojan horse is incorrect because it is a program that looks like a useful program but when you install it it would include a bonus such as a Worm, Backdoor, or some other malware without the installer knowing about it.

Reference(s) used for this question:
Shon Harris AIO v3 , Chapter-5 : Security Models & Architecture AIOv4 Security Architecture and Design (pages 343 - 344) AIOv5 Security Architecture and Design (pages 345 - 346)

QUESTION 372
The Information Technology Security Evaluation Criteria (ITSEC) was written to address which of the following that the Orange Book did not address?

A. integrity and confidentiality.
B. confidentiality and availability.
C. integrity and availability.
D. none of the above.

Correct Answer: C
Explanation:
TCSEC focused on confidentiality while ITSEC added integrity and availability as security goals.

The following answers are incorrect:

integrity and confidentiality. Is incorrect because TCSEC addressed confidentiality.
confidentiality and availability. Is incorrect because TCSEC addressed confidentiality.
none of the above. Is incorrect because ITSEC added integrity and availability as security goals.

QUESTION 373
Which of the following is not a form of passive attack?

A. Scavenging

B. Data diddling
C. Shoulder surfing
D. Sniffing

Correct Answer: B
Explanation:
Data diddling involves alteration of existing data and is extremely common. It is one of the easiest types of crimes to prevent by using access and accounting controls, supervision, auditing, separation of duties, and authorization limits. It is a form of active attack. All other choices are examples of passive attacks, only affecting confidentiality.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, Chapter 10: Law, Investigation, and Ethics (page 645).

QUESTION 374
Which of the following is NOT a proper component of Media Viability Controls?

A. Storage
B. Writing
C. Handling
D. Marking

Correct Answer: B
Explanation:
Media Viability Controls include marking, handling and storage.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 231.

QUESTION 375
Preservation of confidentiality within information systems requires that the information is not disclosed to:

A. Authorized person
B. Unauthorized persons or processes.
C. Unauthorized persons.
D. Authorized persons and processes

Correct Answer: B
Explanation:
Confidentiality assures that the information is not disclosed to unauthorized persons or processes.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 31.

QUESTION 376
Memory management in TCSEC levels B3 and A1 operating systems may utilize "data hiding". What does this mean?

A. System functions are layered, and none of the functions in a given layer can access data outside that layer.
B. Auditing processes and their memory addresses cannot be accessed by user processes.
C. Only security processes are allowed to write to ring zero memory.
D. It is a form of strong encryption cipher.

Correct Answer: A
Explanation:
Data Hiding is protecting data so that it is only available to higher levels this is done and is also performed by layering, when the software in each layer maintains its own global data and does not directly reference data outside its layers.

The following answers are incorrect:

Auditing processes and their memory addresses cannot be accessed by user processes. Is incorrect because this does not offer data hiding.
Only security processes are allowed to write to ring zero memory. This is incorrect, the security kernel would be responsible for this.
It is a form of strong encryption cipher. Is incorrect because this does not conform to the definition of data hiding.

QUESTION 377
Which of the following addresses a portion of the primary memory by specifying the actual address of the memory location?

A. direct addressing
B. Indirect addressing
C. implied addressing
D. indexed addressing

Correct Answer: A
Explanation:
Absolute/Direct

+------+-----+-------------------------------------+ | load | reg | address |
+------+-----+-------------------------------------+

(Effective address = address as given in instruction)

This requires space in an instruction for quite a large address. It is often available on CISC machines which have variable-length instructions, such as x86.

Some RISC machines have a special Load Upper Literal instruction which places a 16-bit constant in the top half of a register. An OR literal instruction can be used to insert a 16-bit constant in the lower half of that register, so that a full 32-bit address can then be used via the register-indirect addressing mode, which itself is provided as "base-plus-offset" with an offset of 0.
http://en.wikipedia.org/wiki/Addressing_mode (Very good coverage of the subject)

also see:
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, page 186.
also see:
http://www.comsci.us/ic/notes/am.html

QUESTION 378
Which of the following best defines add-on security?

A. Physical security complementing logical security measures.
B. Protection mechanisms implemented as an integral part of an information system.
C. Layer security.
D. Protection mechanisms implemented after an information system has become operational.

Correct Answer: D
Explanation:
The Internet Security Glossary (RFC2828) defines add-on security as "The retrofitting of protection mechanisms, implemented by hardware or software, after the [automatic data processing] system has become operational." Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 379
Which of the following choice is NOT normally part of the questions that would be asked in regards to an organization's information security policy?

A. Who is involved in establishing the security policy?
B. Where is the organization's security policy defined?
C. What are the actions that need to be performed in case of a disaster?
D. Who is responsible for monitoring compliance to the organization's security policy?

Correct Answer: C
Explanation:
Actions to be performed in case of a disaster are not normally part of an information security policy but part of a Disaster Recovery Plan (DRP).
Only personnel implicated in the plan should have a copy of the Disaster Recovery Plan whereas everyone should be aware of the contents of the organization's information security policy.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Appendix B, Practice-Level Policy Considerations (page 398).

QUESTION 380
Which of the following is a CHARACTERISTIC of a decision support system (DSS) in regards to Threats and Risks Analysis?

A. DSS is aimed at solving highly structured problems.
B. DSS emphasizes flexibility in the decision making approach of users.
C. DSS supports only structured decision-making tasks.
D. DSS combines the use of models with non-traditional data access and retrieval functions.

Correct Answer: B
Explanation:
DSS emphasizes flexibility in the decision-making approach of users. It is aimed at solving less structured problems, combines the use of models and analytic techniques with traditional data access and retrieval functions and supports semi-structured decision-making tasks.

DSS is sometimes referred to as the Delphi Method or Delphi Technique:
The Delphi technique is a group decision method used to ensure that each member gives an honest opinion of what he or she thinks the result of a particular threat will be. This avoids a group of individuals feeling pressured to go along with others' thought processes and enables them to participate in an independent and anonymous way. Each member of the group provides