QUESTION 288
What is RAD?

A. A development methodology
B. A project management technique
C. A measure of system complexity
D. Risk-assessment diagramming

Correct Answer: A
Explanation:
RAD stands for Rapid Application Development.

RAD is a methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality.

RAD is a programming system that enables programmers to quickly build working programs.

In general, RAD systems provide a number of tools to help build graphical user interfaces that would normally take a large development effort.

Two of the most popular RAD systems for Windows are Visual Basic and Delphi. Historically, RAD systems have tended to emphasize reducing development time, sometimes at the expense of generating in-efficient executable code. Nowadays, though, many RAD systems produce extremely faster code that is optimized.

Conversely, many traditional programming environments now come with a number of visual tools to aid development. Therefore, the line between RAD systems and other development environments has become blurred.

Reference:
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 307)
http://www.webopedia.com

QUESTION 289
Which of the following would be the best reason for separating the test and development environments?

A. To restrict access to systems under test.
B. To control the stability of the test environment.
C. To segregate user and development staff.
D. To secure access to systems under development.

Correct Answer: B
Explanation:
The test environment must be controlled and stable in order to ensure that development projects are tested in a realistic environment which, as far as possible, mirrors the live environment.

Reference(s) used for this question:
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 309).

QUESTION 290
Related to information security, the guarantee that the message sent is the message received with the assurance that the message was not intentionally or unintentionally altered is an example of which of the following?

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

Correct Answer: A
Explanation:
Integrity is the guarantee that the message sent is the message received, and that the message was not intentionally or unintentionally altered.
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 291
What is the main issue with media reuse?

A. Degaussing
B. Data remanence
C. Media destruction
D. Purging

Correct Answer: B
Explanation:
The main issue with media reuse is data remanence, where residual information still resides on a media that has been erased. Degaussing, purging and destruction are ways to handle media that contains data that is no longer needed or used.
Source: WALLHOFF, John, CBK#10 Physical Security (CISSP Study Guide), April 2002 (page 5).

QUESTION 292
As per the Orange Book, what are two types of system assurance?

A. Operational Assurance and Architectural Assurance.
B. Design Assurance and Implementation Assurance.
C. Architectural Assurance and Implementation Assurance.
D. Operational Assurance and Life-Cycle Assurance.

Correct Answer: D
Explanation:
Are the two types of assurance mentioned in the Orange book.

The following answers are incorrect:

Operational Assurance and Architectural Assurance. Is incorrect because Architectural Assurance is not a type of assurance mentioned in the Orange book.
Design Assurance and Implementation Assurance. Is incorrect because neither are types of assurance mentioned in the Orange book.
Architectural Assurance and Implementation Assurance. Is incorrect because neither are types of

assurance mentioned in the Orange book.

QUESTION 293
Which of the following exemplifies proper separation of duties?

A. Operators are not permitted modify the system time.
B. Programmers are permitted to use the system console.
C. Console operators are permitted to mount tapes and disks.
D. Tape operators are permitted to use the system console.

Correct Answer: A
Explanation:
This is an example of Separation of Duties because operators are prevented from modifying the system time which could lead to fraud. Tasks of this nature should be performed by they system administrators.

AIO defines Separation of Duties as a security principle that splits up a critical task among two or more individuals to ensure that one person cannot complete a risky task by himself.

The following answers are incorrect:

Programmers are permitted to use the system console. Is incorrect because programmers should not be permitted to use the system console, this task should be performed by operators. Allowing programmers access to the system console could allow fraud to occur so this is not an example of Separation of Duties..

Console operators are permitted to mount tapes and disks. Is incorrect because operators should be able to mount tapes and disks so this is not an example of Separation of Duties.

Tape operators are permitted to use the system console. Is incorrect because operators should be able to use the system console so this is not an example of Separation of Duties.

References:
OIG CBK Access Control (page 98 - 101)
AIOv3 Access Control (page 182)

QUESTION 294
Related to information security, confidentiality is the opposite of which of the following?

A. closure
B. disclosure
C. disposal
D. disaster

Correct Answer: B
Explanation:
Confidentiality is the opposite of disclosure.
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 295
Which of the following is NOT an administrative control?

A. Logical access control mechanisms
B. Screening of personnel
C. Development of policies, standards, procedures and guidelines
D. Change control procedures

Correct Answer: A
Explanation:
It is considered to be a technical control.

Logical is synonymous with Technical Control. That was the easy answer.

There are three broad categories of access control: Administrative, Technical, and Physical.

Each category has different access control mechanisms that can be carried out manually or automatically. All of these access control mechanisms should work in concert with each other to protect an infrastructure and its data.

Each category of access control has several components that fall within it, as shown here:

Administrative Controls

Policy and procedures
Personnel controls
Supervisory structure
Security-awareness training
Testing

Physical Controls

Network segregation
Perimeter security
Computer controls
Work area separation
Data backups

Technical Controls

System access
Network architecture
Network access
Encryption and protocols
Control zone
Auditing

The following answers are incorrect:

Screening of personnel is considered to be an administrative control
Development of policies, standards, procedures and guidelines is considered to be an administrative control
Change control procedures is considered to be an administrative control.

Reference:
Shon Harris AIO v3 , Chapter - 3: Security Management Practices , Page: 52-54

QUESTION 296
Which of the following computer design approaches is based on the fact that in earlier technologies, the instruction fetch was the longest part of the cycle?

A. Pipelining
B. Reduced Instruction Set Computers (RISC)
C. Complex Instruction Set Computers (CISC)
D. Scalar processors

Correct Answer: C
Explanation:
Complex Instruction Set Computer (CISC) uses instructions that perform many operations per instruction. It was based on the fact that in earlier technologies, the instruction fetch was the longest part of the cycle. Therefore, by packing more operations into an instruction, the number of fetches could be reduced. Pipelining involves overlapping the steps of different instructions to increase the performance in a computer. Reduced Instruction Set Computers (RISC) involve simpler instructions that require fewer clock cycles to execute. Scalar processors are processors that execute one instruction at a time.
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 Architectures and Models (page 188).

QUESTION 297
Buffer overflow and boundary condition errors are subsets of which of the following?

A. Race condition errors.
B. Access validation errors.
C. Exceptional condition handling errors.
D. Input validation errors.

Correct Answer: D
Explanation:
In an input validation error, the input received by a system is not properly checked, resulting in a vulnerability that can be exploited by sending a certain input sequence. There are two important types of input validation errors: buffer overflows (input received is longer than expected input length) and boundary condition error (where an input received causes the system to exceed an assumed boundary). A race condition occurs when there is a delay between the time when a system checks to see if an operation is allowed by the security model and the time when the system actually performs the operation. In an access validation error, the system is vulnerable because the access control mechanism is faulty. In an exceptional condition handling error, the system somehow becomes vulnerable due to an exceptional condition that has arisen.
Source: DUPUIS, Clement, Access Control Systems and Methodology CISSP Open Study Guide, version 1.0, march 2002 (page 105).

QUESTION 298
Which of the following security modes of operation involves the highest risk?

A. Compartmented Security Mode
B. Multilevel Security Mode