A. Direct addressing
B. Indirect addressing
C. Indexed addressing
D. Program addressing

**Correct Answer:** B
**Explanation:**
Indirect addressing is when the address location that is specified in the program instruction contains the address of the final desired location. Direct addressing is when a portion of primary memory is accessed by specifying the actual address of the memory location. Indexed addressing is when the contents of the address defined in the program's instruction is added to that of an index register. Program addressing is not a defined memory addressing mode.
Source: WALLHOFF, John, CBK#6 Security Architecture and Models (CISSP Study Guide), April 2002 (page 2).

**QUESTION 308**
Which of the following is NOT true concerning Application Control?

A. It limits end users use of applications in such a way that only particular screens are visible.
B. Only specific records can be requested through the application controls
C. Particular usage of the application can be recorded for audit purposes
D. It is non-transparent to the endpoint applications so changes are needed to the applications and databases involved

**Correct Answer:** D
**Explanation:**
Source: TIPTON, Harold F.& KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, Auerbach.

**QUESTION 309**
Making sure that the data is accessible when and where it is needed is which of the following?

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

**Correct Answer:** D
**Explanation:**
Availability is making sure that the data is accessible when and where it is needed.
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 310**
What does "System Integrity" mean?

A. The software of the system has been implemented as designed.
B. Users can't tamper with processes they do not own.
C. Hardware and firmware have undergone periodic testing to verify that they are functioning

properly.
D. Design specifications have been verified against the formal top-level specification.

**Correct Answer:** C
**Explanation:**
System Integrity means that all components of the system cannot be tampered with by unauthorized personnel and can be verified that they work properly.

The following answers are incorrect:

The software of the system has been implemented as designed. Is incorrect because this would fall under Trusted system distribution.

Users can't tamper with processes they do not own. Is incorrect because this would fall under Configuration Management.

Design specifications have been verified against the formal top-level specification. Is incorrect because this would fall under Specification and verification.

References:
AIOv3 Security Models and Architecture (pages 302 - 306) DOD TCSEC - http://www.cerberussystems.com/INFOSEC/stds/d520028.htm

**QUESTION 311**
What is it called when a computer uses more than one CPU in parallel to execute instructions?

A. Multiprocessing
B. Multitasking
C. Multithreading
D. Parallel running

**Correct Answer:** A
**Explanation:**
A system with multiple processors is called a multiprocessing system.

Multitasking is incorrect. Multitasking involves sharing the processor amoung all ready processes. Though it appears to the user that multiple processes are executing at the same time, only one process is running at any point in time.

Multithreading is incorrect. The developer can structure a program as a collection of independent threads to achieve better concurrency. For example, one thread of a program might be performing a calculation while another is waiting for additional input from the user.

"Parallel running" is incorrect. This is not a real term and is just a distraction.

References:
CBK, pp. 315-316
AIO3, pp. 234 - 239
**QUESTION 312**
The information security staff's participation in which of the following system development life cycle phases provides maximum benefit to the organization?

A. project initiation and planning phase
B. system design specifications phase

C. development and documentation phase
D. in parallel with every phase throughout the project

**Correct Answer:** D
**Explanation:**
The other answers are not correct because:

You are always looking for the "best" answer. While each of the answers listed here could be considered correct in that each of them require input from the security staff, the best answer is for that input to happen at all phases of the project.

Reference:
Official ISC2 Guide page: 556
All in One Third Edition page: 832 - 833

**QUESTION 313**
What is the goal of the Maintenance phase in a common development process of a security policy?

A. to review the document on the specified review date
B. publication within the organization
C. to write a proposal to management that states the objectives of the policy
D. to present the document to an approving body

**Correct Answer:** A
**Explanation:**
"publication within the organization" is the goal of the Publication Phase "write a proposal to management that states the objectives of the policy" is part of Initial and Evaluation Phase "Present the document to an approving body" is part of Approval Phase.

Reference:
TIPTON, Harold F.& KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 3, 2002, Auerbach Publications.

Also:
KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 286).

**QUESTION 314**
When backing up an applications system's data, which of the following is a key question to be answered first?

A. When to make backups
B. Where to keep backups
C. What records to backup
D. How to store backups

**Correct Answer:** C
**Explanation:**
It is critical that a determination be made of WHAT data is important and should be retained and protected. Without determining the data to be backed up, the potential for error increases. A record or file could be vital and yet not included in a backup routine. Alternatively, temporary or

insignificant files could be included in a backup routine unnecessarily.

The following answers were incorrect:

When to make backups Although it is important to consider schedules for backups, this is done after the decisions are made of what should be included in the backup routine.
Where to keep backups The location of storing backup copies of data (Such as tapes, on- line backups, etc) should be made after determining what should be included in the backup routine and the method to store the backup.
How to store backups The backup methodology should be considered after determining what data should be included in the backup routine.

**QUESTION 315**
Who can best decide what are the adequate technical security controls in a computer- based application system in regards to the protection of the data being used, the criticality of the data, and it's sensitivity level ?

A. System Auditor
B. Data or Information Owner
C. System Manager
D. Data or Information user

**Correct Answer:** B
**Explanation:**
The data or information owner also referred to as "Data Owner" would be the best person. That is the individual or officer who is ultimately responsible for the protection of the information and can therefore decide what are the adequate security controls according to the data sensitivity and data criticality. The auditor would be the best person to determine the adequacy of controls and whether or not they are working as expected by the owner.

The function of the auditor is to come around periodically and make sure you are doing what you are supposed to be doing. They ensure the correct controls are in place and are being maintained securely. The goal of the auditor is to make sure the organization complies with its own policies and the applicable laws and regulations.

Organizations can have internal auditors and/ or external auditors. The external auditors commonly work on behalf of a regulatory body to make sure compliance is being met. For example CobiT, which is a model that most information security auditors follow when evaluating a security program. While many security professionals fear and dread auditors, they can be valuable tools in ensuring the overall security of the organization. Their goal is to find the things you have missed and help you understand how to fix the problem.

The Official ISC2 Guide (OIG) says:
IT auditors determine whether users, owners, custodians, systems, and networks are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction, and other requirements placed on systems. The auditors provide independent assurance to the management on the appropriateness of the security controls. The auditor examines the information systems and determines whether they are designed, configured, implemented, operated, and managed in a way ensuring that the organizational objectives are being achieved. The auditors provide top company management with an independent view of the controls and their effectiveness.

Example:
Bob is the head of payroll. He is therefore the individual with primary responsibility over the

payroll database, and is therefore the information/data owner of the payroll database. In Bob's department, he has Sally and Richard working for him. Sally is responsible for making changes to the payroll database, for example if someone is hired or gets a raise. Richard is only responsible for printing paychecks. Given those roles, Sally requires both read and write access to the payroll database, but Richard requires only read access to it. Bob communicates these requirements to the system administrators (the "information/data custodians") and they set the file permissions for Sally's and Richard's user accounts so that Sally has read/write access, while Richard has only read access.

So in short Bob will determine what controls are required, what is the sensitivily and criticality of the Data. Bob will communicate this to the custodians who will implement the requirements on the systems/DB. The auditor would assess if the controls are in fact providing the level of security the Data Owner expects within the systems/DB. The auditor does not determine the sensitivity of the data or the crititicality of the data.

The other answers are not correct because:

A "system auditor" is never responsible for anything but auditing... not actually making control decisions but the auditor would be the best person to determine the adequacy of controls and then make recommendations.

A "system manager" is really just another name for a system administrator, which is actually an information custodian as explained above.

A "Data or information user" is responsible for implementing security controls on a day-to- day basis as they utilize the information, but not for determining what the controls should be or if they are adequate.

References:
Official ISC2 Guide to the CISSP CBK, Third Edition , Page 477 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 294-298). Auerbach Publications. Kindle Edition.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 3108-3114).

Information Security Glossary
Responsibility for use of information resources

**QUESTION 316**
Which of the following would best classify as a management control?

A. Review of security controls
B. Personnel security
C. Physical and environmental protection
D. Documentation

**Correct Answer:** A
**Explanation:**
Management controls focus on the management of the IT security system and the management of risk for a system.

They are techniques and concerns that are normally addressed by management. Routine evaluations and response to identified vulnerabilities are important elements of managing the risk