of a system, thus considered management controls.

SECURITY CONTROLS: The management, operational, and technical controls (i.e.,safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

SECURITY CONTROL BASELINE: The set of minimum security controls defined for a low-impact, moderate-impact,or high-impact information system.

The following are incorrect answers:
Personnel security, physical and environmental protection and documentation are forms of operational controls.

Reference(s) used for this question:

http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf and
FIPS PUB 200 at http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

QUESTION 317
A trusted system does NOT involve which of the following?

A. Enforcement of a security policy.
B. Sufficiency and effectiveness of mechanisms to be able to enforce a security policy.
C. Assurance that the security policy can be enforced in an efficient and reliable manner.
D. Independently-verifiable evidence that the security policy-enforcing mechanisms are sufficient and effective.

Correct Answer: C
Explanation:
A trusted system is one that meets its intended security requirements. It involves sufficiency and effectiveness, not necessarily efficiency, in enforcing a security policy. Put succinctly, trusted systems have (1) policy, (2) mechanism, and (3) assurance.
Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

QUESTION 318
Which of the following is not a method to protect objects and the data within the objects?

A. Layering
B. Data mining
C. Abstraction
D. Data hiding

Correct Answer: B
Explanation:
Data mining is used to reveal hidden relationships, patterns and trends by running queries on large data stores.

Data mining is the act of collecting and analyzing large quantities of information to determine patterns of use or behavior and use those patterns to form conclusions about past, current, or future behavior. Data mining is typically used by large organizations with large databases of customer or consumer behavior. Retail and credit companies will use data mining to identify buying patterns or trends in geographies, age groups, products, or services. Data mining is essentially the statistical analysis of general information in the absence of specific data.

The following are incorrect answers:

They are incorrect as they all apply to Protecting Objects and the data within them. Layering, abstraction and data hiding are related concepts that can work together to produce modular software that implements an organizations security policies and is more reliable in operation.

Layering is incorrect. Layering assigns specific functions to each layer and communication between layers is only possible through well-defined interfaces. This helps preclude tampering in violation of security policy. In computer programming, layering is the organization of programming into separate functional components that interact in some sequential and hierarchical way, with each layer usually having an interface only to the layer above it and the layer below it.

Abstraction is incorrect. Abstraction "hides" the particulars of how an object functions or stores information and requires the object to be manipulated through well-defined interfaces that can be designed to enforce security policy. Abstraction involves the removal of characteristics from an entity in order to easily represent its essential properties.

Data hiding is incorrect. Data hiding conceals the details of information storage and manipulation within an object by only exposing well defined interfaces to the information rather than the information itslef. For example, the details of how passwords are stored could be hidden inside a password object with exposed interfaces such as check_password, set_password, etc. When a password needs to be verified, the test password is passed to the check_password method and a boolean (true/false) result is returned to indicate if the password is correct without revealing any details of how/where the real passwords are stored. Data hiding maintains activities at different security levels to separate these levels from each other.

The following reference(s) were used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 27535-27540). Auerbach Publications. Kindle Edition.
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 4269-4273). Auerbach Publications. Kindle Edition.

QUESTION 319
An effective information security policy should not have which of the following characteristic?

A. Include separation of duties
B. Be designed with a short- to mid-term focus
C. Be understandable and supported by all stakeholders
D. Specify areas of responsibility and authority

Correct Answer: B
Explanation:
An effective information security policy should be designed with a long-term focus. All other characteristics apply.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Appendix B, Practice-Level Policy Considerations (page 397).

QUESTION 320
What mechanism does a system use to compare the security labels of a subject and an object?

A. Validation Module.
B. Reference Monitor.
C. Clearance Check.
D. Security Module.

Correct Answer: B
Explanation:
Because the Reference Monitor is responsible for access control to the objects by the subjects it compares the security labels of a subject and an object.

According to the OIG: The reference monitor is an access control concept referring to an abstract machine that mediates all accesses to objects by subjects based on information in an access control database. The reference monitor must mediate all access, be protected from modification, be verifiable as correct, and must always be invoked. The reference monitor, in accordance with the security policy, controls the checks that are made in the access control database.

The following are incorrect:

Validation Module. A Validation Module is typically found in application source code and is used to validate data being inputted.
Clearance Check. Is a distractor, there is no such thing other than what someone would do when checking if someone is authorized to access a secure facility.
Security Module. Is typically a general purpose module that prerforms a variety of security related functions.

References:
OIG CBK, Security Architecture and Design (page 324) AIO, 4th Edition, Security Architecture and Design, pp 328-328. Wikipedia - http://en.wikipedia.org/wiki/Reference_monitor

QUESTION 321
What are the three FUNDAMENTAL principles of security?

A. Accountability, confidentiality and integrity
B. Confidentiality, integrity and availability
C. Integrity, availability and accountability
D. Availability, accountability and confidentiality

Correct Answer: B
Explanation:
The following answers are incorrect because:

Accountability, confidentiality and integrity is not the correct answer as Accountability is not one of the fundamental principle of security.
Integrity, availability and accountability is not the correct answer as Accountability is not one of the fundamental principle of security.
Availability, accountability and confidentiality is not the correct answer as Accountability is not one of the fundamental objective of security.

References:
Shon Harris AIO v3 , Chapter - 3: Security Management Practices , Pages: 49-52

QUESTION 322
Which of the following test makes sure the modified or new system includes appropriate access

controls and does not introduce any security holes that might compromise other systems?

A. Recovery testing
B. Security testing
C. Stress/volume testing
D. Interface testing

Correct Answer: B
Explanation:
Security testing makes sure the modified or new system includes appropriate access controls and does not introduce any security holes that might compromise other systems.

Recovery testing checks the system's ability to recover after a software or hardware failure.

Stress/volume testing involves testing an application with large quantities of data in order to evaluate performance during peak hours.
Interface testing evaluates the connection of two or more components that pass information from one area to another.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 300).

QUESTION 323
Which of the following is NOT a technical control?

A. Password and resource management
B. Identification and authentication methods
C. Monitoring for physical intrusion
D. Intrusion Detection Systems

Correct Answer: C
Explanation:
It is considered to be a 'Physical Control'

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, a partial list is shown here. Not all controls fall into a single category, many of the controls will be in two or more categories. Below you have an example with backups where it is in all three categories:

Administrative Controls
Policy and procedures
A backup policy would be in place

Personnel controls
Supervisory structure
Security-awareness training
Testing
Physical Controls

Network segregation
Perimeter security
Computer controls
Work area separation

Data backups (actual storage of the media, i:e Offsite Storage Facility)

Cabling
Technical Controls
System access
Network architecture
Network access
Encryption and protocols
Control zone
Auditing
Backup (Actual software doing the backups)

The following answers are incorrect :

Password and resource management is considered to be a logical or technical control.

Identification and authentication methods is considered to be a logical or technical control.

Intrusion Detection Systems is considered to be a logical or technical control.

Reference:
Shon Harris , AIO v3 , Chapter - 4 : Access Control , Page: 180 - 185

QUESTION 324
What is the act of obtaining information of a higher sensitivity by combining information from lower levels of sensitivity?

A. Polyinstantiation
B. Inference
C. Aggregation
D. Data mining

Correct Answer: C
Explanation:
Aggregation is the act of obtaining information of a higher sensitivity by combining information from lower levels of sensitivity.

The incorrect answers are:

Polyinstantiation is the development of a detailed version of an object from another object using different values in the new object.
Inference is the ability of users to infer or deduce information about data at sensitivity levels for which they do not have access privilege.
Data mining refers to searching through a data warehouse for data correlations.

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 261).