upgrades, and guarding against malicious actions such as denial-of- service (DoS) attacks.

Reference used for this question:

http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
http://www.danielmiessler.com/blog/security-identification-authentication-and-authorization
http://www.merriam-webster.com/dictionary/profess

KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

QUESTION 107
What is the PRIMARY use of a password?

A. Allow access to files.
B. Identify the user.
C. Authenticate the user.
D. Segregate various user's accesses.

Correct Answer: C
Explanation:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 108
Which access control model achieves data integrity through well-formed transactions and separation of duties?

A. Clark-Wilson model
B. Biba model
C. Non-interference model
D. Sutherland model

Correct Answer: A
Explanation:
The Clark-Wilson model differs from other models that are subject- and object- oriented by introducing a third access element programs resulting in what is called an access triple, which prevents unauthorized users from modifying data or programs. The Biba model uses objects and subjects and addresses integrity based on a hierarchical lattice of integrity levels. The non-interference model is related to the information flow model with restrictions on the information flow. The Sutherland model approaches integrity by focusing on the problem of inference.

Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 2: Access Control Systems and Methodology (page 12).
And: KRAUSE, Micki & TIPTON, Harold F., Handbook of Information Security Management, CRC Press, 1997, Domain 1: Access Control.

QUESTION 109
Which access model is most appropriate for companies with a high employee turnover?

A. Role-based access control
B. Mandatory access control
C. Lattice-based access control

D. Discretionary access control

Correct Answer: A
Explanation:
The underlying problem for a company with a lot of turnover is assuring that new employees are assigned the correct access permissions and that those permissions are removed when they leave the company.

Selecting the best answer requires one to think about the access control options in the context of a company with a lot of flux in the employee population. RBAC simplifies the task of assigning permissions because the permissions are assigned to roles which do not change based on who belongs to them. As employees join the company, it is simply a matter of assigning them to the appropriate roles and their permissions derive from their assigned role. They will implicitely inherit the permissions of the role or roles they have been assigned to. When they leave the company or change jobs, their role assignment is revoked/changed appropriately.

Mandatory access control is incorrect. While controlling access based on the clearence level of employees and the sensitivity of obects is a better choice than some of the other incorrect answers, it is not the best choice when RBAC is an option and you are looking for the best solution for a high number of employees constantly leaving or joining the company.

Lattice-based access control is incorrect. The lattice is really a mathematical concept that is used in formally modeling information flow (Bell-Lapadula, Biba, etc). In the context of the question, an abstract model of information flow is not an appropriate choice. CBK, pp. 324-325.

Discretionary access control is incorrect. When an employee joins or leaves the company, the object owner must grant or revoke access for that employee on all the objects they own. Problems would also arise when the owner of an object leaves the company. The complexity of assuring that the permissions are added and removed correctly makes this the least desirable solution in this situation.

References
Alll in One, third edition page 165
RBAC is discussed on pp. 189 through 191 of the ISC(2) guide.

QUESTION 110
Which of the following control pairings include: organizational policies and procedures, pre-employment background checks, strict hiring practices, employment agreements, employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks?

A. Preventive/Administrative Pairing
B. Preventive/Technical Pairing
C. Preventive/Physical Pairing
D. Detective/Administrative Pairing

Correct Answer: A
Explanation:
The Correct Answer: Preventive/Administrative Pairing: These mechanisms include organizational policies and procedures, pre-employment background checks, strict hiring practices, employment agreements, friendly and unfriendly employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems

and networks.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

QUESTION 111
In regards to information classification what is the main responsibility of information (data) owner?

A. determining the data sensitivity or classification level
B. running regular data backups
C. audit the data users
D. periodically check the validity and accuracy of the data

Correct Answer: A
Explanation:
Making the determination to decide what level of classification the information requires is the main responsibility of the data owner.

The data owner within classification is a person from Management who has been entrusted with a data set that belong to the company. It could be for example the Chief Financial Officer (CFO) who has been entrusted with all financial date or it could be the Human Resource Director who has been entrusted with all Human Resource data. The information owner will decide what classification will be applied to the data based on Confidentiality, Integrity, Availability, Criticality, and Sensitivity of the data.

The Custodian is the technical person who will implement the proper classification on objects in accordance with the Data Owner. The custodian DOES NOT decide what classification to apply, it is the Data Owner who will dictate to the Custodian what is the classification to apply.

NOTE:
The term Data Owner is also used within Discretionary Access Control (DAC). Within DAC it means the person who has created an object. For example, if I create a file on my system then I am the owner of the file and I can decide who else could get access to the file. It is left to my discretion. Within DAC access is granted based solely on the Identity of the subject, this is why sometimes DAC is referred to as Identity Based Access Control.

The other choices were not the best answer

Running regular backups is the responsibility of custodian. Audit the data users is the responsibility of the auditors Periodically check the validity and accuracy of the data is not one of the data owner responsibility

Reference(s) used for this question:
KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 14, Chapter 1: Security Management Practices.

QUESTION 112
Which of the following are additional access control objectives?

A. Consistency and utility
B. Reliability and utility
C. Usefulness and utility
D. Convenience and utility

Correct Answer: B
Explanation:
Availability assures that a system's authorized users have timely and uninterrupted access to the information in the system. The additional access control objectives are reliability and utility. These and other related objectives flow from the organizational security policy. This policy is a high-level statement of management intent regarding the control of access to information and the personnel who are authorized to receive that information. Three things that must be considered for the planning and implementation of access control mechanisms are the threats to the system, the system's vulnerability to these threats, and the risk that the threat may materialize.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 32.

QUESTION 113
Which of the following models does NOT include data integrity or conflict of interest?

A. Biba
B. Clark-Wilson
C. Bell-LaPadula
D. Brewer-Nash

Correct Answer: C
Explanation:
Bell LaPadula model (Bell 1975): The granularity of objects and subjects is not predefined, but the model prescribes simple access rights. Based on simple access restrictions the Bell LaPadula model enforces a discretionary access control policy enhanced with mandatory rules. Applications with rigid confidentiality requirements and without strong integrity requirements may properly be modeled.

These simple rights combined with the mandatory rules of the policy considerably restrict the spectrum of applications which can be appropriately modeled.

Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

Also check:
Proceedings of the IFIP TC11 12th International Conference on Information Security, Samos (Greece), May 1996, On Security Models.

QUESTION 114
Which of the following best ensures accountability of users for the actions taken within a system or domain?

A. Identification
B. Authentication
C. Authorization
D. Credentials

Correct Answer: B
Explanation:
Details:
The only way to ensure accountability is if the subject is uniquely identified and authenticated. Identification alone does not provide proof the user is who they claim to be. After showing proper credentials, a user is authorized access to resources.

References:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 4: Access Control (page 126).

QUESTION 115
Access Control techniques do not include which of the following?

A. Rule-Based Access Controls
B. Role-Based Access Control
C. Mandatory Access Control
D. Random Number Based Access Control

Correct Answer: D
Explanation:
Access Control Techniques
Discretionary Access Control
Mandatory Access Control
Lattice Based Access Control
Rule-Based Access Control
Role-Based Access Control
Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 13.

QUESTION 116
Which of the following was developed by the National Computer Security Center (NCSC) for the US Department of Defense ?

A. TCSEC
B. ITSEC
C. DIACAP
D. NIACAP

Correct Answer: A
Explanation:
The Correct Answer: TCSEC; The TCSEC, frequently referred to as the Orange Book, is the centerpiece of the DoD Rainbow Series publications.

Initially issued by the National Computer Security Center (NCSC) an arm of the National Security Agency in 1983 and then updated in 1985, TCSEC was replaced with the development of the Common Criteria international standard originally published in 2005.

References:
KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, pages 197-199.

Wikepedia
http://en.wikipedia.org/wiki/TCSEC

QUESTION 117
Which of the following access control models requires security clearance for subjects?