ISC2

Exam Questions SSCP

System Security Certified Practitioner (SSCP)

NEW QUESTION 1
- (Topic 1)
Which type of password token involves time synchronization?

A. Static password tokens
B. Synchronous dynamic password tokens
C. Asynchronous dynamic password tokens
D. Challenge-response tokens

Answer: B

Explanation:
 Synchronous dynamic password tokens generate a new unique password value at fixed time intervals, so the server and token need to be synchronized for the password to be accepted.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 37).
Also check out: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, chapter 4: Access Control (page 136).

NEW QUESTION 2
- (Topic 1)
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

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.

NEW QUESTION 3
- (Topic 1)
Detective/Technical measures:

A. include intrusion detection systems and automatically-generated violation reports from audit trail information.
B. do not include intrusion detection systems and automatically-generated violation reports from audit trail information.
C. include intrusion detection systems but do not include automatically-generated violation reports from audit trail information.
D. include intrusion detection systems and customised-generated violation reports from audit trail information.

Answer: A

Explanation:
 Detective/Technical measures include intrusion detection systems and automatically-generated violation reports from audit trail information. These reports can indicate variations from "normal" operation or detect known signatures of unauthorized access episodes. In order to limit the amount of audit information flagged and reported by automated violation analysis and reporting mechanisms, clipping levels can be set. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.

NEW QUESTION 4
- (Topic 1)
What is the main concern with single sign-on?

A. Maximum unauthorized access would be possible if a password is disclosed.
B. The security administrator's workload would increase.
C. The users' password would be too hard to remember.
D. User access rights would be increased.

Answer: A

Explanation:
 A major concern with Single Sign-On (SSO) is that if a user's ID and password are compromised, the intruder would have access to all the systems that the user was authorized for.
The following answers are incorrect:
The security administrator's workload would increase. Is incorrect because the security administrator's workload would decrease and not increase. The admin would not be responsible for maintaining multiple user accounts just the one.
The users' password would be too hard to remember. Is incorrect because the users would have less passwords to remember.
User access rights would be increased. Is incorrect because the user access rights would not be any different than if they had to log into systems manually.

NEW QUESTION 5
- (Topic 1)

Which of the following biometric characteristics cannot be used to uniquely authenticate an individual's identity?

A. Retina scans
B. Iris scans
C. Palm scans
D. Skin scans

Answer: D

Explanation:
The following are typical biometric characteristics that are used to uniquely authenticate an individual's identity:
Fingerprints Retina scans Iris scans Facial scans Palm scans Hand geometry Voice
Handwritten signature dynamics
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 39.
And: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 127-131).

NEW QUESTION 6
- (Topic 1)
To control access by a subject (an active entity such as individual or process) to an object (a passive entity such as a file) involves setting up:

A. Access Rules
B. Access Matrix
C. Identification controls
D. Access terminal

Answer: A

Explanation:
Controlling access by a subject (an active entity such as individual or process) to an object (a passive entity such as a file) involves setting up access rules.
These rules can be classified into three access control models: Mandatory, Discretionary, and Non-Discretionary.
An access matrix is one of the means used to implement access control.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION 7
- (Topic 1)
Which of the following is a trusted, third party authentication protocol that was developed under Project Athena at MIT?

A. Kerberos
B. SESAME
C. KryptoKnight
D. NetSP

Answer: A

Explanation:
Kerberos is a trusted, third party authentication protocol that was developed under Project Athena at MIT.
Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. A free implementation of this protocol is available from the Massachusetts Institute of Technology. Kerberos is available in many commercial products as well.
The Internet is an insecure place. Many of the protocols used in the Internet do not provide any security. Tools to "sniff" passwords off of the network are in common use by systems crackers. Thus, applications which send an unencrypted password over the network are extremely vulnerable. Worse yet, other client/server applications rely on the client program to be "honest" about the identity of the user who is using it. Other applications rely on the client to restrict its activities to those which it is allowed to do, with no other enforcement by the server.
Some sites attempt to use firewalls to solve their network security problems. Unfortunately, firewalls assume that "the bad guys" are on the outside, which is often a very bad
assumption. Most of the really damaging incidents of computer crime are carried out by insiders. Firewalls also have a significant disadvantage in that they restrict how your users can use the Internet. (After all, firewalls are simply a less extreme example of the dictum that there is nothing more secure then a computer which is not connected to the network --- and powered off!) In many places, these restrictions are simply unrealistic and unacceptable.
Kerberos was created by MIT as a solution to these network security problems. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server have used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.
Kerberos is freely available from MIT, under a copyright permission notice very similar to the one used for the BSD operating and X11 Windowing system. MIT provides Kerberos in source form, so that anyone who wishes to use it may look over the code for themselves and assure themselves that the code is trustworthy. In addition, for those who prefer to rely on a professional supported product, Kerberos is available as a product from many different vendors.
In summary, Kerberos is a solution to your network security problems. It provides the tools of authentication and strong cryptography over the network to help you secure your information systems across your entire enterprise. We hope you find Kerberos as useful as it has been to us. At MIT, Kerberos has been invaluable to our Information/Technology architecture.
KryptoKnight is a Peer to Peer authentication protocol incorporated into the NetSP product from IBM.
SESAME is an authentication and access control protocol, that also supports communication confidentiality and integrity. It provides public key based authentication along with the Kerberos style authentication, that uses symmetric key cryptography. Sesame supports the Kerberos protocol and adds some security extensions like public key based authentication and an ECMA-style Privilege Attribute Service. The complete Sesame protocol is a two step process. In the first step, the client successfully authenticates itself to the Authentication Server and obtains a ticket that can be presented to the Privilege Attribute Server. In the second step, the initiator obtains proof of his access rights in the form of Privilege Attributes Certificate (PAC). The PAC is a specific form of Access Control Certificate as defined in the ECMA-219 document. This document describes the extensions to Kerberos for public key based authentication as adopted in Sesame.
SESAME, KryptoKnight, and NetSP never took off and the protocols are no longer commonly used.
References:
http://www.cmf.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html#whatis and
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 40.

NEW QUESTION 8
- (Topic 1)

What is the most critical characteristic of a biometric identifying system?

A. Perceived intrusiveness
B. Storage requirements
C. Accuracy
D. Scalability

Answer: C

Explanation:
Accuracy is the most critical characteristic of a biometric identifying verification system.
Accuracy is measured in terms of false rejection rate (FRR, or type I errors) and false acceptance rate (FAR or type II errors).
The Crossover Error Rate (CER) is the point at which the FRR equals the FAR and has become the most important measure of biometric system accuracy.
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 1, Biometric Identification (page 9).

NEW QUESTION 9
- (Topic 1)
In biometrics, the "one-to-one" search used to verify claim to an identity made by a person is considered:

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

Answer: A

Explanation:
Biometric devices can be use for either IDENTIFICATION or AUTHENTICATION
ONE TO ONE is for AUTHENTICATION
This means that you as a user would provide some biometric credential such as your fingerprint. Then they will compare the template that you have provided with the one stored in the Database. If the two are exactly the same that prove that you are who you pretend to be.
ONE TO MANY is for IDENTIFICATION
A good example of this would be within airport. Many airports today have facial recognition cameras, as you walk through the airport it will take a picture of your face and then compare the template (your face) with a database full of templates and see if there is a match between your template and the ones stored in the Database. This is for IDENTIFICATION of a person.
Some additional clarification or comments that might be helpful are: Biometrics establish authentication using specific information and comparing results to expected data. It does not perform well for identification purposes such as scanning for a person's face in a moving crowd for example.
Identification methods could include: username, user ID, account number, PIN, certificate, token, smart card, biometric device or badge.
Auditing is a process of logging or tracking what was done after the identity and authentication process is completed.
Authorization is the rights the subject is given and is performed after the identity is established.
Reference OIG (2007) p148, 167
Authentication in biometrics is a "one-to-one" search to verify claim to an identity made by a person.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.

NEW QUESTION 10
- (Topic 1)
Controls to keep password sniffing attacks from compromising computer systems include which of the following?

A. static and recurring passwords.
B. encryption and recurring passwords.
C. one-time passwords and encryption.
D. static and one-time passwords.

Answer: C

Explanation:
To minimize the chance of passwords being captured one-time passwords would prevent a password sniffing attack because once used it is no longer valid. Encryption will also minimize these types of attacks.
The following answers are correct:
static and recurring passwords. This is incorrect because if there is no encryption then someone password sniffing would be able to capture the password much easier if it never changed.
encryption and recurring passwords. This is incorrect because while encryption helps, recurring passwords do nothing to minimize the risk of passwords being captured.
static and one-time passwords. This is incorrect because while one-time passwords will prevent these types of attacks, static passwords do nothing to minimize the risk of passwords being captured.

NEW QUESTION 10
- (Topic 1)
Which of the following is NOT a type of motion detector?

A. Photoelectric sensor
B. Passive infrared sensors
C. Microwave Sensor.
D. Ultrasonic Sensor.

Answer: A

Explanation:

A photoelectric sensor does not "directly" sense motion there is a narrow beam that won't set off the sensor unless the beam is broken. Photoelectric sensors, along with dry contact switches, are a type of perimeter intrusion detector.

All of the other answers are valid types of motion detectors types.

The content below on the different types of sensors is from Wikepedia: Indoor Sensors

These types of sensors are designed for indoor use. Outdoor use would not be advised due to false alarm vulnerability and weather durability.Passive infrared detectors

C:\Users\MCS\Desktop\1.jpg Passive Infrared Sensor

The passive infrared detector (PIR) is one of the most common detectors found in household and small business environments because it offers affordable and reliable functionality. The term passive means the detector is able to function without the need to generate and radiate its own energy (unlike ultrasonic and microwave volumetric intrusion detectors that are "active" in operation). PIRs are able to distinguish if an infrared emitting object is present by first learning the ambient temperature of the monitored space and then detecting a change in the temperature caused by the presence of an object. Using the principle of differentiation, which is a check of presence or nonpresence, PIRs verify if an intruder or object is actually there. Creating individual zones of detection where each zone comprises one or more layers can achieve differentiation. Between the zones there are areas of no sensitivity (dead zones) that are used by the sensor for comparison.

Ultrasonic detectors

Using frequencies between 15 kHz and 75 kHz, these active detectors transmit ultrasonic sound waves that are inaudible to humans. The Doppler shift principle is the underlying method of operation, in which a change in frequency is detected due to object motion. This is caused when a moving object changes the frequency of sound waves around it. Two conditions must occur to successfully detect a Doppler shift event:

There must be motion of an object either towards or away from the receiver.

The motion of the object must cause a change in the ultrasonic frequency to the receiver relative to the transmitting frequency.

The ultrasonic detector operates by the transmitter emitting an ultrasonic signal into the area to be protected. The sound waves are reflected by solid objects (such as the surrounding floor, walls and ceiling) and then detected by the receiver. Because ultrasonic waves are transmitted through air, then hard-surfaced objects tend to reflect most of the ultrasonic energy, while soft surfaces tend to absorb most energy.

When the surfaces are stationary, the frequency of the waves detected by the receiver will be equal to the transmitted frequency. However, a change in frequency will occur as a result of the Doppler principle, when a person or object is moving towards or away from the detector. Such an event initiates an alarm signal. This technology is considered obsolete by many alarm professionals, and is not actively installed.

Microwave detectors

This device emits microwaves from a transmitter and detects any reflected microwaves or reduction in beam intensity using a receiver. The transmitter and receiver are usually combined inside a single housing (monostatic) for indoor applications, and separate housings (bistatic) for outdoor applications. To reduce false alarms this type of detector is usually combined with a passive infrared detector or "Dualtec" alarm.

Microwave detectors respond to a Doppler shift in the frequency of the reflected energy, by a phase shift, or by a sudden reduction of the level of received energy. Any of these effects may indicate motion of an intruder.

Photo-electric beams

Photoelectric beam systems detect the presence of an intruder by transmitting visible or infrared light beams across an area, where these beams may be obstructed. To improve the detection surface area, the beams are often employed in stacks of two or more. However, if an intruder is aware of the technology's presence, it can be avoided. The technology can be an effective long-range detection system, if installed in stacks of three or more where the transmitters and receivers are staggered to create a fence-like barrier. Systems are available for both internal and external applications. To prevent a clandestine attack using a secondary light source being used to hold the detector in a 'sealed' condition whilst an intruder passes through, most systems use and detect a modulated light source.

Glass break detectors

The glass break detector may be used for internal perimeter building protection. When glass breaks it generates sound in a wide band of frequencies. These can range from infrasonic, which is below 20 hertz (Hz) and can not be heard by the human ear, through the audio band from 20 Hz to 20 kHz which humans can hear, right up to ultrasonic, which is above 20 kHz and again cannot be heard. Glass break acoustic detectors are mounted in close proximity to the glass panes and listen for sound frequencies associated with glass breaking. Seismic glass break detectors are different in that they are installed on the glass pane. When glass breaks it produces specific shock frequencies which travel through the glass and often through the window frame and the surrounding walls and ceiling. Typically, the most intense frequencies generated are between 3 and 5 kHz, depending on the type of glass and the presence of a plastic interlayer. Seismic glass break detectors "feel" these shock frequencies and in turn generate an alarm condition.

The more primitive detection method involves gluing a thin strip of conducting foil on the inside of the glass and putting low-power electrical current through it. Breaking the glass is practically guaranteed to tear the foil and break the circuit.

Smoke, heat, and carbon monoxide detectors

C:\Users\MCS\Desktop\1.jpg Heat Detection System
Most systems may also be equipped with smoke, heat, and/or carbon monoxide detectors. These are also known as 24 hour zones (which are on at all times). Smoke detectors and heat detectors protect from the risk of fire and carbon monoxide detectors protect from the risk of carbon monoxide. Although an intruder alarm panel may also have these detectors connected, it may not meet all the local fire code requirements of a fire alarm system.
Other types of volumetric sensors could be:
Active Infrared
Passive Infrared/Microware combined Radar
Accoustical Sensor/Audio Vibration Sensor (seismic) Air Turbulence

NEW QUESTION 11
- (Topic 1)
Which of the following is NOT a system-sensing wireless proximity card?

A. magnetically striped card
B. passive device
C. field-powered device
D. transponder

Answer: A

Explanation:
 Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, page 342.

NEW QUESTION 16
- (Topic 1)
Logical or technical controls involve the restriction of access to systems and the protection of information. Which of the following statements pertaining to these types of controls is correct?

A. Examples of these types of controls include policies and procedures, securityawareness training, background checks, work habit checks but do not include a review of vacation history, and also do not include increased supervision.
B. Examples of these types of controls do not include encryption, smart cards, access lists, and transmission protocols.
C. Examples of these types of controls are encryption, smart cards, access lists, and transmission protocols.
D. Examples of these types of controls include policies and procedures, security awareness training, background checks, work habit checks, a review of vacation history, and increased supervision.

Answer: C

Explanation:
 Logical or technical controls involve the restriction of access to systems and the protection of information. Examples of these types of controls are encryption, smart cards, access lists, and transmission protocols.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION 20
- (Topic 1)
What does the Clark-Wilson security model focus on?

A. Confidentiality
B. Integrity
C. Accountability
D. Availability

Answer: B

Explanation:
 The Clark-Wilson model addresses integrity. It incorporates mechanisms to enforce internal and external consistency, a separation of duty, and a mandatory integrity policy.
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 205).

NEW QUESTION 24
- (Topic 1)
Which of the following security models does NOT concern itself with the flow of data?

A. The information flow model
B. The Biba model
C. The Bell-LaPadula model
D. The noninterference model

Answer: D

Explanation:
The goal of a noninterference model is to strictly separate differing security levels to assure that higher-level actions do not determine what lower-level users can see. This is in contrast to other security models that control information flows between differing levels of users, By maintaining strict separation of security levels, a noninterference model minimizes leakages that might happen through a covert channel.
The Bell-LaPadula model is incorrect. The Bell-LaPadula model is concerned with confidentiality and bases access control decsions on the classfication of objects and the clearences of subjects.
The information flow model is incorrect. The information flow models have a similar framework to the Bell-LaPadula model and control how information may flow between objects based on security classes.
The Biba model is incorrect. The Biba model is concerned with integrity and is a complement to the Bell-LaPadula model in that higher levels of integrity are more trusted than lower levels. Access control us based on these integrity levels to assure that read/write operations do not decrease an object's integrity.
References:
CBK, pp 325 - 326
AIO3, pp. 290 - 291

NEW QUESTION 29
- (Topic 1)
Which of the following protocol was used by the INITIAL version of the Terminal Access Controller Access Control System TACACS for communication between clients and servers?

A. TCP
B. SSL
C. UDP
D. SSH

Answer: C

Explanation:
The original TACACS, developed in the early ARPANet days, had very limited functionality and used the UDP transport. In the early 1990s, the protocol was extended to include additional functionality and the transport changed to TCP.
TACACS is defined in RFC 1492, and uses (either TCP or UDP) port 49 by default. TACACS allows a client to accept a username and password and send a query to a TACACS authentication server, sometimes called a TACACS daemon or simply TACACSD. TACACSD uses TCP and usually runs on port 49. It would determine whether to accept or deny the authentication request and send a response back.
TACACS+
TACACS+ and RADIUS have generally replaced TACACS and XTACACS in more recently built or updated networks. TACACS+ is an entirely new protocol and is not compatible with TACACS or XTACACS. TACACS+ uses the Transmission Control Protocol (TCP) and RADIUS uses the User Datagram Protocol (UDP). Since TCP is connection oriented
protocol, TACACS+ does not have to implement transmission control. RADIUS, however, does have to detect and correct transmission errors like packet loss, timeout etc. since it rides on UDP which is connectionless.
RADIUS encrypts only the users' password as it travels from the RADIUS client to RADIUS server. All other information such as the username, authorization, accounting are transmitted in clear text. Therefore it is vulnerable to different types of attacks. TACACS+ encrypts all the information mentioned above and therefore does not have the vulnerabilities present in the RADIUS protocol.
RADIUS and TACACS + are client/ server protocols, which means the server portion cannot send unsolicited commands to the client portion. The server portion can only speak when spoken to. Diameter is a peer-based protocol that allows either end to initiate communication. This functionality allows the Diameter server to send a message to the access server to request the user to provide another authentication credential if she is attempting to access a secure resource.
Reference(s) used for this question: http://en.wikipedia.org/wiki/TACACS
and
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 239). McGraw- Hill. Kindle Edition.

NEW QUESTION 31
- (Topic 1)
The control measures that are intended to reveal the violations of security policy using software and hardware are associated with:

A. Preventive/physical
B. Detective/technical
C. Detective/physical
D. Detective/administrative

Answer: B

Explanation:
The detective/technical control measures are intended to reveal the violations of security policy using technical means.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the
Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.

NEW QUESTION 32
- (Topic 1)
Which access control model enables the OWNER of the resource to specify what subjects can access specific resources based on their identity?

A. Discretionary Access Control
B. Mandatory Access Control
C. Sensitive Access Control
D. Role-based Access Control

Answer: A

Explanation:
Data owners decide who has access to resources based only on the identity of the person accessing the resource.
The following answers are incorrect :
Mandatory Access Control : users and data owners do not have as much freedom to determine who can access files. The operating system makes the final decision and can override the users' wishes and access decisions are based on security labels.
Sensitive Access Control : There is no such access control in the context of the above question.
Role-based Access Control : uses a centrally administered set of controls to determine how subjects and objects interact , also called as non discretionary access control.
In a mandatory access control (MAC) model, users and data owners do not have as much freedom to determine who can access files. The operating system makes the final decision and can override the users' wishes. This model is much more structured and strict and is based on a security label system. Users are given a security clearance (secret, top secret, confidential, and so on), and data is classified in the same way. The clearance and classification data is stored in the security labels, which are bound to the specific subjects and objects. When the system makes a decision about fulfilling a request to access an object, it is based on the clearance of the subject, the classification of the object, and the security policy of the system. The rules for how subjects access objects are made by the security officer, configured by the administrator, enforced by the operating system, and supported by security technologies
Reference : Shon Harris , AIO v3 , Chapter-4 : Access Control , Page : 163-165

NEW QUESTION 33
- (Topic 1)
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

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.

NEW QUESTION 34
- (Topic 1)
Identification and authentication are the keystones of most access control systems. Identification establishes:

A. User accountability for the actions on the system.
B. Top management accountability for the actions on the system.
C. EDP department accountability for the actions of users on the system.
D. Authentication for actions on the system

Answer: A

Explanation:
Identification and authentication are the keystones of most access control systems. Identification establishes user accountability for the actions on the system.
The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system. This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.
Once a person has been identified through the user ID or a similar value, she must be authenticated, which means she must prove she is who she says she is. Three general factors can be used for authentication: something a person knows, something a person has, and something a person is. They are also commonly called authentication by knowledge, authentication by ownership, and authentication by characteristic.
For a user to be able to access a resource, he first must prove he is who he claims to be, has the necessary credentials, and has been given the necessary rights or privileges to perform the actions he is requesting. Once these steps are completed successfully, the user can access and use network resources; however, it is necessary to track the user's activities and enforce accountability for his actions.
Identification describes a method of ensuring that a subject (user, program, or process) is the entity it claims to be. Identification can be provided with the use of a username or account number. To be properly authenticated, the subject is usually required to provide a second piece to the credential set. This piece could be a password, passphrase,
cryptographic key, personal identification number (PIN), anatomical attribute, or token.
These two credential items are compared to information that has been previously stored for this subject. If these credentials match the stored information, the subject is authenticated. But we are not done yet. Once the subject provides its credentials and is properly identified, the system it is trying to access needs to determine if this subject has been given the necessary rights and privileges to carry out the requested actions. The system will look at some type of access control matrix or compare security labels to verify that this subject may indeed access the requested resource and perform the actions it is attempting. If the system determines that the subject may access the resource, it authorizes the subject.
Although identification, authentication, authorization, and accountability have close and complementary definitions, each has distinct functions that fulfill a specific requirement in the process of access control. A user may be properly identified and authenticated to the network, but he may not have the authorization to access

the files on the file server. On the other hand, a user may be authorized to access the files on the file server, but until she is properly identified and authenticated, those resources are out of reach.
Reference(s) used for this question:
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition: Access Control ((ISC)2 Press) (Kindle Locations 889-892). Auerbach Publications. Kindle Edition.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 3875-3878). McGraw-Hill. Kindle Edition.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 3833-3848). McGraw-Hill. Kindle Edition.
and
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

NEW QUESTION 36
- (Topic 1)
When submitting a passphrase for authentication, the passphrase is converted into ...

A. a virtual password by the system
B. a new passphrase by the system
C. a new passphrase by the encryption technology
D. a real password by the system which can be used forever

Answer: A

Explanation:
Passwords can be compromised and must be protected. In the ideal case, a password should only be used once. The changing of passwords can also fall between these two extremes.
Passwords can be required to change monthly, quarterly, or at other intervals, depending on the criticality of the information needing protection and the password's frequency of use.
Obviously, the more times a password is used, the more chance there is of it being compromised.
It is recommended to use a passphrase instead of a password. A passphrase is more resistant to attacks. The passphrase is converted into a virtual password by the system. Often time the passphrase will exceed the maximum length supported by the system and it must be trucated into a Virtual Password.
Reference(s) used for this question: http://www.itl.nist.gov/fipspubs/fip112.htm
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36 & 37.

NEW QUESTION 39
- (Topic 1)
A department manager has read access to the salaries of the employees in his/her department but not to the salaries of employees in other departments. A database security mechanism that enforces this policy would typically be said to provide which of the following?

A. Content-dependent access control
B. Context-dependent access control
C. Least privileges access control
D. Ownership-based access control

Answer: A

Explanation:
When access control is based on the content of an object, it is considered to be content dependent access control.
Content-dependent access control is based on the content itself. The following answers are incorrect:
context-dependent access control. Is incorrect because this type of control is based on what the context is, facts about the data rather than what the object contains.
least privileges access control. Is incorrect because this is based on the least amount of rights needed to perform their jobs and not based on what is contained in the database. ownership-based access control. Is incorrect because this is based on the owner of the data and and not based on what is contained in the database.
References:
OIG CBK Access Control (page 191)

NEW QUESTION 44
- (Topic 1)
In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on :

A. sex of a person
B. physical attributes of a person
C. age of a person
D. voice of a person

Answer: B

Explanation:
Today implementation of fast, accurate reliable and user-acceptable biometric identification systems is already under way.
From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Page 7.

NEW QUESTION 49
- (Topic 1)
The Orange Book is founded upon which security policy model?

A. The Biba Model
B. The Bell LaPadula Model

C. Clark-Wilson Model
D. TEMPEST

Answer: B

Explanation:
From the glossary of Computer Security Basics:
The Bell-LaPadula model is the security policy model on which the Orange Book requirements are based. From the Orange Book definition, "A formal state transition model of computer security policy that describes a set of access control rules. In this formal model, the entities in a computer system are divided into abstract sets of subjects and objects. The notion of secure state is defined and it is proven that each state transition preserves security by moving from secure state to secure state; thus, inductively proving the system is secure. A system state is defined to be 'secure' if the only permitted access modes of subjects to objects are in accordance with a specific security policy. In order to determine whether or not a specific access mode is allowed, the clearance of a subject is compared to the classification of the object and a determination is made as to whether the subject is authorized for the specific access mode."
The Biba Model is an integrity model of computer security policy that describes a set of rules. In this model, a subject may not depend on any object or other subject that is less trusted than itself.
The Clark Wilson Model is an integrity model for computer security policy designed for a commercial environment. It addresses such concepts as nondiscretionary access control, privilege separation, and least privilege. TEMPEST is a government program that prevents the compromising electrical and electromagnetic signals that emanate from computers and related equipment from being intercepted and deciphered.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, 1991.
Also: U.S. Department of Defense, Trusted Computer System Evaluation Criteria (Orange Book), DOD 5200.28-STD. December 1985 (also available here).

NEW QUESTION 52
- (Topic 1)
How would nonrepudiation be best classified as?

A. A preventive control
B. A logical control
C. A corrective control
D. A compensating control

Answer: A

Explanation:
Systems accountability depends on the ability to ensure that senders cannot deny sending information and that receivers cannot deny receiving it. Because the mechanisms implemented in nonrepudiation prevent the ability to successfully repudiate an action, it can be considered as a preventive control.
Source: STONEBURNER, Gary, NIST Special Publication 800-33: Underlying Technical Models for Information Technology Security, National Institute of Standards and Technology, December 2001, page 7.

NEW QUESTION 54
- (Topic 1)
In addition to the accuracy of the biometric systems, there are other factors that must also be considered:

A. These factors include the enrollment time and the throughput rate, but not acceptability.
B. These factors do not include the enrollment time, the throughput rate, and acceptability.
C. These factors include the enrollment time, the throughput rate, and acceptability.
D. These factors include the enrollment time, but not the throughput rate, neither the acceptability.

Answer: C

Explanation:
In addition to the accuracy of the biometric systems, there are other factors that must also be considered.
These factors include the enrollment time, the throughput rate, and acceptability. Enrollment time is the time it takes to initially "register" with a system by providing samples
of the biometric characteristic to be evaluated. An acceptable enrollment time is around two
minutes.
For example, in fingerprint systems, the actual fingerprint is stored and requires approximately 250kb per finger for a high quality image. This level of information is required for one-to-many searches in forensics applications on very large databases.
In finger-scan technology, a full fingerprint is not stored-the features extracted from this fingerprint are stored using a small template that requires approximately 500 to 1000 bytes of storage. The original fingerprint cannot be reconstructed from this template.
Updates of the enrollment information may be required because some biometric characteristics, such as voice and signature, may change with time.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37 & 38.

NEW QUESTION 57
- (Topic 1)
In biometrics, "one-to-many" search against database of stored biometric images is done in:

A. Authentication
B. Identification
C. Identities
D. Identity-based access control

Answer: B

Explanation:
In biometrics, identification is a "one-to-many" search of an individual's characteristics from a database of stored images.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.

NEW QUESTION 61

- (Topic 1)
Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It does not permit management to:

A. specify what users can do
B. specify which resources they can access
C. specify how to restrain hackers
D. specify what operations they can perform on a system.

Answer: C

Explanation:
 Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to specify what users can do, which resources they can access, and what operations they can perform on a system. Specifying HOW to restrain hackers is not directly linked to access control.
Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 12.

NEW QUESTION 65
- (Topic 1)
What is the primary role of smartcards in a PKI?

A. Transparent renewal of user keys
B. Easy distribution of the certificates between the users
C. Fast hardware encryption of the raw data
D. Tamper resistant, mobile storage and application of private keys of the users

Answer: D

Explanation:
 Reference: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw- Hill/Osborne, page 139;
SNYDER, J., What is a SMART CARD?.
Wikipedia has a nice definition at: http://en.wikipedia.org/wiki/Tamper_resistance Security
Tamper-resistant microprocessors are used to store and process private or sensitive information, such as private keys or electronic money credit. To prevent an attacker from
retrieving or modifying the information, the chips are designed so that the information is not accessible through external means and can be accessed only by the embedded software, which should contain the appropriate security measures.
Examples of tamper-resistant chips include all secure cryptoprocessors, such as the IBM 4758 and chips used in smartcards, as well as the Clipper chip.
It has been argued that it is very difficult to make simple electronic devices secure against tampering, because numerous attacks are possible, including:
physical attack of various forms (microprobing, drills, files, solvents, etc.) freezing the device
applying out-of-spec voltages or power surges applying unusual clock signals
inducing software errors using radiation
measuring the precise time and power requirements of certain operations (see power analysis)
Tamper-resistant chips may be designed to zeroise their sensitive data (especially cryptographic keys) if they detect penetration of their security encapsulation or out-of- specification environmental parameters. A chip may even be rated for "cold zeroisation", the ability to zeroise itself even after its power supply has been crippled.
Nevertheless, the fact that an attacker may have the device in his possession for as long as he likes, and perhaps obtain numerous other samples for testing and practice, means that it is practically impossible to totally eliminate tampering by a sufficiently motivated opponent. Because of this, one of the most important elements in protecting a system is overall system design. In particular, tamper-resistant systems should "fail gracefully" by ensuring that compromise of one device does not compromise the entire system. In this manner, the attacker can be practically restricted to attacks that cost less than the expected return from compromising a single device (plus, perhaps, a little more for kudos). Since the most sophisticated attacks have been estimated to cost several hundred thousand dollars to carry out, carefully designed systems may be invulnerable in practice.

NEW QUESTION 67
- (Topic 1)
Which of the following biometric parameters are better suited for authentication use over a long period of time?

A. Iris pattern
B. Voice pattern
C. Signature dynamics
D. Retina pattern

Answer: A

Explanation:
 The iris pattern is considered lifelong. Unique features of the iris are: freckles, rings, rifts, pits, striations, fibers, filaments, furrows, vasculature and coronas. Voice, signature and retina patterns are more likely to change over time, thus are not as suitable for authentication over a long period of time without needing re-enrollment. Source: FERREL, Robert G, Questions and Answers for the CISSP Exam, domain 1 (derived from the Information Security Management Handbook, 4th Ed., by Tipton & Krause).

NEW QUESTION 71
- (Topic 1)
Who first described the DoD multilevel military security policy in abstract, formal terms?

A. David Bell and Leonard LaPadula
B. Rivest, Shamir and Adleman
C. Whitfield Diffie and Martin Hellman
D. David Clark and David Wilson

Answer: A

Explanation:
 It was David Bell and Leonard LaPadula who, in 1973, first described the DoD multilevel military security policy in abstract, formal terms. The Bell-LaPadula is a Mandatory Access Control (MAC) model concerned with confidentiality. Rivest, Shamir and Adleman (RSA) developed the RSA encryption algorithm. Whitfield Diffie and Martin Hellman published the Diffie-Hellman key agreement algorithm in 1976. David Clark and David Wilson developed the Clark-Wilson integrity model, more appropriate for security in commercial activities.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (pages 78,109).

NEW QUESTION 74
- (Topic 1)
Which of the following is not a two-factor authentication mechanism?

A. Something you have and something you know.
B. Something you do and a password.
C. A smartcard and something you are.
D. Something you know and a password.

Answer: D

Explanation:
 Something you know and a password fits within only one of the three ways authentication could be done. A password is an example of something you know, thereby something you know and a password does not constitute a two-factor authentication as both are in the same category of factors.
A two-factor (strong) authentication relies on two different kinds of authentication factors out of a list of three possible choice:
something you know (e.g. a PIN or password),
something you have (e.g. a smart card, token, magnetic card),
something you are is mostly Biometrics (e.g. a fingerprint) or something you do (e.g. signature dynamics).
TIP FROM CLEMENT:
On the real exam you can expect to see synonyms and sometimes sub-categories under the main categories. People are familiar with Pin, Passphrase, Password as subset of Something you know.
However, when people see choices such as Something you do or Something you are they immediately get confused and they do not think of them as subset of Biometrics where you have Biometric implementation based on behavior and physilogical attributes. So something you do falls under the Something you are category as a subset.
Something your do would be signing your name or typing text on your keyboard for example.
Strong authentication is simply when you make use of two factors that are within two different categories.
Reference(s) used for this question:
Shon Harris, CISSP All In One, Fifth Edition, pages 158-159

NEW QUESTION 77
- (Topic 1)
Which of the following is not a logical control when implementing logical access security?

A. access profiles.
B. userids.
C. employee badges.
D. passwords.

Answer: C

Explanation:
 Employee badges are considered Physical so would not be a logical control. The following answers are incorrect:
userids. Is incorrect because userids are a type of logical control.
access profiles. Is incorrect because access profiles are a type of logical control. passwords. Is incorrect because passwords are a type of logical control.

NEW QUESTION 80
- (Topic 1)
Which access control model was proposed for enforcing access control in government and military applications?

A. Bell-LaPadula model
B. Biba model
C. Sutherland model
D. Brewer-Nash model

Answer: A

Explanation:
 The Bell-LaPadula model, mostly concerned with confidentiality, was proposed for enforcing access control in government and military applications. It supports mandatory access control by determining the access rights from the security levels associated with subjects and objects. It also supports discretionary access control by checking access rights from an access matrix. The Biba model, introduced in 1977, the Sutherland model, published in 1986, and the Brewer-Nash model, published in 1989, are concerned with integrity.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 2: Access Control Systems and Methodology (page 11).

NEW QUESTION 85
- (Topic 1)
This is a common security issue that is extremely hard to control in large environments. It occurs when a user has more computer rights, permissions, and access than what is required for the tasks the user needs to fulfill. What best describes this scenario?

A. Excessive Rights
B. Excessive Access
C. Excessive Permissions
D. Excessive Privileges

Answer: D

Explanation:
Even thou all 4 terms are very close to each other, the best choice is Excessive Privileges which would include the other three choices presented.
Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 645.
and

NEW QUESTION 88
- (Topic 1)
Which of the following access control models requires defining classification for objects?

A. Role-based access control
B. Discretionary access control
C. Identity-based access control
D. Mandatory access control

Answer: D

Explanation:
With mandatory access control (MAC), the authorization of a subject's access to an object is dependant upon labels, which indicate the subject's clearance, and classification of objects.
The Following answers were incorrect:
Identity-based Access Control is a type of Discretionary Access Control (DAC), they are synonymous.
Role Based Access Control (RBAC) and Rule Based Access Control (RuBAC or RBAC) are types of Non Discretionary Access Control (NDAC).
Tip:
When you have two answers that are synonymous they are not the right choice for sure.
There is only one access control model that makes use of Label, Clearances, and Categories, it is Mandatory Access Control, none of the other one makes use of those items.
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, Chapter 2: Access control systems (page 33).

NEW QUESTION 90
- (Topic 1)
What is one disadvantage of content-dependent protection of information?

A. It increases processing overhead.
B. It requires additional password entry.
C. It exposes the system to data locking.
D. It limits the user's individual address space.

Answer: A

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

NEW QUESTION 93
- (Topic 1)
The following is NOT a security characteristic we need to consider while choosing a biometric identification systems:

A. data acquisition process
B. cost
C. enrollment process
D. speed and user interface

Answer: B

Explanation:
Cost is a factor when considering Biometrics but it is not a security characteristic.
All the other answers are incorrect because they are security characteristics related to Biometrics.
data acquisition process can cause a security concern because if the process is not fast and efficient it can discourage individuals from using the process.
enrollment process can cause a security concern because the enrollment process has to be quick and efficient. This process captures data for authentication.
speed and user interface can cause a security concern because this also impacts the users acceptance rate of biometrics. If they are not comfortable with the interface and speed they might sabotage the devices or otherwise attempt to circumvent them.
References:
OIG Access Control (Biometrics) (pgs 165-167)
From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Pages 5-6.
in process of correction

NEW QUESTION 97
- (Topic 1)
What mechanism automatically causes an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters?

A. Central station alarm
B. Proprietary alarm
C. A remote station alarm
D. An auxiliary station alarm

Answer: D

Explanation:
Auxiliary station alarms automatically cause an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters. They are usually Municipal Fire Alarm Boxes are installed at your business or building, they are wired directly into the fire station.
Central station alarms are operated by private security organizations. It is very similar to a proprietary alarm system (see below). However, the biggest difference is the monitoring and receiving of alarm is done off site at a central location manned by non staff members. It is a third party.
Proprietary alarms are similar to central stations alarms except that monitoring is performed directly on the protected property. This type of alarm is usually use to protect large industrials or commercial buildings. Each of the buildings in the same vincinity has their own alarm system, they are all wired together at a central location within one of the building acting as a common receiving point. This point is usually far away from the other building so it is not under the same danger. It is usually man 24 hours a day by a trained team who knows how to react under different conditions.
A remote station alarm is a direct connection between the signal-initiating device at the protected property and the signal-receiving device located at a remote station, such as the fire station or usually a monitoring service. This is the most popular type of implementation and the owner of the premise must pay a monthly monitoring fee. This is what most people use in their home where they get a company like ADT to receive the alarms on their behalf.
A remote system differs from an auxiliary system in that it does not use the municipal fire of police alarm circuits.
Reference(s) used for this question:
ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 11: Physical Security (page 211).
and
Great presentation J.T.A. Stone on SlideShare

NEW QUESTION 101
- (Topic 1)
Which of the following is not a preventive login control?

A. Last login message
B. Password aging
C. Minimum password length
D. Account expiration

Answer: A

Explanation:
The last login message displays the last login date and time, allowing a user to discover if their account was used by someone else. Hence, this is rather a detective control.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (page 63).

NEW QUESTION 103
- (Topic 1)
How can an individual/person best be identified or authenticated to prevent local masquarading attacks?

A. UserId and password
B. Smart card and PIN code
C. Two-factor authentication
D. Biometrics

Answer: D

Explanation:
The only way to be truly positive in authenticating identity for access is to base the authentication on the physical attributes of the persons themselves (i.e., biometric
identification). Physical attributes cannot be shared, borrowed, or duplicated. They ensure that you do identify the person, however they are not perfect and they would have to be supplemented by another factor.
Some people are getting thrown off by the term Masquarade. In general, a masquerade is a disguise. In terms of communications security issues, a masquerade is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism. Spoofing is another term used to describe this type of attack as well.
A UserId only provides for identification.
A password is a weak authentication mechanism since passwords can be disclosed, shared, written down, and more.
A smart card can be stolen and its corresponding PIN code can be guessed by an intruder. A smartcard can be borrowed by a friend of yours and you would have no clue as to who is really logging in using that smart card.
Any form of two-factor authentication not involving biometrics cannot be as reliable as a biometric system to identify the person.
Biometric identifying verification systems control people. If the person with the correct hand, eye, face, signature, or voice is not present, the identification and verification cannot take place and the desired action (i.e., portal passage, data, or resource access) does not occur.
As has been demonstrated many times, adversaries and criminals obtain and successfully use access cards, even those that require the addition of a PIN. This is because these systems control only pieces of plastic (and sometimes information), rather than people. Real asset and resource protection can only be accomplished by people, not cards and information, because unauthorized persons can (and do) obtain the cards and information.
Further, life-cycle costs are significantly reduced because no card or PIN administration system or personnel are required. The authorized person does not lose physical characteristics (i.e., hands, face, eyes, signature, or voice), but cards and PINs are continuously lost, stolen, or forgotten. This is why card access systems require systems and people to administer, control, record, and issue (new) cards and PINs. Moreover, the cards are an expensive and recurring cost.
NOTE FROM CLEMENT:
This question has been generating lots of interest. The keyword in the question is: Individual (the person) and also the authenticated portion as well.
I totally agree with you that Two Factors or Strong Authentication would be the strongest means of authentication. However the question is not asking what is the strongest mean of authentication, it is asking what is the best way to identify the user (individual) behind the technology. When answering questions do not make assumptions to facts not presented in the question or answers.
Nothing can beat Biometrics in such case. You cannot lend your fingerprint and pin to someone else, you cannot borrow one of my eye balls to defeat the Iris or Retina scan. This is why it is the best method to authenticate the user.
I think the reference is playing with semantics and that makes it a bit confusing. I have improved the question to make it a lot clearer and I have also improve the explanations attached with the question.
The reference mentioned above refers to authenticating the identity for access. So the distinction is being made that there is identity and there is authentication. In the case of physical security the enrollment process is where the identity of the user would be validated and then the biometrics features provided by the user

would authenticate the user on a one to one matching basis (for authentication) with the reference contained in the database of biometrics templates. In the case of system access, the user might have to provide a username, a pin, a passphrase, a smart card, and then provide his biometric attributes.

Biometric can also be used for Identification purpose where you do a one to many match. You take a facial scan of someone within an airport and you attempt to match it with a large database of known criminal and terrorists. This is how you could use biometric for Identification.

There are always THREE means of authentication, they are: Something you know (Type 1)

Something you have (Type 2)

Something you are (Type 3)

Reference(s) used for this question:

TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1) , 2000, CRC Press, Chapter 1, Biometric Identification (page 7).

and

Search Security at http://searchsecurity.techtarget.com/definition/masquerade

NEW QUESTION 108

- (Topic 1)

Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished:

A. through access control mechanisms that require identification and authentication and through the audit function.

B. through logical or technical controls involving the restriction of access to systems and the protection of information.

C. through logical or technical controls but not involving the restriction of access to systems and the protection of information.

D. through access control mechanisms that do not require identification and authentication and do not operate through the audit function.

Answer: A

Explanation:

 Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished through access control mechanisms that require identification and authentication and through the audit function. These controls must be in accordance with and accurately represent the organization's security policy. Assurance procedures ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION 111

- (Topic 1)

What is Kerberos?

A. A three-headed dog from the egyptian mythology.

B. A trusted third-party authentication protocol.

C. A security model.

D. A remote authentication dial in user server.

Answer: B

Explanation:

 Is correct because that is exactly what Kerberos is. The following answers are incorrect:

A three-headed dog from Egyptian mythology. Is incorrect because we are dealing with Information Security and not the Egyptian mythology but the Greek Mythology.

A security model. Is incorrect because Kerberos is an authentication protocol and not just a security model.

A remote authentication dial in user server. Is incorrect because Kerberos is not a remote authentication dial in user server that would be called RADIUS.

NEW QUESTION 116

- (Topic 1)

Which of the following is most appropriate to notify an internal user that session monitoring is being conducted?

A. Logon Banners

B. Wall poster

C. Employee Handbook

D. Written agreement

Answer: D

Explanation:

 This is a tricky question, the keyword in the question is Internal users.

There are two possible answers based on how the question is presented, this question could either apply to internal users or ANY anonymous/external users. Internal users should always have a written agreement first, then logon banners serve as a constant reminder.

Banners at the log-on time should be used to notify external users of any monitoring that is being conducted. A good banner will give you a better legal stand and also makes it obvious the user was warned about who should access the system, who is authorized and unauthorized, and if it is an unauthorized user then he is fully aware of trespassing. Anonymous/External users, such as those logging into a web site, ftp server or even a mail server; their only notification system is the use of a logon banner.

References used for this question:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 50.

and

Shon Harris, CISSP All-in-one, 5th edition, pg 873

NEW QUESTION 117

- (Topic 1)

Technical controls such as encryption and access control can be built into the operating system, be software applications, or can be supplemental hardware/software units. Such controls, also known as logical controls, represent which pairing?

A. Preventive/Administrative Pairing

B. Preventive/Technical Pairing

C. Preventive/Physical Pairing
D. Detective/Technical Pairing

Answer: B

Explanation:
 Preventive/Technical controls are also known as logical controls and can be built into the operating system, be software applications, or can be supplemental hardware/software units.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION 120
- (Topic 1)
What is considered the most important type of error to avoid for a biometric access control system?

A. Type I Error
B. Type II Error
C. Combined Error Rate
D. Crossover Error Rate

Answer: B

Explanation:
 When a biometric system is used for access control, the most important error is the false accept or false acceptance rate, or Type II error, where the system would accept an impostor.
A Type I error is known as the false reject or false rejection rate and is not as important in the security context as a type II error rate. A type one is when a valid company employee is rejected by the system and he cannot get access even thou it is a valid user.
The Crossover Error Rate (CER) is the point at which the false rejection rate equals the false acceptance rate if your would create a graph of Type I and Type II errors. The lower the CER the better the device would be.
The Combined Error Rate is a distracter and does not exist.
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 1, Biometric Identification (page 10).

NEW QUESTION 121
- (Topic 1)
Which of the following would be an example of the best password?

A. golf001
B. Elizabeth
C. T1me4g0lF
D. password

Answer: C

Explanation:
 The best passwords are those that are both easy to remember and hard to crack using a dictionary attack. The best way to create passwords that fulfil both criteria is to use two small unrelated words or phonemes, ideally with upper and lower case characters, a special character, and/or a number. Shouldn't be used: common names, DOB, spouse, phone numbers, words found in dictionaries or system defaults.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 1.

NEW QUESTION 122
- (Topic 1)
Which access control model would a lattice-based access control model be an example of?

A. Mandatory access control.
B. Discretionary access control.
C. Non-discretionary access control.
D. Rule-based access control.

Answer: A

Explanation:
 In a lattice model, there are pairs of elements that have the least upper bound of values and greatest lower bound of values. In a Mandatory Access Control (MAC) model, users and data owners do not have as much freedom to determine who can access files.
TIPS FROM CLEMENT
Mandatory Access Control is in place whenever you have permissions that are being imposed on the subject and the subject cannot arbitrarily change them. When the subject/owner of the file can change permissions at will, it is discretionary access control.
Here is a breakdown largely based on explanations provided by Doug Landoll. I am reproducing below using my own word and not exactly how Doug explained it:
FIRST: The Lattice
A lattice is simply an access control tool usually used to implement Mandatory Access Control (MAC) and it could also be used to implement RBAC but this is not as common. The lattice model can be used for Integrity level or file permissions as well. The lattice has a least upper bound and greatest lower bound. It makes use of pair of elements such as the subject security clearance pairing with the object sensitivity label.
SECOND: DAC (Discretionary Access Control)
Let's get into Discretionary Access Control: It is an access control method where the owner (read the creator of the object) will decide who has access at his own discretion. As we all know, users are sometimes insane. They will share their files with other users based on their identity but nothing prevent the user from further sharing it with other users on the network. Very quickly you loose control on the flow of information and who has access to what. It is used in small and friendly environment where a low level of security is all that is required.
THIRD: MAC (Mandatory Access Control)
All of the following are forms of Mandatory Access Control: Mandatory Access control (MAC) (Implemented using the lattice)
You must remember that MAC makes use of Security Clearance for the subject and also Labels will be assigned to the objects. The clearance of the Subject must

dominate (be equal or higher) the clearance of the Object being accessed. The label attached to the object will indicate the sensitivity leval and the categories the object belongs to. The categories are used to implement the Need to Know.
All of the following are forms of Non Discretionary Access Control:
Role Based Access Control (RBAC)
Rule Based Access Control (Think Firewall in this case)
The official ISC2 book says that RBAC (synonymous with Non Discretionary Access Control) is a form of DAC but they are simply wrong. RBAC is a form of Non Discretionary Access Control. Non Discretionary DOES NOT equal mandatory access control as there is no labels and clearance involved.
I hope this clarifies the whole drama related to what is what in the world of access control. In the same line of taught, you should be familiar with the difference between Explicit
permission (the user has his own profile) versus Implicit (the user inherit permissions by
being a member of a role for example).
The following answers are incorrect:
Discretionary access control. Is incorrect because in a Discretionary Access Control (DAC) model, access is restricted based on the authorization granted to the users. It is identity based access control only. It does not make use of a lattice.
Non-discretionary access control. Is incorrect because Non-discretionary Access Control (NDAC) uses the role-based access control method to determine access rights and permissions. It is often times used as a synonym to RBAC which is Role Based Access Control. The user inherit permission from the role when they are assigned into the role. This type of access could make use of a lattice but could also be implemented without the use of a lattice in some case. Mandatory Access Control was a better choice than this one, but RBAC could also make use of a lattice. The BEST answer was MAC.
Rule-based access control. Is incorrect because it is an example of a Non-discretionary Access Control (NDAC) access control mode. You have rules that are globally applied to all users. There is no such thing as a lattice being use in Rule-Based Access Control.
References:
AIOv3 Access Control (pages 161 - 168)
AIOv3 Security Models and Architecture (pages 291 - 293)

NEW QUESTION 123
- (Topic 1)
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

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 implicitly 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.

NEW QUESTION 127
- (Topic 1)
Which TCSEC level is labeled Controlled Access Protection?

A. C1
B. C2
C. C3
D. B1

Answer: B

Explanation:
C2 is labeled Controlled Access Protection.
The TCSEC defines four divisions: D, C, B and A where division A has the highest security. Each division represents a significant difference in the trust an individual or organization
can place on the evaluated system. Additionally divisions C, B and A are broken into a series of hierarchical subdivisions called classes: C1, C2, B1, B2, B3 and A1.
Each division and class expands or modifies as indicated the requirements of the immediately prior division or class.
D — Minimal protection
Reserved for those systems that have been evaluated but that fail to meet the requirements for a higher division
C — Discretionary protection
C1 — Discretionary Security Protection Identification and authentication Separation of users and data
Discretionary Access Control (DAC) capable of enforcing access limitations on an individual basis
Required System Documentation and user manuals C2 — Controlled Access Protection
More finely grained DAC
Individual accountability through login procedures Audit trails

Object reuse Resource isolation

B — Mandatory protection

B1 — Labeled Security Protection

Informal statement of the security policy model Data sensitivity labels

Mandatory Access Control (MAC) over selected subjects and objects Label exportation capabilities

All discovered flaws must be removed or otherwise mitigated Design specifications and verification

B2 — Structured Protection

Security policy model clearly defined and formally documented DAC and MAC enforcement extended to all subjects and objects

Covert storage channels are analyzed for occurrence and bandwidth Carefully structured into protection-critical and non-protection-critical elements Design and implementation enable more comprehensive testing and review Authentication mechanisms are strengthened

Trusted facility management is provided with administrator and operator segregation Strict configuration management controls are imposed

B3 — Security Domains

Satisfies reference monitor requirements

Structured to exclude code not essential to security policy enforcement Significant system engineering directed toward minimizing complexity Security administrator role defined

Audit security-relevant events

Automated imminent intrusion detection, notification, and response Trusted system recovery procedures

Covert timing channels are analyzed for occurrence and bandwidth

An example of such a system is the XTS-300, a precursor to the XTS-400 A — Verified protection

A1 — Verified Design Functionally identical to B3

Formal design and verification techniques including a formal top-level specification Formal management and distribution procedures

An example of such a system is Honeywell's Secure Communications Processor SCOMP, a precursor to the XTS-400

Beyond A1

System Architecture demonstrates that the requirements of self-protection and completeness for reference monitors have been implemented in the Trusted Computing Base (TCB).

Security Testing automatically generates test-case from the formal top-level specification or formal lower-level specifications.

Formal Specification and Verification is where the TCB is verified down to the source code level, using formal verification methods where feasible.

Trusted Design Environment is where the TCB is designed in a trusted facility with only trusted (cleared) personnel.

The following are incorrect answers: C1 is Discretionary security

C3 does not exists, it is only a detractor

B1 is called Labeled Security Protection.

Reference(s) used for this question:

HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.

and

AIOv4 Security Architecture and Design (pages 357 - 361) AIOv5 Security Architecture and Design (pages 358 - 362)

NEW QUESTION 130

- (Topic 1)

Considerations of privacy, invasiveness, and psychological and physical comfort when using the system are important elements for which of the following?

A. Accountability of biometrics systems
B. Acceptability of biometrics systems
C. Availability of biometrics systems
D. Adaptability of biometrics systems

Answer: B

Explanation:

Acceptability refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 39.

NEW QUESTION 133

- (Topic 1)

In which of the following security models is the subject's clearance compared to the object's classification such that specific rules can be applied to control how the subject-to-object interactions take place?

A. Bell-LaPadula model
B. Biba model
C. Access Matrix model
D. Take-Grant model

Answer: A

Explanation:

The Bell-LAPadula model is also called a multilevel security system because users with different clearances use the system and the system processes data with different classifications. Developed by the US Military in the 1970s.

A security model maps the abstract goals of the policy to information system terms by specifying explicit data structures and techniques necessary to enforce the security policy. A security model is usually represented in mathematics and analytical ideas, which are mapped to system specifications and then developed by programmers through programming code. So we have a policy that encompasses security goals, such as "each subject must be authenticated and authorized before accessing an object." The security model takes this requirement and provides the necessary mathematical formulas, relationships, and logic structure to be followed to accomplish this goal.

A system that employs the Bell-LaPadula model is called a multilevel security system because users with different clearances use the system, and the system processes data at different classification levels. The level at which information is classified determines the handling procedures that should be used. The Bell-LaPadula model is a state machine model that enforces the confidentiality aspects of access control. A matrix and security levels are used to determine if subjects can access different objects. The subject's clearance is compared to the object's classification and then specific rules are applied to control how subject-to-object subject-to-object interactions can take place.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 369). McGraw- Hill. Kindle Edition.

NEW QUESTION 137

- (Topic 1)
Which security model introduces access to objects only through programs?

A. The Biba model
B. The Bell-LaPadula model
C. The Clark-Wilson model
D. The information flow model

Answer: C

Explanation:
 In the Clark-Wilson model, the subject no longer has direct access to objects but instead must access them through programs (well -formed transactions).
The Clark–Wilson integrity model provides a foundation for specifying and analyzing an integrity policy for a computing system.
The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. An integrity policy describes how the data items in the system should be kept valid from one state of the system to the next and specifies the capabilities of various principals in the system. The model defines enforcement rules and certification rules.
Clark–Wilson is more clearly applicable to business and industry processes in which the integrity of the information content is paramount at any level of classification.
Integrity goals of Clark–Wilson model:
Prevent unauthorized users from making modification (Only this one is addressed by the Biba model).
Separation of duties prevents authorized users from making improper modifications. Well formed transactions: maintain internal and external consistency i.e. it is a series of operations that are carried out to transfer the data from one consistent state to the other.
The following are incorrect answers:
The Biba model is incorrect. The Biba model is concerned with integrity and controls access to objects based on a comparison of the security level of the subject to that of the object.
The Bell-LaPdaula model is incorrect. The Bell-LaPaula model is concerned with confidentiality and controls access to objects based on a comparison of the clearence level of the subject to the classification level of the object.
The information flow model is incorrect. The information flow model uses a lattice where objects are labelled with security classes and information can flow either upward or at the
same level. It is similar in framework to the Bell-LaPadula model. References:
ISC2 Official Study Guide, Pages 325 - 327 AIO3, pp. 284 - 287
AIOv4 Security Architecture and Design (pages 338 - 342) AIOv5 Security Architecture and Design (pages 341 - 344) Wikipedia at:
https://en.wikipedia.org/wiki/Clark-Wilson_model

NEW QUESTION 140
- (Topic 1)
Which of the following security controls might force an operator into collusion with personnel assigned organizationally within a different function in order to gain access to unauthorized data?

A. Limiting the local access of operations personnel
B. Job rotation of operations personnel
C. Management monitoring of audit logs
D. Enforcing regular password changes

Answer: A

Explanation:
 The questions specifically said: "within a different function" which eliminate Job Rotation as a choice.
Management monitoring of audit logs is a detective control and it would not prevent collusion.
Changing passwords regularly would not prevent such attack.
This question validates if you understand the concept of separation of duties and least privilege. By having operators that have only the minimum access level they need and only what they need to do their duties within a company, the operations personnel would be force to use collusion to defeat those security mechanism.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION 143
- (Topic 1)
An attack initiated by an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization is known as a(n):

A. active attack
B. outside attack
C. inside attack
D. passive attack

Answer: C

Explanation:
 An inside attack is an attack initiated by an entity inside the security perimeter, an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization whereas an outside attack is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system. An active attack attempts to alter system resources to affect their operation and a passive attack attempts to learn or make use of the information from the system but does not affect system resources.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION 144
- (Topic 1)
The primary service provided by Kerberos is which of the following?

A. non-repudiation
B. confidentiality
C. authentication

D. authorization

Answer: C

Explanation:
 The Answer authentication. Kerberos is an authentication service. It can use single-factor or multi-factor authentication methods.
The following answers are incorrect:
non-repudiation. Since Kerberos deals primarily with symmetric cryptography, it does not help with non-repudiation.
confidentiality. Once the client is authenticated by Kerberos and obtains its session key and ticket, it may use them to assure confidentiality of its communication with a server; however, that is not a Kerberos service as such.
authorization. Although Kerberos tickets may include some authorization information, the meaning of the authorization fields is not standardized in the Kerberos specifications, and authorization is not a primary Kerberos service.
The following reference(s) were/was used to create this question:
ISC2 OIG,2007 p. 179-184
Shon Harris AIO v.3 152-155

NEW QUESTION 146
- (Topic 1)
What security model is dependent on security labels?

A. Discretionary access control
B. Label-based access control
C. Mandatory access control
D. Non-discretionary access control

Answer: C

Explanation:
 With mandatory access control (MAC), the authorization of a subject's access to an object is dependant upon labels, which indicate the subject's clearance, and the classification or sensitivity of the object. Label-based access control is not defined. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

NEW QUESTION 151
- (Topic 1)
Which of the following questions is less likely to help in assessing physical and environmental protection?

A. Are entry codes changed periodically?
B. Are appropriate fire suppression and prevention devices installed and working?
C. Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?
D. Is physical access to data transmission lines controlled?

Answer: C

Explanation:
 Physical security and environmental security are part of operational controls, and are measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. All the questions above are useful in assessing physical and environmental protection except for the one regarding processes that ensuring that unauthorized individuals cannot access information, which is more a production control.
Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self- Assessment Guide for Information Technology Systems, November 2001 (Pages A-21 to A-24).

NEW QUESTION 155
- (Topic 1)
Which of the following is NOT a form of detective administrative control?

A. Rotation of duties
B. Required vacations
C. Separation of duties
D. Security reviews and audits

Answer: C

Explanation:
 Detective administrative controls warn of administrative control violations. Rotation of duties, required vacations and security reviews and audits are forms of detective administrative controls. Separation of duties is the practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process, thus a preventive control rather than a detective control.
Source: DUPUIS, Cl?ment, Access Control Systems and Methodology CISSP Open Study Guide, version 1.0 (march 2002).

NEW QUESTION 158
- (Topic 2)
Related to information security, availability is the opposite of which of the following?

A. delegation
B. distribution
C. documentation
D. destruction

Answer: D

Explanation:

Availability is the opposite of "destruction."
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

NEW QUESTION 163
- (Topic 2)
The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system is referred to as?

A. Confidentiality
B. Availability
C. Integrity
D. Reliability

Answer: B

Explanation:
 An company security program must:
1) assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability;
2) protect informationcommensurate with the level of risk and magnitude ofharmresulting fromloss, misuse, unauthorized access, or modification.
The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them.
The following are incorrect answers:
Confidentiality - The information requires protection from unauthorized disclosure and only the INTENDED recipient should have access to the meaning of the data either in storage or in transit.
Integrity - The information must be protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to:
Authenticity –A third party must be able to verify that the content of a message has not been changed in transit.
Non-repudiation – The origin or the receipt of a specific message must be verifiable by a third party.
Accountability - A security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
Reference used for this question:
RFC 2828
and
SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (page 5).

NEW QUESTION 168
- (Topic 2)
Which of the following should NOT be performed by an operator?

A. Implementing the initial program load
B. Monitoring execution of the system
C. Data entry
D. Controlling job flow

Answer: C

Explanation:
 Under the principle of separation of duties, an operator should not be performing data entry. This should be left to data entry personnel.
System operators represent a class of users typically found in data center environments where mainframe systems are used. They provide day-to-day operations of the mainframe environment, ensuring that scheduled jobs are running effectively and troubleshooting problems that may arise. They also act as the arms and legs of the mainframe environment, load and unloading tape and results of job print runs. Operators have elevated privileges, but less than those of system administrators. If misused, these privileges may be used to circumvent the system's security policy. As such, use of these
privileges should be monitored through audit logs.
Some of the privileges and responsibilities assigned to operators include:
Implementing the initial program load: This is used to start the operating system. The boot process or initial program load of a system is a critical time for ensuring system security. Interruptions to this process may reduce the integrity of the system or cause the system to crash, precluding its availability.
Monitoring execution of the system: Operators respond to various events, to include errors, interruptions, and job completion messages.
Volume mounting: This allows the desired application access to the system and its data. Controlling job flow: Operators can initiate, pause, or terminate programs. This may allow
an operator to affect the scheduling of jobs. Controlling job flow involves the manipulation
of configuration information needed by the system. Operators with the ability to control a job or application can cause output to be altered or diverted, which can threaten the confidentiality.
Bypass label processing: This allows the operator to bypass security label information to run foreign tapes (foreign tapes are those from a different data center that would not be using the same label format that the system could run). This privilege should be strictly controlled to prevent unauthorized access.
Renaming and relabeling resources: This is sometimes necessary in the mainframe environment to allow programs to properly execute. Use of this privilege should be monitored, as it can allow the unauthorized viewing of sensitive information.
Reassignment of ports and lines: Operators are allowed to reassign ports or lines. If misused, reassignment can cause program errors, such as sending sensitive output to an unsecured location. Furthermore, an incidental port may be opened, subjecting the system to an attack through the creation of a new entry point into the system.
Reference(s) 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 19367-19395). Auerbach Publications. Kindle Edition.

NEW QUESTION 173
- (Topic 2)
When considering an IT System Development Life-cycle, security should be:

A. Mostly considered during the initiation phase.
B. Mostly considered during the development phase.
C. Treated as an integral part of the overall system design.
D. Added once the design is completed.

Answer: C

Explanation:

Security must be considered in information system design. Experience has shown it is very difficult to implement security measures properly and successfully after a system has been developed, so it should be integrated fully into the system life-cycle process. This includes establishing security policies, understanding the resulting security requirements, participating in the evaluation of security products, and finally in the engineering, design, implementation, and disposal of the system.

Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page 7).

NEW QUESTION 176
- (Topic 2)
Ensuring least privilege does not require:

A. Identifying what the user's job is.
B. Ensuring that the user alone does not have sufficient rights to subvert an important process.
C. Determining the minimum set of privileges required for a user to perform their duties.
D. Restricting the user to required privileges and nothing more.

Answer: B

Explanation:

Ensuring that the user alone does not have sufficient rights to subvert an important process is a concern of the separation of duties principle and it does not concern the least privilege principle.
Source: DUPUIS, Clément, Access Control Systems and Methodology CISSP Open Study
Guide, version 1.0, march 2002 (page 33).

NEW QUESTION 177
- (Topic 2)
Who is ultimately responsible for the security of computer based information systems within an organization?

A. The tech support team
B. The Operation Team.
C. The management team.
D. The training team.

Answer: C

Explanation:

If there is no support by management to implement, execute, and enforce security policies and procedure, then they won't work. Senior management must be involved in this because they have an obligation to the organization to protect the assests . The requirement here is for management to show "due diligence" in establishing an effective compliance, or security program.
The following answers are incorrect:
The tech support team. Is incorrect because the ultimate responsibility is with management for the security of computer-based information systems.
The Operation Team. Is incorrect because the ultimate responsibility is with management for the security of computer-based information systems.
The Training Team. Is incorrect because the ultimate responsibility is with management for the security of computer-based information systems.
Reference(s) used for this question:
OIG CBK Information Security Management and Risk Management (page 20 - 22)

NEW QUESTION 180
- (Topic 2)
Risk analysis is MOST useful when applied during which phase of the system development process?

A. Project initiation and Planning
B. Functional Requirements definition
C. System Design Specification
D. Development and Implementation

Answer: A

Explanation:

In most projects the conditions for failure are established at the beginning of the project. Thus risk management should be established at the commencement of the project with a risk assessment during project initiation.
As it is clearly stated in the ISC2 book: Security should be included at the first phase of development and throughout all of the phases of the system development life cycle. This is a key concept to understand for the purpose for the exam.
The most useful time is to undertake it at project initiation, although it is often valuable to update the current risk analysis at later stages.
Attempting to retrofit security after the SDLC is completed would cost a lot more money and might be impossible in some cases. Look at the family of browsers we use today, for the past 8 years they always claim that it is the most secure version that has been released and within days vulnerabilities will be found.
Risks should be monitored throughout the SDLC of the project and reassessed when appropriate.
The phases of the SDLC can very from one source to another one. It could be as simple as Concept, Design, and Implementation. It could also be expanded to include more phases such as this list proposed within the ISC2 Official Study book:
Project Initiation and Planning Functional Requirements Definition System Design Specification Development and Implementation
Documentations and Common Program Controls
Testing and Evaluation Control, certification and accreditation (C&A) Transition to production (Implementation)
And there are two phases that will extend beyond the SDLC, they are: Operation and Maintenance Support (O&M)
Revisions and System Replacement (Disposal)
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 291).
and
The Official ISC2 Guide to the CISSP CBK , Second Edition, Page 182-185

NEW QUESTION 183
- (Topic 2)
Which of the following is an advantage of prototyping?

A. Prototype systems can provide significant time and cost savings.
B. Change control is often less complicated with prototype systems.
C. It ensures that functions or extras are not added to the intended system.
D. Strong internal controls are easier to implement.

Answer: A

Explanation:
Prototype systems can provide significant time and cost savings, however they also have several disadvantages. They often have poor internal controls, change control becomes much more complicated and it often leads to functions or extras being added to the system that were not originally intended.
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 306).

NEW QUESTION 188
- (Topic 2)
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.

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)

NEW QUESTION 193
- (Topic 2)
Which of the following is most concerned with personnel security?

A. Management controls
B. Operational controls
C. Technical controls
D. Human resources controls

Answer: B

Explanation:
Many important issues in computer security involve human users, designers, implementers, and managers.
A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs. Since operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems), personnel security is considered a form of operational control.
Operational controls are put in place to improve security of a particular system (or group of systems). They often require specialized expertise and often rely upon management activities as well as technical controls. Implementing dual control and making sure that you have more than one person that can perform a task would fall into this category as well.
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.
Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access of misuse, facilitate detection of security violations, and support security requirements for applications and data.
Reference use for this question:
NIST SP 800-53 Revision 4 http://dx.doi.org/10.6028/NIST.SP.800-53r4 You can get it as a word document by clicking HERE
NIST SP 800-53 Revision 4 has superseded the document below:
SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Page A-18).

NEW QUESTION 196
- (Topic 2)
Which of the following is NOT a basic component of security architecture?

A. Motherboard
B. Central Processing Unit (CPU
C. Storage Devices
D. Peripherals (input/output devices)

Answer: A

Explanation:
The CPU, storage devices and peripherals each have specialized roles in the security archecture. The CPU, or microprocessor, is the brains behind a computer system and performs calculations as it solves problemes and performs system tasks. Storage devices provide both long- and short-term stoarge of information that the CPU has either processed or may process. Peripherals (scanners, printers, modems, etc) are devices that either input datra or receive the data output by the CPU.
The motherboard is the main circuit board of a microcomputer and contains the connectors for attaching additional boards. Typically, the motherboard contains the CPU, BIOS, memory, mass storage interfaces, serial and parallel ports, expansion slots, and all the controllers required to control standard peripheral devices.
Reference(s) used for this question:
TIPTON, Harold F., The Official (ISC)2 Guide to the CISSP CBK (2007), page 308.

NEW QUESTION 200
- (Topic 2)
What can be defined as: It confirms that users' needs have been met by the supplied solution ?

A. Accreditation
B. Certification
C. Assurance
D. Acceptance

Answer: D

Explanation:
Acceptance confirms that users' needs have been met by the supplied solution. Verification and Validation informs Acceptance by establishing the evidence – set against acceptance criteria - to determine if the solution meets the users' needs. Acceptance should also explicitly address any integration or interoperability requirements involving other equipment or systems. To enable acceptance every user and system requirement must have a 'testable' characteristic.
Accreditation is the formal acceptance of security, adequacy, authorization for operation and acceptance of existing risk. Accreditation is the formal declaration by a Designated Approving Authority (DAA) that an IS is approved to operate in a particular security mode using a prescribed set of safeguards to an acceptable level of risk.
Certification is the formal testing of security safeguards and assurance is the degree of confidence that the implemented security measures work as intended. The certification is a Comprehensive evaluation of the technical and nontechnical security features of an IS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified ecurity requirements.
Assurance is the descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality. For example, an evaluation may require that all source code is kept in a change management system, or that full functional testing is performed. The Common Criteria provides a catalogue of these, and the requirements may vary from one evaluation to the next. The requirements for particular targets or types of products are documented in the Security Targets (ST) and Protection Profiles (PP), respectively.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 4, August 1999.
and
Official ISC2 Guide to the CISSP CBK, Second Edition, on page 211. and
http://www.aof.mod.uk/aofcontent/tactical/randa/content/randaintroduction.htm

NEW QUESTION 204
- (Topic 2)
Which of the following best corresponds to the type of memory addressing where the address location that is specified in the program instruction contains the address of the final desired location?

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

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).

NEW QUESTION 205
- (Topic 2)
What can best be defined as high-level statements, beliefs, goals and objectives?

A. Standards
B. Policies
C. Guidelines
D. Procedures

Answer: B

Explanation:
Policies are high-level statements, beliefs, goals and objectives and the general means for their attainment for a specific subject area. Standards are mandatory activities, action, rules or regulations designed to provide policies with the support structure and specific direction they require to be effective. Guidelines are more general statements of how to achieve the policies objectives by providing a framework within which to implement procedures. Procedures spell out the specific steps of how the policy and supporting standards and how guidelines will be implemented.
Source: HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.

NEW QUESTION 207

- (Topic 2)
A channel within a computer system or network that is designed for the authorized transfer of information is identified as a(n)?

A. Covert channel
B. Overt channel
C. Opened channel
D. Closed channel

Answer: B

Explanation:
 An overt channel is a path within a computer system or network that is designed for the authorized transfer of data. The opposite would be a covert channel which is an unauthorized path.
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.
All of the other choices are bogus detractors. Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten
Domains of Computer Security, 2001, John Wiley & Sons, Page 219. and
Shon Harris, CISSP All In One (AIO), 6th Edition , page 380 and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 378). McGraw- Hill. Kindle Edition.

NEW QUESTION 212
- (Topic 2)
Which of the following is NOT a common integrity goal?

A. Prevent unauthorized users from making modifications.
B. Maintain internal and external consistency.
C. Prevent authorized users from making improper modifications.
D. Prevent paths that could lead to inappropriate disclosure.

Answer: D

Explanation:
 Inappropriate disclosure is a confidentiality, not an integrity goal.
All of the other choices above are integrity goals addressed by the Clark-Wilson integrity model.
The Clark-Wilson model is an integrity model that addresses all three integrity goals:
* 1. prevent unauthorized users from making modifications,
* 2. prevent authorized users from making improper modifications, and
* 3. maintain internal and external consistency through auditing. NOTE: Biba address only the first goal of integrity above
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 1384). McGraw- Hill. Kindle Edition.

NEW QUESTION 213
- (Topic 2)
What prevents a process from accessing another process' data?

A. Memory segmentation
B. Process isolation
C. The reference monitor
D. Data hiding

Answer: B

Explanation:
 Process isolation is where each process has its own distinct address space for its application code and data. In this way, it is possible to prevent each process from accessing another process' data. This prevents data leakage, or modification to the data while it is in memory. Memory segmentation is a virtual memory management mechanism. The reference monitor is an abstract machine that mediates all accesses to objects by subjects. Data hiding, also known as information hiding, is a mechanism that makes information available at one processing level is not available at another level.
Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

NEW QUESTION 218
- (Topic 2)
Which of the following is the act of performing tests and evaluations to test a system's security level to see if it complies with the design specifications and security requirements?

A. Validation
B. Verification
C. Assessment
D. Accuracy

Answer: B

Explanation:
 Verification vs. Validation:
Verification determines if the product accurately represents and meets the specifications. A product can be developed that does not match the original specifications. This step ensures that the specifications are properly met.
Validation determines if the product provides the necessary solution intended real-world problem. In large projects, it is easy to lose sight of overall goal. This exercise ensures that the main goal of the project is met.
From DITSCAP:

* 6.3.2. Phase 2, Verification. The Verification phase shall include activities to verify compliance of the system with previously agreed security requirements. For each life-cycle development activity, DoD Directive 5000.1 (reference (i)), there is a corresponding set of security activities, enclosure 3, that shall verify compliance with the security requirements and evaluate vulnerabilities.

* 6.3.3. Phase 3, Validation. The Validation phase shall include activities to evaluate the fully integrated system to validate system operation in a specified computing environment with an acceptable level of residual risk. Validation shall culminate in an approval to operate.

You must also be familiar with Verification and Validation for the purpose of the exam. A simple definition for Verification would be whether or not the developers followed the design specifications along with the security requirements. A simple definition for Validation would be whether or not the final product meets the end user needs and can be use for a specific purpose.

Wikipedia has an informal description that is currently written as: Validation can be expressed by the query "Are you building the right thing?" and Verification by "Are you building it right?

NOTE:

DITSCAP was replaced by DIACAP some time ago (2007). While DITSCAP had defined both a verification and a validation phase, the DIACAP only has a validation phase. It may not make a difference in the answer for the exam; however, DIACAP is the cornerstone policy of DOD C&A and IA efforts today. Be familiar with both terms just in case all of a sudden the exam becomes updated with the new term.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 1106). McGraw- Hill. Kindle Edition.

http://iase.disa.mil/ditscap/DITSCAP.html https://en.wikipedia.org/wiki/Verification_and_validation For the definition of "validation" in DIACAP, Click Here Further sources for the phases in DIACAP, Click Here

NEW QUESTION 223
- (Topic 2)
Who is responsible for implementing user clearances in computer-based information systems at the B3 level of the TCSEC rating ?

A. Security administrators
B. Operators
C. Data owners
D. Data custodians

Answer: A

Explanation:
Security administrator functions include user-oriented activities such as setting user clearances, setting initial password, setting other security characteristics for new users or changing security profiles for existing users. Data owners have the ultimate responsibility for protecting data, thus determining proper user access rights to data. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION 227
- (Topic 2)
What is the appropriate role of the security analyst in the application system development or acquisition project?

A. policeman
B. control evaluator & consultant
C. data owner
D. application user

Answer: B

Explanation:
The correct answer is "control evaluator & consultant". During any system development or acquisition, the security staff should evaluate security controls and advise (or consult) on the strengths and weaknesses with those responsible for making the final decisions on the project.

The other answers are not correct because:

policeman - It is never a good idea for the security staff to be placed into this type of role (though it is sometimes unavoidable). During system development or acquisition, there should be no need of anyone filling the role of policeman.

data owner - In this case, the data owner would be the person asking for the new system to manage, control, and secure information they are responsible for. While it is possible the security staff could also be the data owner for such a project if they happen to have responsibility for the information, it is also possible someone else would fill this role. Therefore, the best answer remains "control evaluator & consultant".

application user - Again, it is possible this could be the security staff, but it could also be many other people or groups. So this is not the best answer.

Reference:

Official ISC2 Guide page: 555 - 560

All in One Third Edition page: 832 - 846

NEW QUESTION 229
- (Topic 2)
Which of the following describes a computer processing architecture in which a language compiler or pre-processor breaks program instructions down into basic operations that can be performed by the processor at the same time?

A. Very-Long Instruction-Word Processor (VLIW)
B. Complex-Instruction-Set-Computer (CISC)
C. Reduced-Instruction-Set-Computer (RISC)
D. Super Scalar Processor Architecture (SCPA)

Answer: A

Explanation:
Very long instruction word (VLIW) describes a computer processing architecture in which a language compiler or pre-processor breaks program instruction down into basic operations that can be performed by the processor in parallel (that is, at the same time). These operations are put into a very long instruction word which the processor can then take apart without further analysis, handing each operation to an appropriate functional unit.

The following answer are incorrect:

The term "CISC" (complex instruction set computer or computing) refers to computers designed with a full set of computer instructions that were intended to provide needed capabilities in the most efficient way. Later, it was discovered that, by reducing the full set to only the most frequently used instructions, the computer would get more work done in a shorter amount of time for most applications. Intel's Pentium microprocessors are CISC microprocessors.

The PowerPC microprocessor, used in IBM's RISC System/6000 workstation and Macintosh computers, is a RISC microprocessor. RISC takes each of the longer, more complex instructions from a CISC design and reduces it to multiple instructions that are shorter and faster to process. RISC technology has been a staple of mobile devices for decades, but it is now finally poised to take on a serious role in data center servers and server virtualization. The latest RISC processors support virtualization and will change the way computing resources scale to meet workload demands.

A superscalar CPU architecture implements a form of parallelism called instruction level parallelism within a single processor. It therefore allows faster CPU throughput than would otherwise be possible at a given clock rate. A superscalar processor executes more than one instruction during a clock cycle by simultaneously dispatching multiple instructions to redundant functional units on the processor. Each functional unit is not a separate CPU core but an execution resource within a single CPU such as an arithmetic logic unit, a bit shifter, or a multiplier.

Reference(s) Used for this question: http://whatis.techtarget.com/definition/0,,sid9_gci214395,00.html
and
http://searchcio-midmarket.techtarget.com/definition/CISC and
http://en.wikipedia.org/wiki/Superscalar

NEW QUESTION 231
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SSCP Practice Exam Features:

* SSCP Questions and Answers Updated Frequently

* SSCP Practice Questions Verified by Expert Senior Certified Staff

* SSCP Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SSCP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The SSCP Practice Test Here