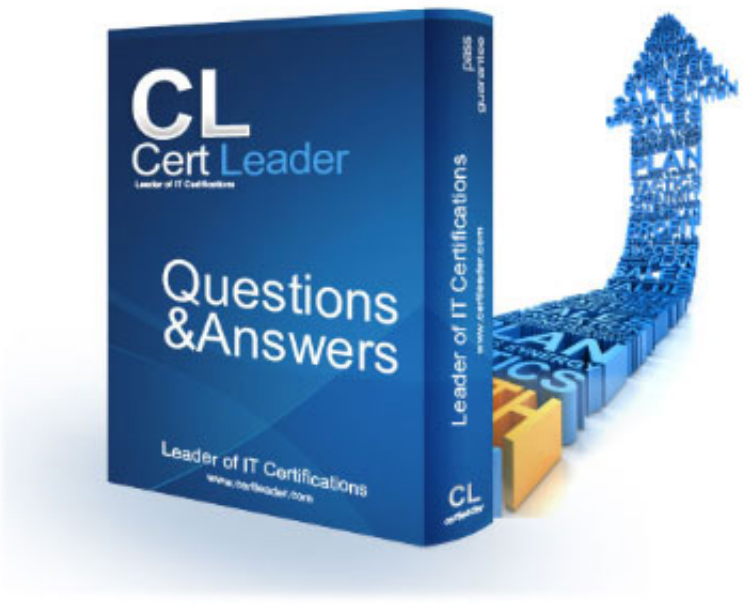
SSCP Dumps

System Security Certified Practitioner (SSCP)

https://www.certleader.com/SSCP-dumps.html



NEW QUESTION 1
- (Topic 1)
A potential problem related to the physical installation of the Iris Scanner in regards to the usage of the iris pattern within a biometric system is:

A. concern that the laser beam may cause eye damage
B. the iris pattern changes as a person grows older.
C. there is a relatively high rate of false accepts.
D. the optical unit must be positioned so that the sun does not shine into the aperture.

Answer: D

Explanation:
Because the optical unit utilizes a camera and infrared light to create the images, sun light can impact the aperture so it must not be positioned in direct light of any type. Because the subject does not need to have direct contact with the optical reader, direct light can impact the reader.
An Iris recognition is a form of biometrics that is based on the uniqueness of a subject's iris. A camera like device records the patterns of the iris creating what is known as Iriscode.
It is the unique patterns of the iris that allow it to be one of the most accurate forms of biometric identification of an individual. Unlike other types of biometics, the iris rarely changes over time. Fingerprints can change over time due to scaring and manual labor, voice patterns can change due to a variety of causes, hand geometry can also change as well. But barring surgery or an accident it is not usual for an iris to change. The subject has a high-resoulution image taken of their iris and this is then converted to Iriscode. The current standard for the Iriscode was developed by John Daugman. When the subject attempts to be authenticated an infrared light is used to capture the iris image and this image is then compared to the Iriscode. If there is a match the subject's identity is confirmed. The subject does not need to have direct contact with the optical reader so it is a less invasive means of authentication then retinal scanning would be.
Reference(s) used for this question: AIO, 3rd edition, Access Control, p 134. AIO, 4th edition, Access Control, p 182.
Wikipedia - http://en.wikipedia.org/wiki/Iris_recognition The following answers are incorrect:
concern that the laser beam may cause eye damage. The optical readers do not use laser so, concern that the laser beam may cause eye damage is not an issue.
the iris pattern changes as a person grows older. The question asked about the physical installation of the scanner, so this was not the best answer. If the question would have been about long term problems then it could have been the best choice. Recent research has shown that Irises actually do change over time:
http://www.nature.com/news/ageing- eyes-hinder-biometric-scans-1.10722
there is a relatively high rate of false accepts. Since the advent of the Iriscode there is a very low rate of false accepts, in fact the algorithm used has never had a false match. This all depends on the quality of the equipment used but because of the uniqueness of the iris even when comparing identical twins, iris patterns are unique.

NEW QUESTION 2
- (Topic 1)
Which of following is not a service provided by AAA servers (Radius, TACACS and DIAMETER)?

A. Authentication
B. Administration
C. Accounting
D. Authorization

Answer: B

Explanation:
Radius, TACACS and DIAMETER are classified as authentication, authorization, and accounting (AAA) servers.
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 33.
also see:
The term "AAA" is often used, describing cornerstone concepts [of the AIC triad] Authentication, Authorization, and Accountability. Left out of the AAA acronym is Identification which is required before the three "A's" can follow. Identity is a claim, Authentication proves an identity, Authorization describes the action you can perform on a system once you have been identified and authenticated, and accountability holds users accountable for their actions.
Reference: CISSP Study Guide, Conrad Misenar, Feldman p. 10-11, (c) 2010 Elsevier.

NEW QUESTION 3
- (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 4
- (Topic 1)
In the Bell-LaPadula model, the Star-property is also called:

A. The simple security property
B. The confidentiality property

C. The confinement property
D. The tranquility property

Answer: B

Explanation:
The Bell-LaPadula model focuses on data confidentiality and access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity.
In this formal model, the entities in an information system are divided into subjects and objects.
The notion of a "secure state" is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby proving that the system satisfies the security objectives of the model.
The Bell-LaPadula model is built on the concept of a state machine with a set of allowable states in a system. The transition from one state to another state is defined by transition functions.
A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a security policy.
To determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object (more precisely, to the combination of classification and set of compartments, making up the security level) to determine if the subject is authorized for the specific access mode.
The clearance/classification scheme is expressed in terms of a lattice. The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties:
The Simple Security Property - a subject at a given security level may not read an object at a higher security level (no read-up).
The property (read "star"-property) - a subject at a given security level must not write to any object at a lower security level (no write-down). The property is also known as the Confinement property.
The Discretionary Security Property - use an access control matrix to specify the discretionary access control.
The transfer of information from a high-sensitivity document to a lower-sensitivity document may happen in the Bell-LaPadula model via the concept of trusted subjects. Trusted Subjects are not restricted by the property. Untrusted subjects are.
Trusted Subjects must be shown to be trustworthy with regard to the security policy. This security model is directed toward access control and is characterized by the phrase: "no read up, no write down." Compare the Biba model, the Clark-Wilson model and the Chinese Wall.
With Bell-LaPadula, users can create content only at or above their own security level (i.e. secret researchers can create secret or top-secret files but may not create public files; no write-down). Conversely, users can view content only at or below their own security level
(i.e. secret researchers can view public or secret files, but may not view top-secret files; no read-up).
Strong Property
The Strong Property is an alternative to the Property in which subjects may write to objects with only a matching security level. Thus, the write-up operation permitted in the usual Property is not present, only a write-to-same level operation. The Strong Property is usually discussed in the context of multilevel database management systems and is motivated by integrity concerns.
Tranquility principle
The tranquility principle of the Bell-LaPadula model states that the classification of a subject or object does not change while it is being referenced. There are two forms to the tranquility principle: the "principle of strong tranquility" states that security levels do not change during the normal operation of the system and the "principle of weak tranquility" states that security levels do not change in a way that violates the rules of a given security policy.
Another interpretation of the tranquility principles is that they both apply only to the period of time during which an operation involving an object or subject is occurring. That is, the strong tranquility principle means that an object's security level/label will not change during an operation (such as read or write); the weak tranquility principle means that an object's security level/label may change in a way that does not violate the security policy during an operation.
Reference(s) used for this question: http://en.wikipedia.org/wiki/Biba_Model
http://en.wikipedia.org/wiki/Mandatory_access_control http://en.wikipedia.org/wiki/Discretionary_access_control http://en.wikipedia.org/wiki/Clark-Wilson_model
http://en.wikipedia.org/wiki/Brewer_and_Nash_model

NEW QUESTION 5
- (Topic 1)
In which of the following model are Subjects and Objects identified and the permissions applied to each subject/object combination are specified. Such a model can be used to quickly summarize what permissions a subject has for various system objects.

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

Answer: A

Explanation:
An access control matrix is a table of subjects and objects indicating what actions individual subjects can take upon individual objects. Matrices are data structures that programmers implement as table lookups that will be used and enforced by the operating system.
This type of access control is usually an attribute of DAC models. The access rights can be assigned directly to the subjects (capabilities) or to the objects (ACLs).
Capability Table
A capability table specifies the access rights a certain subject possesses pertaining to specific objects. A capability table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL.
Access control lists (ACLs)
ACLs are used in several operating systems, applications, and router configurations. They are lists of subjects that are authorized to access a specific object, and they define what level of authorization is granted. Authorization can be specific to an individual, group, or role. ACLs map values from the access control matrix to the object.
Whereas a capability corresponds to a row in the access control matrix, the ACL corresponds to a column of the matrix.
NOTE: Ensure you are familiar with the terms Capability and ACLs for the purpose of the exam.
Resource(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 5264-5267). McGraw-Hill. Kindle Edition.
or
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Page 229 and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1923-1925). Auerbach Publications. Kindle Edition.

NEW QUESTION 6
- (Topic 1)
Which of the following questions is less likely to help in assessing identification and authentication controls?

A. Is a current list maintained and approved of authorized users and their access?

B. Are passwords changed at least every ninety days or earlier if needed?
C. Are inactive user identifications disabled after a specified period of time?
D. Is there a process for reporting incidents?

Answer: D

Explanation:
Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. Reporting incidents is more related to incident response capability (operational control) than to identification and authentication (technical control).
Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self- Assessment Guide for Information Technology Systems, November 2001 (Pages A-30 to A-32).

NEW QUESTION 7
- (Topic 1)
Which of the following can best eliminate dial-up access through a Remote Access Server as a hacking vector?

A. Using a TACACS+ server.
B. Installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall.
C. Setting modem ring count to at least 5.
D. Only attaching modems to non-networked hosts.

Answer: B

Explanation:
Containing the dial-up problem is conceptually easy: by installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall, any access to internal resources through the RAS can be filtered as would any other connection coming from the Internet.
The use of a TACACS+ Server by itself cannot eliminate hacking.
Setting a modem ring count to 5 may help in defeating war-dialing hackers who look for modem by dialing long series of numbers.
Attaching modems only to non-networked hosts is not practical and would not prevent these hosts from being hacked.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 2: Hackers.

NEW QUESTION 8
- (Topic 1)
Which of the following biometric devices has the lowest user acceptance level?

A. Retina Scan
B. Fingerprint scan
C. Hand geometry
D. Signature recognition

Answer: A

Explanation:
According to the cited reference, of the given options, the Retina scan has the lowest user acceptance level as it is needed for the user to get his eye close to a device and it is not user friendly and very intrusive.
However, retina scan is the most precise with about one error per 10 millions usage. Look at the 2 tables below. If necessary right click on the image and save it on your
desktop for a larger view or visit the web site directly at
https://sites.google.com/site/biometricsecuritysolutions/crossover-accuracy . Biometric Comparison Chart

BIOMETRICS COMPARISON CHART

Biometric	Verify	ID	Accuracy	Reliability	Error Rate	Errors	False Pos.	False Neg.
Fingerprint	Yes	Yes	Very High	High	1 in 500+	dryness, dirt, age	Ext. Diff.	Ext. Diff.
Facial Recognition	Yes	No	High	Medium	no data	lighting, age, glasses, hair	Difficult	Easy
Hand Geometry	Yes	No	High	Medium	1 in 500	hand injury, age	Very Diff.	Medium
Speaker Recognition	Yes	No	Medium	Low	1 in 50	noise, weather, colds	Medium	Easy
Iris Scan	Yes	Yes	Very High	High	1 in 131,000	poor lighting	Very Diff.	Very Diff.
Retinal Scan	Yes	Yes	Very High	High	1 in 10,000,000	glasses	Ext. Diff.	Ext. Diff.
Signature Recognition	Yes	No	Medium	Low	1 in 50	changing signatures	Medium	Easy
Keystroke Recognition	Yes	No	Low	Low	no data	hand injury, tiredness	Difficult	Easy
DNA	Yes	Yes	Very High	High	no data	none	Ext. Diff.	Ext. Diff.

Biometric	Security Level	Long-term Stability	User Acceptance	Intrusive	Ease of Use	Low Cost	Hardware	Standards
Fingerprint	High	High	Medium	Somewhat	High	Yes	Special, cheap	Yes
Facial Recognition	Medium	Medium	Medium	Non	Medium	Yes	Common, cheap	?
Hand Geometry	Medium	Medium	Medium	Non	High	No	Special, mid-price	?
Speaker Recognition	Medium	Medium	High	Non	High	Yes	Common, cheap	?
Iris Scan	High	High	Medium	Non	Medium	No	Special, expensive	?
Retinal Scan	High	High	Medium	Very	Low	No	Special, expensive	?
Signature Recognition	Medium	Medium	Medium	Non	High	Yes	Special, mid-price	?
Keystroke Recognition	Medium	Low	High	Non	High	Yes	Common, cheap	?
DNA	High	High	Low	Extremely	Low	No	Special, expensive	Yes

C:\Users\MCS\Desktop\1.jpg

Aspect descriptions

Verify	Whether or not the Biometric is capable of verification. Verification is the process where an input is compared to specific data previously recorded from the user to see if the person is who they claim to be
ID	Whether or not the Biometric is capable of identification. Identification is the process where an input is compared to a large data set previously recorded from many peoplelo see which person the user is.
Accuracy	How well the Biometric is able to tell individuals apart. This is partially determined by the amount of information gathered as well as the number of possible different data results.
Reliability	How dependable the Biometric is for recognition purposes.
Error Rate	This is calculated as the crossing point when graphed of false positives and false negtives created using this Biometric.
Errors	Typical causes of errors for this Biometric.
False Pos.	How easy it is to create a false positive reading with this biometric (someone is able to impersonate someone else)
False Neg.	How easy it is to create a false negative reading with this biometric (someone is able to avoid identification as oneself)
Security Level	The highest level of security that this Biometric is capable of working at.
Long-term Stability	How well this Biometric continues to work without data updates over long periods of time.
User Acceptance	How willing the public is to use this Biometric.
Intrusiveness	How much the Biometric is considered to invade one's privacy or require interaction by the user.
Ease of Use	How easy this Biometric is for both the user and the personnel involved.
Low Cost	Whether or not there is a low cost option for this Biometric to be used.
Hardware	Type and cost of hardware required to use this Biometric.
Standards	Whether or not standards exist for this Biometric.

C:\Users\MCS\Desktop\1.jpg
Biometric Aspect Descriptions Reference(s) used for this question:
RHODES, Keith A., Chief Technologist, United States General Accounting Office, National Preparedness, Technologies to Secure Federal Buildings, April 2002

(page 10).
and
https://sites.google.com/site/biometricsecuritysolutions/crossover-accuracy

NEW QUESTION 9
- (Topic 1)
Which of the following would assist the most in Host Based intrusion detection?

A. audit trails.
B. access control lists.
C. security clearances.
D. host-based authentication.

Answer: A

Explanation:
To assist in Intrusion Detection you would review audit logs for access violations.
The following answers are incorrect:
access control lists. This is incorrect because access control lists determine who has access to what but do not detect intrusions.
security clearances. This is incorrect because security clearances determine who has access to what but do not detect intrusions.
host-based authentication. This is incorrect because host-based authentication determine who have been authenticated to the system but do not dectect intrusions.

NEW QUESTION 10
- (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 10
- (Topic 1)
Which security model is based on the military classification of data and people with clearances?

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

Answer: C

Explanation:
The Bell-LaPadula model is a confidentiality model for information security based on the military classification of data, on people with clearances and data with a classification or sensitivity model. The Biba, Clark-Wilson and Brewer-Nash models are concerned with integrity.
Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

NEW QUESTION 13
- (Topic 1)
Which of the following is the most reliable authentication method for remote access?

A. Variable callback system
B. Synchronous token
C. Fixed callback system
D. Combination of callback and caller ID

Answer: B

Explanation:
A Synchronous token generates a one-time password that is only valid for a short period of time. Once the password is used it is no longer valid, and it expires if

not entered in the acceptable time frame.
The following answers are incorrect:
Variable callback system. Although variable callback systems are more flexible than fixed callback systems, the system assumes the identity of the individual unless two-factor authentication is also implemented. By itself, this method might allow an attacker access as a trusted user.
Fixed callback system. Authentication provides assurance that someone or something is who or what he/it is supposed to be. Callback systems authenticate a person, but anyone can pretend to be that person. They are tied to a specific place and phone number, which can be spoofed by implementing call-forwarding.
Combination of callback and Caller ID. The caller ID and callback functionality provides greater confidence and auditability of the caller's identity. By disconnecting and calling back only authorized phone numbers, the system has a greater confidence in the location of the call. However, unless combined with strong authentication, any individual at the location could obtain access.
The following reference(s) were/was used to create this question: Shon Harris AIO v3 p. 140, 548
ISC2 OIG 2007 p. 152-153, 126-127

NEW QUESTION 14
- (Topic 1)
What is the main objective of proper separation of duties?

A. To prevent employees from disclosing sensitive information.
B. To ensure access controls are in place.
C. To ensure that no single individual can compromise a system.
D. To ensure that audit trails are not tampered with.

Answer: C

Explanation:
The primary objective of proper separation of duties is to ensure that one person acting alone cannot compromise the company's security in any way. A proper separation of duties does not prevent employees from disclosing information, nor does it ensure that access controls are in place or that audit trails are not tampered with. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, Chapter 12: Operations Security (Page 808).

NEW QUESTION 15
- (Topic 1)
Which of the following is not a physical control for physical security?

A. lighting
B. fences
C. training
D. facility construction materials

Answer: C

Explanation:
Some physical controls include fences, lights, locks, and facility construction materials. Some administrative controls include facility selection and construction, facility management, personnel controls, training, and emergency response and procedures.
From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 3rd. Ed., Chapter 6, page 403.

NEW QUESTION 20
- (Topic 1)
Which of the following control pairings include: organizational policies and procedures, pre- employment background checks, strict hiring practices, employment agreements, employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks?

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

Answer: A

Explanation:
The Answer: Preventive/Administrative Pairing: These mechanisms include organizational policies and procedures, pre-employment background checks, strict hiring practices, employment agreements, friendly and unfriendly employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION 23
- (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 28
- (Topic 1)
Which of the following statements pertaining to access control is false?

A. Users should only access data on a need-to-know basis.
B. If access is not explicitly denied, it should be implicitly allowed.
C. Access rights should be granted based on the level of trust a company has on a subject.
D. Roles can be an efficient way to assign rights to a type of user who performs certain tasks.

Answer: B

Explanation:
Access control mechanisms should default to no access to provide the necessary level of security and ensure that no security holes go unnoticed. If access is not explicitly allowed, it should be implicitly denied.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, Chapter 4: Access Control (page 143).

NEW QUESTION 30
- (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 35
- (Topic 1)
Which of the following floors would be most appropriate to locate information processing facilities in a 6-stories building?

A. Basement
B. Ground floor
C. Third floor
D. Sixth floor

Answer: C

Explanation:
You data center should be located in the middle of the facility or the core of a building to provide protection from natural disasters or bombs and provide easier access to emergency crewmembers if necessary. By being at the core of the facility the external wall would act as a secondary layer of protection as well.
Information processing facilities should not be located on the top floors of buildings in case of a fire or flooding coming from the roof. Many crimes and theft have also been conducted by simply cutting a large hole on the roof.
They should not be in the basement because of flooding where water has a natural tendancy to flow down :-) Even a little amount of water would affect your operation

considering the quantity of electrical cabling sitting directly on the cement floor under under your raise floor.
The data center should not be located on the first floor due to the presence of the main entrance where people are coming in and out. You have a lot of high traffic areas such as the elevators, the loading docks, cafeteria, coffee shopt, etc.. Really a bad location for a data center.
So it was easy to come up with the answer by using the process of elimination where the top, the bottom, and the basement are all bad choices. That left you with only one possible answer which is the third floor.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 5th Edition, Page 425.

NEW QUESTION 39
- (Topic 1)
This baseline sets certain thresholds for specific errors or mistakes allowed and the amount of these occurrences that can take place before it is considered suspicious?

A. Checkpoint level
B. Ceiling level
C. Clipping level
D. Threshold level

Answer: C

Explanation:
Organizations usually forgive a particular type, number, or pattern of violations, thus permitting a predetermined number of user errors before gathering this data for analysis. An organization attempting to track all violations, without sophisticated statistical computing ability, would be unable to manage the sheer quantity of such data. To make a violation listing effective, a clipping level must be established.
The clipping level establishes a baseline for violation activities that may be normal user errors. Only after this baseline is exceeded is a violation record produced. This solution is particularly effective for small- to medium-sized installations. Organizations with large-scale computing facilities often track all violations and use statistical routines to cull out the minor infractions (e.g., forgetting a password or mistyping it several times).
If the number of violations being tracked becomes unmanageable, the first step in correcting the problems should be to analyze why the condition has occurred. Do users understand how they are to interact with the computer resource? Are the rules too difficult to follow? Violation tracking and analysis can be valuable tools in assisting an organization to develop thorough but useable controls. Once these are in place and records are produced that accurately reflect serious violations, tracking and analysis become the first line of defense. With this procedure, intrusions are discovered before major damage occurs and sometimes early enough to catch the perpetrator. In addition, business protection and preservation are strengthened.
The following answers are incorrect:
All of the other choices presented were simply detractors. The following reference(s) were used for this question:
Handbook of Information Security Management

NEW QUESTION 44
- (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 46
- (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 51
- (Topic 1)
What are the components of an object's sensitivity label?

A. A Classification Set and a single Compartment.
B. A single classification and a single compartment.
C. A Classification Set and user credentials.
D. A single classification and a Compartment Set.

Answer: D

Explanation:
Both are the components of a sensitivity label. The following are incorrect:
A Classification Set and a single Compartment. Is incorrect because the nomenclature "Classification Set" is incorrect, there only one classifcation and it is not a "single compartment" but a Compartment Set.
A single classification and a single compartment. Is incorrect because while there only is one classifcation, it is not a "single compartment" but a Compartment Set.
A Classification Set and user credentials. Is incorrect because the nomenclature "Classification Set" is incorrect, there only one classifcation and it is not "user credential" but a Compartment Set. The user would have their own sensitivity label.

NEW QUESTION 55
- (Topic 1)
In an organization where there are frequent personnel changes, non-discretionary access control using Role Based Access Control (RBAC) is useful because:

A. people need not use discretion
B. the access controls are based on the individual's role or title within the organization.
C. the access controls are not based on the individual's role or title within the organization
D. the access controls are often based on the individual's role or title within the organization

Answer: B

Explanation:
In an organization where there are frequent personnel changes, non- discretionary access control (also called Role Based Access Control) is useful because the access controls are based on the individual's role or title within the organization. You can easily configure a new employee acces by assigning the user to a role that has been predefine. The user will implicitly inherit the permissions of the role by being a member of that role.
These access permissions defined within the role do not need to be changed whenever a new person takes over the role.
Another type of non-discretionary access control model is the Rule Based Access Control (RBAC or RuBAC) where a global set of rule is uniformly applied to all subjects accessing the resources. A good example of RuBAC would be a firewall.
This question is a sneaky one, one of the choice has only one added word to it which is often. Reading questions and their choices very carefully is a must for the real exam. Reading it twice if needed is recommended.
Shon Harris in her book list the following ways of managing RBAC: Role-based access control can be managed in the following ways:
Non-RBAC Users are mapped directly to applications and no roles are used. (No roles being used)
Limited RBAC Users are mapped to multiple roles and mapped directly to other types of
applications that do not have role-based access functionality. (A mix of roles for applications that supports roles and explicit access control would be used for applications that do not support roles)
Hybrid RBAC Users are mapped to multiapplication roles with only selected rights assigned to those roles.
Full RBAC Users are mapped to enterprise roles. (Roles are used for all access being granted)
NIST defines RBAC as:
Security administration can be costly and prone to error because administrators usually specify access control lists for each user on the system individually. With RBAC, security is managed at a level that corresponds closely to the organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. Security administration with RBAC consists of determining the operations that must be executed by persons in particular jobs, and assigning employees to the proper roles. Complexities introduced by mutually exclusive roles or role hierarchies are handled by the RBAC software, making security administration easier.
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 32.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition McGraw-Hill. and
http://csrc.nist.gov/groups/SNS/rbac/

NEW QUESTION 56
- (Topic 1)
What is called a sequence of characters that is usually longer than the allotted number for a password?

A. passphrase
B. cognitive phrase
C. anticipated phrase
D. Real phrase

Answer: A

Explanation:
A passphrase is a sequence of characters that is usually longer than the allotted number for a password.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, page 37.

NEW QUESTION 60

- (Topic 1)
Which division of the Orange Book deals with discretionary protection (need-to-know)?

A. D
B. C
C. B
D. A

Answer: B

Explanation:
C deals with discretionary protection. See matric below:

TNI/TCSEC MATRIX

	A1	B3	B2	B1	C2	C1
DISCRETIONARY ACCESS						
Discretionary Access Control						
Identification and Authentication						
System Integrity						
System Architecture						
Security Testing						
Security Features User's Guide Trusted Facility Manual Design Documentation Test Documentation						
CONTROLLED ACCESS						
Protect Audit Trails						
Object Reuse						
MANDATORY ACCESS CONTROL						
Labels						
Mandatory Access Control						
Process isolation in system architecture						
Design Specification & Verification						
Device labels						
Subject Sensitivity Labels						
Trusted Path						
Separation of Administrator and User functions						
Covert Channel Analysis (Only Covert Storage Channel at B2)						
Trusted Facility Management						
Configuration Management						
Trusted Recovery						
Covert Channel Analysis (Both Timing and Covert Channel analysis at B3)						
Security Administrator Role Defined						
Monitor events and notify security personnel						
Trusted Distribution						
Formal Methods						
	A1	B3	B2	B1	C2	C1

C:\Users\MCS\Desktop\1.jpg
TCSEC Matric
The following are incorrect answers:
D is incorrect. D deals with minimal security.
B is incorrect. B deals with mandatory protection. A is incorrect. A deals with verified protection. Reference(s) used for this question:
CBK, p. 329 ?C 330
and
Shon Harris, CISSP All In One (AIO), 6th Edition , page 392-393

NEW QUESTION 62
- (Topic 1)
What is called an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics?

A. Biometrics
B. Micrometrics
C. Macrometrics
D. MicroBiometrics

Answer: A

Explanation:
The Answer Biometrics; Biometrics are defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 37,38.

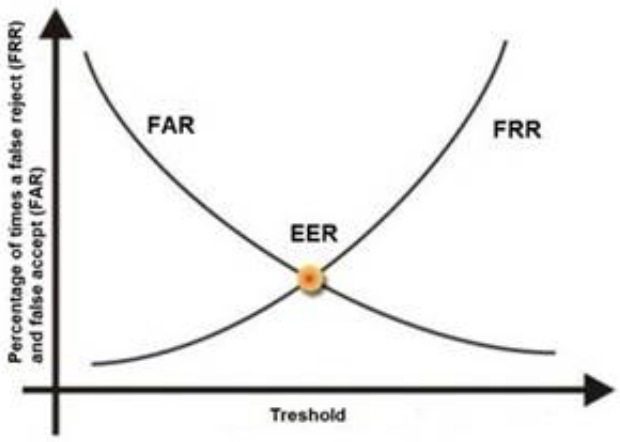
NEW QUESTION 63
- (Topic 1)
When a biometric system is used, which error type deals with the possibility of GRANTING access to impostors who should be REJECTED?

A. Type I error
B. Type II error
C. Type III error
D. Crossover error

Answer: B

Explanation:
When the biometric system accepts impostors who should have been rejected , it is called a Type II error or False Acceptance Rate or False Accept Rate. Biometrics verifies an individual??s identity by analyzing a unique personal attribute or behavior, which is one of the most effective and accurate methods of

verifying identification.
Biometrics is a very sophisticated technology; thus, it is much more expensive and complex than the other types of identity verification processes. A biometric system can make authentication decisions based on an individual??s behavior, as in signature dynamics, but these can change over time and possibly be forged. Biometric systems that base authentication decisions on physical attributes (iris, retina, fingerprint) provide more accuracy, because physical attributes typically don??t change much, absent some disfiguring injury, and are harder to impersonate.
When a biometric system rejects an authorized individual, it is called a Type I error (False Rejection Rate (FRR) or False Reject Rate (FRR)).
When the system accepts impostors who should be rejected, it is called a Type II error (False Acceptance Rate (FAR) or False Accept Rate (FAR)). Type II errors are the most dangerous and thus the most important to avoid.
The goal is to obtain low numbers for each type of error, but When comparing different biometric systems, many different variables are used, but one of the most important metrics is the crossover error rate (CER).
The accuracy of any biometric method is measured in terms of Failed Acceptance Rate (FAR) and Failed Rejection Rate (FRR). Both are expressed as percentages. The FAR is the rate at which attempts by unauthorized users are incorrectly accepted as valid. The FRR is just the opposite. It measures the rate at which authorized users are denied access.
The relationship between FRR (Type I) and FAR (Type II) is depicted in the graphic below . As one rate increases, the other decreases. The Cross-over Error Rate (CER) is sometimes considered a good indicator of the overall accuracy of a biometric system. This
is the point at which the FRR and the FAR have the same value. Solutions with a lower CER are typically more accurate.
See graphic below from Biometria showing this relationship. The Cross-over Error Rate (CER) is also called the Equal Error Rate (EER), the two are synonymous.



C:\Users\MCS\Desktop\1.jpg Cross Over Error Rate
The other answers are incorrect:
Type I error is also called as False Rejection Rate where a valid user is rejected by the system.
Type III error : there is no such error type in biometric system.
Crossover error rate stated in percentage , represents the point at which false rejection equals the false acceptance rate.
Reference(s) used for this question: http://www.biometria.sk/en/principles-of-biometrics.html
and
Shon Harris, CISSP All In One (AIO), 6th Edition , Chapter 3, Access Control, Page 188- 189
and
Tech Republic, Reduce Multi_Factor Authentication Cost

NEW QUESTION 68
- (Topic 1)
What is the main focus of the Bell-LaPadula security model?

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

Answer: C

Explanation:
The Bell-LaPadula model is a formal model dealing with confidentiality.
The Bell?CLaPadula Model (abbreviated BLP) is a state machine model used for enforcing access control in government and military applications. It was developed by David Elliott Bell and Leonard J. LaPadula, subsequent to strong guidance from Roger R. Schell to formalize the U.S. Department of Defense (DoD) multilevel security (MLS) policy. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g."Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public").
The Bell?CLaPadula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity. In this formal model, the entities in an information system are divided into subjects and objects.
The notion of a "secure state" is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby inductively proving that the system satisfies the security objectives of the model. The Bell?CLaPadula model is built on the concept of a state machine with a set of allowable states in a computer network system. The transition from one state to another state is defined by transition functions.
A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a security policy. To determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object (more precisely, to the combination of classification and set of compartments, making up the security level) to determine if the subject is authorized for the specific access mode.
The clearance/classification scheme is expressed in terms of a lattice. The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties:
The Simple Security Property - a subject at a given security level may not read an object at
a higher security level (no read-up).
The -property (read "star"-property) - a subject at a given security level must not write to any object at a lower security level (no write-down). The -property is also known as the Confinement property.
The Discretionary Security Property - use of an access matrix to specify the discretionary access control.
The following are incorrect answers:
Accountability is incorrect. Accountability requires that actions be traceable to the user that performed them and is not addressed by the Bell-LaPadula model.
Integrity is incorrect. Integrity is addressed in the Biba model rather than Bell-Lapadula. Availability is incorrect. Availability is concerned with assuring that data/services are available to authorized users as specified in service level objectives and is not addressed by the Bell-Lapadula model.
References: CBK, pp. 325-326
AIO3, pp. 279 - 284
AIOv4 Security Architecture and Design (pages 333 - 336) AIOv5 Security Architecture and Design (pages 336 - 338)

Wikipedia at https://en.wikipedia.org/wiki/Bell-La_Padula_model

NEW QUESTION 69
- (Topic 1)
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 73
- (Topic 1)
Sensitivity labels are an example of what application control type?

A. Preventive security controls
B. Detective security controls
C. Compensating administrative controls
D. Preventive accuracy controls

Answer: A

Explanation:
Sensitivity labels are a preventive security application controls, such as are firewalls, reference monitors, traffic padding, encryption, data classification, one-time passwords, contingency planning, separation of development, application and test environments.
The incorrect answers are:
Detective security controls - Intrusion detection systems (IDS), monitoring activities, and audit trails.
Compensating administrative controls - There no such application control. Preventive accuracy controls - data checks, forms, custom screens, validity checks, contingency planning, and backups. Sources:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 264).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Application Controls, Figure 7.1 (page 360).

NEW QUESTION 75
- (Topic 1)
In the context of access control, locks, gates, guards are examples of which of the following?

A. Administrative controls
B. Technical controls
C. Physical controls
D. Logical controls

Answer: C

Explanation:
Administrative, technical and physical controls are categories of access control mechanisms.
Logical and Technical controls are synonymous. So both of them could be eliminated as possible choices.
Physical Controls: These are controls to protect the organization??s people and physical environment, such as locks, gates, and guards. Physical controls may be called ??operational controls?? in some contexts.
Physical security covers a broad spectrum of controls to protect the physical assets (primarily the people) in an organization. Physical Controls are sometimes referred to as ??operational?? controls in some risk management frameworks. These controls range from doors, locks, and windows to environment controls, construction standards, and guards. Typically, physical security is based on the notion of establishing security zones or concentric areas within a facility that require increased security as you get closer to the
valuable assets inside the facility. Security zones are the physical representation of the defense-in-depth principle discussed earlier in this chapter. Typically, security zones are associated with rooms, offices, floors, or smaller elements, such as a cabinet or storage locker. The design of the physical security controls within the facility must take into account the protection of the asset as well as the individuals working in that area.
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 1301-1303). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1312-1318). Auerbach Publications. Kindle Edition.

NEW QUESTION 79
- (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 84
- (Topic 1)
Which of the following is the LEAST user accepted biometric device?

A. Fingerprint
B. Iris scan
C. Retina scan
D. Voice verification

Answer: C

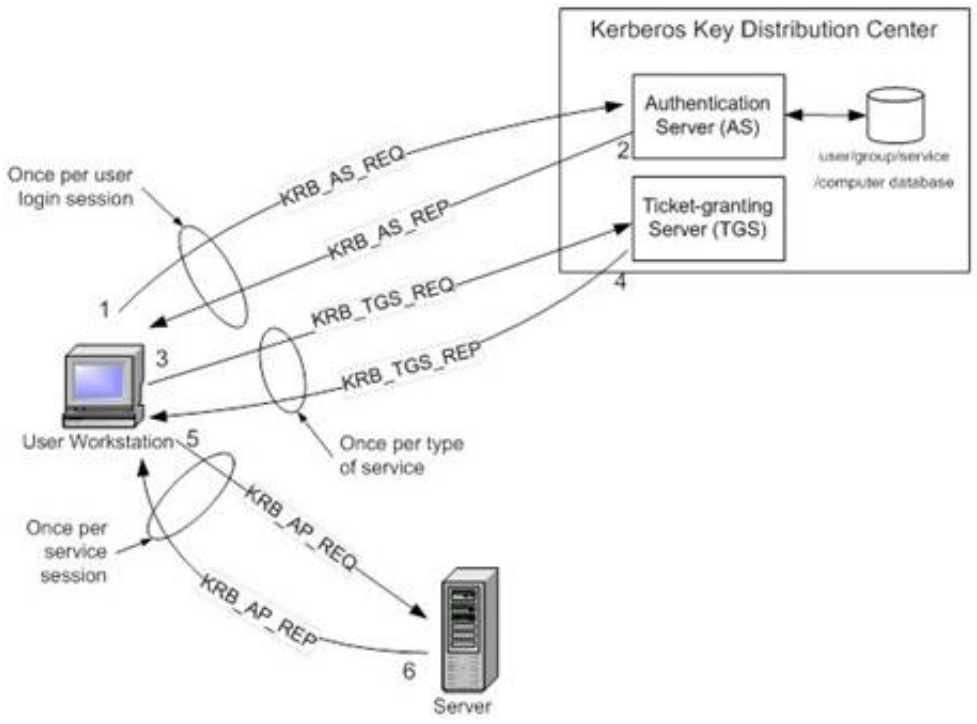
Explanation:
The biometric device that is least user accepted is the retina scan, where a system scans the blood-vessel pattern on the backside of the eyeball. When using this device, an individual has to place their eye up to a device, and may require a puff of air to be blown into the eye. The iris scan only needs for an individual to glance at a camera that could be placed above a door.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, Chapter 4: Access Control (page 131).

NEW QUESTION 87
- (Topic 1)
Which of the following is NOT true of the Kerberos protocol?

A. Only a single login is required per session.
B. The initial authentication steps are done using public key algorithm.
C. The KDC is aware of all systems in the network and is trusted by all of them
D. It performs mutual authentication

Answer: B

Explanation:
Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. It has the following characteristics:
It is secure: it never sends a password unless it is encrypted.
Only a single login is required per session. Credentials defined at login are then passed between resources without the need for additional logins.
The concept depends on a trusted third party ?C a Key Distribution Center (KDC). The KDC is aware of all systems in the network and is trusted by all of them.
It performs mutual authentication, where a client proves its identity to a server and a server proves its identity to the client.
Kerberos introduces the concept of a Ticket-Granting Server/Service (TGS). A client that wishes to use a service has to receive a ticket from the TGS ?C a ticket is a time-limited
cryptographic message ?C giving it access to the server. Kerberos also requires an Authentication Server (AS) to verify clients. The two servers combined make up a KDC.
Within the Windows environment, Active Directory performs the functions of the KDC. The following figure shows the sequence of events required for a client to gain access to a service using Kerberos authentication. Each step is shown with the Kerberos message associated with it, as defined in RFC 4120 ??The Kerberos Network Authorization Service (V5)??.



C:\Users\MCS\Desktop\1.jpg Kerberos Authentication Step by Step
Step 1: The user logs on to the workstation and requests service on the host. The workstation sends a message to the Authorization Server requesting a ticket granting ticket (TGT).
Step 2: The Authorization Server verifies the user??s access rights in the user database and creates a TGT and session key. The Authorization Sever encrypts the results using a key derived from the user??s password and sends a message back to the user workstation.
The workstation prompts the user for a password and uses the password to decrypt the incoming message. When decryption succeeds, the user will be able to use the TGT to request a service ticket.
Step 3: When the user wants access to a service, the workstation client application sends a request to the Ticket Granting Service containing the client name, realm name and a timestamp. The user proves his identity by sending an authenticator encrypted with the session key received in Step 2.
Step 4: The TGS decrypts the ticket and authenticator, verifies the request, and creates a ticket for the requested server. The ticket contains the client name and optionally the client IP address. It also contains the realm name and ticket lifespan. The TGS returns the ticket to the user workstation. The returned message contains two copies of a server session key
?C one encrypted with the client password, and one encrypted by the service password.
Step 5: The client application now sends a service request to the server containing the ticket received in Step 4 and an authenticator. The service authenticates the request by decrypting the session key. The server verifies that the ticket and authenticator match, and then grants access to the service. This step as described does not include the authorization performed by the Intel AMT device, as described later.
Step 6: If mutual authentication is required, then the server will reply with a server authentication message.
The Kerberos server knows "secrets" (encrypted passwords) for all clients and servers under its control, or it is in contact with other secure servers that have this information. These "secrets" are used to encrypt all of the messages shown in the figure above.
To prevent "replay attacks," Kerberos uses timestamps as part of its protocol definition. For timestamps to work properly, the clocks of the client and the server need to be in synch as much as possible. In other words, both computers need to be set to the same time and date. Since the clocks of two computers are often out of synch, administrators can establish a policy to establish the maximum acceptable difference to Kerberos between a client's clock and server's clock. If the difference between a client's clock and the server's clock is less than the maximum time difference specified in this policy, any timestamp used in a session between the two computers will be considered authentic. The maximum difference is usually set to five minutes.
Note that if a client application wishes to use a service that is "Kerberized" (the service is configured to perform Kerberos authentication), the client must also be Kerberized so that it expects to support the necessary message responses.
For more information about Kerberos, see http://web.mit.edu/kerberos/www/.
References:
Introduction to Kerberos Authentication from Intel
and
http://www.zeroshell.net/eng/kerberos/Kerberos-definitions/#1.3.5.3 and
http://www.ietf.org/rfc/rfc4120.txt

NEW QUESTION 89
- (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 92
- (Topic 1)
What kind of certificate is used to validate a user identity?

A. Public key certificate

B. Attribute certificate
C. Root certificate
D. Code signing certificate

Answer: A

Explanation:
In cryptography, a public key certificate (or identity certificate) is an electronic document which incorporates a digital signature to bind together a public key with an identity ?? information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.
In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). In a web of trust scheme, the signature is of either the user (a self-signed certificate) or other users ("endorsements"). In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together.
In computer security, an authorization certificate (also known as an attribute certificate) is a digital document that describes a written permission from the issuer to use a service or a resource that the issuer controls or has access to use. The permission can be delegated.
Some people constantly confuse PKCs and ACs. An analogy may make the distinction clear. A PKC can be considered to be like a passport: it identifies the holder, tends to last for a long time, and should not be trivial to obtain. An AC is more like an entry visa: it is typically issued by a different authority and does not last for as long a time. As acquiring an entry visa typically requires presenting a passport, getting a visa can be a simpler process.
A real life example of this can be found in the mobile software deployments by large service providers and are typically applied to platforms such as Microsoft Smartphone (and related), Symbian OS, J2ME, and others.
In each of these systems a mobile communications service provider may customize the mobile terminal client distribution (ie. the mobile phone operating system or application environment) to include one or more root certificates each associated with a set of capabilities or permissions such as "update firmware", "access address book", "use radio interface", and the most basic one, "install and execute". When a developer wishes to enable distribution and execution in one of these controlled environments they must acquire a certificate from an appropriate CA, typically a large commercial CA, and in the process they usually have their identity verified using out-of-band mechanisms such as a combination of phone call, validation of their legal entity through government and commercial databases, etc., similar to the high assurance SSL certificate vetting process, though often there are additional specific requirements imposed on would-be developers/publishers. Once the identity has been validated they are issued an identity certificate they can use to sign their software; generally the software signed by the developer or publisher's identity certificate is not distributed but rather it is submitted to processor to possibly test or profile the content before generating an authorization certificate which is unique to the particular software release. That certificate is then used with an ephemeral asymmetric key-pair to sign the software as the last step of preparation for distribution. There are many advantages to separating the identity and authorization certificates especially relating to risk mitigation of new content being accepted into the system and key management as well as recovery from errant software which can be used as attack vectors.
References:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 540.
http://en.wikipedia.org/wiki/Attribute_certificate http://en.wikipedia.org/wiki/Public_key_certificate

NEW QUESTION 97
- (Topic 1)
In Synchronous dynamic password tokens:

A. The token generates a new password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).
B. The token generates a new non-unique password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).
C. The unique password is not entered into a system or workstation along with an owner's PIN.
D. The authentication entity in a system or workstation knows an owner's secret key and PIN, and the entity verifies that the entered password is invalid and that it was entered during the invalid time window.

Answer: A

Explanation:
Synchronous dynamic password tokens:
- The token generates a new password value at fixed time intervals (this password could be the time of day encrypted with a secret key).
- the unique password is entered into a system or workstation along with an owner's PIN.
- The authentication entity in a system or workstation knows an owner's secret key and PIN, and the entity verifies that the entered password is valid and that it was entered during the valid time window.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

NEW QUESTION 99
- (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 101
- (Topic 1)
What is called the act of a user professing an identity to a system, usually in the form of a log-on ID?

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

Answer: B

Explanation:
Identification is the act of a user professing an identity to a system, usually in the form of a log-on ID to the system.
Identification is nothing more than claiming you are somebody. You identify yourself when you speak to someone on the phone that you don??t know, and they ask you who they??re speaking to. When you say, ??I??m Jason.??, you??ve just identified yourself.
In the information security world, this is analogous to entering a username. It??s not analogous to entering a password. Entering a password is a method for verifying that you are who you identified yourself as.
NOTE: The word "professing" used above means: "to say that you are, do, or feel something when other people doubt what you say". This is exactly what happen when you provide your identifier (identification), you claim to be someone but the system cannot take your word for it, you must further Authenticate to the system to prove who you claim to be.
The following are incorrect answers:
Authentication: is how one proves that they are who they say they are. When you claim to be Jane Smith by logging into a computer system as ??jsmith??, it??s most likely going to ask you for a password. You??ve claimed to be that person by entering the name into the username field (that??s the identification part), but now you have to prove that you are really that person.
Many systems use a password for this, which is based on ??something you know??, i.e. a secret between you and the system.
Another form of authentication is presenting something you have, such as a driver??s license, an RSA token, or a smart card.
You can also authenticate via something you are. This is the foundation for biometrics. When you do this, you first identify yourself and then submit a thumb print, a retina scan, or another form of bio-based authentication.
Once you??ve successfully authenticated, you have now done two things: you??ve claimed to be someone, and you??ve proven that you are that person. The only thing that??s left is for the
system to determine what you??re allowed to do.
Authorization: is what takes place after a person has been both identified and authenticated; it??s the step determines what a person can then do on the system. An example in people terms would be someone knocking on your door at night. You say, ??Who is it???, and wait for a response. They say, ??It??s John.?? in order to identify themselves. You ask them to back up into the light so you can see them through the peephole. They do so, and you authenticate them based on what they look like (biometric). At that point you decide they can come inside the house.
If they had said they were someone you didn??t want in your house (identification), and you then verified that it was that person (authentication), the authorization phase would not include access to the inside of the house.
Confidentiality: Is one part of the CIA triad. It prevents sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. A good example is a credit card number while shopping online, the merchant needs it to clear the transaction but you do not want your informaiton exposed over the network, you would use a secure link such as SSL, TLS, or some tunneling tool to protect the information from prying eyes between point A and point B. Data encryption is a common method of ensuring confidentiality.
The other parts of the CIA triad are listed below:
Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). In addition, some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash. If an unexpected change occurs, a backup copy must be available to restore the affected data to its correct state.
Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed, providing a certain measure of redundancy and failover, providing adequate communications bandwidth and preventing the occurrence of bottlenecks, implementing emergency backup power systems, keeping current with all necessary system upgrades, and guarding against malicious actions such as denial-of- service (DoS) attacks.
Reference used for this question:
http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA http://www.danielmiessler.com/blog/security-identification-authentication-and-authorization http://www.merriam-webster.com/dictionary/profess
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

NEW QUESTION 106
- (Topic 1)
In biometric identification systems, the parts of the body conveniently available for identification are:

A. neck and mouth
B. hands, face, and eyes
C. feet and hair
D. voice and neck

Answer: B

Explanation:
Today implementation of fast, accurate, reliable, and user-acceptable biometric identification systems are already under way. Because most identity authentication takes place when a people are fully clothed (neck to feet and wrists), the parts of the body conveniently available for this purpose are hands, face, and eyes. From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Page 7.

NEW QUESTION 110
- (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 113
- (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 implicitely inherit the permissions of the role or roles they have been assigned to. When they leave the company or change jobs, their role assignment is revoked/changed appropriately.
Mandatory access control is incorrect. While controlling access based on the clearence level of employees and the sensitivity of obects is a better choice than some of the other incorrect answers, it is not the best choice when RBAC is an option and you are looking for the best solution for a high number of employees constantly leaving or joining the company.
Lattice-based access control is incorrect. The lattice is really a mathematical concept that is used in formally modeling information flow (Bell-Lapadula, Biba, etc). In the context of the question, an abstract model of information flow is not an appropriate choice. CBK, pp. 324- 325.
Discretionary access control is incorrect. When an employee joins or leaves the company, the object owner must grant or revoke access for that employee on all the objects they own. Problems would also arise when the owner of an object leaves the company. The complexity of assuring that the permissions are added and removed correctly makes this the least desirable solution in this situation.
References
Alll in One, third edition page 165
RBAC is discussed on pp. 189 through 191 of the ISC(2) guide.

NEW QUESTION 117
- (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 121
- (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 122
- (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 126
- (Topic 2)
Which of the following statements pertaining to the security kernel is incorrect?

A. The security kernel is made up of mechanisms that fall under the TCB and implements and enforces the reference monitor concept.
B. The security kernel must provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof.
C. The security kernel must be small enough to be able to be tested and verified in a complete and comprehensive manner.
D. The security kernel is an access control concept, not an actual physical component.

Answer: D

Explanation:
The reference monitor, not the security kernel is an access control concept.
The security kernel is made up of software, and firmware components that fall within the TCB and implements and enforces the reference monitor concept. The security kernel mediates all access and functions between subjects and objects. The security kernel is the core of the TCB and is the most commonly used approach to building trusted computing systems.
There are three main requirements of the security kernel:
• It must provide isolation for the processes carrying out the reference monitor concept, and the processes must be tamperproof.
• It must be invoked for every access attempt and must be impossible to circumvent. Thus, the security kernel must be implemented in a complete and foolproof way.
• It must be small enough to be able to be tested and verified in a complete and comprehensive manner.
The following answers are incorrect:
The security kernel is made up of mechanisms that fall under the TCB and implements and enforces the reference monitor concept. Is incorrect because this is the definition of the security kernel.
The security kernel must provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof. Is incorrect because this is one of the three requirements that make up the security kernel.
The security kernel must be small enough to be able to be tested and verified in a complete and comprehensive manner. Is incorrect because this is one of the three requirements that make up the security kernel.

NEW QUESTION 128
- (Topic 2)
Which must bear the primary responsibility for determining the level of protection needed for information systems resources?

A. IS security specialists
B. Senior Management
C. Senior security analysts
D. systems Auditors

Answer: B

Explanation:
If there is no support by senior 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. It is senior management that could face legal repercussions if they do not have sufficient controls in place.
The following answers are incorrect:
IS security specialists. Is incorrect because it is not the best answer. Senior management bears the primary responsibility for determining the level of protection needed.
Senior security analysts. Is incorrect because it is not the best answer. Senior management bears the primary responsibility for determining the level of protection needed.
systems auditors. Is incorrect because it is not the best answer, system auditors are responsible that the controls in place are effective. Senior management bears the primary responsibility for determining the level of protection needed.

NEW QUESTION 130
- (Topic 2)
During which phase of an IT system life cycle are security requirements developed?

A. Operation
B. Initiation
C. Functional design analysis and Planning
D. Implementation

Answer: C

Explanation:
The software development life cycle (SDLC) (sometimes referred to as the System Development Life Cycle) is the process of creating or altering software systems, and the models and methodologies that people use to develop these systems.
The NIST SP 800-64 revision 2 has within the description section of para 3.2.1:
This section addresses security considerations unique to the second SDLC phase. Key security activities for this phase include:
• Conduct the risk assessment and use the results to supplement the baseline security controls;
• Analyze security requirements;
• Perform functional and security testing;
• Prepare initial documents for system certification and accreditation; and
• Design security architecture.
Reviewing this publication you may want to pick development/acquisition. Although initiation would be a decent choice, it is correct to say during this phase you would only brainstorm the idea of security requirements. Once you start to develop and acquire hardware/software components then you would also develop the security controls for these. The Shon Harris reference below is correct as well.
Shon Harris' Book (All-in-One CISSP Certification Exam Guide) divides the SDLC differently:
Project initiation
Functional design analysis and planning System design specifications
Software development Installation Maintenance support

Revision and replacement
According to the author (Shon Harris), security requirements should be developed during the functional design analysis and planning phase.
SDLC POSITIONING FROM NIST 800-64

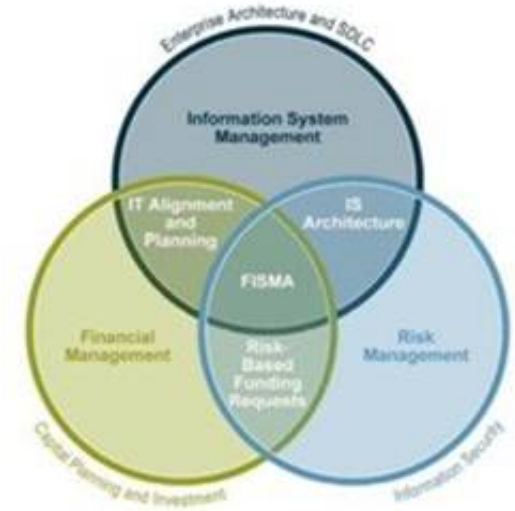


FIGURE 2-1. POSITIONING SECURITY CONSIDERATIONS

C:\Users\MCS\Desktop\1.jpg
SDLC Positioning in the enterprise
Information system security processes and activities provide valuable input into managing IT systems and their development, enabling risk identification, planning and mitigation. A risk management approach involves continually balancing the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the complete information system development life cycle (see Figure 2-1 above). The most effective way to implement risk management is to identify critical assets and operations, as well as systemic vulnerabilities across the agency. Risks are shared and not bound by organization, revenue source, or topologies. Identification and verification of critical assets and operations and their interconnections can be achieved through the system security planning process, as well as through the compilation of information from the Capital Planning and Investment Control (CPIC) and Enterprise Architecture (EA) processes to establish insight into the agency??s vital business operations, their supporting assets, and existing interdependencies and relationships.
With critical assets and operations identified, the organization can and should perform a business impact analysis (BIA). The purpose of the BIA is to relate systems and assets with the critical services they provide and assess the consequences of their disruption. By identifying these systems, an agency can manage security effectively by establishing priorities. This positions the security office to facilitate the IT program??s cost-effective performance as well as articulate its business impact and value to the agency.
SDLC OVERVIEW FROM NIST 800-64
SDLC Overview from NIST 800-64 Revision 2

C:\Users\MCS\Desktop\1.jpg
NIST 800-64 Revision 2 is one publication within the NISTstandards that I would recommend you look at for more details about the SDLC. It describe in great details what activities would take place and they have a nice diagram for each of the phases of the SDLC. You will find a copy at:
http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf DISCUSSION:
Different sources present slightly different info as far as the phases names are concerned.
People sometimes gets confused with some of the NIST standards. For example NIST 800-64 Security Considerations in the Information System Development Life Cycle has slightly different names, the activities mostly remains the same.
NIST clearly specifies that Security requirements would be considered throughout ALL of the phases. The keyword here is considered, if a question is about which phase they would be developed than Functional Design Analysis would be the correct choice.
Within the NIST standard they use different phase, howeverr under the second phase you will see that they talk specifically about Security Functional requirements analysis which confirms it is not at the initiation stage so it become easier to come out with the answer to this question. Here is what is stated:
The security functional requirements analysis considers the system security environment, including the enterprise information security policy and the enterprise security architecture. The analysis should address all requirements for confidentiality, integrity, and availability of information, and should include a review of all legal, functional, and other security requirements contained in applicable laws, regulations, and guidance.
At the initiation step you would NOT have enough detailed yet to produce the Security Requirements. You are mostly brainstorming on all of the issues listed but you do not develop them all at that stage.
By considering security early in the information system development life cycle (SDLC), you may be able to avoid higher costs later on and develop a more secure system from the start.
NIST says:
NIST`s Information Technology Laboratory recently issued Special Publication (SP) 800- 64, Security Considerations in the Information System Development Life Cycle, by Tim Grance, Joan Hash, and Marc Stevens, to help organizations include security requirements in their planning for every phase of the system life cycle, and to select, acquire, and use appropriate and cost-effective security controls.
I must admit this is all very tricky but reading skills and paying attention to KEY WORDS is a must for this exam.
References:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, Fifth Edition, Page 956
and
NIST S-64 Revision 2 at http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf and
http://www.mks.com/resources/resource-pages/software-development-life-cycle-sdlc- system-development

NEW QUESTION 132
- (Topic 2)

Which of the following is best defined as a mode of system termination that automatically leaves system processes and components in a secure state when a failure occurs or is detected in a system?

A. Fail proof
B. Fail soft
C. Fail safe
D. Fail Over

Answer: C

Explanation:
NOTE: This question is referring to a system which is Logical/Technical, so it is in the context of a system that you must choose the right answer. This is very important to read the question carefully and to identify the context whether it is in the Physical world or in the Technical/Logical world.
RFC 2828 (Internet Security Glossary) defines fail safe as a mode of system termination that automatically leaves system processes and components in a secure state when a failure occurs or is detected in the system.
A secure state means in the Logical/Technical world that no access would be granted or no packets would be allowed to flow through the system inspecting the packets such as a firewall for example.
If the question would have made reference to a building or something specific to the Physical world then the answer would have been different. In the Physical World everything becomes open and full access would be granted. See the valid choices below for the Physical context.
Fail-safe in the physical security world is when doors are unlocked automatically in case of emergency. Used in environment where humans work around. As human safety is prime concern during Fire or other hazards.
The following were all wrong choices:
Fail-secure in the physical security world is when doors are locked automatically in case of emergency. Can be in an area like Cash Locker Room provided there should be alternative manually operated exit door in case of emergency.
Fail soft is selective termination of affected non-essential system functions and processes when a failure occurs or is detected in the system.
Fail Over is a redundancy mechanism and does not apply to this question.
There is a great post within the CCCure Forums on this specific QUESTION NO: :
saintrockz who is a long term contributor to the forums did outstanding research and you have the results below. The CCCure forum is a gold mine where thousands of QUESTION NO: s related to the CBK have been discussed.
According to the Official ISC2 Study Guide (OIG):
Fault Tolerance is defined as built-in capability of a system to provide continued correct execution in the presence of a limited number of hardware or software faults. It means a system can operate in the presence of hardware component failures. A single component failure in a fault-tolerant system will not cause a system interruption because the alternate component will take over the task transparently. As the cost of components continues to drop, and the demand for system availability increases, many non-fault-tolerant systems have redundancy built-in at the subsystem level. As a result, many non-fault-tolerant systems can tolerate hardware faults - consequently, the line between a fault-tolerant system and a non-fault-tolerant system becomes increasingly blurred.
According to Common Criteria:
Fail Secure - Failure with preservation of secure state, which requires that the TSF (TOE security functions) preserve a secure state in the face of the identified failures.
Acc. to The CISSP Prep Guide, Gold Ed.:
Fail over - When one system/application fails, operations will automatically switch to the backup system.
Fail safe - Pertaining to the automatic protection of programs and/or processing systems to maintain safety when a hardware or software failure is detected in a system.
Fail secure - The system preserves a secure state during and after identified failures occur. Fail soft - Pertaining to the selective termination of affected non-essential processing when a hardware or software failure is detected in a system.
Acc. to CISSP for Dummies:
Fail closed - A control failure that results all accesses blocked. Fail open - A control failure that results in all accesses permitted.
Failover - A failure mode where, if a hardware or software failure is detected, the system automatically transfers processing to a hot backup component, such as a clustered server. Fail-safe - A failure mode where, if a hardware or software failure is detected, program execution is terminated, and the system is protected from compromise.
Fail-soft (or resilient) - A failure mode where, if a hardware or software failure is detected, certain, noncritical processing is terminated, and the computer or network continues to
function in a degraded mode.
Fault-tolerant - A system that continues to operate following failure of a computer or network component.
It's good to differentiate this concept in Physical Security as well: Fail-safe
• Door defaults to being unlocked
• Dictated by fire codes
Fail-secure
• Door defaults to being locked
Reference(s) used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION 136
- (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 138
- (Topic 2)
Step-by-step instructions used to satisfy control requirements is called a:

A. policy
B. standard
C. guideline
D. procedure

Answer: D

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

NEW QUESTION 140
- (Topic 2)
Which of the following is responsible for MOST of the security issues?

A. Outside espionage
B. Hackers
C. Personnel
D. Equipment failure

Answer: C

Explanation:
Personnel cause more security issues than hacker attacks, outside espionage, or equipment failure.
The following answers are incorrect because:
Outside espionage is incorrect as it is not the best answer. Hackers is also incorrect as it is not the best answer. Equipment failure is also incorrect as it is not the best answer.
Reference : Shon Harris AIO v3 , Chapter-3: Security Management Practices , Page : 56

NEW QUESTION 141
- (Topic 2)
Which of the following BEST explains why computerized information systems frequently fail to meet the needs of users?

A. Inadequate quality assurance (QA) tools.
B. Constantly changing user needs.
C. Inadequate user participation in defining the system's requirements.
D. Inadequate project management.

Answer: C

Explanation:
Inadequate user participation in defining the system's requirements. Most projects fail to meet the needs of the users because there was inadequate input in the initial steps of the project from the user community and what their needs really are.
The other answers, while potentially valid, are incorrect because they do not represent the most common problem assosciated with information systems failing to meet the needs of users.
References: All in One pg 834
Only users can define what their needs are and, therefore, what the system should accomplish. Lack of adequate user involvement, especially in the systems requirements phase, will usually result in a system that doesn't fully or adequately address the needs of the user.
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 296).

NEW QUESTION 146
- (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 147
- (Topic 2)
A Security Kernel is defined as a strict implementation of a reference monitor mechanism responsible for enforcing a security policy. To be secure, the kernel must meet three basic conditions, what are they?

A. Confidentiality, Integrity, and Availability
B. Policy, mechanism, and assurance
C. Isolation, layering, and abstraction
D. Completeness, Isolation, and Verifiability

Answer: D

Explanation:
A security kernel is responsible for enforcing a security policy. It is a strict implementation of a reference monitor mechanism. The architecture of a kernel operating system is typically layered, and the kernel should be at the lowest and most primitive level.
It is a small portion of the operating system through which all references to information and all changes to authorizations must pass. In theory, the kernel implements access control and information flow control between implemented objects according to the security policy.
To be secure, the kernel must meet three basic conditions: completeness (all accesses to information must go through the kernel),
isolation (the kernel itself must be protected from any type of unauthorized access),
and verifiability (the kernel must be proven to meet design specifications).
The reference monitor, as noted previously, is an abstraction, but there may be a reference validator, which usually runs inside the security kernel and is responsible for performing security access checks on objects, manipulating privileges, and generating any resulting security audit messages.
A term associated with security kernels and the reference monitor is the trusted computing base (TCB). The TCB is the portion of a computer system that contains all elements of the system responsible for supporting the security policy and the isolation of objects. The security capabilities of products for use in the TCB can be verified through various evaluation criteria, such as the earlier Trusted Computer System Evaluation Criteria (TCSEC) and the current Common Criteria standard.
Many of these security terms??reference monitor, security kernel, TCB??are defined loosely by vendors for purposes of marketing literature. Thus, it is necessary for security professionals to read the small print and between the lines to fully understand what the vendor is offering in regard to security features.
TIP FOR THE EXAM:
The terms Security Kernel and Reference monitor are synonymous but at different levels. As it was explained by Diego:
While the Reference monitor is the concept, the Security kernel is the implementation of such concept (via hardware, software and firmware means).
The two terms are the same thing, but on different levels: one is conceptual, one is "technical"
The following are incorrect answers: Confidentiality, Integrity, and Availability Policy, mechanism, and assurance Isolation, layering, and abstraction
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 13858-13875). Auerbach Publications. Kindle Edition.

NEW QUESTION 150
- (Topic 2)
Which of the following describes a logical form of separation used by secure computing systems?

A. Processes use different levels of security for input and output devices.
B. Processes are constrained so that each cannot access objects outside its permitted domain.
C. Processes conceal data and computations to inhibit access by outside processes.
D. Processes are granted access based on granularity of controlled objects.

Answer: B

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

NEW QUESTION 154
- (Topic 2)
What would BEST define a covert channel?

A. An undocumented backdoor that has been left by a programmer in an operating system
B. An open system port that should be closed.
C. A communication channel that allows transfer of information in a manner that violates the system's security policy.
D. A trojan horse.

Answer: C

Explanation:
The Answer A communication channel that allows transfer of information in a manner that violates the system's security policy.
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. The channel to transfer this unauthorized data is the result of one of the following conditions:• Oversight in the development of the product

• Improper implementation of access controls
• Existence of a shared resource between the two entities
• Installation of a Trojan horse
The following answers are incorrect:
An undocumented backdoor that has been left by a programmer in an operating system is incorrect because it is not a means by which unauthorized transfer of information takes place. Such backdoor is usually referred to as a Maintenance Hook.
An open system port that should be closed is incorrect as it does not define a covert channel.
A trojan horse is incorrect because it is a program that looks like a useful program but when you install it it would include a bonus such as a Worm, Backdoor, or some other malware without the installer knowing about it.
Reference(s) used for this question:
Shon Harris AIO v3 , Chapter-5 : Security Models & Architecture AIOv4 Security Architecture and Design (pages 343 - 344) AIOv5 Security Architecture and Design (pages 345 - 346)

NEW QUESTION 159
- (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 163
- (Topic 2)
What can best be defined as the sum of protection mechanisms inside the computer, including hardware, firmware and software?

A. Trusted system
B. Security kernel
C. Trusted computing base
D. Security perimeter

Answer: C

Explanation:
The Trusted Computing Base (TCB) is defined as the total combination of protection mechanisms within a computer system. The TCB includes hardware, software, and firmware. These are part of the TCB because the system is sure that these components will enforce the security policy and not violate it.
The security kernel is made up of hardware, software, and firmware components at fall within the TCB and implements and enforces the reference monitor concept.
Reference:
AIOv4 Security Models and Architecture pgs 268, 273

NEW QUESTION 164
- (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 166
- (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 170
- (Topic 2)
Which of the following is best defined as an administrative declaration by a designated authority that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards?

A. Certification
B. Declaration
C. Audit
D. Accreditation

Answer: D

Explanation:
Accreditation: is an administrative declaration by a designated authority that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards. It is usually based on a technical certification of the system's security mechanisms.
Certification: Technical evaluation (usually made in support of an accreditation action) of an information system\'s security features and other safeguards to establish the extent to which the system\'s design and implementation meet specified security requirements. Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION 174
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SSCP Exam with Our Prep Materials Via below:

https://www.certleader.com/SSCP-dumps.html