

[January 2018 Lead2pass 2018 New CISSP Exam PDF Ensure CISSP Certification Exam Pass 100% 2873q

Lead2pass 2018 New CISSP Exam PDF Ensure CISSP Certification Exam Pass Successfully:

<https://www.lead2pass.com/cissp.html> QUESTION 1The type of discretionary access control (DAC) that is based on an individual's identity is also called: A. Identity-based Access controlB. Rule-based Access controlC. Non-Discretionary Access ControlD. Lattice-based Access controlAnswer: AExplanation:An identity-based access control is a type of Discretionary Access Control (DAC) that is based on an individual's identity. DAC is good for low level security environment. The owner of the file decides who has access to the file. If a user creates a file, he is the owner of that file. An identifier for this user is placed in the file header and/or in an access control matrix within the operating system. Ownership might also be granted to a specific individual. For example, a manager for a certain department might be made the owner of the files and resources within her department. A system that uses discretionary access control (DAC) enables the owner of the resource to specify which subjects can access specific resources. This model is called discretionary because the control of access is based on the discretion of the owner. Many times department managers, or business unit managers, are the owners of the data within their specific department. Being the owner, they can specify who should have access and who should not. QUESTION 2Which access control type has a central authority that determine to what objects the subjects have access to and it is based on role or on the organizational security policy? A. Mandatory Access ControlB. Discretionary Access ControlC. Non-Discretionary Access ControlD. Rule-based Access control Answer: CExplanation:Non Discretionary Access Control include Role Based Access Control (RBAC) and Rule Based Access Control (RBAC or RuBAC). RBAC being a subset of NDAC, it was easy to eliminate RBAC as it was covered under NDAC already. Some people think that RBAC is synonymous with NDAC but RuBAC would also fall into this category. Discretionary Access control is for environment with very low level of security. There is no control on the dissemination of the information. A user who has access to a file can copy the file or further share it with other users. Rule Based Access Control is when you have ONE set of rules applied uniformly to all users. A good example would be a firewall at the edge of your network. A single rule based is applied against any packets received from the internet. Mandatory Access Control is a very rigid type of access control. The subject must dominate the object and the subject must have a Need To Know to access the information. Objects have labels that indicate the sensitivity (classification) and there is also categories to enforce the Need To Know (NTK). QUESTION 3Which 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 PairingB. Preventive/Technical PairingC. Preventive/Physical PairingD. Detective/Administrative Pairing Answer: AExplanation: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. QUESTION 4External consistency ensures that the data stored in the database is: A. in-consistent with the real world.B. remains consistant when sent from one system to another.C. consistent with the logical world.D. consistent with the real world. Answer: DExplanation:External consistency ensures that the data stored in the database is consistent with the real world. QUESTION 5A central authority determines what subjects can have access to certain objects based on the organizational security policy is called: A. Mandatory Access ControlB. Discretionary Access ControlC. Non-Discretionary Access ControlD. Rule-based Access control Answer: CExplanation:A central authority determines what subjects can have access to certain objects based on the organizational security policy. The key focal point of this question is the 'central authority' that determines access rights. Cecilia one of the quiz user has sent me feedback informing me that NIST defines MAC as: "MAC Policy means that Access Control Policy Decisions are made by a CENTRAL AUTHORITY. Which seems to indicate there could be two good answers to this question. However if you read the NISTR document mentioned in the references below, it is also mentioned that: MAC is the most mentioned NDAC policy. So MAC is a form of NDAC policy. Within the same document it is also mentioned: "In general, all access control policies other than DAC are grouped in the category of non-discretionary access control (NDAC). As the name implies, policies in this category have rules that are not established at the discretion of the user. Non-discretionary policies establish controls that cannot be changed by users, but only through administrative action." Under NDAC you have two choices:Rule Based Access control and Role Base Access Control MAC is implemented using RULES which makes it fall under RBAC which is a form of NDAC. It is a subset of NDAC. This question is representative of what you can expect on the real exam where you have more than once choice that seems to be right. However, you have to look closely if

one of the choices would be higher level or if one of the choice falls under one of the other choice. In this case NDAC is a better choice because MAC is falling under NDAC through the use of Rule Based Access Control. The following are incorrect answers:

MANDATORY ACCESS CONTROL In Mandatory Access Control the labels of the object and the clearance of the subject determines access rights, not a central authority. Although a central authority (Better known as the Data Owner) assigns the label to the object, the system does the determination of access rights automatically by comparing the Object label with the Subject clearance. The subject clearance MUST dominate (be equal or higher) than the object being accessed. The need for a MAC mechanism arises when the security policy of a system dictates that:

- 1 Protection decisions must not be decided by the object owner.
- 2 The system must enforce the protection decisions (i.e., the system enforces the security policy over the wishes or intentions of the object owner).

Usually a labeling mechanism and a set of interfaces are used to determine access based on the MAC policy; for example, a user who is running a process at the Secret classification should not be allowed to read a file with a label of Top Secret. This is known as the "simple security rule," or "no read up." Conversely, a user who is running a process with a label of Secret should not be allowed to write to a file with a label of Confidential. This rule is called the "*-property" (pronounced "star property") or "no write down." The *-property is required to maintain system security in an automated environment.

DISCRETIONARY ACCESS CONTROL In Discretionary Access Control the rights are determined by many different entities, each of the persons who have created files and they are the owner of that file, not one central authority. DAC leaves a certain amount of access control to the discretion of the object's owner or anyone else who is authorized to control the object's access. For example, it is generally used to limit a user's access to a file; it is the owner of the file who controls other users' accesses to the file. Only those users specified by the owner may have some combination of read, write, execute, and other permissions to the file. DAC policy tends to be very flexible and is widely used in the commercial and government sectors. However, DAC is known to be inherently weak for two reasons: First, granting read access is transitive; for example, when Ann grants Bob read access to a file, nothing stops Bob from copying the contents of Ann's file to an object that Bob controls. Bob may now grant any other user access to the copy of Ann's file without Ann's knowledge. Second, DAC policy is vulnerable to Trojan horse attacks. Because programs inherit the identity of the invoking user, Bob may, for example, write a program for Ann that, on the surface, performs some useful function, while at the same time destroys the contents of Ann's files. When investigating the problem, the audit files would indicate that Ann destroyed her own files. Thus, formally, the drawbacks of DAC are as follows:

- Discretionary Access Control (DAC) Information can be copied from one object to another; therefore, there is no real assurance on the flow of information in a system.
- No restrictions apply to the usage of information when the user has received it.
- The privileges for accessing objects are decided by the owner of the object, rather than through a system-wide policy that reflects the organization's security requirements.

ACLs and owner/group/other access control mechanisms are by far the most common mechanism for implementing DAC policies. Other mechanisms, even though not designed with DAC in mind, may have the capabilities to implement a DAC policy.

RULE BASED ACCESS CONTROL In Rule-based Access Control a central authority could in fact determine what subjects can have access when assigning the rules for access. However, the rules actually determine the access and so this is not the most correct answer. RuBAC (as opposed to RBAC, role-based access control) allow users to access systems and information based on pre determined and configured rules. It is important to note that there is no commonly understood definition or formally defined standard for rule-based access control as there is for DAC, MAC, and RBAC. "Rule-based access" is a generic term applied to systems that allow some form of organization-defined rules, and therefore rule-based access control encompasses a broad range of systems. RuBAC may in fact be combined with other models, particularly RBAC or DAC. A RuBAC system intercepts every access request and compares the rules with the rights of the user to make an access decision. Most of the rule-based access control relies on a security label system, which dynamically composes a set of rules defined by a security policy. Security labels are attached to all objects, including files, directories, and devices. Sometime roles to subjects (based on their attributes) are assigned as well. RuBAC meets the business needs as well as the technical needs of controlling service access. It allows business rules to be applied to access control—for example, customers who have overdue balances may be denied service access. As a mechanism for MAC, rules of RuBAC cannot be changed by users. The rules can be established by any attributes of a system related to the users such as domain, host, protocol, network, or IP addresses. For example, suppose that a user wants to access an object in another network on the other side of a router. The router employs RuBAC with the rule composed by the network addresses, domain, and protocol to decide whether or not the user can be granted access. If employees change their roles within the organization, their existing authentication credentials remain in effect and do not need to be re configured. Using rules in conjunction with roles adds greater flexibility because rules can be applied to people as well as to devices. Rule-based access control can be combined with role-based access control, such that the role of a user is one of the attributes in rule setting. Some provisions of access control systems have rule-based policy engines in addition to a role-based policy engine and certain implemented dynamic policies [Des03]. For example, suppose that two of the

primary types of software users are product engineers and quality engineers. Both groups usually have access to the same data, but they have different roles to perform in relation to the data and the application's function. In addition, individuals within each group have different job responsibilities that may be identified using several types of attributes such as developing programs and testing areas. Thus, the access decisions can be made in real time by a scripted policy that regulates the access between the groups of product engineers and quality engineers, and each individual within these groups. Rules can either replace or complement role-based access control. However, the creation of rules and security policies is also a complex process, so each organization will need to strike the appropriate balance.

QUESTION 6 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 information 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.

<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>

QUESTION 7 Which one of the following factors is NOT one on which Authentication is based? A. Type 1 Something you know, such as a PIN or password B. Type 2 Something you have, such as an ATM card or smart card C. Type 3 Something you are (based upon one or more intrinsic physical or behavioral traits), such as a fingerprint or retina scan D. Type 4 Something you are, such as a system administrator or security administrator
Answer: D
Explanation: Authentication is based on the following three factor types: Type 1 Something you know, such as a PIN or password Type 2 Something you have, such as an ATM card or smart card Type 3 Something you are (Unique physical

characteristic), such as a fingerprint or retina scan QUESTION 8A central authority determines what subjects can have access to certain objects based on the organizational security policy is called: A. Mandatory Access Control B. Discretionary Access Control C. Non-Discretionary Access Control D. Rule-based Access control Answer: C Explanation: A central authority determines what subjects can have access to certain objects based on the organizational security policy. The key focal point of this question is the 'central authority' that determines access rights. Cecilia one of the quiz user has sent me feedback informing me that NIST defines MAC as: "MAC Policy means that Access Control Policy Decisions are made by a CENTRAL AUTHORITY. Which seems to indicate there could be two good answers to this question. However if you read the NISTR document mentioned in the references below, it is also mentioned that: MAC is the most mentioned NDAC policy. So MAC is a form of NDAC policy. Within the same document it is also mentioned: "In general, all access control policies other than DAC are grouped in the category of non-discretionary access control (NDAC). As the name implies, policies in this category have rules that are not established at the discretion of the user. Non-discretionary policies establish controls that cannot be changed by users, but only through administrative action." Under NDAC you have two choices: Rule Based Access control and Role Base Access Control MAC is implemented using RULES which makes it fall under RBAC which is a form of NDAC. It is a subset of NDAC. This question is representative of what you can expect on the real exam where you have more than once choice that seems to be right. However, you have to look closely if one of the choices would be higher level or if one of the choice falls under one of the other choice. In this case NDAC is a better choice because MAC is falling under NDAC through the use of Rule Based Access Control. The following are incorrect answers: MANDATORY ACCESS CONTROL In Mandatory Access Control the labels of the object and the clearance of the subject determines access rights, not a central authority. Although a central authority (Better known as the Data Owner) assigns the label to the object, the system does the determination of access rights automatically by comparing the Object label with the Subject clearance. The subject clearance MUST dominate (be equal or higher) than the object being accessed. The need for a MAC mechanism arises when the security policy of a system dictates that: 1 Protection decisions must not be decided by the object owner. 2 The system must enforce the protection decisions (i.e., the system enforces the security policy over the wishes or intentions of the object owner). Usually a labeling mechanism and a set of interfaces are used to determine access based on the MAC policy; for example, a user who is running a process at the Secret classification should not be allowed to read a file with a label of Top Secret. This is known as the "simple security rule," or "no read up." Conversely, a user who is running a process with a label of Secret should not be allowed to write to a file with a label of Confidential. This rule is called the "*-property" (pronounced "star property") or "no write down." The *-property is required to maintain system security in an automated environment. DISCRETIONARY ACCESS CONTROL In Discretionary Access Control the rights are determined by many different entities, each of the persons who have created files and they are the owner of that file, not one central authority. DAC leaves a certain amount of access control to the discretion of the object's owner or anyone else who is authorized to control the object's access. For example, it is generally used to limit a user's access to a file; it is the owner of the file who controls other users' accesses to the file. Only those users specified by the owner may have some combination of read, write, execute, and other permissions to the file. DAC policy tends to be very flexible and is widely used in the commercial and government sectors. However, DAC is known to be inherently weak for two reasons: First, granting read access is transitive; for example, when Ann grants Bob read access to a file, nothing stops Bob from copying the contents of Ann's file to an object that Bob controls. Bob may now grant any other user access to the copy of Ann's file without Ann's knowledge. Second, DAC policy is vulnerable to Trojan horse attacks. Because programs inherit the identity of the invoking user, Bob may, for example, write a program for Ann that, on the surface, performs some useful function, while at the same time destroys the contents of Ann's files. When investigating the problem, the audit files would indicate that Ann destroyed her own files. Thus, formally, the drawbacks of DAC are as follows: - Discretionary Access Control (DAC) Information can be copied from one object to another; therefore, there is no real assurance on the flow of information in a system. - No restrictions apply to the usage of information when the user has received it. - The privileges for accessing objects are decided by the owner of the object, rather than through a system-wide policy that reflects the organization's security requirements. ACLs and owner/group/other access control mechanisms are by far the most common mechanism for implementing DAC policies. Other mechanisms, even though not designed with DAC in mind, may have the capabilities to implement a DAC policy. RULE BASED ACCESS CONTROL In Rule-based Access Control a central authority could in fact determine what subjects can have access when assigning the rules for access. However, the rules actually determine the access and so this is not the most correct answer. RuBAC (as opposed to RBAC, role-based access control) allow users to access systems and information based on pre determined and configured rules. It is important to note that there is no commonly understood definition or formally defined standard for rule-based access control as there is for DAC, MAC, and RBAC. "Rule-based access" is a generic term applied to systems that allow some form of organization-defined rules, and therefore rule-based access control encompasses a broad range of systems. RuBAC may in fact be

combined with other models, particularly RBAC or DAC. A RuBAC system intercepts every access request and compares the rules with the rights of the user to make an access decision. Most of the rule-based access control relies on a security label system, which dynamically composes a set of rules defined by a security policy. Security labels are attached to all objects, including files, directories, and devices. Sometime roles to subjects (based on their attributes) are assigned as well. RuBAC meets the business needs as well as the technical needs of controlling service access. It allows business rules to be applied to access control--for example, customers who have overdue balances may be denied service access. As a mechanism for MAC, rules of RuBAC cannot be changed by users. The rules can be established by any attributes of a system related to the users such as domain, host, protocol, network, or IP addresses. For example, suppose that a user wants to access an object in another network on the other side of a router. The router employs RuBAC with the rule composed by the network addresses, domain, and protocol to decide whether or not the user can be granted access. If employees change their roles within the organization, their existing authentication credentials remain in effect and do not need to be re configured. Using rules in conjunction with roles adds greater flexibility because rules can be applied to people as well as to devices. Rule-based access control can be combined with role-based access control, such that the role of a user is one of the attributes in rule setting. Some provisions of access control systems have rule- based policy engines in addition to a role-based policy engine and certain implemented dynamic policies [Des03]. For example, suppose that two of the primary types of software users are product engineers and quality engineers. Both groups usually have access to the same data, but they have different roles to perform in relation to the data and the application's function. In addition, individuals within each group have different job responsibilities that may be identified using several types of attributes such as developing programs and testing areas. Thus, the access decisions can be made in real time by a scripted policy that regulates the access between the groups of product engineers and quality engineers, and each individual within these groups. Rules can either replace or complement role-based access control. However, the creation of rules and security policies is also a complex process, so each organization will need to strike the appropriate balance.

QUESTION 9 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.

<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> QUESTION 10 What is called the verification that the user's claimed identity is valid and is usually implemented through a user password at log-on time? A. Authentication B. Identification C. Integrity D.

Confidentiality Answer: A Explanation: Authentication is verification that the user's claimed identity is valid and is usually implemented through a user password at log-on time. **CISSP dumps full version (PDF&VCE):**

<https://www.lead2pass.com/cissp.html> **Large amount of free CISSP** exam questions on Google Drive:

https://drive.google.com/open?id=1393N8RayZN4QJ8sxxg6_3cIRxwNv8QGTq