CISA Q&As

Certified Information Systems Auditor

Pass Isaca CISA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/cisa.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Isaca Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following should be the PRIMARY consideration when developing an IT strategy?

A. IT key performance indicators based on business objectives

B. Alignment with overall business objectives

C. Alignment with the IT investment portfolio

D. Short and long-term plans for the enterprise IT architecture

Correct Answer: B

QUESTION 2

The PRIMARY focus of a post-implementation review is to verify that:

A. enterprise architecture (EA) has been complied with.

B. user requirements have been met.

C. acceptance testing has been properly executed.

D. user access controls have been adequately designed.

Correct Answer: B

QUESTION 3

A business unit uses an e-commerce application with a strong password policy. Many customers complain that they cannot remember their passwords because they are too long and complex. The business unit states it is imperative to improve the customer experience. The information security manager should FIRST:

A. change the password policy to improve the customer experience.

B. recommend implementing two-factor authentication.

C. research alternative secure methods of identity verification.

D. evaluate the impact of the customer\\'s experience on business revenue.

Correct Answer: C

QUESTION 4

Which of the following is NOT an example of preventive control?

A. Physical access control like locks and door

B. User login screen which allows only authorize user to access website

C. Encrypt the data so that only authorize user can view the same

D. Duplicate checking of a calculations

Correct Answer: C

The word NOT is used as a keyword in the question. You need to find out a security control from given options which in not preventive. Duplicate checking of a calculation is a detective control and not a preventive control.

For your exam you should know below information about different security controls

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to

circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught)

outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an

attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process.

This oversight acts as a deterrent, curbing an attacker\\'s appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events. When users begin to understand that by authenticating into a system to

perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with

their actions is avoided at all costs. It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if

the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and

cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control

rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The

only way to bypass the control is to

find a flaw in the control\\'s implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the

required controls, there may exist other

technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk. For example, the access control policy may state that the authentication process must

be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of

the authentication process to support the policy statement. Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the

security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of

least privilege. However, the detective

nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk. As mentioned previously, strongly managed access privileges provided to

an authenticated user offer the ability to reduce the risk exposure of the enterprise\\'s assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are

provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the

transaction. 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.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the

environment to a secure state. A security

incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its

tracks. Corrective controls can take

many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may

affect access controls, their applicability, status, or management. Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not

correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install. Additionally, an employee may be transferred, quit, or be on temporary

leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and

financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

For your exam you should know below information about different security controls

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to

circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught)

outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an

attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process.

This oversight acts as a deterrent, curbing an attacker\\'s appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity

of

the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that

an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and

cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control

rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The

only way to bypass the control is to find a flaw in the control\\'s implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the

required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly.

Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes,

such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of

least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to

reduce the risk exposure of the enterprise\\'s assets by limiting the capabilities that authenticated user has. However, there are

few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the

use of applied access controls will offer visibility into the transaction. 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.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the

environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls

must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may

affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls

placed on system files or even have default administrative accounts unknowingly implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program,

potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

The other examples belong to Preventive control.

Reference:

CISA Review Manual 2014 Page number 44

and

Official ISC2 CISSP guide 3rd edition Page number 50 and 51

QUESTION 5

Multiple invoices are usually received for individual purchase orders, since purchase orders require staggered delivery dates. Which of the following is the BEST audit technique to test for duplicate payments?

A. Run the data on the software programs used to process supplier payments.

B. Use generalized audit software on the invoice transaction file.

C. Run the data on the software programs used to process purchase orders.

D. Use generalized audit software on the purchase order transaction file.

Correct Answer: A