Q2

Terminate the developer's logical access to IT resources. To protect IT assets, terminating logical access to IT resources is the first and most important action to take after management has confirmed the employee's clear intention to leave the enterprise.

Q3

Design phase

Planning for implementation should begin well in advance of the actual implementation date. A formal implementation plan should be constructed in the design phase and revised as the development progresses.

Q4

A Post-Implementation Review (PIR) is conducted after completing a project. Its purpose is to evaluate whether project objectives were met, to determine how effectively the project was run, to learn lessons for the future, and to ensure that the organization gets the greatest possible benefit from the project.

Q5

Earned value analysis

Earned value analysis (EVA) is an industry standard method for measuring a project's progress at any given point in time, forecasting its completion date and final cost, and analyzing variances in the schedule and budget as the project proceeds. It compares the planned amount of work with what has actually been completed to determine if the cost, schedule and work accomplished are progressing in accordance with the plan. EVA works most effectively if a well-formed work breakdown structure exists.

Q7

Data Owner

Data owners should have the authority and responsibility for granting access to the data

Q8

Warm Site

A warm site is the most appropriate solution because it provides basic infrastructure and most of the required IT equipment to affordably meet the business requirements. The remainder of the equipment needed can be provided through vendor agreements within a few days. The RTO is the amount of time allowed for the recovery of a business function or resource after a disaster occurs. The RPO is determined based on the acceptable data loss in case of a disruption of operations. The RPO indicates the earliest point in time that is acceptable to recover the data, and it effectively quantifies the permissible amount of data loss in case of interruption.

Qts 11

Mitigation.

A reciprocal agreement in which two organizations agree to provide computing resources to each other in the event of a disaster is a form of risk mitigation. This usually works well if both organizations have similar information processing facilities. Because the intended effect of reciprocal agreements is to have a functional DRP, it is a risk mitigation strategy.

Q13

By digitally signing all e-mail messages, the receiver will be able to validate the authenticity of the sender. Encrypting all e-mail messages would ensure that only the intended recipient will be able to open the message; however, it would not ensure the authenticity of the sender. Compressing all e-mail messages would reduce the size of the message, but would not ensure the authenticity. Password protecting all e-mail messages would ensure that only those who have the password would be able to open the message; however, it would not ensure the authenticity of the sender.

Q.Which of the following is MOST relevant to an IS auditor evaluating how the project manager has monitored the progress of the project?

Gantt charts

The bank's IS auditor should:

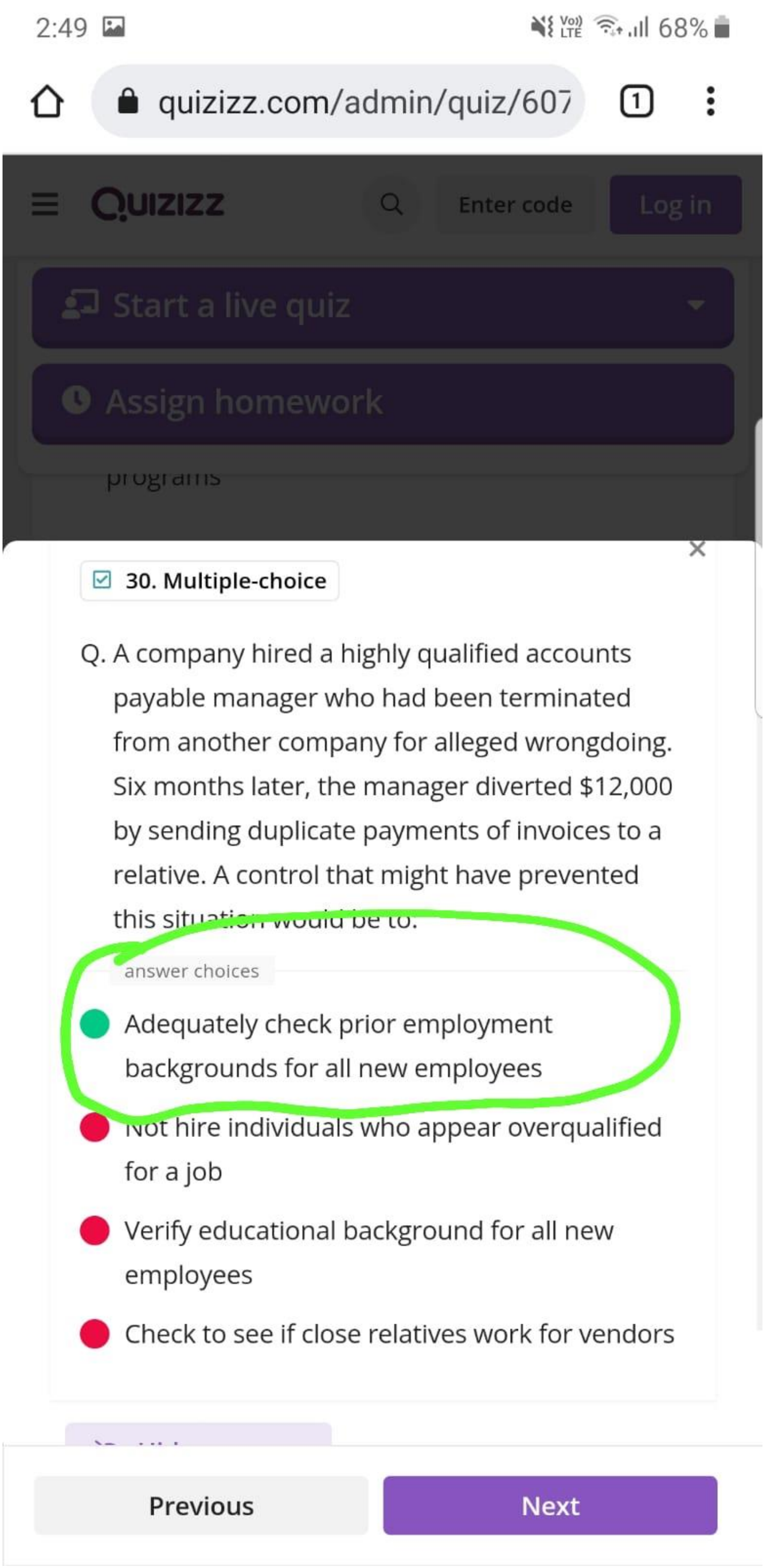
Verify that the agreed-on SLAs were achievable by the outsourcing vendor.

Verify that adequate and complete reports of SLA achievement were prepared by the vendor's IS department in good time for the monthly SLA management meetings.

Verify that the SLA achievement reports highlighted any failures, included a reasonable explanation for the failures and outlined measures in place to ensure the failures did not recur.

Beta Testing is performed by “real users” of the software application in “real environment” and it can be considered as a form of external User Acceptance Testing. It is the final test before shipping a product to the customers. Direct feedback from customers is a major advantage of Beta Testing. This testing helps to test products in customer’s environment.

Beta version of the software is released to a limited number of end-users of the product to obtain feedback on the product quality. Beta testing reduces product failure risks and provides increased quality of the product through customer validation.



☑ 30. Multiple-choice

Q. A company hired a highly qualified accounts payable manager who had been terminated from another company for alleged wrongdoing. Six months later, the manager diverted $12,000 by sending duplicate payments of invoices to a relative. A control that might have prevented this situation would be to:

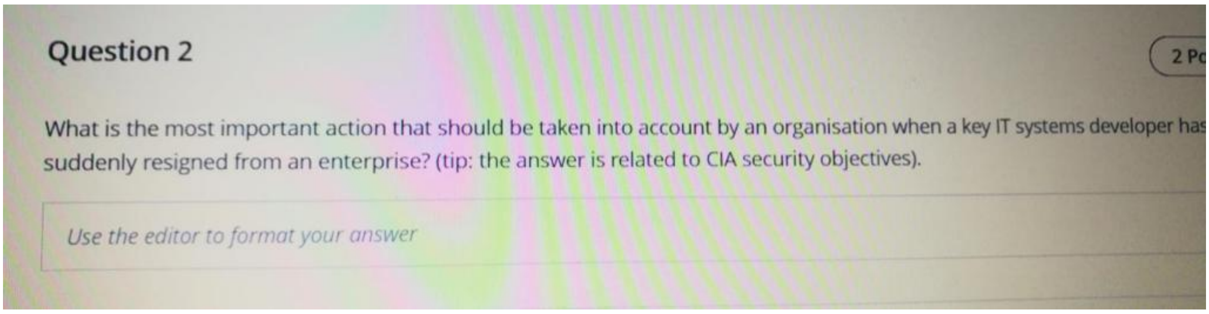
answer choices

[✓ 🟢 Adequately check prior employment backgrounds for all new employees]

🔴 Not hire individuals who appear overqualified for a job

🔴 Verify educational background for all new employees

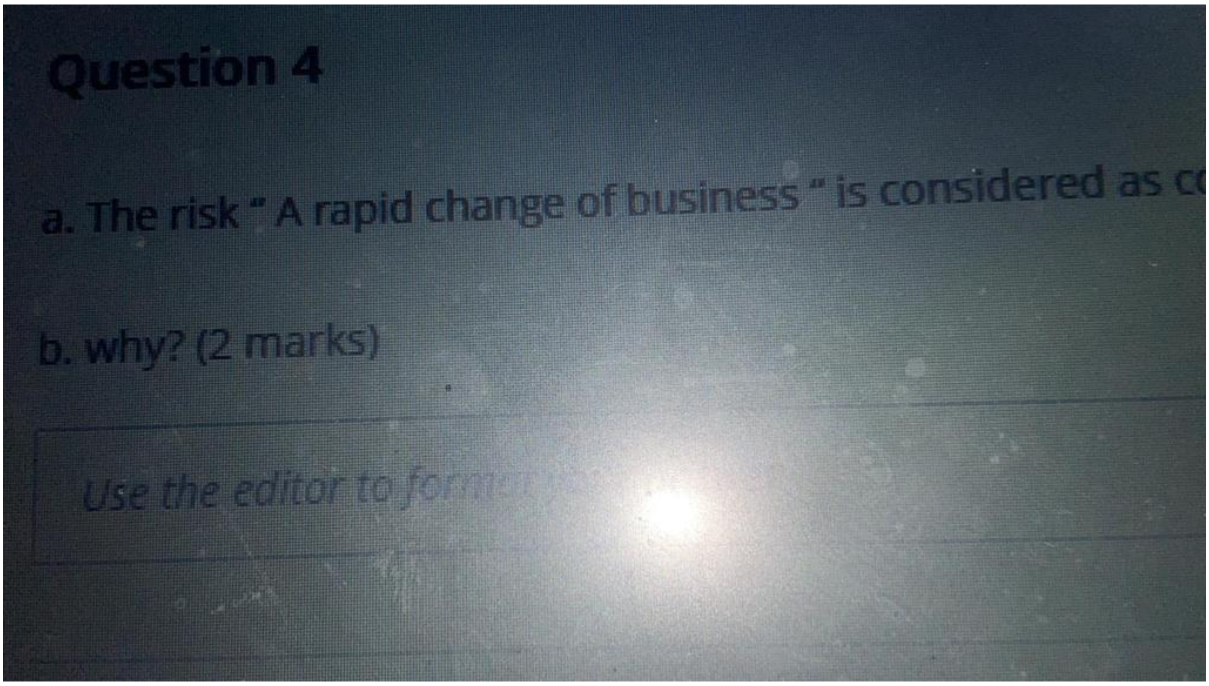
🔴 Check to see if close relatives work for vendors



Question 2

2 Po

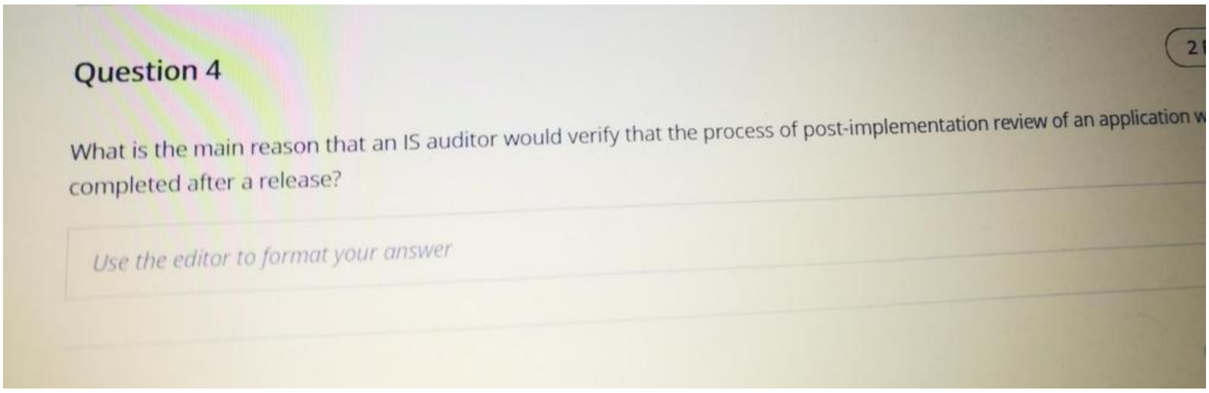
What is the most important action that should be taken into account by an organisation when a key IT systems developer has suddenly resigned from an enterprise? (tip: the answer is related to CIA security objectives).



Question 4

a. The risk " A rapid change of business " is considered as co

b. why? (2 marks)

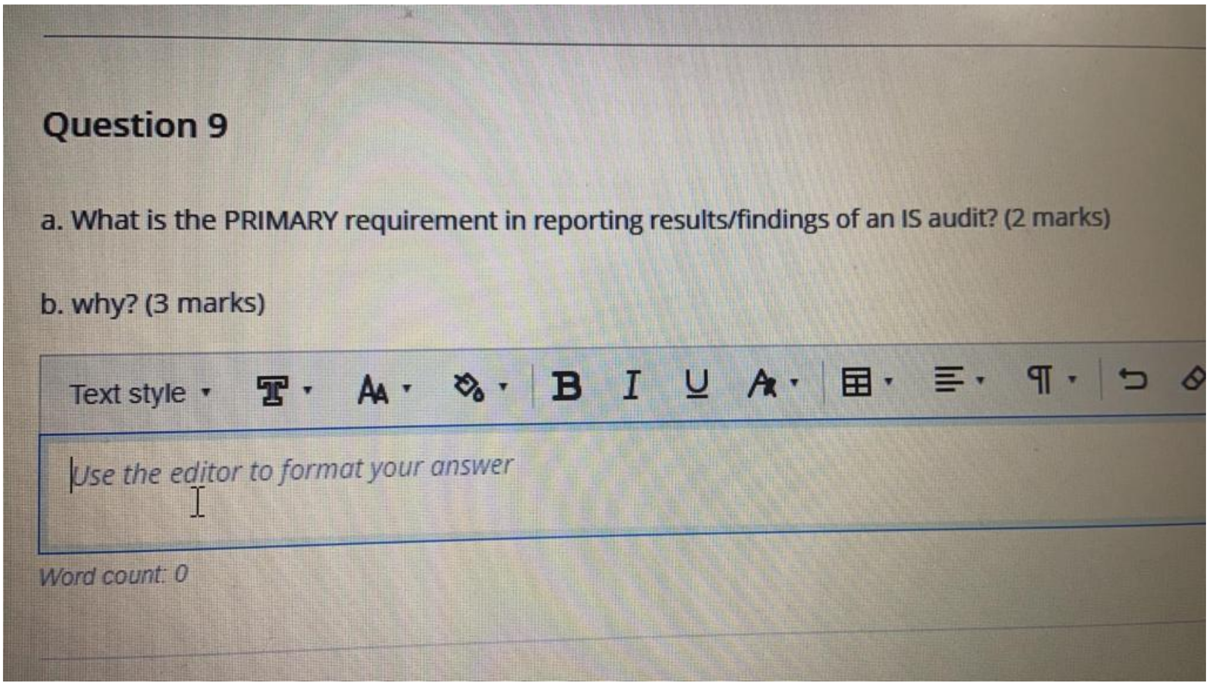


Question 4

2

What is the main reason that an IS auditor would verify that the process of post-implementation review of an application w
completed after a release?

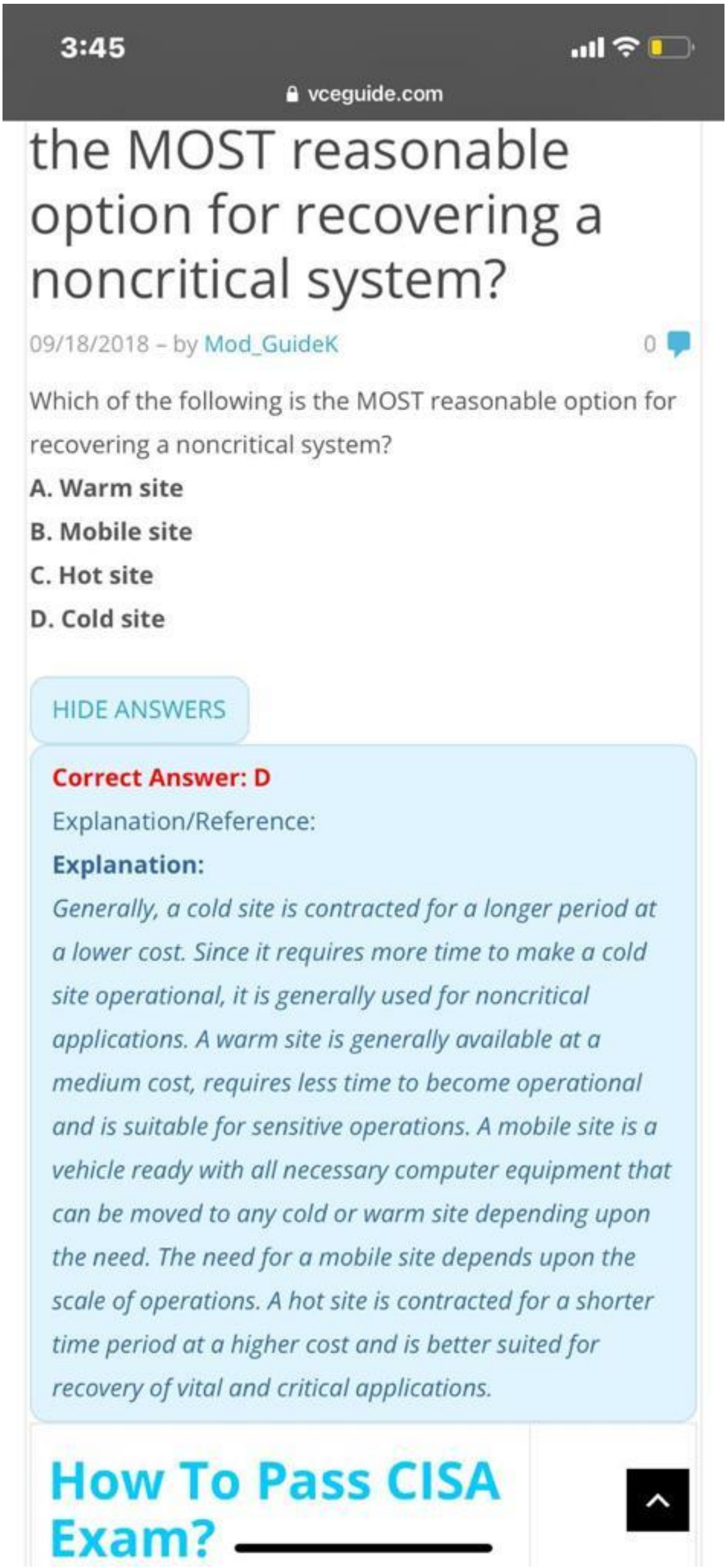
Use the editor to format your answer



Question 9

a. What is the PRIMARY requirement in reporting results/findings of an IS audit? (2 marks)

b. why? (3 marks)



the MOST reasonable option for recovering a noncritical system?

09/18/2018 – by Mod_GuideK

Which of the following is the MOST reasonable option for recovering a noncritical system?

A. Warm site

B. Mobile site

C. Hot site

D. Cold site

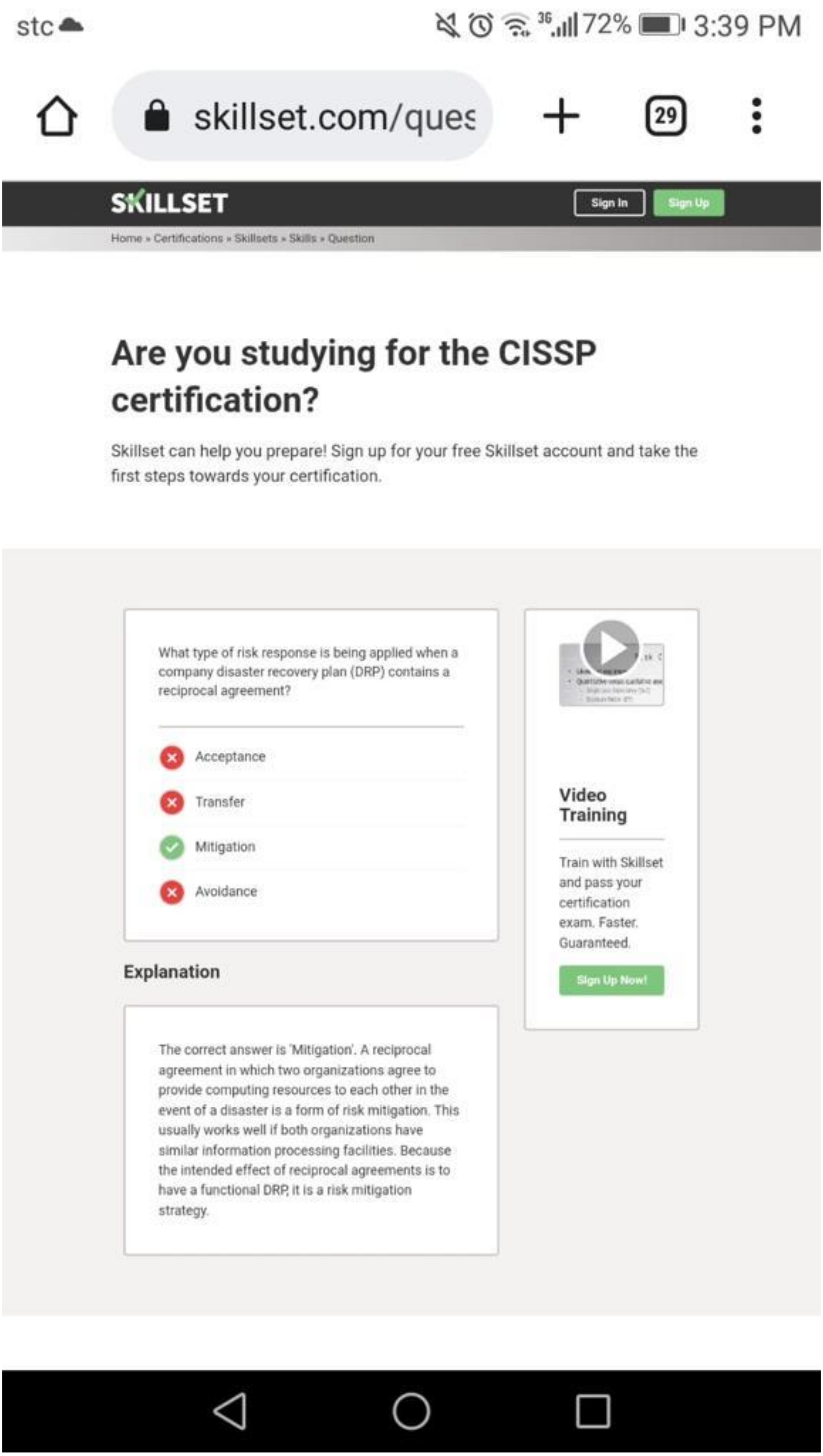
Correct Answer: D

Explanation/Reference:

Explanation:

Generally, a cold site is contracted for a longer period at a lower cost. Since it requires more time to make a cold site operational, it is generally used for noncritical applications. A warm site is generally available at a medium cost, requires less time to become operational and is suitable for sensitive operations. A mobile site is a vehicle ready with all necessary computer equipment that can be moved to any cold or warm site depending upon the need. The need for a mobile site depends upon the scale of operations. A hot site is contracted for a shorter time period at a higher cost and is better suited for recovery of vital and critical applications.

How To Pass CISA Exam?



Are you studying for the CISSP certification?

Skillset can help you prepare! Sign up for your free Skillset account and take the first steps towards your certification.

What type of risk response is being applied when a company disaster recovery plan (DRP) contains a reciprocal agreement?

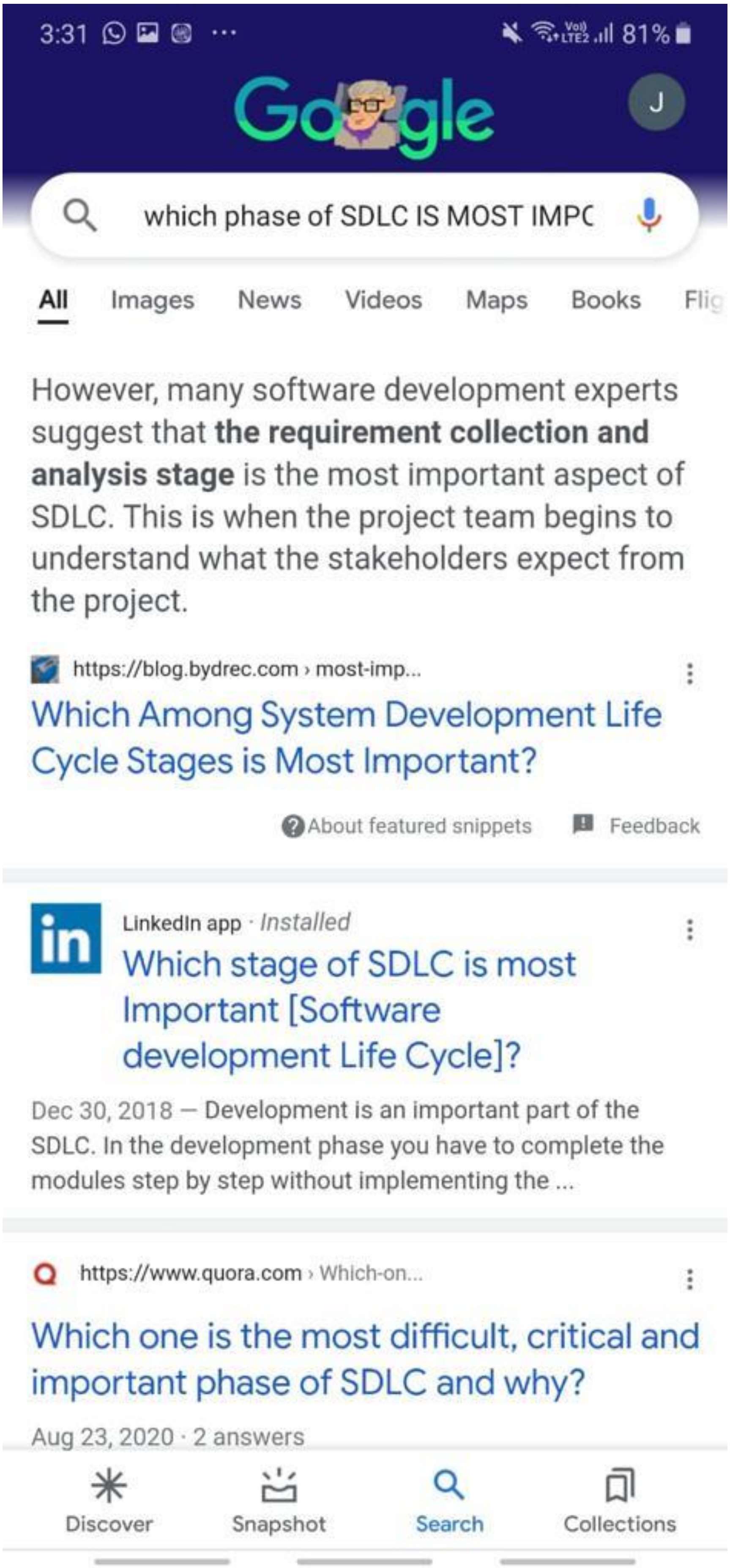
- ☒ Acceptance
- ☒ Transfer
- ✓ Mitigation
- ☒ Avoidance

Explanation

The correct answer is 'Mitigation'. A reciprocal agreement in which two organizations agree to provide computing resources to each other in the event of a disaster is a form of risk mitigation. This usually works well if both organizations have similar information processing facilities. Because the intended effect of reciprocal agreements is to have a functional DRP, it is a risk mitigation strategy.

Video Training

Train with Skillset and pass your certification exam. Faster. Guaranteed.



which phase of SDLC IS MOST IMPC

However, many software development experts suggest that **the requirement collection and analysis stage** is the most important aspect of SDLC. This is when the project team begins to understand what the stakeholders expect from the project.

https://blog.bydrec.com › most-imp...

Which Among System Development Life Cycle Stages is Most Important?

About featured snippets Feedback

LinkedIn app · *Installed*

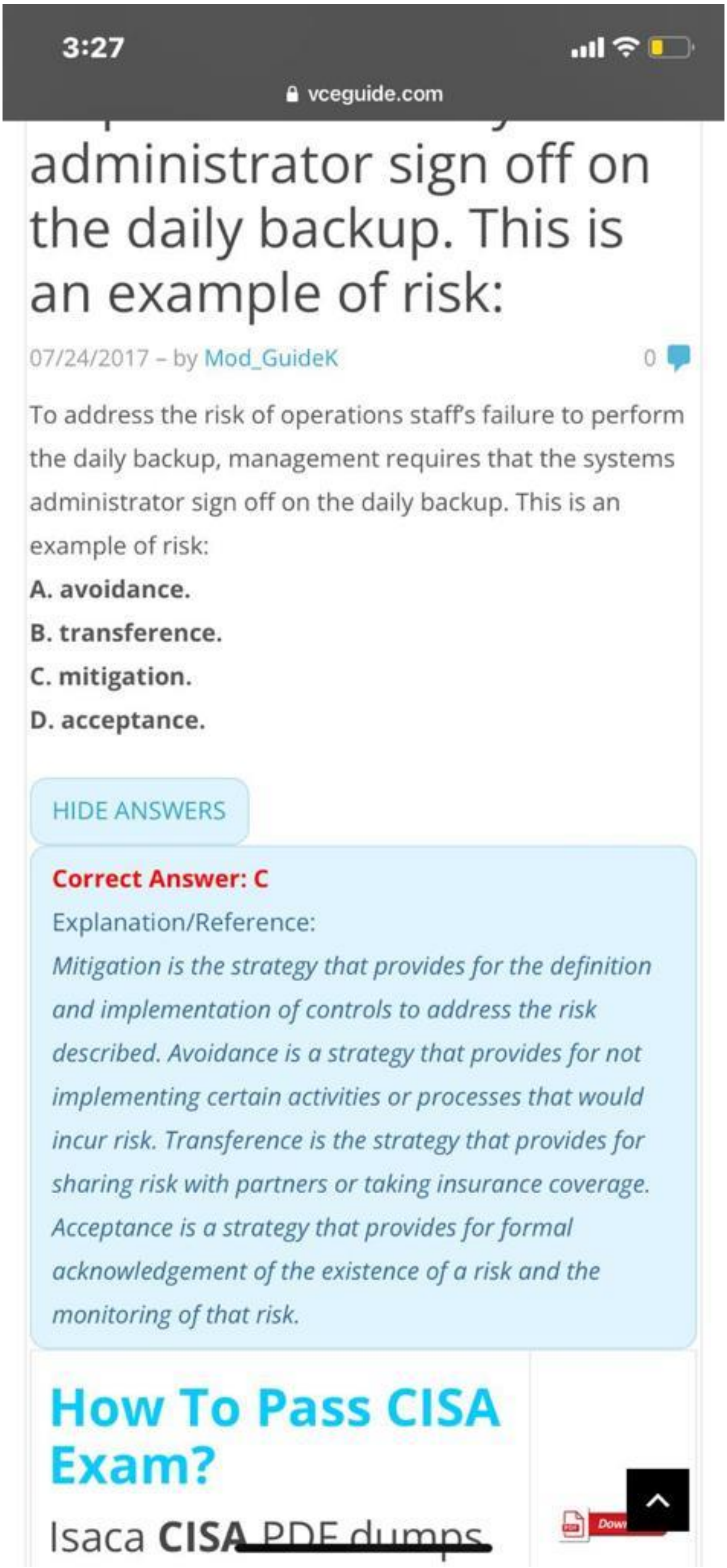
Which stage of SDLC is most Important [Software development Life Cycle]?

Dec 30, 2018 — Development is an important part of the SDLC. In the development phase you have to complete the modules step by step without implementing the ...

https://www.quora.com › Which-on...

Which one is the most difficult, critical and important phase of SDLC and why?

Aug 23, 2020 · 2 answers



administrator sign off on the daily backup. This is an example of risk:

07/24/2017 – by Mod_GuideK 0

To address the risk of operations staff's failure to perform the daily backup, management requires that the systems administrator sign off on the daily backup. This is an example of risk:

A. avoidance.

B. transference.

C. mitigation.

D. acceptance.

HIDE ANSWERS

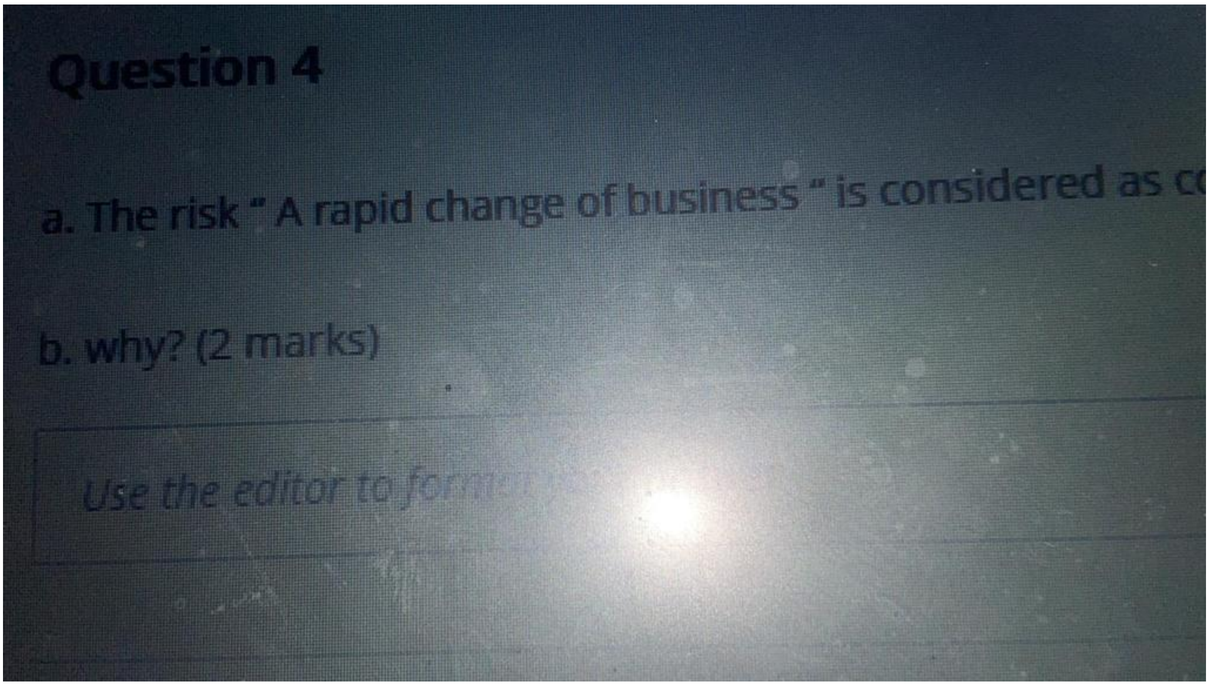
Correct Answer: C

Explanation/Reference:

Mitigation is the strategy that provides for the definition and implementation of controls to address the risk described. Avoidance is a strategy that provides for not implementing certain activities or processes that would incur risk. Transference is the strategy that provides for sharing risk with partners or taking insurance coverage. Acceptance is a strategy that provides for formal acknowledgement of the existence of a risk and the monitoring of that risk.

How To Pass CISA Exam?

Isaca **CISA** PDF dumps

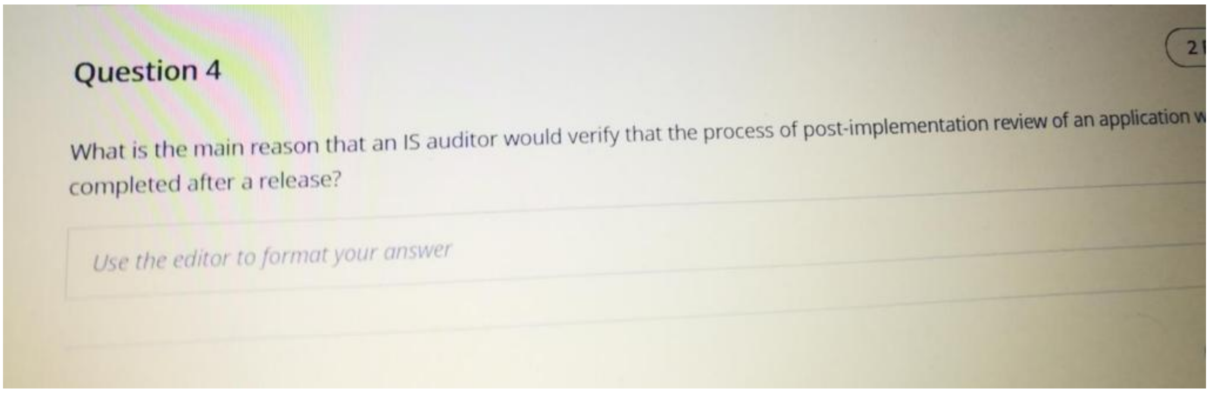


Question 4

a. The risk " A rapid change of business " is considered as co

b. why? (2 marks)

Use the editor to form

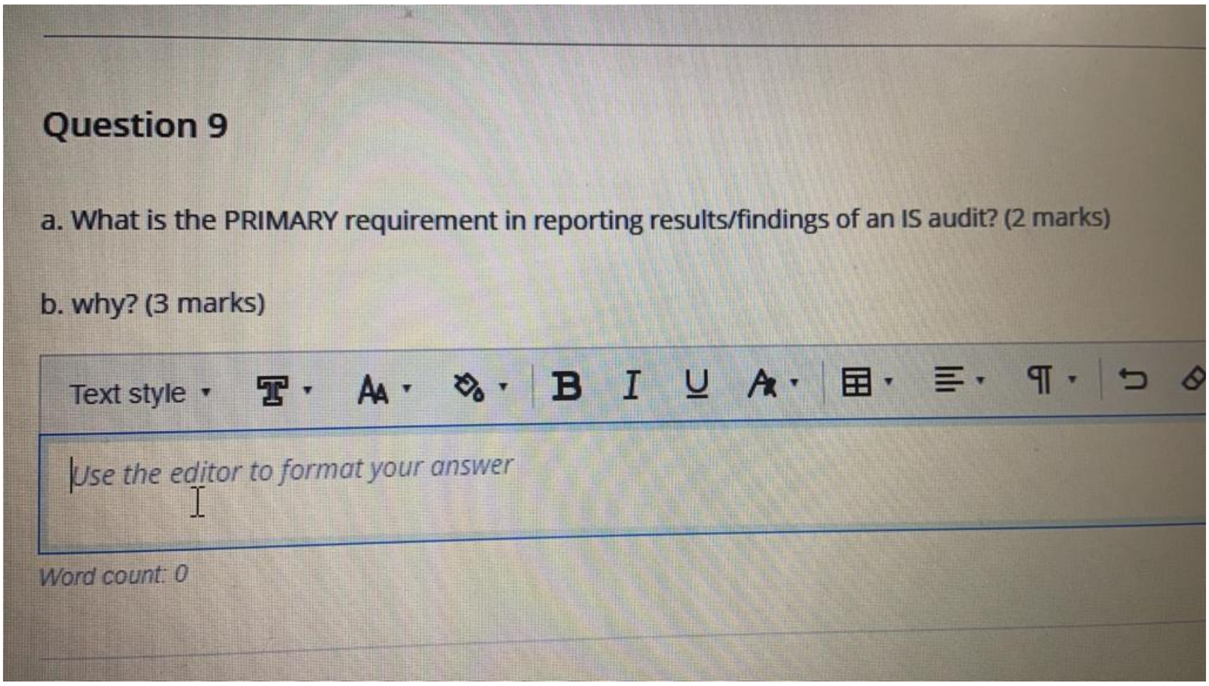


2

Question 4

What is the main reason that an IS auditor would verify that the process of post-implementation review of an application w completed after a release?

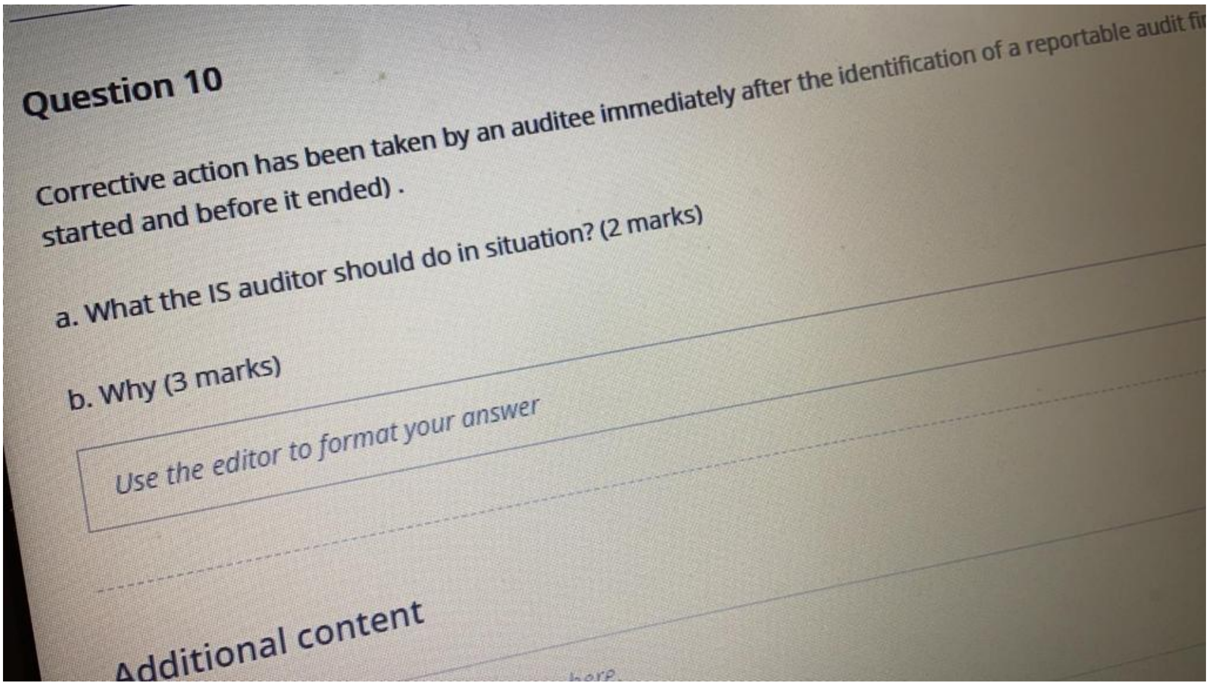
Use the editor to format your answer



Question 9

a. What is the PRIMARY requirement in reporting results/findings of an IS audit? (2 marks)

b. why? (3 marks)

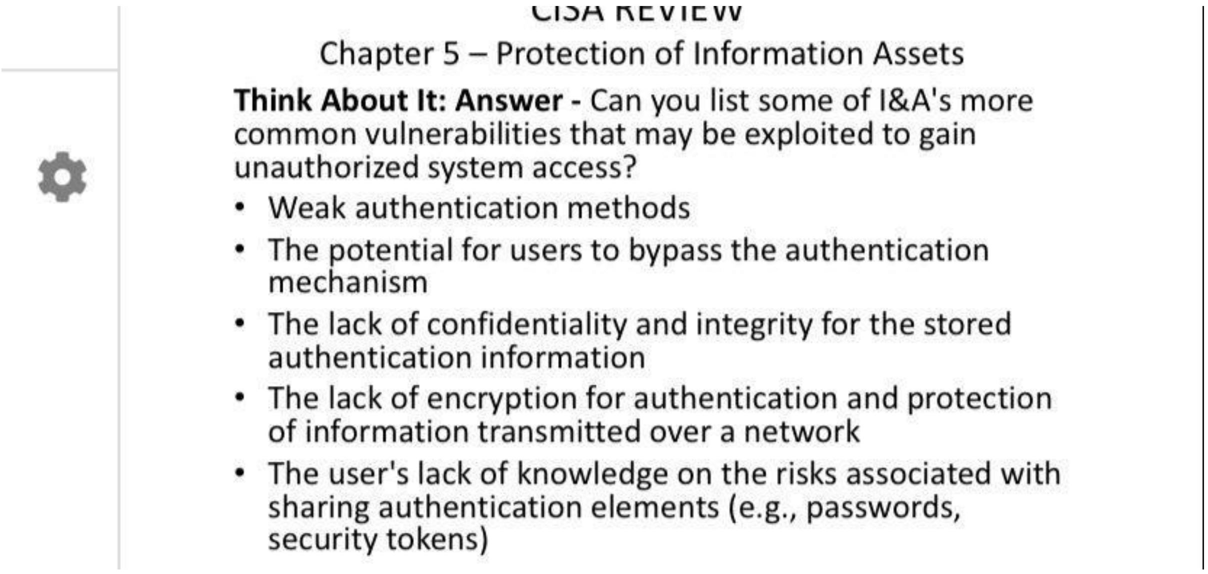


Question 10

Corrective action has been taken by an auditee immediately after the identification of a reportable audit fi started and before it ended) .

a. What the IS auditor should do in situation? (2 marks)

b. Why (3 marks)

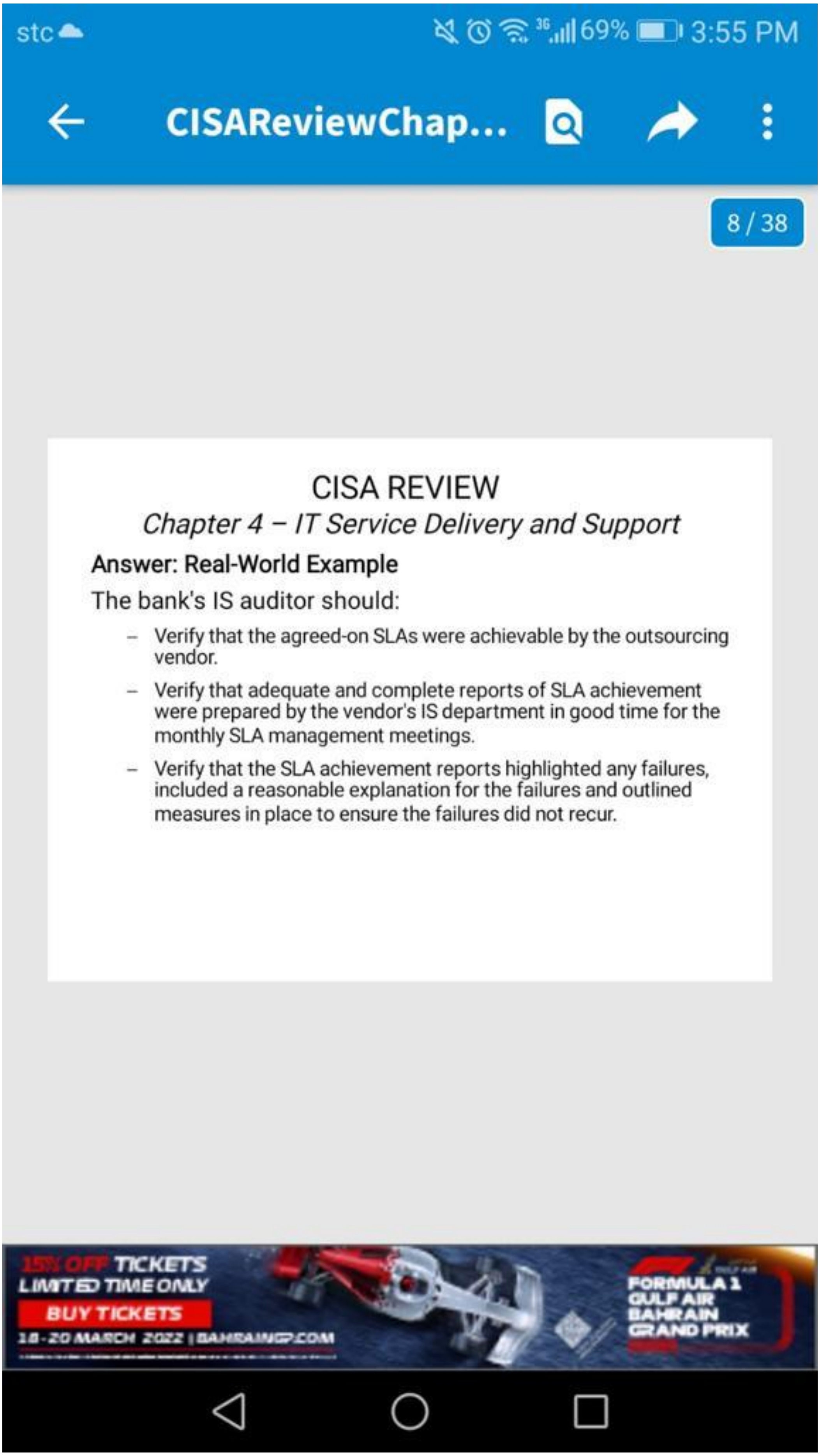


CISA REVIEW

Chapter 5 – Protection of Information Assets

Think About It: Answer - Can you list some of I&A's more common vulnerabilities that may be exploited to gain unauthorized system access?

- Weak authentication methods
- The potential for users to bypass the authentication mechanism
- The lack of confidentiality and integrity for the stored authentication information
- The lack of encryption for authentication and protection of information transmitted over a network
- The user's lack of knowledge on the risks associated with sharing authentication elements (e.g., passwords, security tokens)



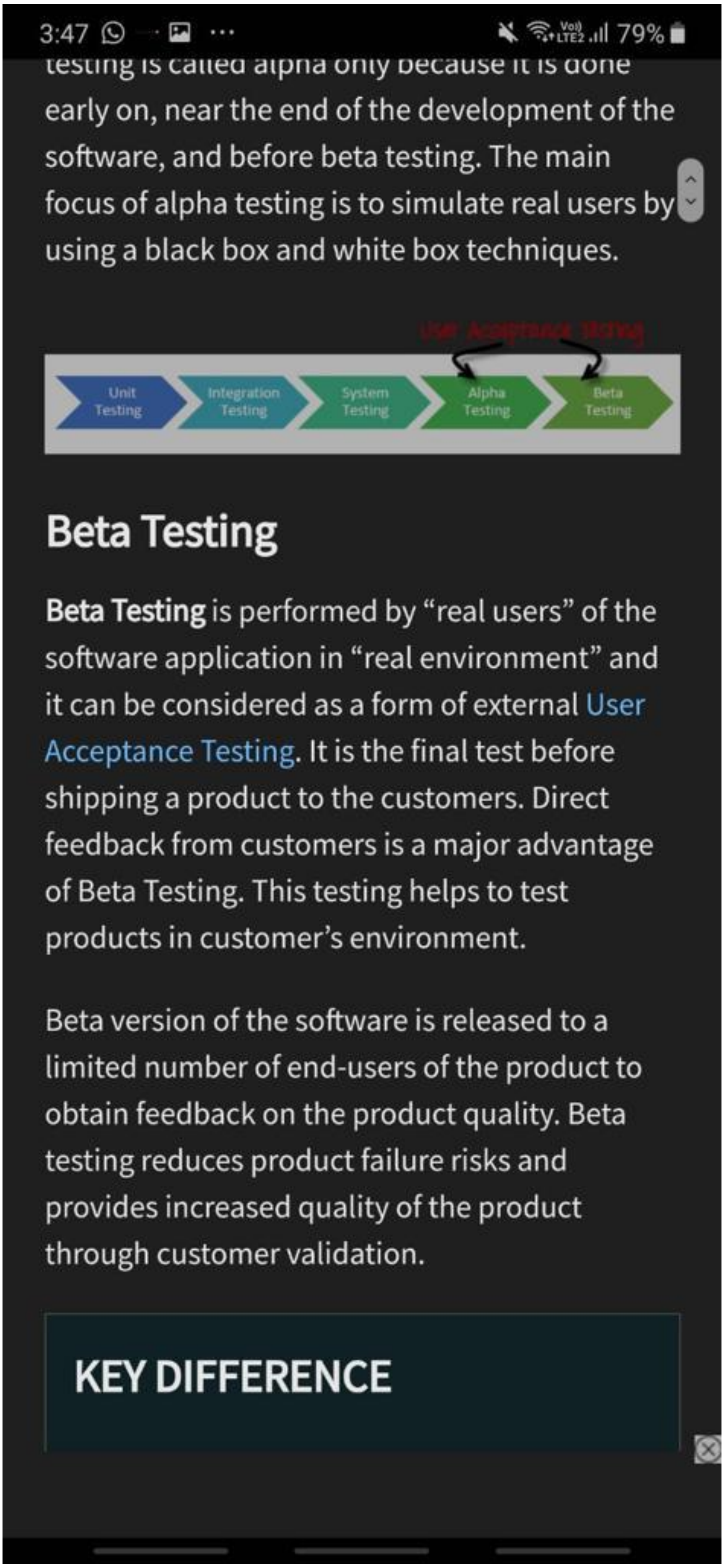
CISA REVIEW

Chapter 4 – IT Service Delivery and Support

Answer: Real-World Example

The bank's IS auditor should:

- Verify that the agreed-on SLAs were achievable by the outsourcing vendor.
- Verify that adequate and complete reports of SLA achievement were prepared by the vendor's IS department in good time for the monthly SLA management meetings.
- Verify that the SLA achievement reports highlighted any failures, included a reasonable explanation for the failures and outlined measures in place to ensure the failures did not recur.



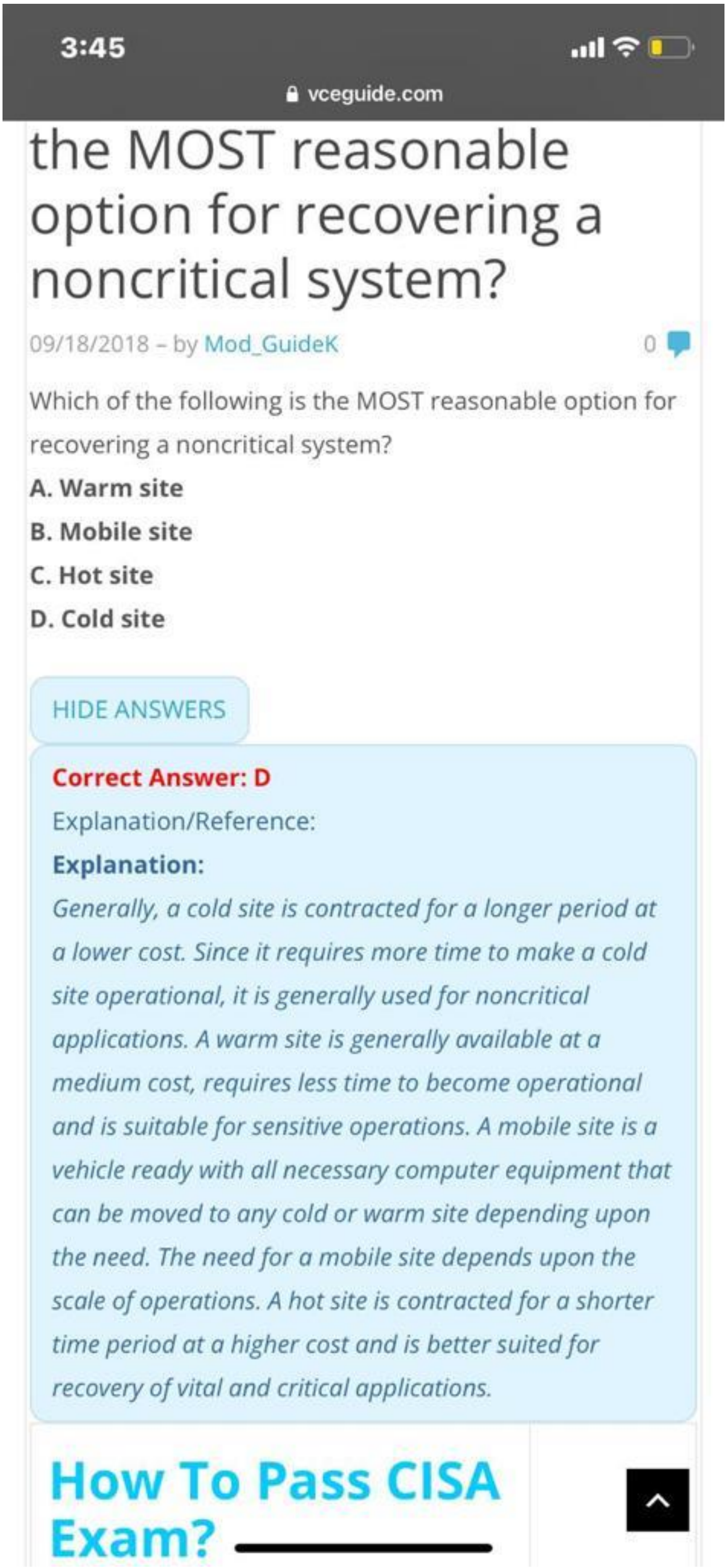
testing is called alpha only because it is done early on, near the end of the development of the software, and before beta testing. The main focus of alpha testing is to simulate real users by using a black box and white box techniques.

Beta Testing

Beta Testing is performed by "real users" of the software application in "real environment" and it can be considered as a form of external User Acceptance Testing. It is the final test before shipping a product to the customers. Direct feedback from customers is a major advantage of Beta Testing. This testing helps to test products in customer's environment.

Beta version of the software is released to a limited number of end-users of the product to obtain feedback on the product quality. Beta testing reduces product failure risks and provides increased quality of the product through customer validation.

KEY DIFFERENCE



the MOST reasonable option for recovering a noncritical system?

09/18/2018 – by Mod_GuideK

Which of the following is the MOST reasonable option for recovering a noncritical system?

A. Warm site

B. Mobile site

C. Hot site

D. Cold site

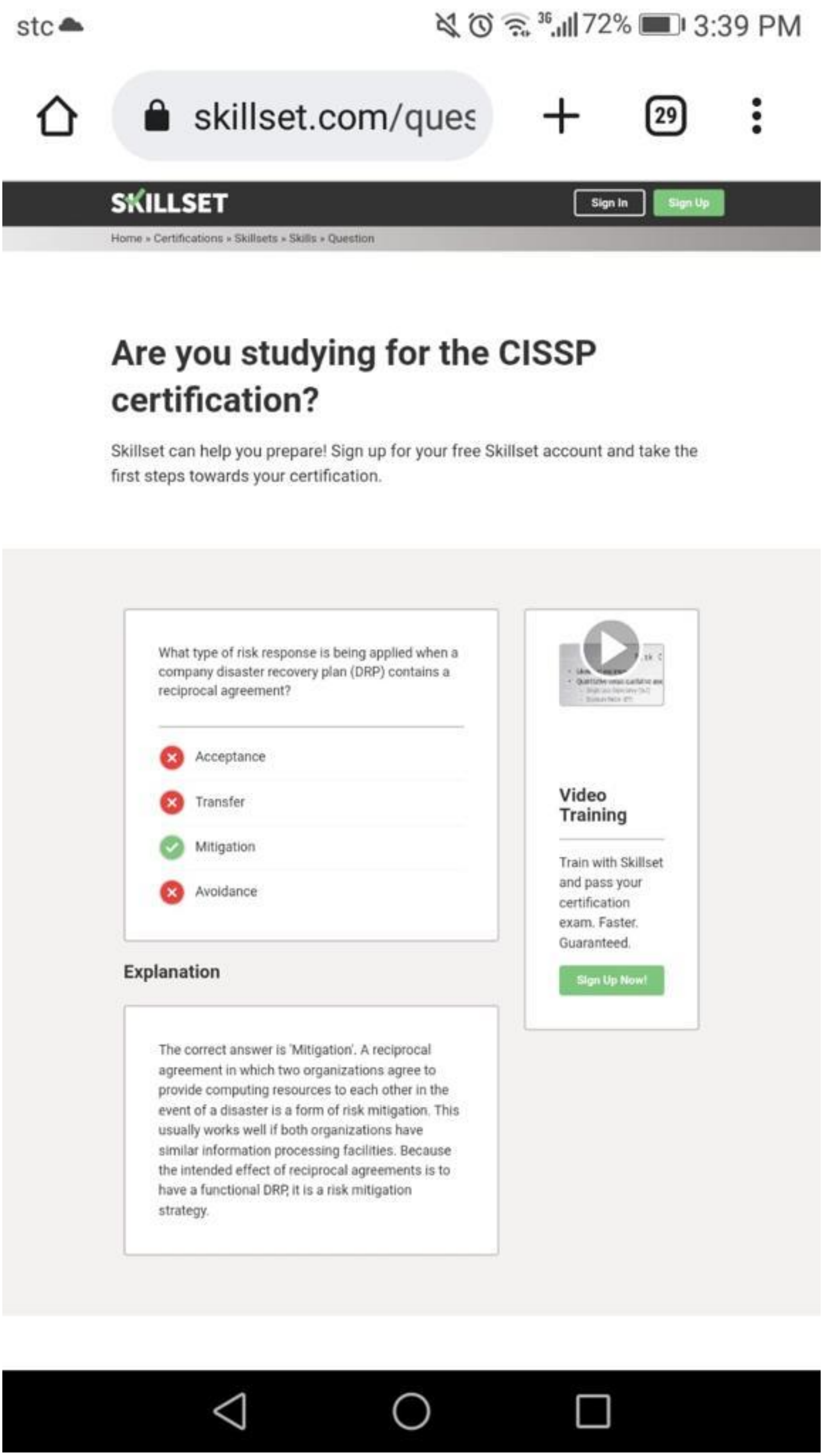
Correct Answer: D

Explanation/Reference:

Explanation:

Generally, a cold site is contracted for a longer period at a lower cost. Since it requires more time to make a cold site operational, it is generally used for noncritical applications. A warm site is generally available at a medium cost, requires less time to become operational and is suitable for sensitive operations. A mobile site is a vehicle ready with all necessary computer equipment that can be moved to any cold or warm site depending upon the need. The need for a mobile site depends upon the scale of operations. A hot site is contracted for a shorter time period at a higher cost and is better suited for recovery of vital and critical applications.

How To Pass CISA Exam?



Are you studying for the CISSP certification?

Skillset can help you prepare! Sign up for your free Skillset account and take the first steps towards your certification.

What type of risk response is being applied when a company disaster recovery plan (DRP) contains a reciprocal agreement?

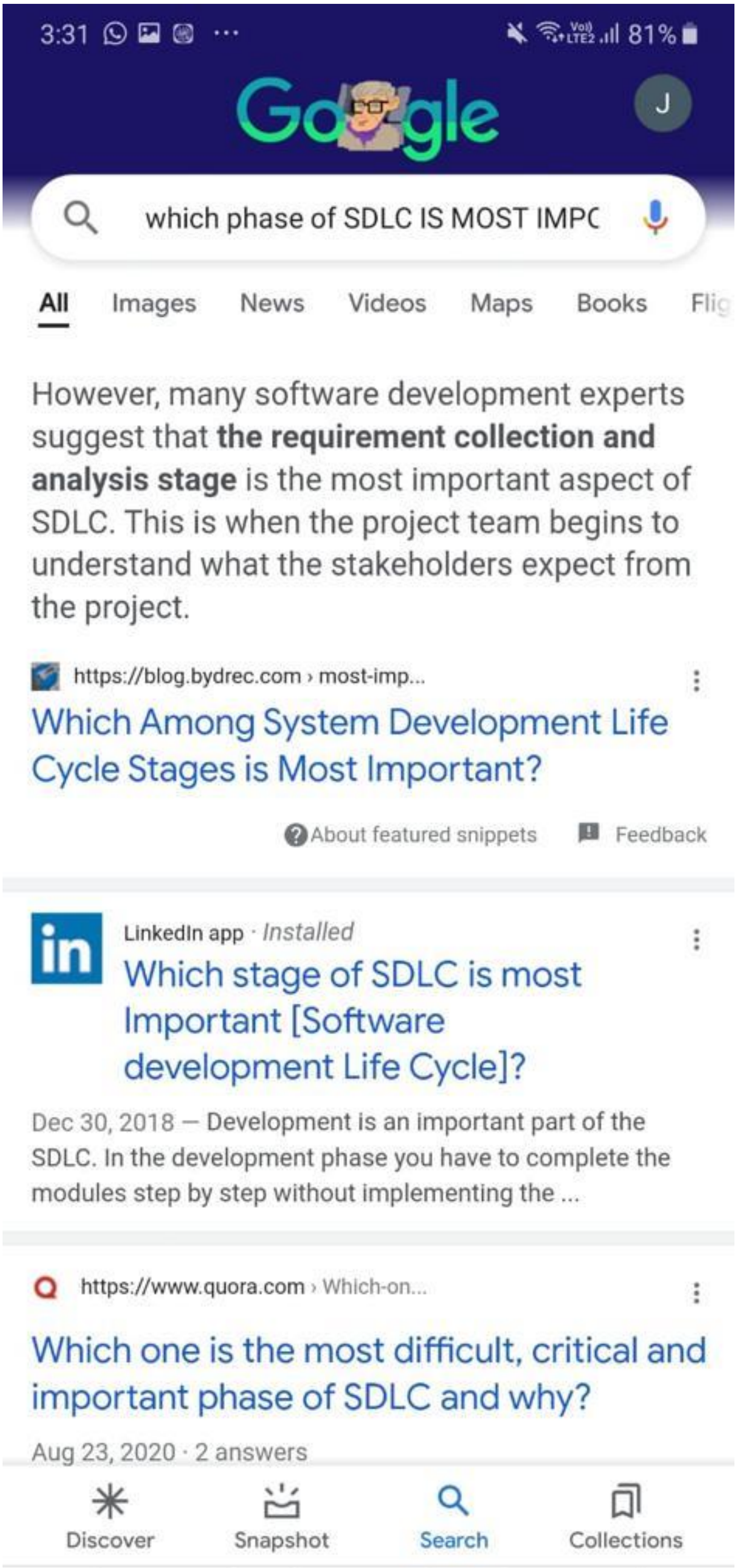
- ✗ Acceptance
- ✗ Transfer
- ✓ Mitigation
- ✗ Avoidance

Explanation

The correct answer is 'Mitigation'. A reciprocal agreement in which two organizations agree to provide computing resources to each other in the event of a disaster is a form of risk mitigation. This usually works well if both organizations have similar information processing facilities. Because the intended effect of reciprocal agreements is to have a functional DRP, it is a risk mitigation strategy.

Video Training

Train with Skillset and pass your certification exam. Faster. Guaranteed.



However, many software development experts suggest that **the requirement collection and analysis stage** is the most important aspect of SDLC. This is when the project team begins to understand what the stakeholders expect from the project.

https://blog.bydrec.com › most-imp...

Which Among System Development Life Cycle Stages is Most Important?

LinkedIn app · *Installed*

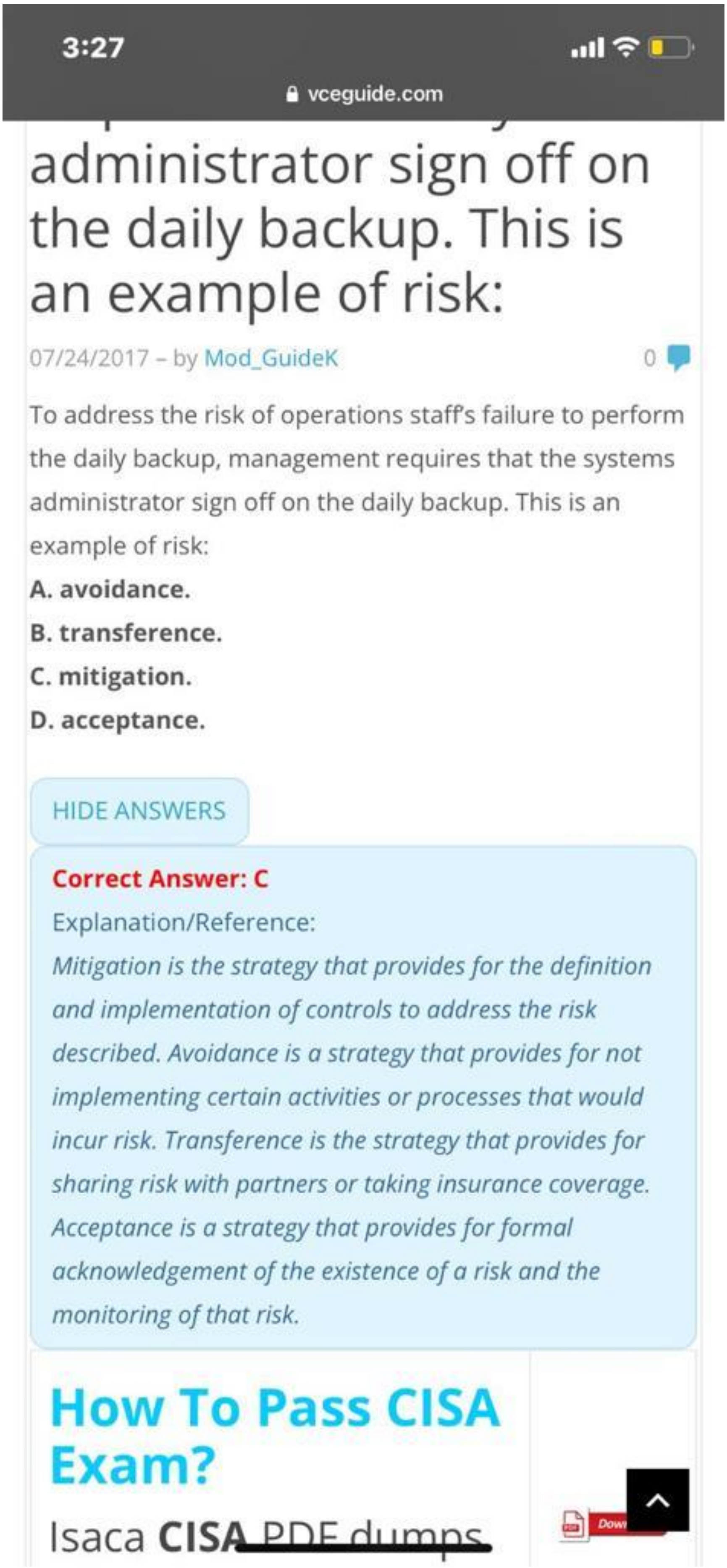
Which stage of SDLC is most Important [Software development Life Cycle]?

Dec 30, 2018 — Development is an important part of the SDLC. In the development phase you have to complete the modules step by step without implementing the ...

https://www.quora.com › Which-on...

Which one is the most difficult, critical and important phase of SDLC and why?

Aug 23, 2020 · 2 answers



administrator sign off on the daily backup. This is an example of risk:

07/24/2017 – by Mod_GuideK 0

To address the risk of operations staff's failure to perform the daily backup, management requires that the systems administrator sign off on the daily backup. This is an example of risk:

A. avoidance.

B. transference.

C. mitigation.

D. acceptance.

HIDE ANSWERS

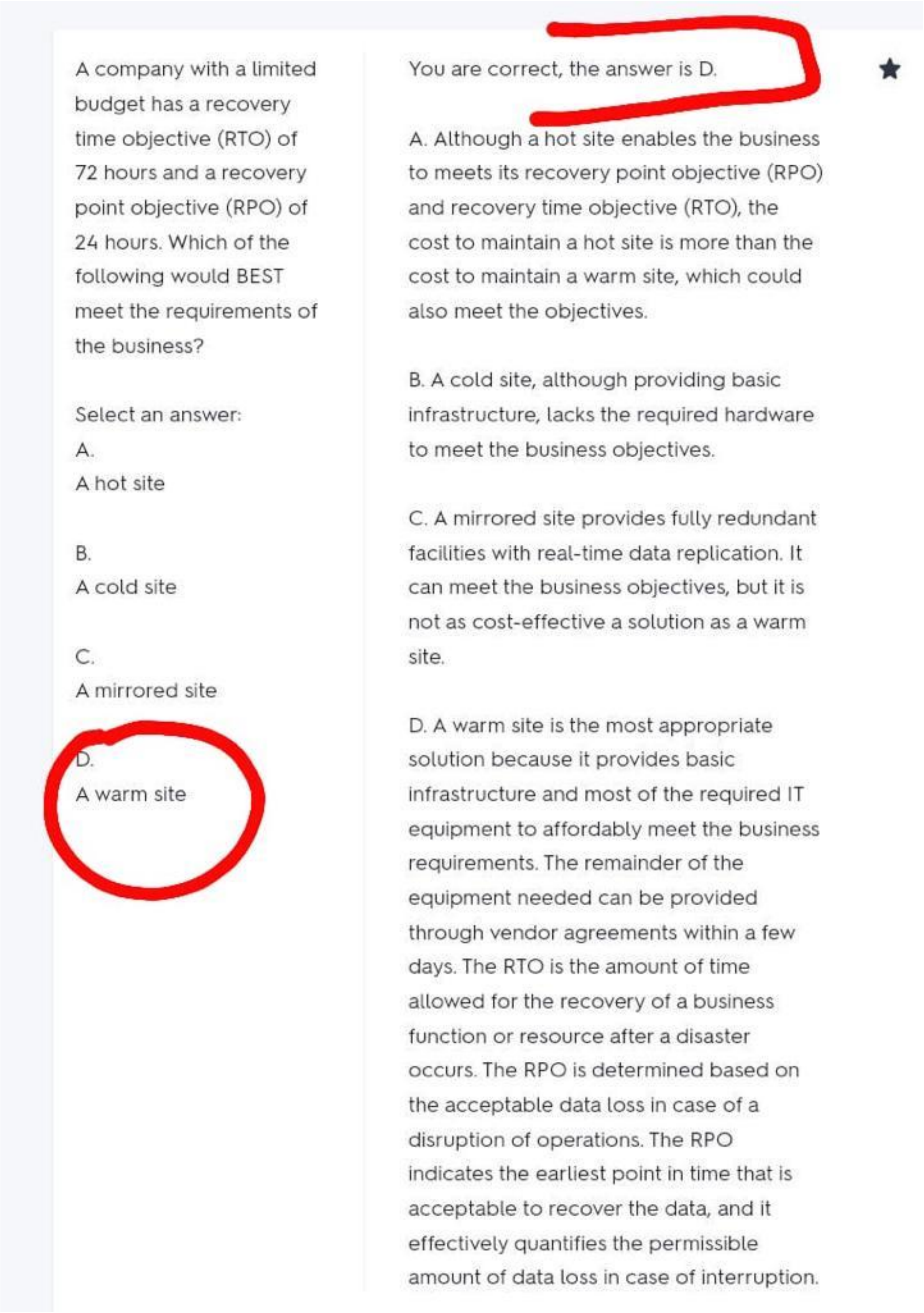
Correct Answer: C

Explanation/Reference:

Mitigation is the strategy that provides for the definition and implementation of controls to address the risk described. Avoidance is a strategy that provides for not implementing certain activities or processes that would incur risk. Transference is the strategy that provides for sharing risk with partners or taking insurance coverage. Acceptance is a strategy that provides for formal acknowledgement of the existence of a risk and the monitoring of that risk.

How To Pass CISA Exam?

Isaca **CISA** PDF dumps



A company with a limited budget has a recovery time objective (RTO) of 72 hours and a recovery point objective (RPO) of 24 hours. Which of the following would BEST meet the requirements of the business?

Select an answer:

A.
A hot site

B.
A cold site

C.
A mirrored site

[✓ D.
A warm site]

You are correct, the answer is D.

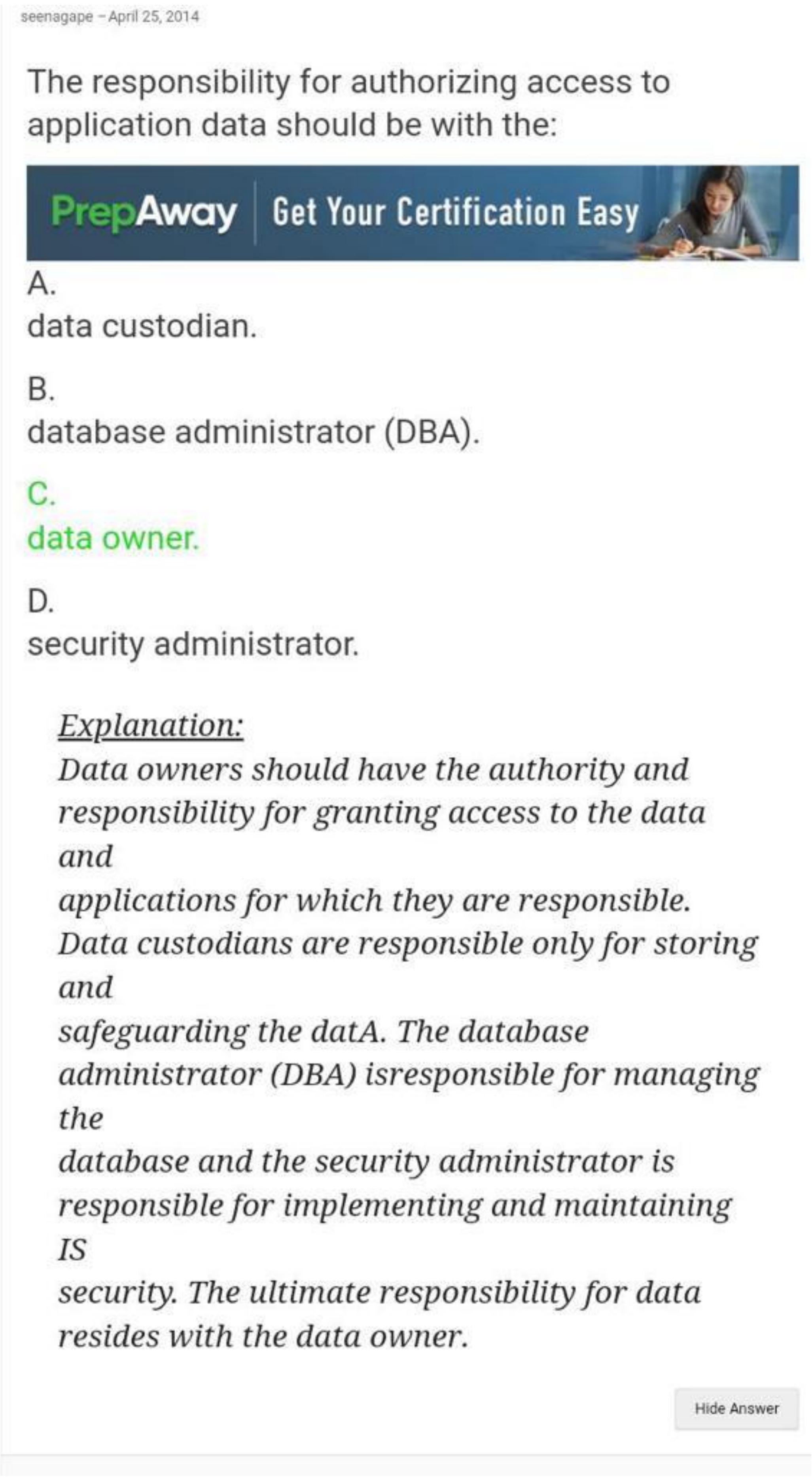
★

A. Although a hot site enables the business to meets its recovery point objective (RPO) and recovery time objective (RTO), the cost to maintain a hot site is more than the cost to maintain a warm site, which could also meet the objectives.

B. A cold site, although providing basic infrastructure, lacks the required hardware to meet the business objectives.

C. A mirrored site provides fully redundant facilities with real-time data replication. It can meet the business objectives, but it is not as cost-effective a solution as a warm site.

D. A warm site is the most appropriate solution because it provides basic infrastructure and most of the required IT equipment to affordably meet the business requirements. The remainder of the equipment needed can be provided through vendor agreements within a few days. The RTO is the amount of time allowed for the recovery of a business function or resource after a disaster occurs. The RPO is determined based on the acceptable data loss in case of a disruption of operations. The RPO indicates the earliest point in time that is acceptable to recover the data, and it effectively quantifies the permissible amount of data loss in case of interruption.



seenagape – April 25, 2014

The responsibility for authorizing access to application data should be with the:

A.
data custodian.

B.
database administrator (DBA).

C.
data owner.

D.
security administrator.

Explanation:

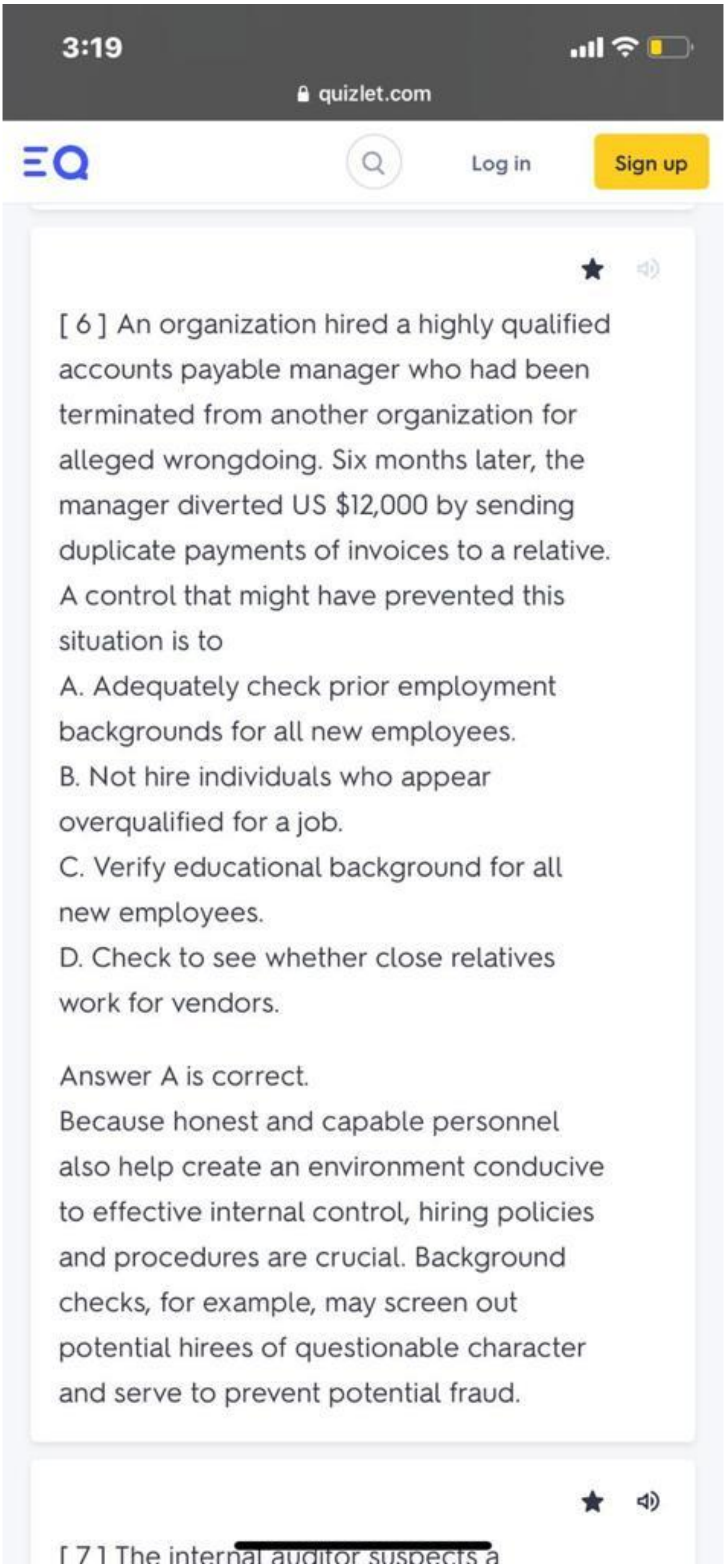
Data owners should have the authority and responsibility for granting access to the data and

applications for which they are responsible. Data custodians are responsible only for storing and

safeguarding the datA. The database administrator (DBA) isresponsible for managing the

database and the security administrator is responsible for implementing and maintaining IS

security. The ultimate responsibility for data resides with the data owner.



[6] An organization hired a highly qualified accounts payable manager who had been terminated from another organization for alleged wrongdoing. Six months later, the manager diverted US $12,000 by sending duplicate payments of invoices to a relative. A control that might have prevented this situation is to

A. Adequately check prior employment backgrounds for all new employees.

B. Not hire individuals who appear overqualified for a job.

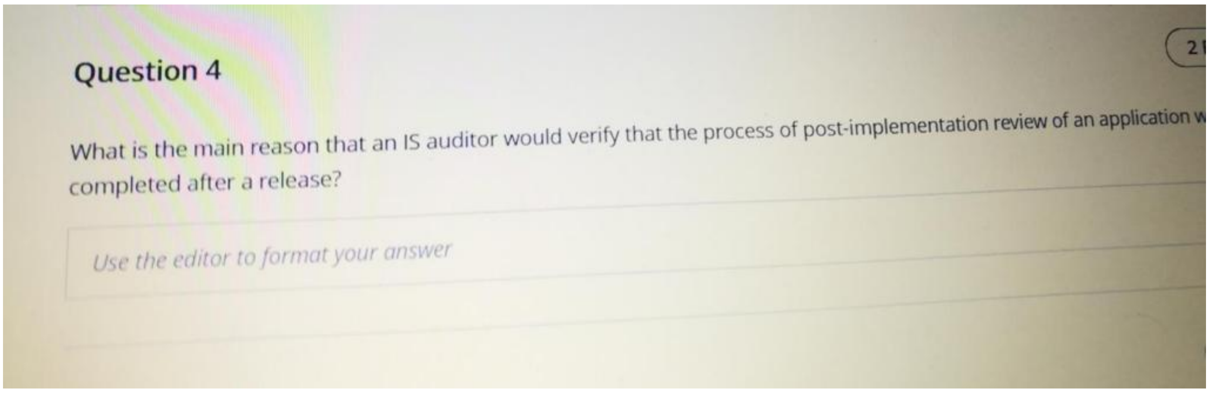
C. Verify educational background for all new employees.

D. Check to see whether close relatives work for vendors.

Answer A is correct.

Because honest and capable personnel also help create an environment conducive to effective internal control, hiring policies and procedures are crucial. Background checks, for example, may screen out potential hirees of questionable character and serve to prevent potential fraud.

[7] The internal auditor suspects a

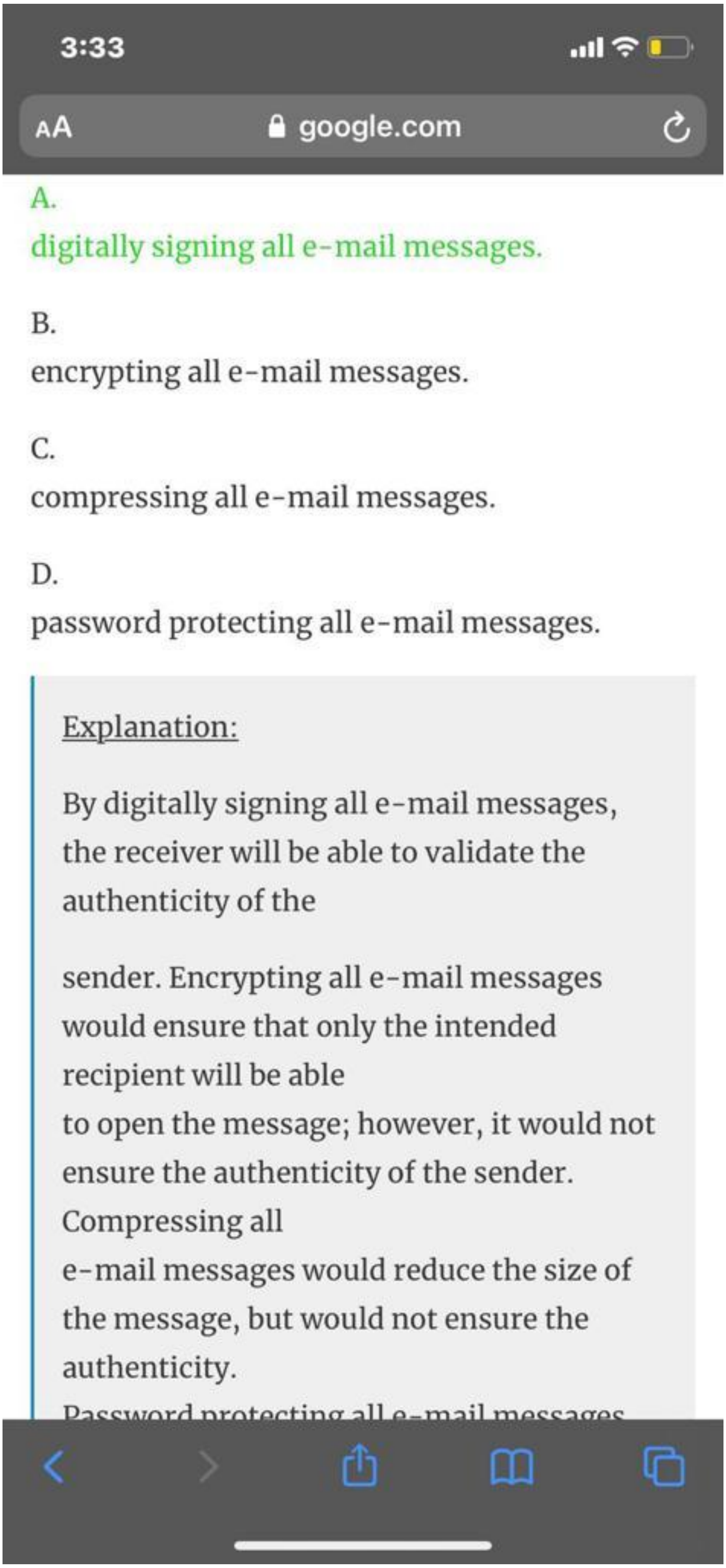


2

Question 4

What is the main reason that an IS auditor would verify that the process of post-implementation review of an application w
completed after a release?

Use the editor to format your answer



A.

digitally signing all e-mail messages.

B.

encrypting all e-mail messages.

C.

compressing all e-mail messages.

D.

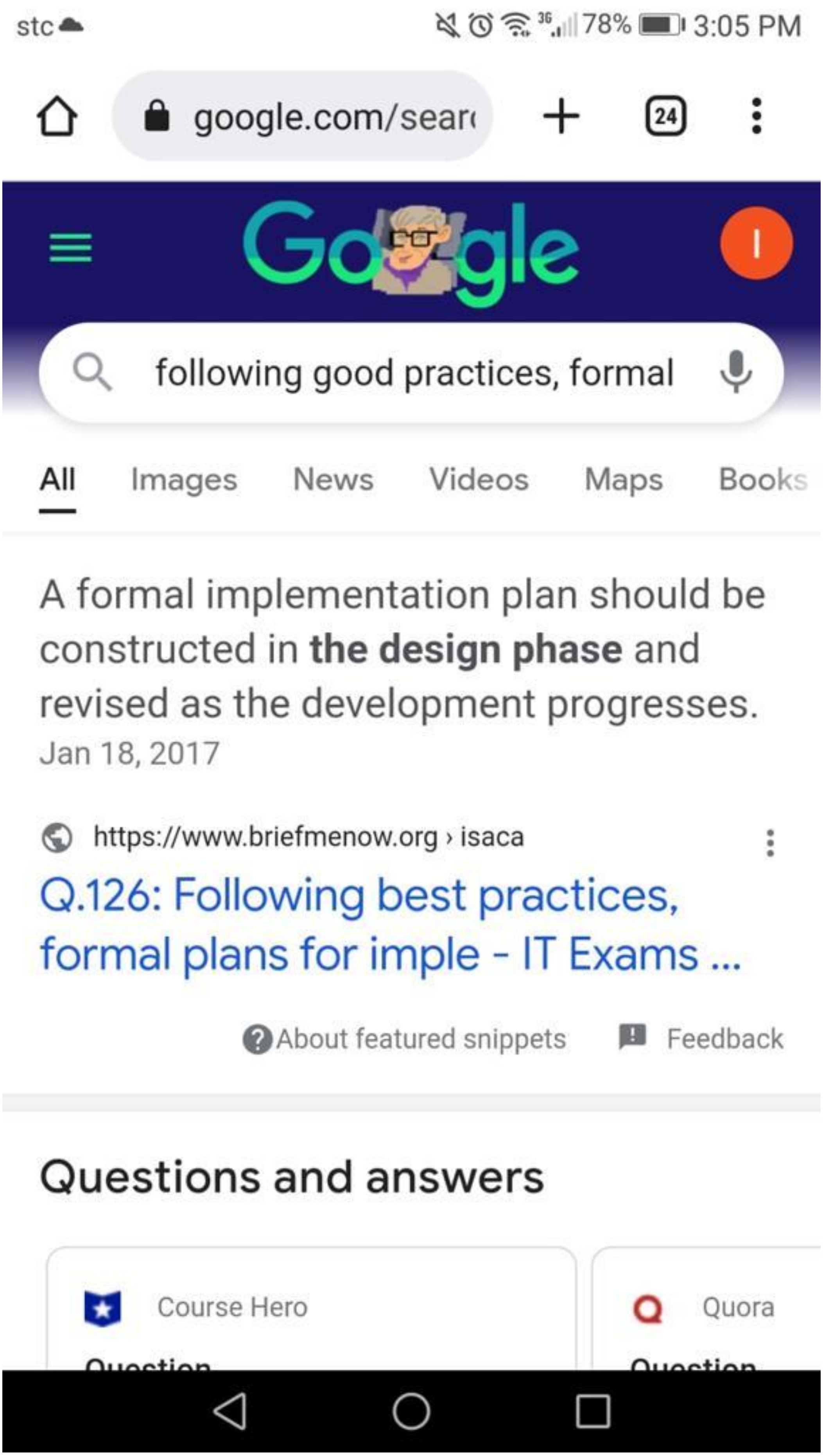
password protecting all e-mail messages.

Explanation:

By digitally signing all e-mail messages, the receiver will be able to validate the authenticity of the

sender. Encrypting all e-mail messages would ensure that only the intended recipient will be able to open the message; however, it would not ensure the authenticity of the sender. Compressing all e-mail messages would reduce the size of the message, but would not ensure the authenticity.

Password protecting all e-mail messages



following good practices, formal

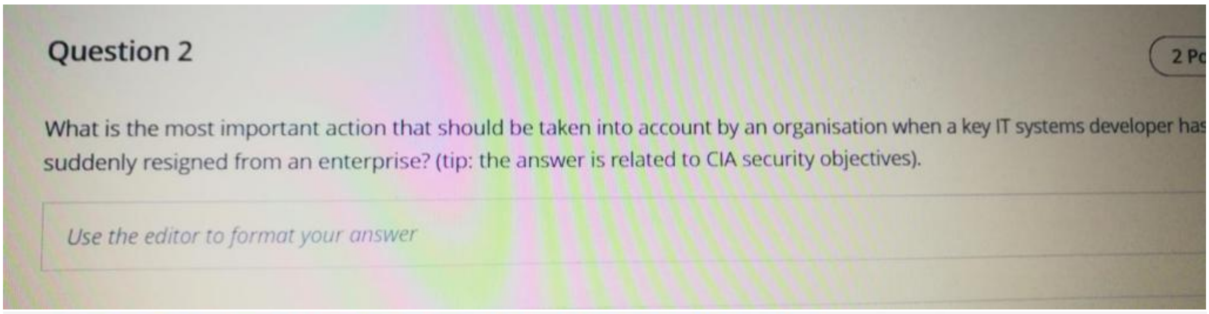
A formal implementation plan should be constructed in **the design phase** and revised as the development progresses.

Jan 18, 2017

https://www.briefmenow.org › isaca

Q.126: Following best practices, formal plans for imple - IT Exams ...

Questions and answers

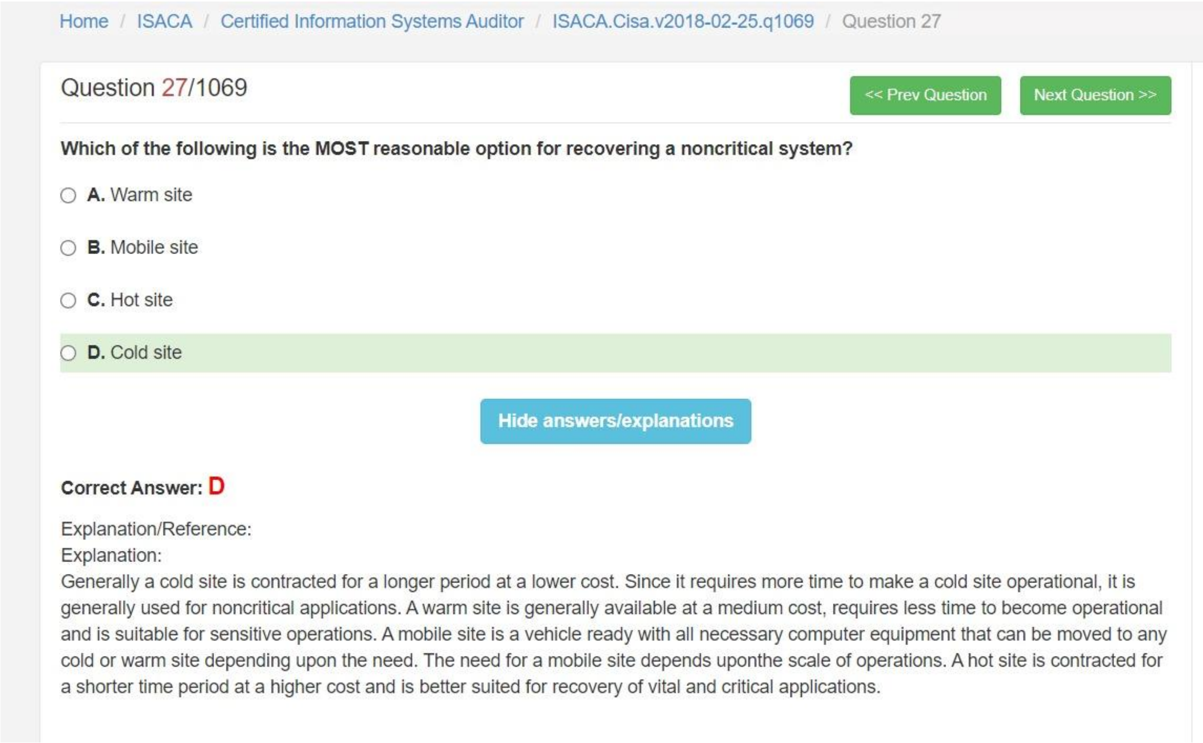


Question 2

2 Po

What is the most important action that should be taken into account by an organisation when a key IT systems developer has suddenly resigned from an enterprise? (tip: the answer is related to CIA security objectives).

Use the editor to format your answer



Home / ISACA / Certified Information Systems Auditor / ISACA.Cisa.v2018-02-25.q1069 / Question 27

Question 27/1069

<< Prev Question Next Question >>

Which of the following is the MOST reasonable option for recovering a noncritical system?

○ **A.** Warm site

○ **B.** Mobile site

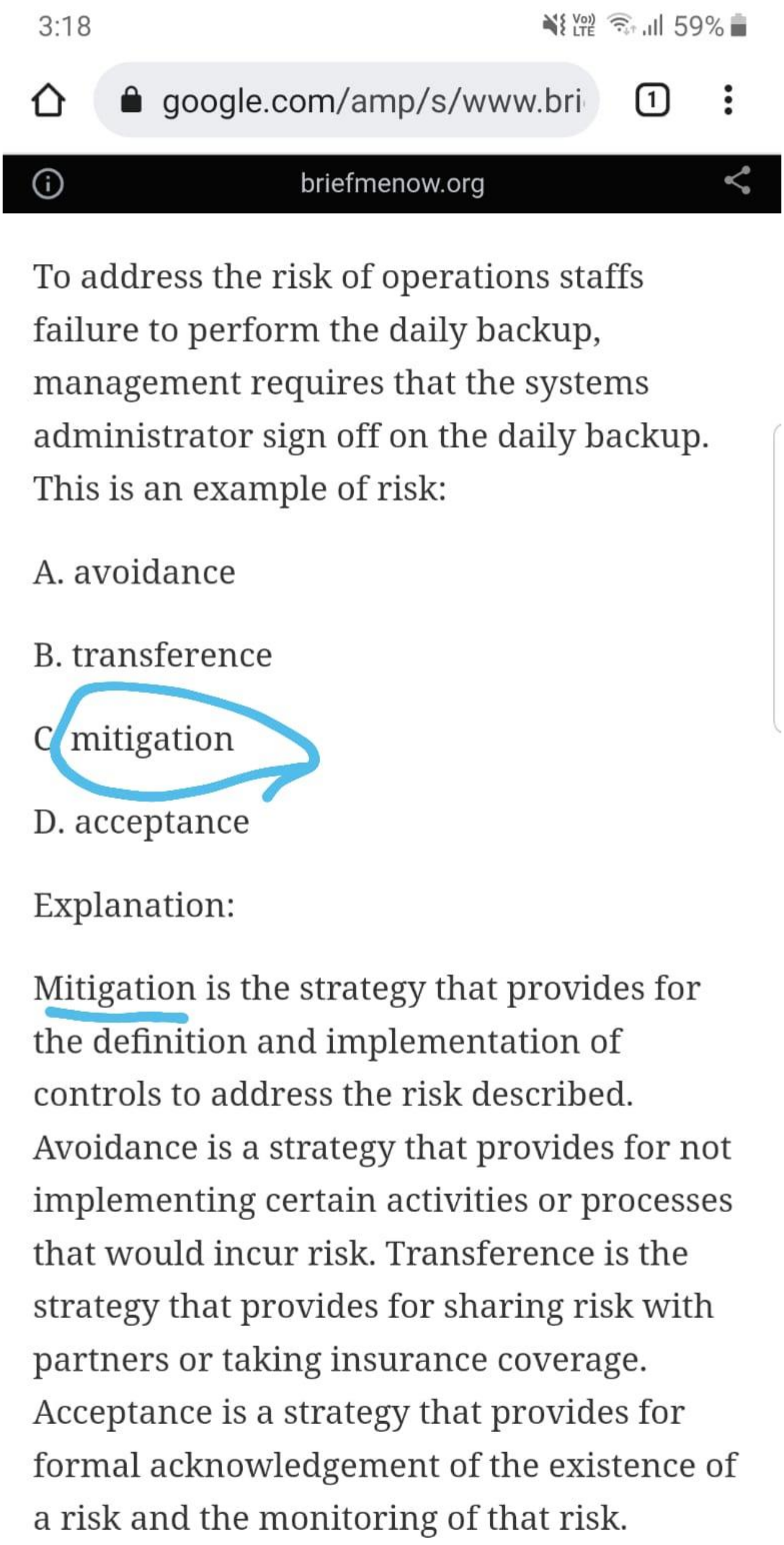
○ **C.** Hot site

○ **D.** Cold site

Hide answers/explanations

Correct Answer: D

Explanation/Reference:
Explanation:
Generally a cold site is contracted for a longer period at a lower cost. Since it requires more time to make a cold site operational, it is generally used for noncritical applications. A warm site is generally available at a medium cost, requires less time to become operational and is suitable for sensitive operations. A mobile site is a vehicle ready with all necessary computer equipment that can be moved to any cold or warm site depending upon the need. The need for a mobile site depends uponthe scale of operations. A hot site is contracted for a shorter time period at a higher cost and is better suited for recovery of vital and critical applications.



To address the risk of operations staffs failure to perform the daily backup, management requires that the systems administrator sign off on the daily backup. This is an example of risk:

A. avoidance

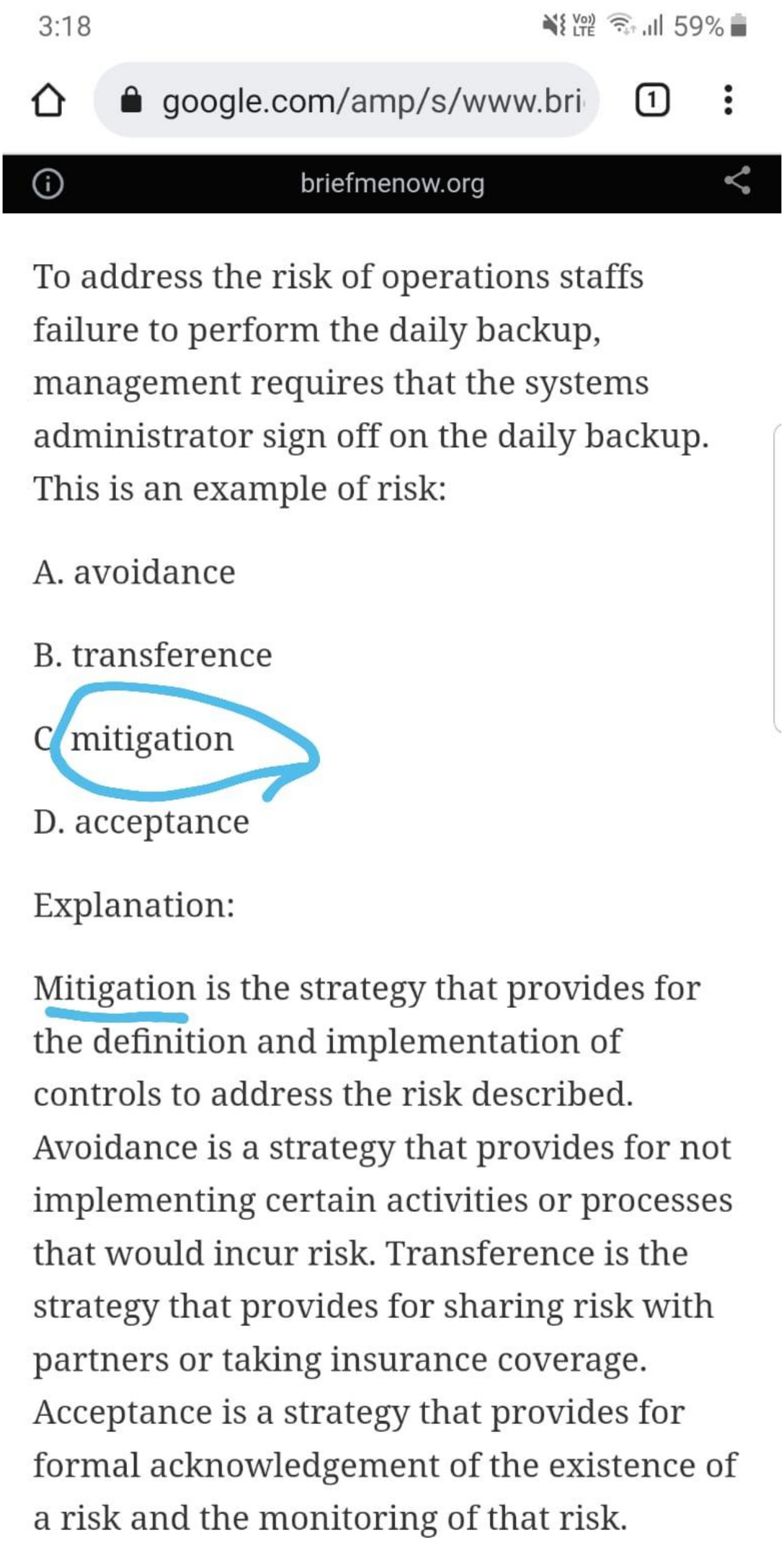
B. transference

[✓ C. mitigation]

D. acceptance

Explanation:

Mitigation is the strategy that provides for the definition and implementation of controls to address the risk described. Avoidance is a strategy that provides for not implementing certain activities or processes that would incur risk. Transference is the strategy that provides for sharing risk with partners or taking insurance coverage. Acceptance is a strategy that provides for formal acknowledgement of the existence of a risk and the monitoring of that risk.



To address the risk of operations staffs failure to perform the daily backup, management requires that the systems administrator sign off on the daily backup. This is an example of risk:

A. avoidance

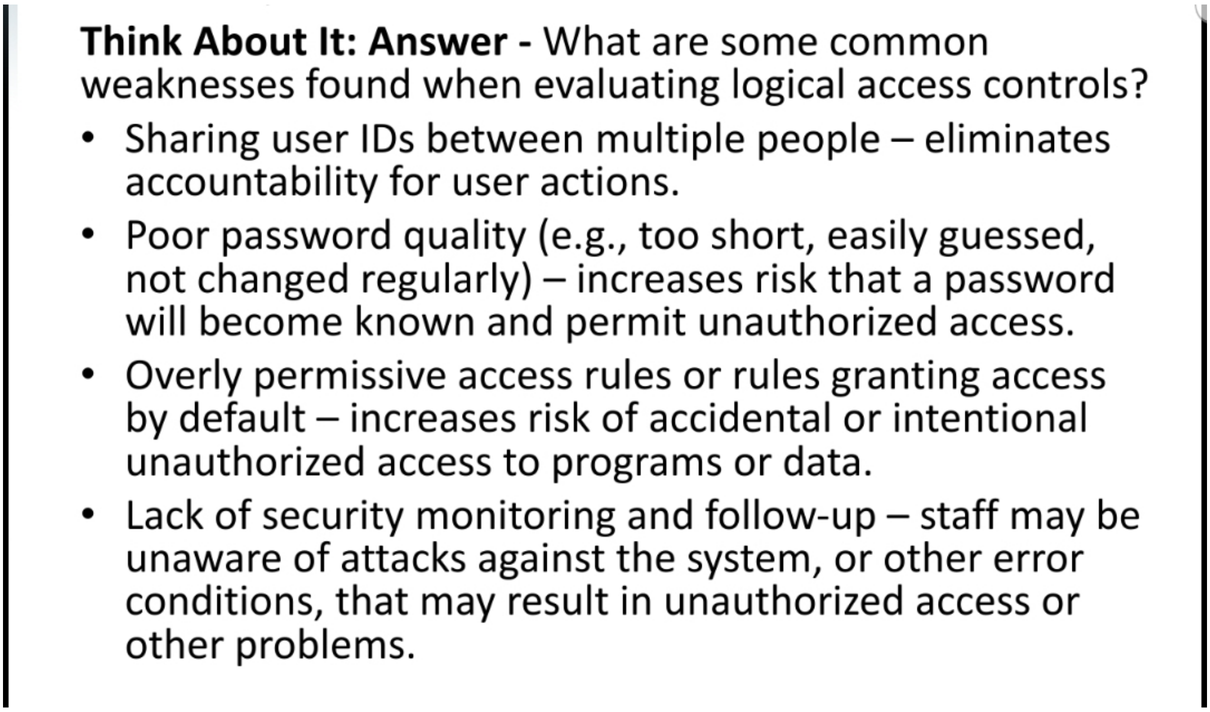
B. transference

[✓ C. mitigation]

D. acceptance

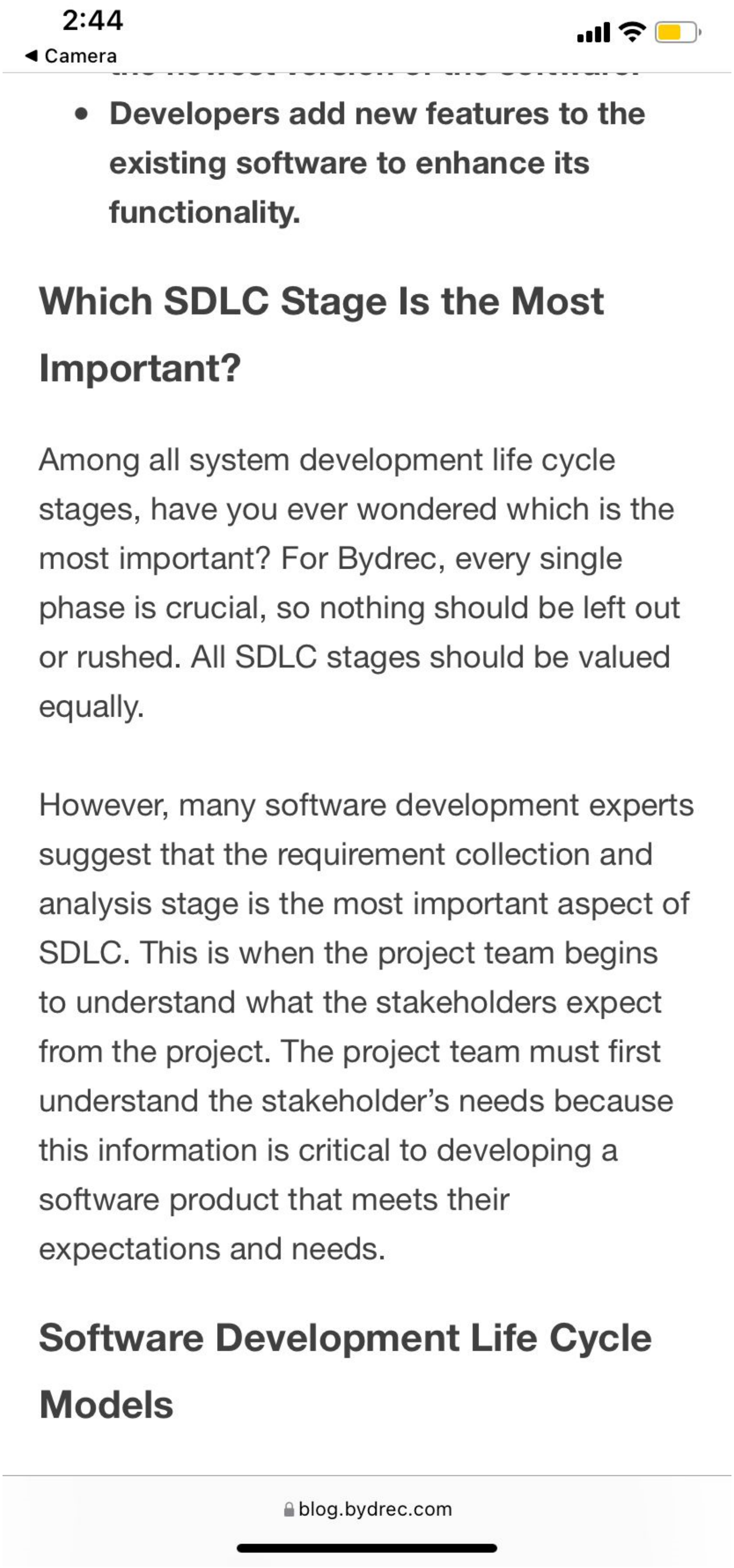
Explanation:

Mitigation is the strategy that provides for the definition and implementation of controls to address the risk described. Avoidance is a strategy that provides for not implementing certain activities or processes that would incur risk. Transference is the strategy that provides for sharing risk with partners or taking insurance coverage. Acceptance is a strategy that provides for formal acknowledgement of the existence of a risk and the monitoring of that risk.



Think About It: Answer - What are some common weaknesses found when evaluating logical access controls?

- Sharing user IDs between multiple people – eliminates accountability for user actions.
- Poor password quality (e.g., too short, easily guessed, not changed regularly) – increases risk that a password will become known and permit unauthorized access.
- Overly permissive access rules or rules granting access by default – increases risk of accidental or intentional unauthorized access to programs or data.
- Lack of security monitoring and follow-up – staff may be unaware of attacks against the system, or other error conditions, that may result in unauthorized access or other problems.



- **Developers add new features to the existing software to enhance its functionality.**

Which SDLC Stage Is the Most Important?

Among all system development life cycle stages, have you ever wondered which is the most important? For Bydrec, every single phase is crucial, so nothing should be left out or rushed. All SDLC stages should be valued equally.

However, many software development experts suggest that the requirement collection and analysis stage is the most important aspect of SDLC. This is when the project team begins to understand what the stakeholders expect from the project. The project team must first understand the stakeholder's needs because this information is critical to developing a software product that meets their expectations and needs.

Software Development Life Cycle Models

Think About It: Answer - What are some common weaknesses found when evaluating logical access controls?

- Sharing user IDs between multiple people – eliminates accountability for user actions.
- Poor password quality (e.g., too short, easily guessed, not changed regularly) – increases risk that a password will become known and permit unauthorized access.
- Overly permissive access rules or rules granting access by default – increases risk of accidental or intentional unauthorized access to programs or data.
- Lack of security monitoring and follow-up – staff may be unaware of attacks against the system, or other error conditions, that may result in unauthorized access or other problems.