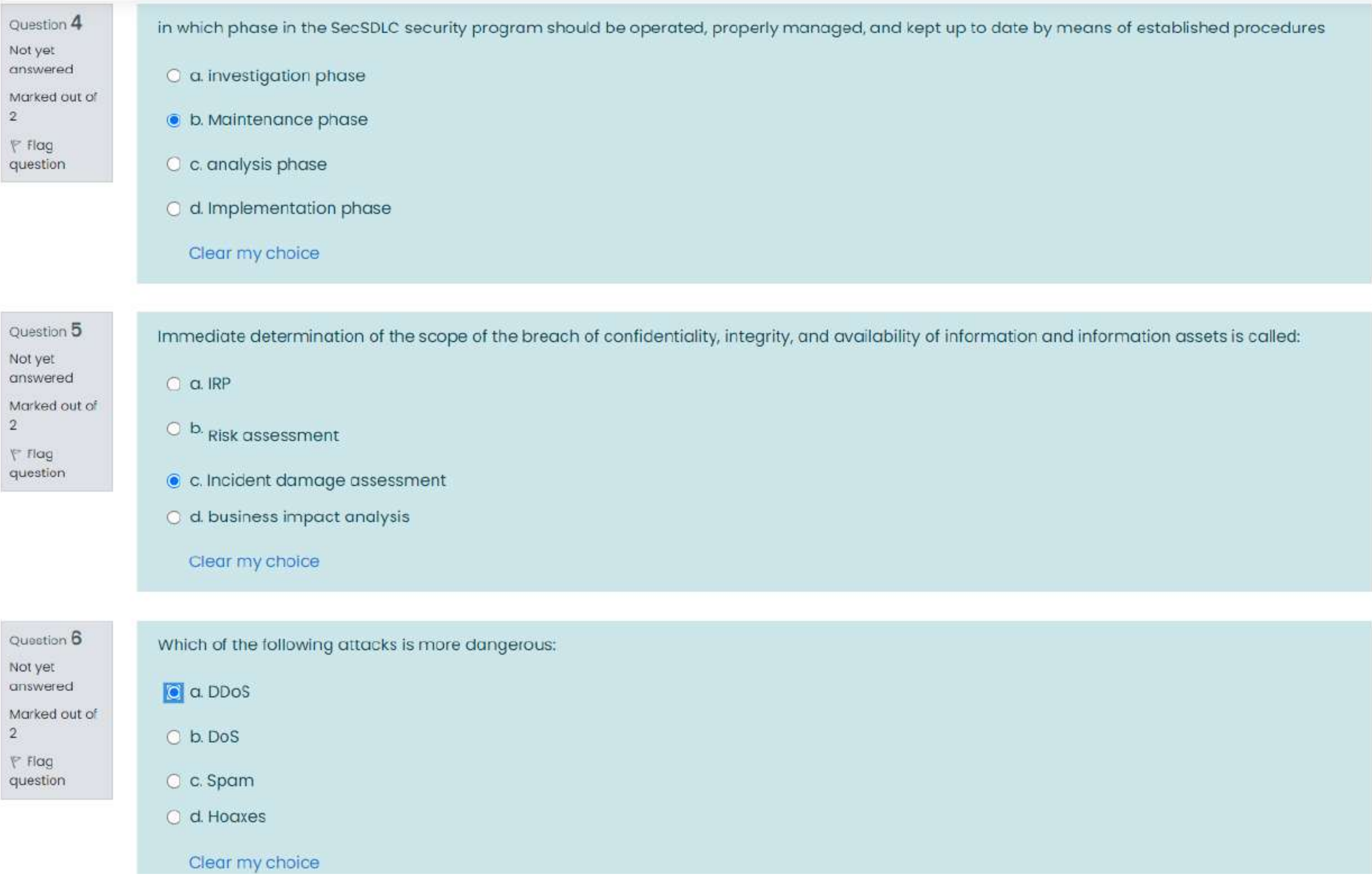


Question **4**

Not yet answered

Marked out of 2

in which phase in the SecSDLC security program should be operated, properly managed, and kept up to date by means of established procedures

○ a. investigation phase

● b. Maintenance phase

○ c. analysis phase

○ d. Implementation phase

Question **5**

Not yet answered

Marked out of 2

Immediate determination of the scope of the breach of confidentiality, integrity, and availability of information and information assets is called:

○ a. IRP

○ b. Risk assessment

● c. Incident damage assessment

○ d. business impact analysis

Question **6**

Not yet answered

Marked out of 2

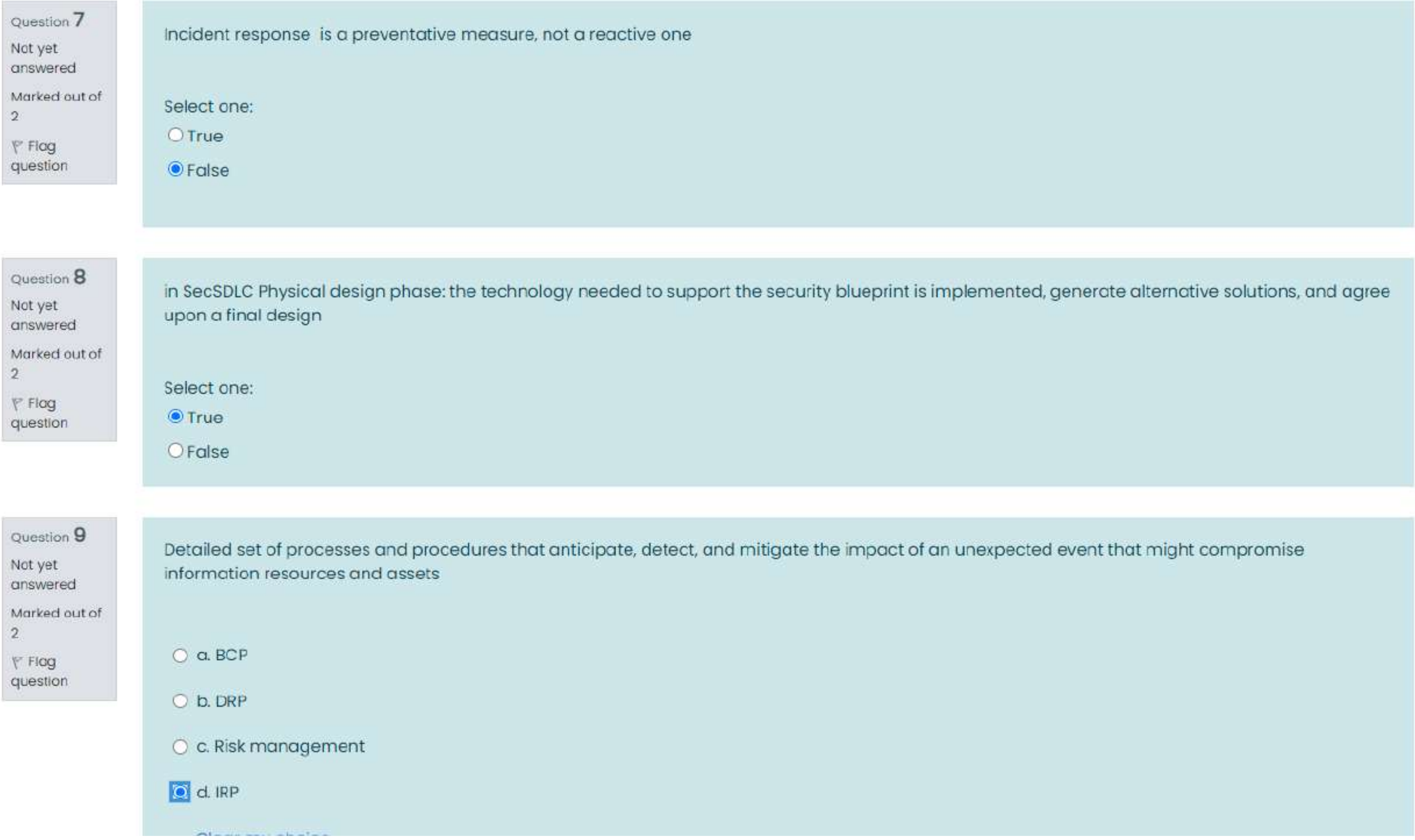
Which of the following attacks is more dangerous:

● a. DDoS

○ b. DoS

○ c. Spam

○ d. Hoaxes



Question 7

Not yet answered

Marked out of 2

Flag question

Incident response is a preventative measure, not a reactive one

Select one:

○ True

● False

Question 8

Not yet answered

Marked out of 2

Flag question

in SecSDLC Physical design phase: the technology needed to support the security blueprint is implemented, generate alternative solutions, and agree upon a final design

Select one:

● True

○ False

Question 9

Not yet answered

Marked out of 2

Flag question

Detailed set of processes and procedures that anticipate, detect, and mitigate the impact of an unexpected event that might compromise information resources and assets

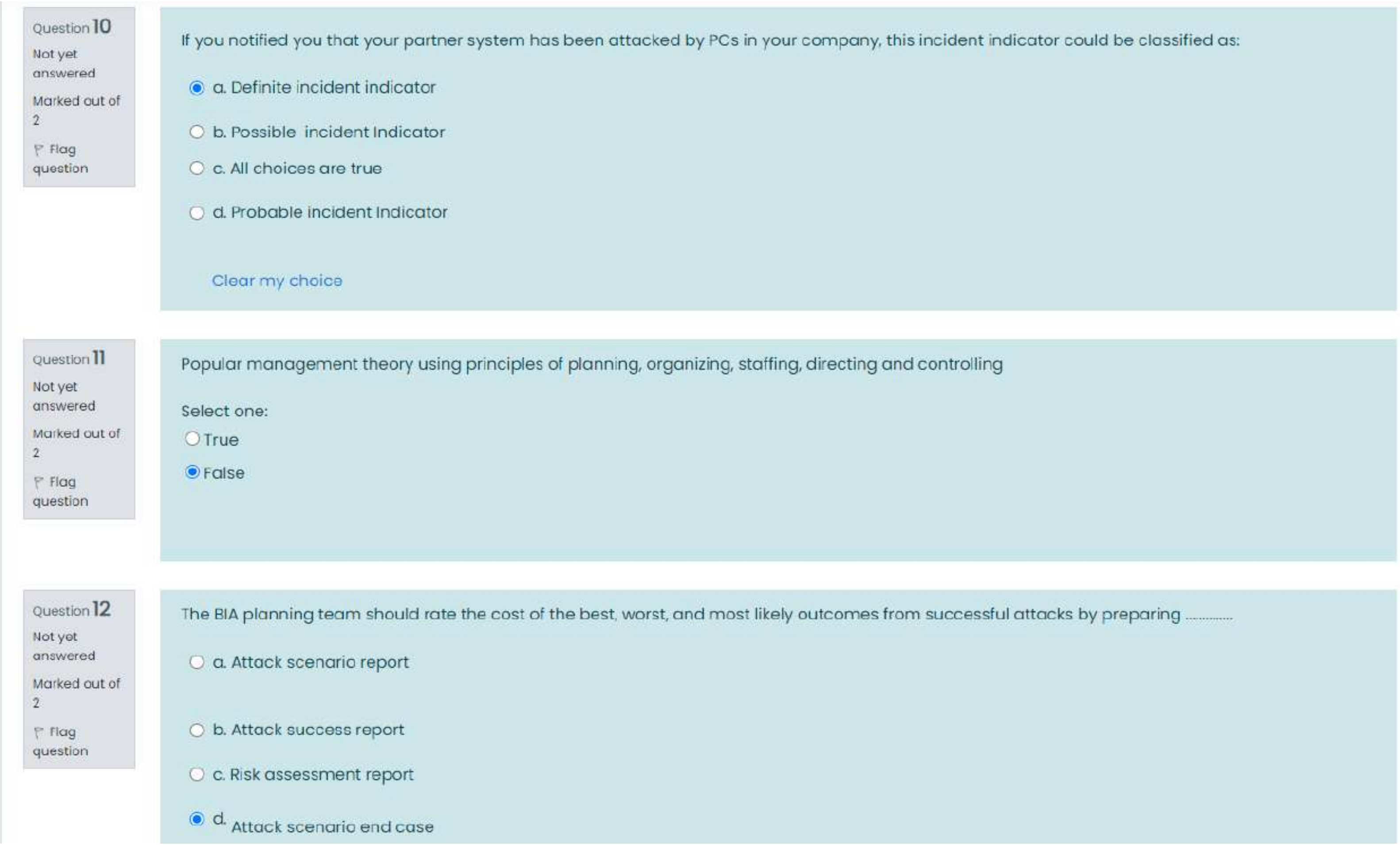
○ a. BCP

○ b. DRP

○ c. Risk management

● d. IRP

Clear my choice



Question 10
Not yet answered
Marked out of 2
Flag question

If you notified you that your partner system has been attacked by PCs in your company, this incident indicator could be classified as:

● a. Definite incident indicator

○ b. Possible incident Indicator

○ c. All choices are true

○ d. Probable incident Indicator

Clear my choice

Question 11
Not yet answered
Marked out of 2
Flag question

Popular management theory using principles of planning, organizing, staffing, directing and controlling

Select one:

○ True

● False

Question 12
Not yet answered
Marked out of 2
Flag question

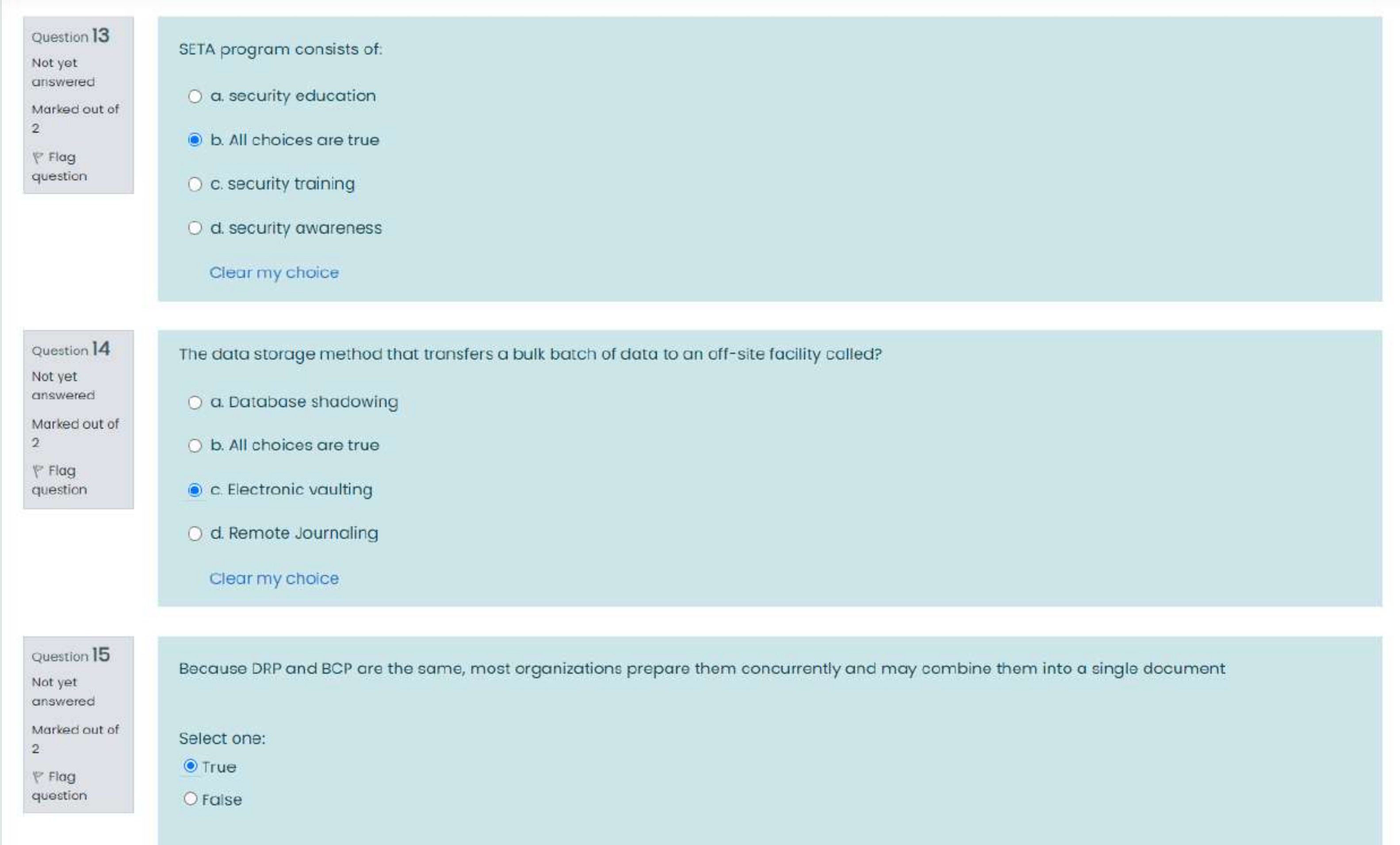
The BIA planning team should rate the cost of the best, worst, and most likely outcomes from successful attacks by preparing ....

○ a. Attack scenario report

○ b. Attack success report

○ c. Risk assessment report

● d. Attack scenario end case



Question 13

Not yet answered

Marked out of 2

Flag question

SETA program consists of:

○ a. security education

● b. All choices are true

○ c. security training

○ d. security awareness

Clear my choice

Question 14

Not yet answered

Marked out of 2

Flag question

The data storage method that transfers a bulk batch of data to an off-site facility called?

○ a. Database shadowing

○ b. All choices are true

● c. Electronic vaulting

○ d. Remote Journaling

Clear my choice

Question 15

Not yet answered

Marked out of 2

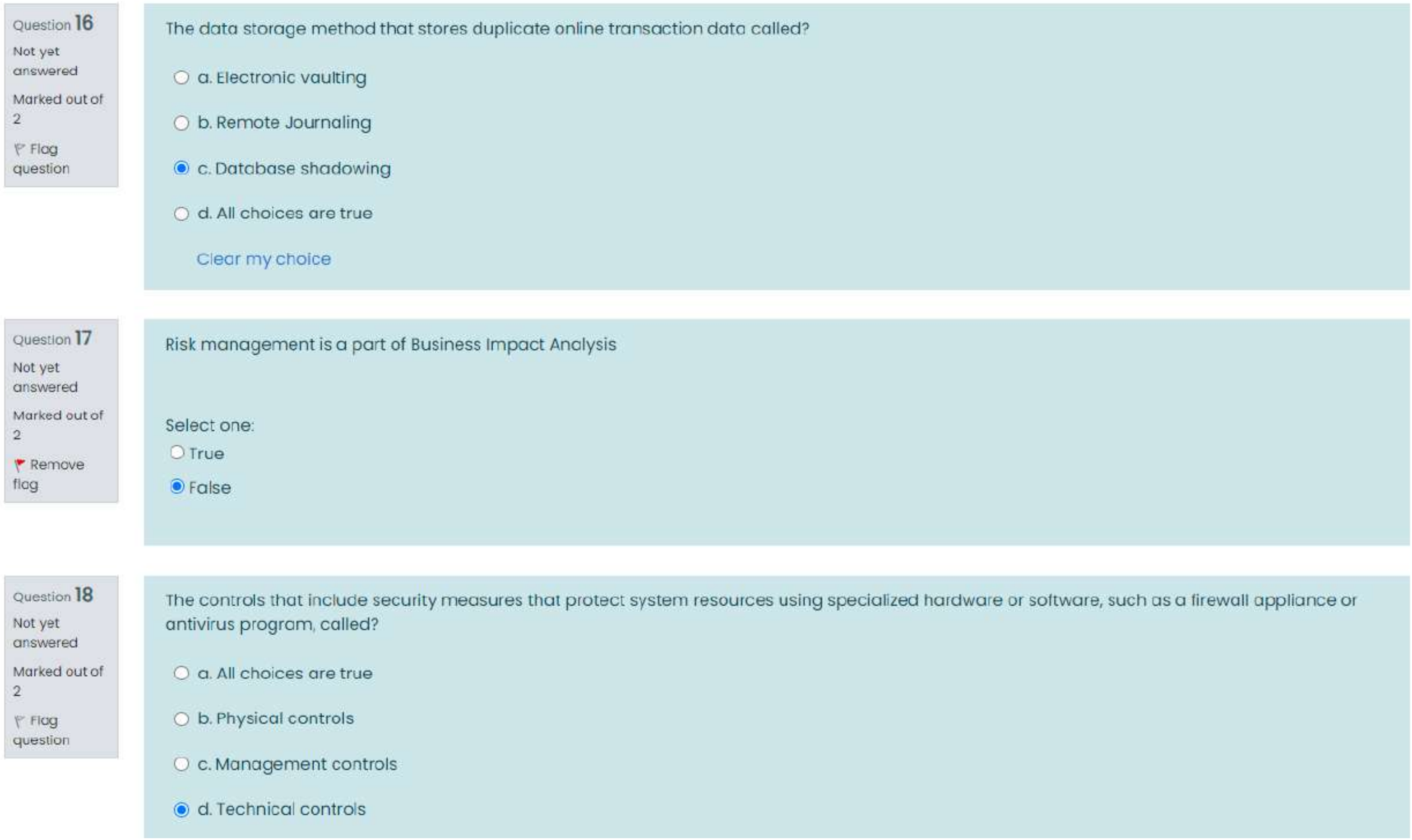
Flag question

Because DRP and BCP are the same, most organizations prepare them concurrently and may combine them into a single document

Select one:

● True

○ False



Question 16

Not yet answered

Marked out of 2

Flag question

The data storage method that stores duplicate online transaction data called?

○ a. Electronic vaulting

○ b. Remote Journaling

● c. Database shadowing

○ d. All choices are true

Clear my choice

Question 17

Not yet answered

Marked out of 2

Remove flag

Risk management is a part of Business Impact Analysis

Select one:

○ True

● False

Question 18

Not yet answered

Marked out of 2

Flag question

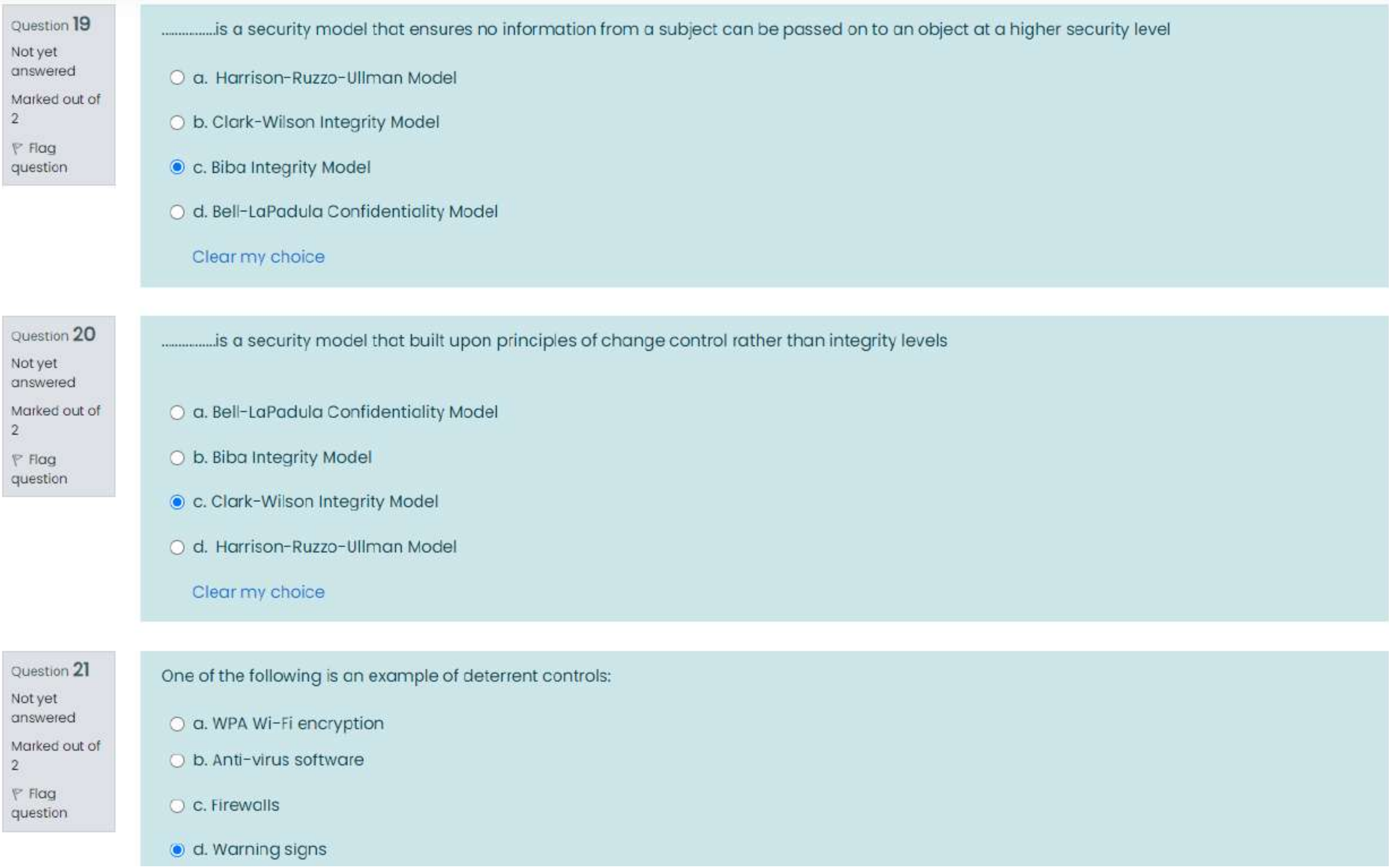
The controls that include security measures that protect system resources using specialized hardware or software, such as a firewall appliance or antivirus program, called?

○ a. All choices are true

○ b. Physical controls

○ c. Management controls

● d. Technical controls



Question **19**

Not yet answered

Marked out of 2

Flag question

...............is a security model that ensures no information from a subject can be passed on to an object at a higher security level

○ a. Harrison-Ruzzo-Ullman Model

○ b. Clark-Wilson Integrity Model

● c. Biba Integrity Model

○ d. Bell-LaPadula Confidentiality Model

Clear my choice

Question **20**

Not yet answered

Marked out of 2

Flag question

...............is a security model that built upon principles of change control rather than integrity levels

○ a. Bell-LaPadula Confidentiality Model

○ b. Biba Integrity Model

● c. Clark-Wilson Integrity Model

○ d. Harrison-Ruzzo-Ullman Model

Clear my choice

Question **21**

Not yet answered

Marked out of 2

Flag question

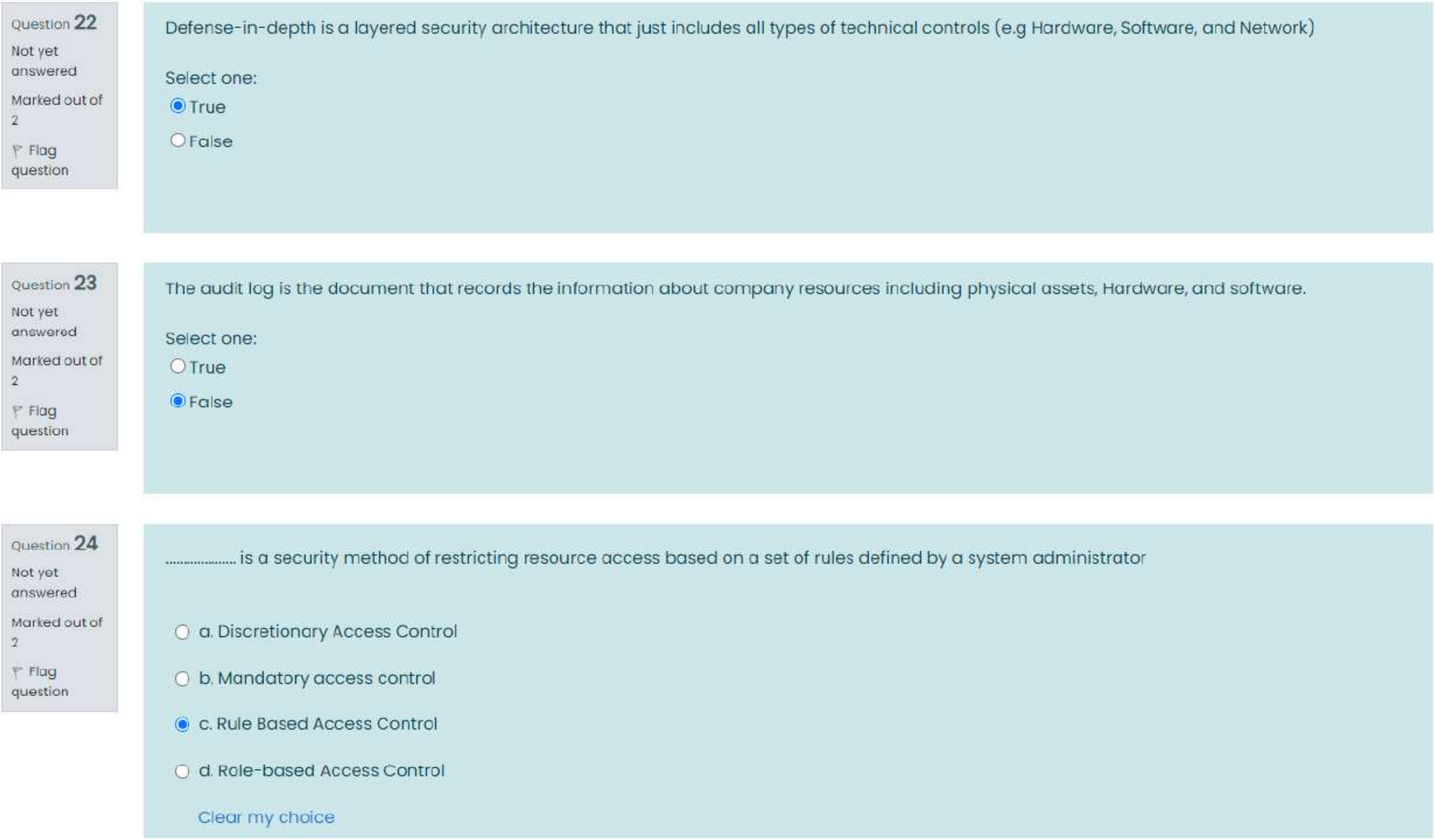
One of the following is an example of deterrent controls:

○ a. WPA Wi-Fi encryption

○ b. Anti-virus software

○ c. Firewalls

● d. Warning signs



Question 22

Not yet answered

Marked out of 2

Flag question

Defense-in-depth is a layered security architecture that just includes all types of technical controls (e.g Hardware, Software, and Network)

Select one:

● True

○ False

Question 23

Not yet answered

Marked out of 2

Flag question

The audit log is the document that records the information about company resources including physical assets, Hardware, and software.

Select one:

○ True

● False

Question 24

Not yet answered

Marked out of 2

Flag question

.... is a security method of restricting resource access based on a set of rules defined by a system administrator

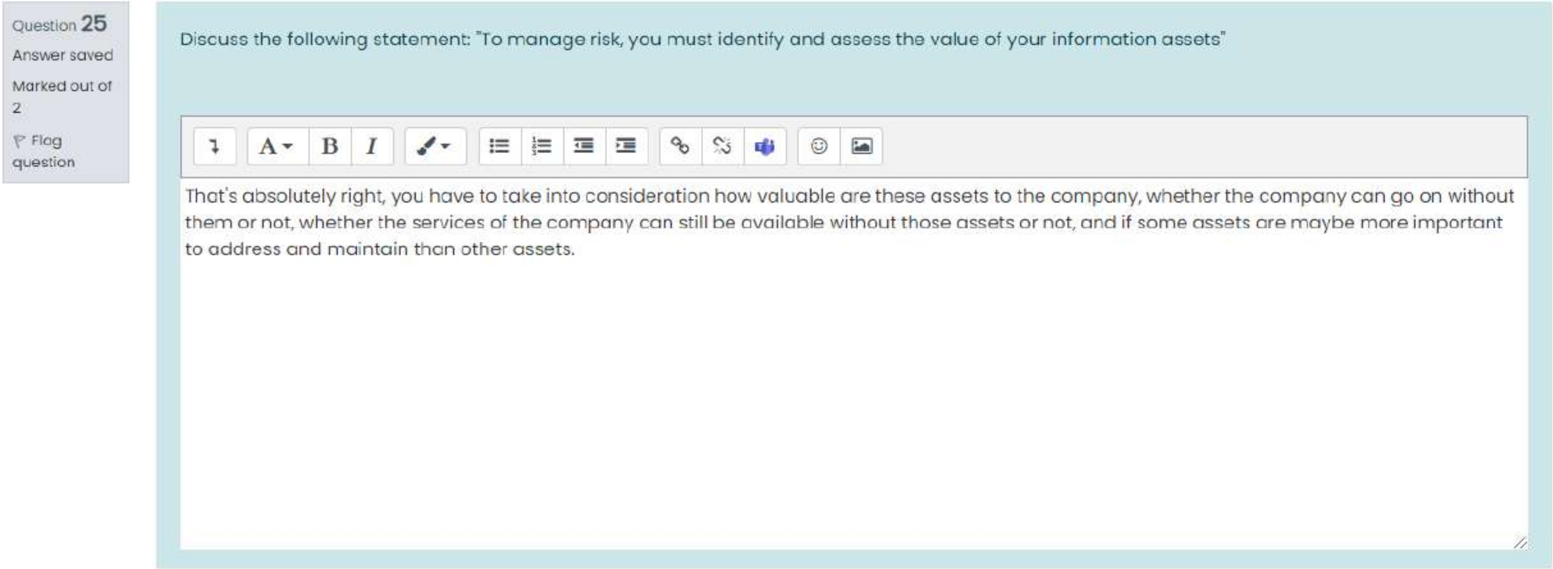
○ a. Discretionary Access Control

○ b. Mandatory access control

● c. Rule Based Access Control

○ d. Role-based Access Control

Clear my choice



Question 25

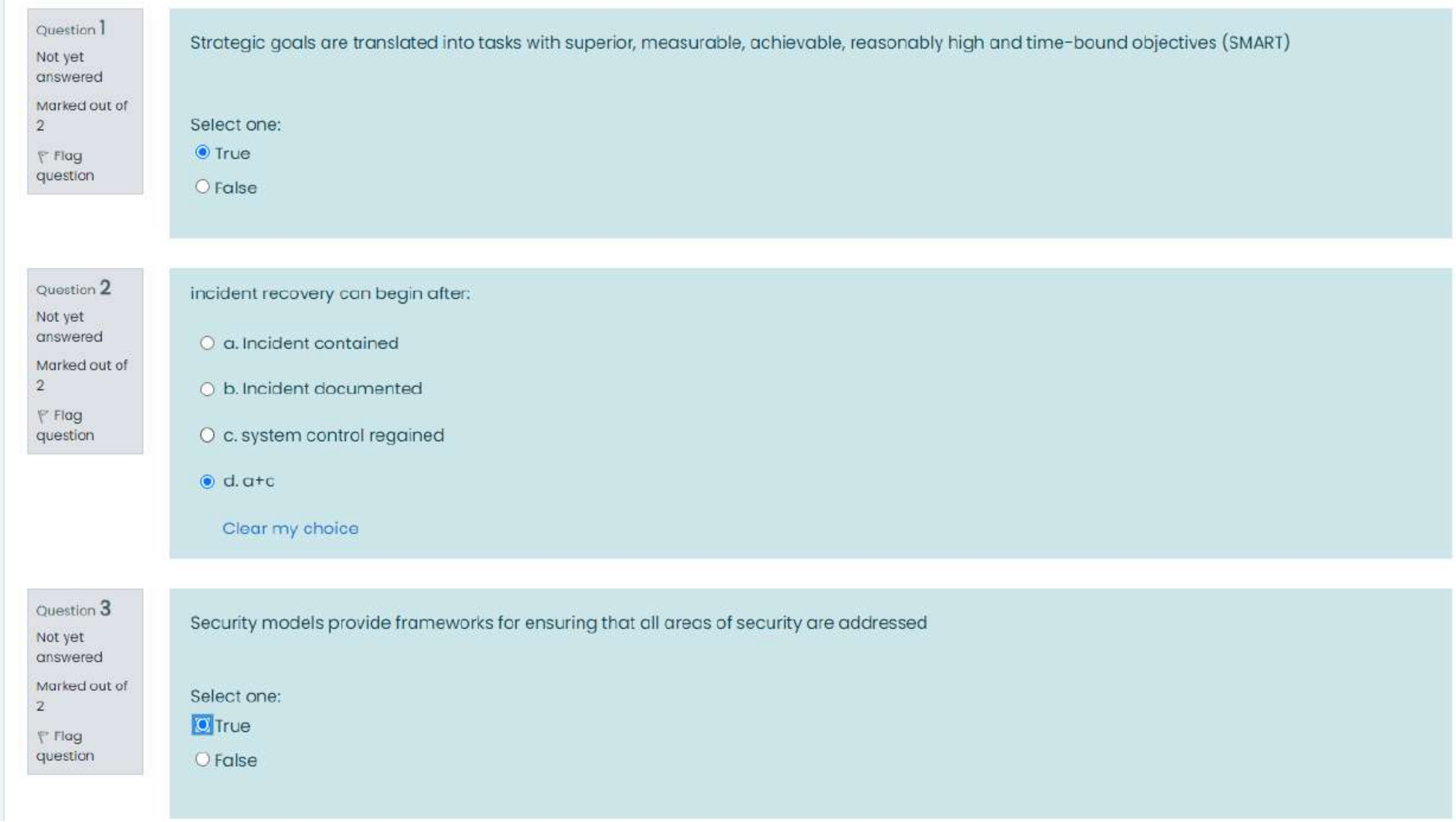
Answer saved

Marked out of 2

Flag question

Discuss the following statement: "To manage risk, you must identify and assess the value of your information assets"

That's absolutely right, you have to take into consideration how valuable are these assets to the company, whether the company can go on without them or not, whether the services of the company can still be available without those assets or not, and if some assets are maybe more important to address and maintain than other assets.



Question 1

Not yet answered

Marked out of 2

Flag question

Strategic goals are translated into tasks with superior, measurable, achievable, reasonably high and time-bound objectives (SMART)

Select one:

● True

○ False

Question 2

Not yet answered

Marked out of 2

Flag question

incident recovery can begin after:

○ a. Incident contained

○ b. Incident documented

○ c. system control regained

● d. a+c

Clear my choice

Question 3

Not yet answered

Marked out of 2

Flag question

Security models provide frameworks for ensuring that all areas of security are addressed

Select one:

● True

○ False