

CISSP-2018^{Q&As}

Certified Information Systems Security Professional 2018

Pass ISC CISSP-2018 Exam with 100% Guarantee

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

<https://www.pass2lead.com/cissp-2018.html>

100% Passing Guarantee
100% Money Back Assurance

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

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



QUESTION 1

DRAG DROP

Order the below steps to create an effective vulnerability management process.

Select and Place:

<u>Step</u>		<u>Order</u>
Identify risks		1
Implement patch deployment		2
Implement recurring scanning schedule		3
Identify assets		4
Implement change management		5

Correct Answer:

<u>Step</u>		<u>Order</u>
	Identify assets	1
	Identify risks	2
	Implement change management	3
	Implement patch deployment	4
	Implement recurring scanning schedule	5

QUESTION 2

DRAG DROP

Match the access control type to the example of the control type. Drag each access control type net to its corresponding example.

Select and Place:

Access Control Type		Example
Administrative		Labeling of sensitive data
Technical		Biometrics for authentication
Logical		Constrained user interface
Physical		Radio Frequency Identification (RFID) badge

Correct Answer:

Access Control Type		Example
	Administrative	Labeling of sensitive data
	Logical	Biometrics for authentication
	Technical	Constrained user interface
	Physical	Radio Frequency Identification (RFID) badge

QUESTION 3

DRAG DROP

What is the correct order of steps in an information security assessment?

Place the information security assessment steps on the left next to the numbered boxes on the right in the correct order.

Select and Place:

<u>Actions</u>		<u>Steps</u>
Define the perimeter.		Step 1
Identify the vulnerability.		Step 2
Assess the risk.		Step 3
Determine the actions.		Step 4

Correct Answer:

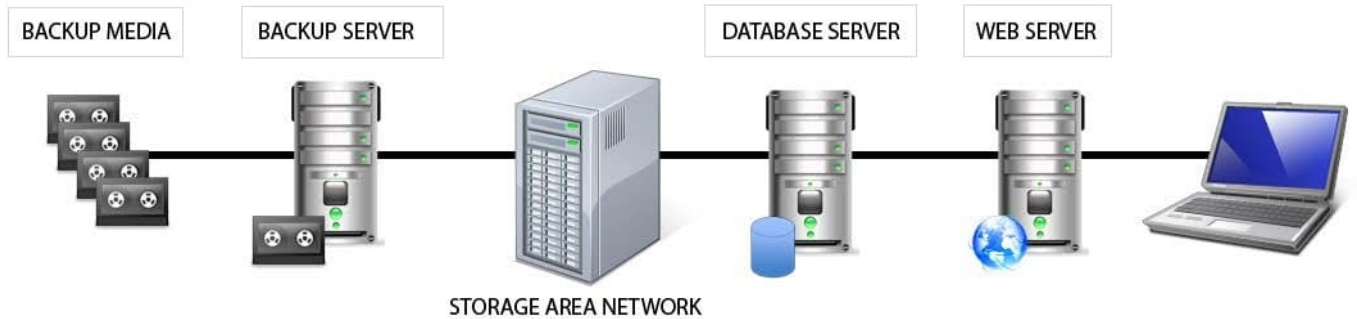
<u>Actions</u>		<u>Steps</u>
	Identify the vulnerability.	Step 1
	Define the perimeter.	Step 2
	Assess the risk.	Step 3
	Determine the actions.	Step 4

QUESTION 4

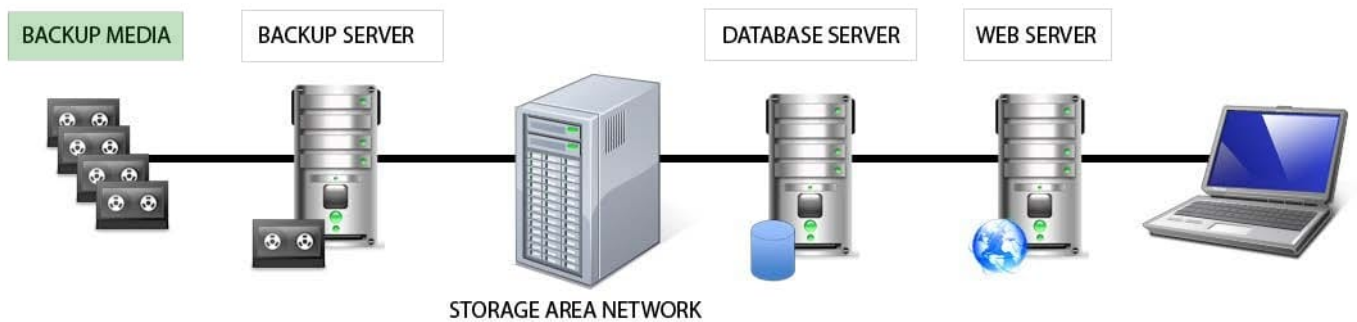
HOTSPOT

Identify the component that MOST likely lacks digital accountability related to information access. Click on the correct device in the image below.

Hot Area:



Correct Answer:



QUESTION 5

DRAG DROP

Match the name of access control model with its associated restriction.

Drag each access control model to its appropriate restriction access on the right.

Select and Place:

Access Control Model

- Mandatory Access Control
- Discretionary Access Control(DAC)
- Role Based Access Control (RBAC)
- Rule Based Access Control

Restrictions

- End user cannot set controls
- Subject has total control over objects
- Dynamically assigns permissions to particular duties based on job function
- Dynamically assigns roles to subjects based on criteria assigned by a custodian

Correct Answer:

Access Control Model

-
-
-
-

Restrictions

- Mandatory Access Control
End user cannot set controls
- Discretionary Access Control(DAC)
Subject has total control over objects
- Role Based Access Control (RBAC)
Dynamically assigns permissions to particular duties based on job function
- Rule Based Access Control
Dynamically assigns roles to subjects based on criteria assigned by a custodian

[Latest CISSP-2018 Dumps](#)

[CISSP-2018 Practice Test](#)

[CISSP-2018 Brindumps](#)