

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

Match the functional roles in an external audit to their responsibilities. Drag each role on the left to its corresponding responsibility on the right.

Select and Place:

<u>Role</u>		<u>Responsibility</u>
Executive management	<input type="text"/>	Approve audit budget and resource allocation.
Audit committee	<input type="text"/>	Provide audit oversight.
Compliance officer	<input type="text"/>	Ensure the achievement and maintenance of organizational requirements with applicable certifications.
External auditor	<input type="text"/>	Develop and maintain knowledge and subject-matter expertise relevant to the type of audit.

Correct Answer:

<u>Role</u>		<u>Responsibility</u>
<input type="text"/>	Executive management	Approve audit budget and resource allocation.
<input type="text"/>	Audit committee	Provide audit oversight.
<input type="text"/>	External auditor	Ensure the achievement and maintenance of organizational requirements with applicable certifications.
<input type="text"/>	Compliance officer	Develop and maintain knowledge and subject-matter expertise relevant to the type of audit.

QUESTION 2

DRAG DROP

Match the types of e-authentication tokens to their description.

Drag each e-authentication token on the left to its corresponding description on the right.

Select and Place:

E-Authentication Token		Description
Memorized Secret Token		A physical or electronic token stores a set of secrets between the claimant and the credential service provider
Out-of-Band Token		A physical token that is uniquely addressable and can receive a verifier-selected secret of one-time use
Look-up Secret Token		A series of responses to a set of prompts or challenges established by the subscriber and credential service provider during the registration process
Pre-registered Knowledge Token		A secret shared between the subscriber and credential service provider that is typically character strings

Correct Answer:

E-Authentication Token		Description
	Look-up Secret Token	A physical or electronic token stores a set of secrets between the claimant and the credential service provider
	Out-of-Band Token	A physical token that is uniquely addressable and can receive a verifier-selected secret of one-time use
	Pre-registered Knowledge Token	A series of responses to a set of prompts or challenges established by the subscriber and credential service provider during the registration process
	Memorized Secret Token	A secret shared between the subscriber and credential service provider that is typically character strings

QUESTION 3

DRAG DROP

Drag the following Security Engineering terms on the left to the BEST definition on the right.

Select and Place:

Security Engineering

Definition

Security Risk Treatment

The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the **adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.**

Threat Assessment

A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the **circumstance or event occurs, and the likelihood of occurrence.**

Protection Needs

The method used to identify and characterize the dangers anticipated **throughout the life cycle of the system.**

Risk

The method used to identify feasible security **risk mitigation options and plans.**

Correct Answer:

Security Engineering

Definition

Protection Needs

The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.

Threat Assessment

The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.

Security Risk Treatment

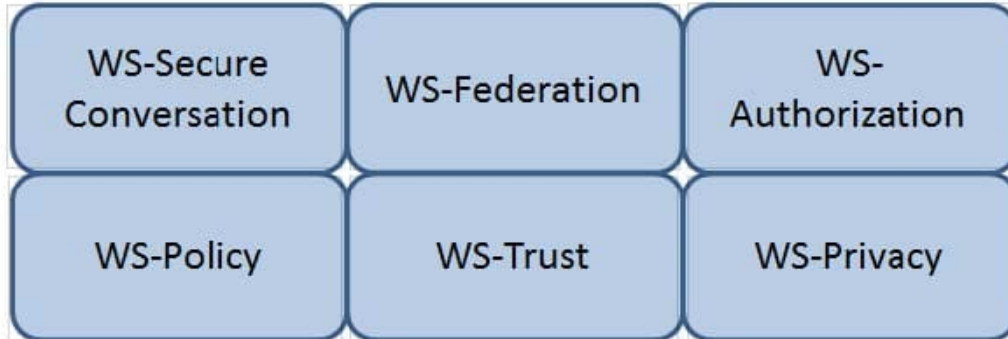
The method used to identify feasible security risk mitigation options and plans.

QUESTION 4

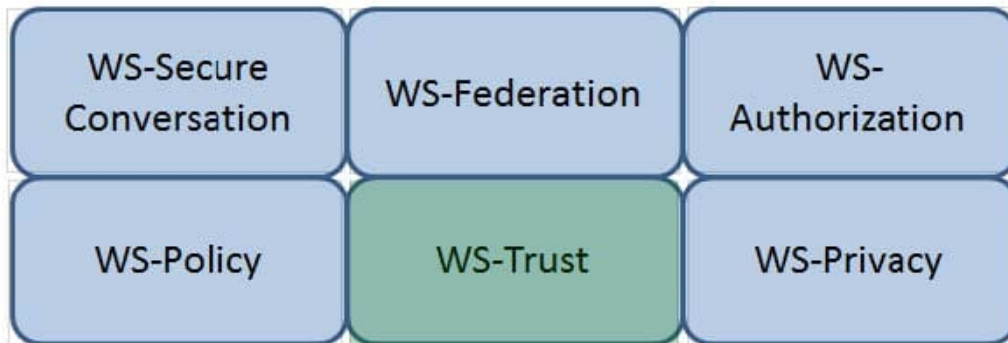
HOTSPOT

Which Web Services Security (WS-Security) specification negotiates how security tokens will be issued, renewed and validated? Click on the correct specification in the image below.

Hot Area:



Correct Answer:



QUESTION 5

DRAG DROP

A software security engineer is developing a black box-based test plan that will measure the system's reaction to incorrect or illegal inputs or unexpected operational errors and situations. Match the functional testing techniques on the left with the correct input parameters on the right.

Select and Place:

<u>Functional Testing Techniques</u>		<u>Input Parameter Selection</u>
State-Based Analysis		Select one input that does not belong to any of the identified partitions.
Equivalence Class Analysis		Select inputs that are at the external limits of the domain of valid values.
Decision Table Analysis		Select invalid combinations of input values.
Boundary Value Analysis		Select unexpected inputs corresponding to each known condition.

Correct Answer:

<u>Functional Testing Techniques</u>		<u>Input Parameter Selection</u>
	Equivalence Class Analysis	Select one input that does not belong to any of the identified partitions.
	Boundary Value Analysis	Select inputs that are at the external limits of the domain of valid values.
	Decision Table Analysis	Select invalid combinations of input values.
	State-Based Analysis	Select unexpected inputs corresponding to each known condition.

QUESTION 6

DRAG DROP

In which order, from MOST to LEAST impacted, does user awareness training reduce the occurrence of the events below?

Select and Place:

<u>Event</u>		<u>Order</u>
Disloyal employees		1
User instigated		2
Targeted infiltration		3
Virus infiltrations		4

Correct Answer:

<u>Event</u>		<u>Order</u>
	Disloyal employees	1
	User-instigated	2
	Targeted infiltration	3
	Virus infiltrations	4

QUESTION 7

DRAG DROP

Place in order, from BEST (1) to WORST (4), the following methods to reduce the risk of data remanence on magnetic media.

Select and Place:

Sequence		Method
1		Overwriting
2		Degaussing
3		Destruction
4		Deleting

Correct Answer:

Sequence		Method
	3	Overwriting
	2	Degaussing
	1	Destruction
	4	Deleting

QUESTION 8

DRAG DROP

Drag the following Security Engineering terms on the left to the BEST definition on the right.

Select and Place:

Security Engineering Term	Definition
	Risk A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of
	Protection Needs Assessment The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
	Threat Assessment The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
	Security Risk Treatment The method used to identify feasible security risk mitigation options and plans.

Correct Answer:

Security Engineering Term		Definition
Risk		A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of
Security Risk Treatment		The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Protection Needs Assessment		The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Threat Assessment		The method used to identify feasible security risk mitigation options and plans.

QUESTION 9

DRAG DROP

Given the various means to protect physical and logical assets, match the access management area to the technology.

Select and Place:

Area		Technolog
Facilities		Encryption
Devices		Window
Information		Firewall
Systems		Authenticatio

Correct Answer:

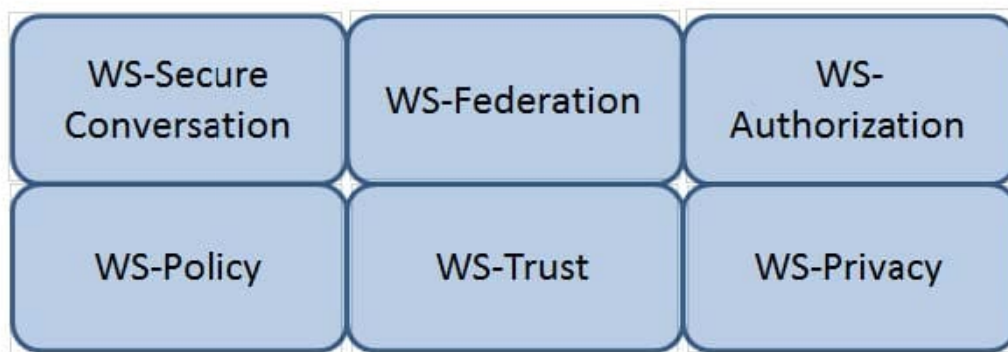
Area		Technolog
	Information	Encryption
	Facilities	Window
	Devices	Firewall
	Systems	Authenticatio

QUESTION 10

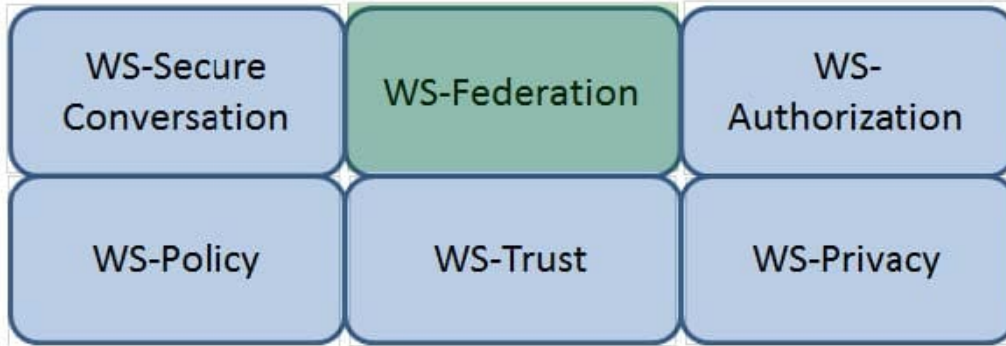
HOTSPOT

Which Web Services Security (WS-Security) specification maintains a single authenticated identity across multiple dissimilar environments? Click on the correct specification in the image below.

Hot Area:



Correct Answer:



QUESTION 11

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		Restrictions
Mandatory Access Control	<input type="text"/>	End user cannot set controls
Discretionary Access Control(DAC)	<input type="text"/>	Subject has total control over objects
Role Based Access Control (RBAC)	<input type="text"/>	Dynamically assigns permissions to particular duties based on job function
Rule Based Access Control	<input type="text"/>	Dynamically assigns roles to subjects bases on criteria assigned by a custodian

Correct Answer:

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

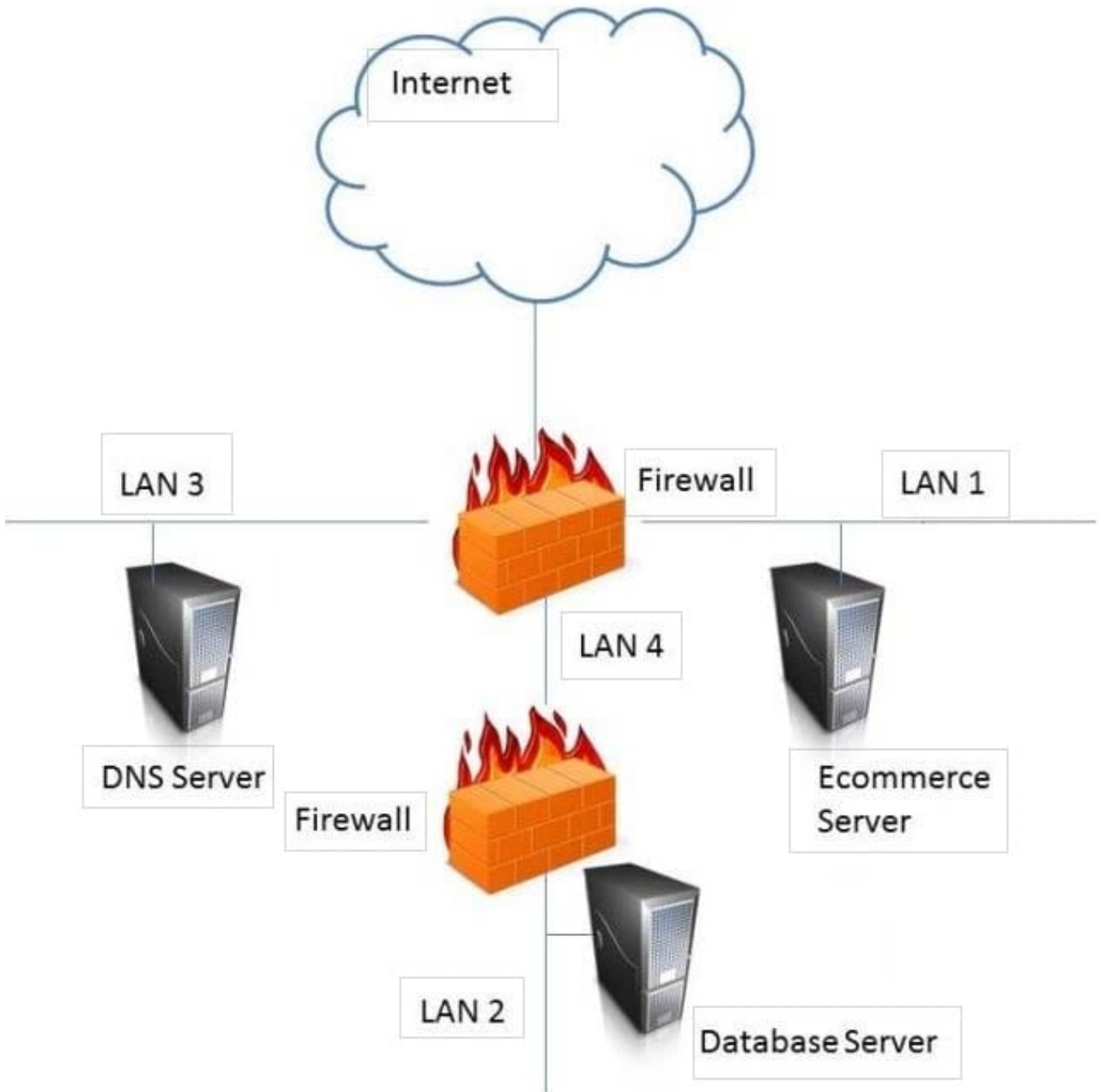
Dynamically assigns roles to subjects based on criteria assigned by a custodian

QUESTION 12

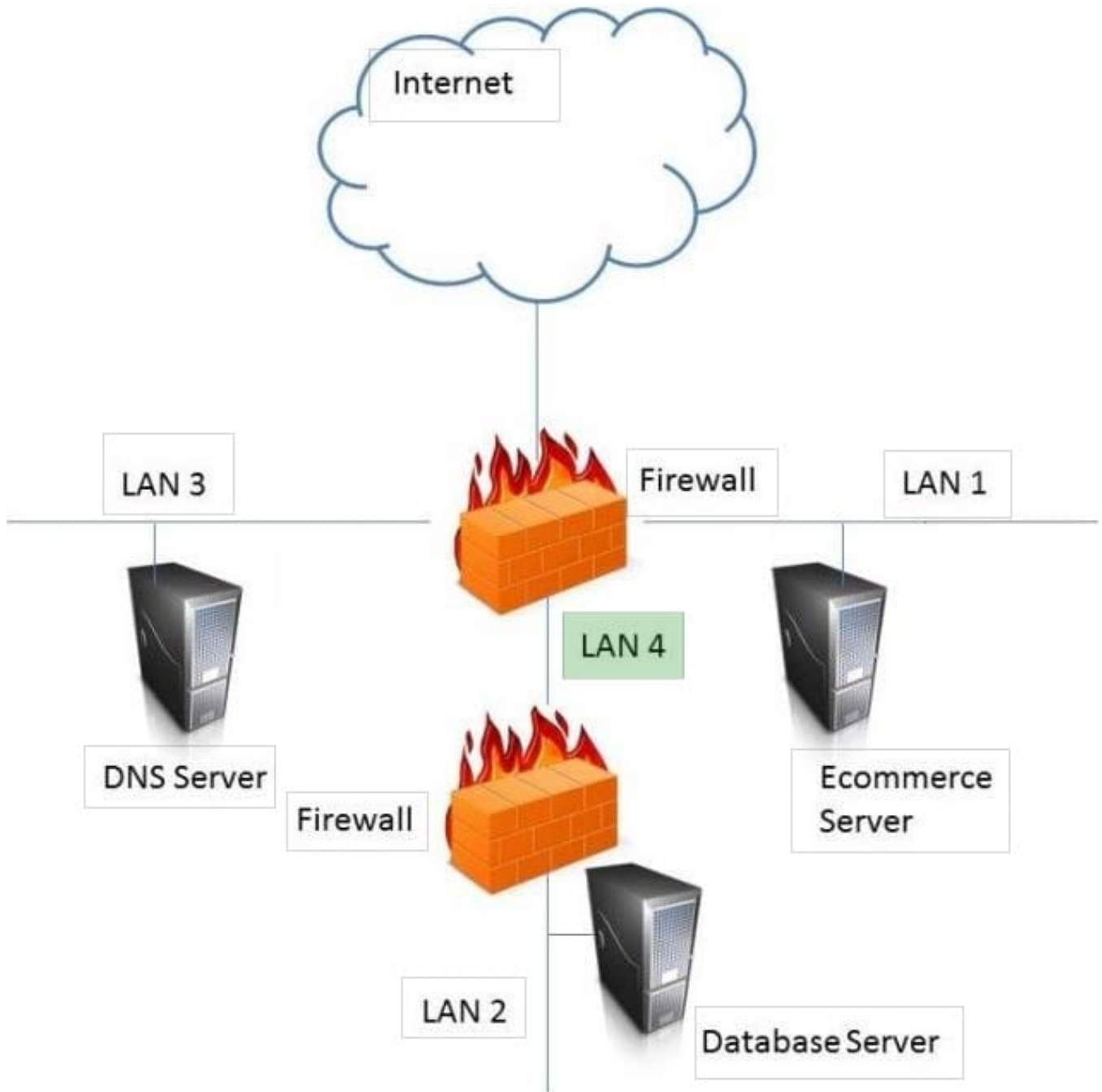
HOTSPOT

In the network design below, where is the MOST secure Local Area Network (LAN) segment to deploy a Wireless Access Point (WAP) that provides contractors access to the Internet and authorized enterprise services?

Hot Area:



Correct Answer:



QUESTION 13

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 14

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 15

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