

**100%** Money Back  
**Guarantee**

**Vendor:**ISC

**Exam Code:**CISSP-2018

**Exam Name:**Certified Information Systems Security  
Professional 2018

**Version:**Demo

## QUESTION 1

### DRAG DROP

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

Select and Place:

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

Correct Answer:

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

---

## QUESTION 2

### 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

Protection Needs

## Definition

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 3

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 4

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
	<b>Risk</b>	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
	<b>Protection Needs Assessment</b>	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.
	<b>Threat Assessment</b>	The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
	<b>Security Risk Treatment</b>	The method used to identify feasible security risk mitigation options and plans.

Correct Answer:

Security Engineering Term		Definition
<b>Risk</b>		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
<b>Security Risk Treatment</b>		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.
<b>Protection Needs Assessment</b>		The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
<b>Threat Assessment</b>		The method used to identify feasible security risk mitigation options and plans.

## 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

### Restrictions

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


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

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 6

### DRAG DROP

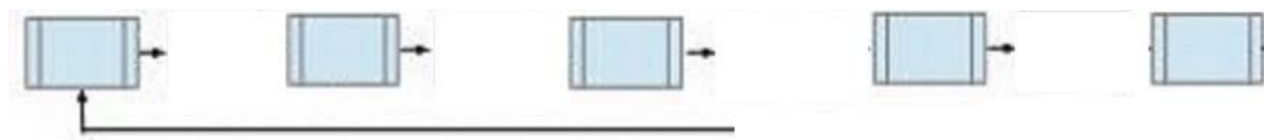
During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is

fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.

What is the best approach for the CISO?

Below are the common phases to creating a Business Continuity/Disaster Recovery (BC/DR) plan. Drag the remaining BC\DR phases to the appropriate corresponding location.

Select and Place:



- Risk Assessment
- Business Impact Analysis
- Mitigation Strategy Development
- BC\DR Plan Development
- Training, Testing & Auditing
- Plan Maintenance

Correct Answer:



Plan Maintenance

## QUESTION 7

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 8

DRAG DROP

Place the following information classification steps in sequential order.

Select and Place:

## Steps

**Declassify information when appropriate**

**Apply the appropriate security markings**

**Conduct periodic classification reviews**

**Assign a classification level**

**Document the information assets**

## Order

Step

Step

Step

Step

Step

Correct Answer:

## Steps


**Document the information assets**

**Assign a classification level**

**Apply the appropriate security markings**

**Conduct periodic classification reviews**

**Declassify information when appropriate**

## Order

Step

Step

Step

Step

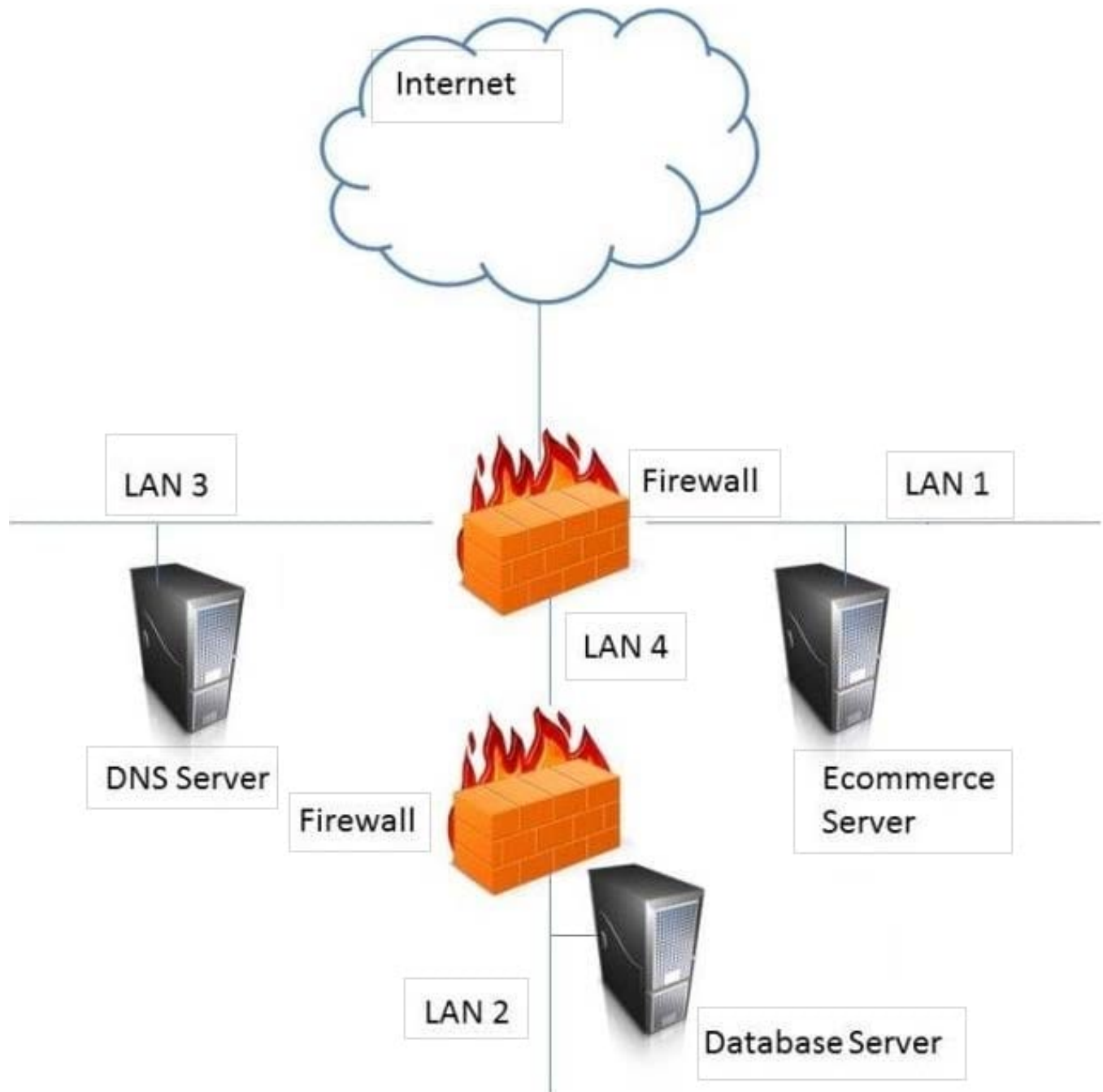
Step

## QUESTION 9

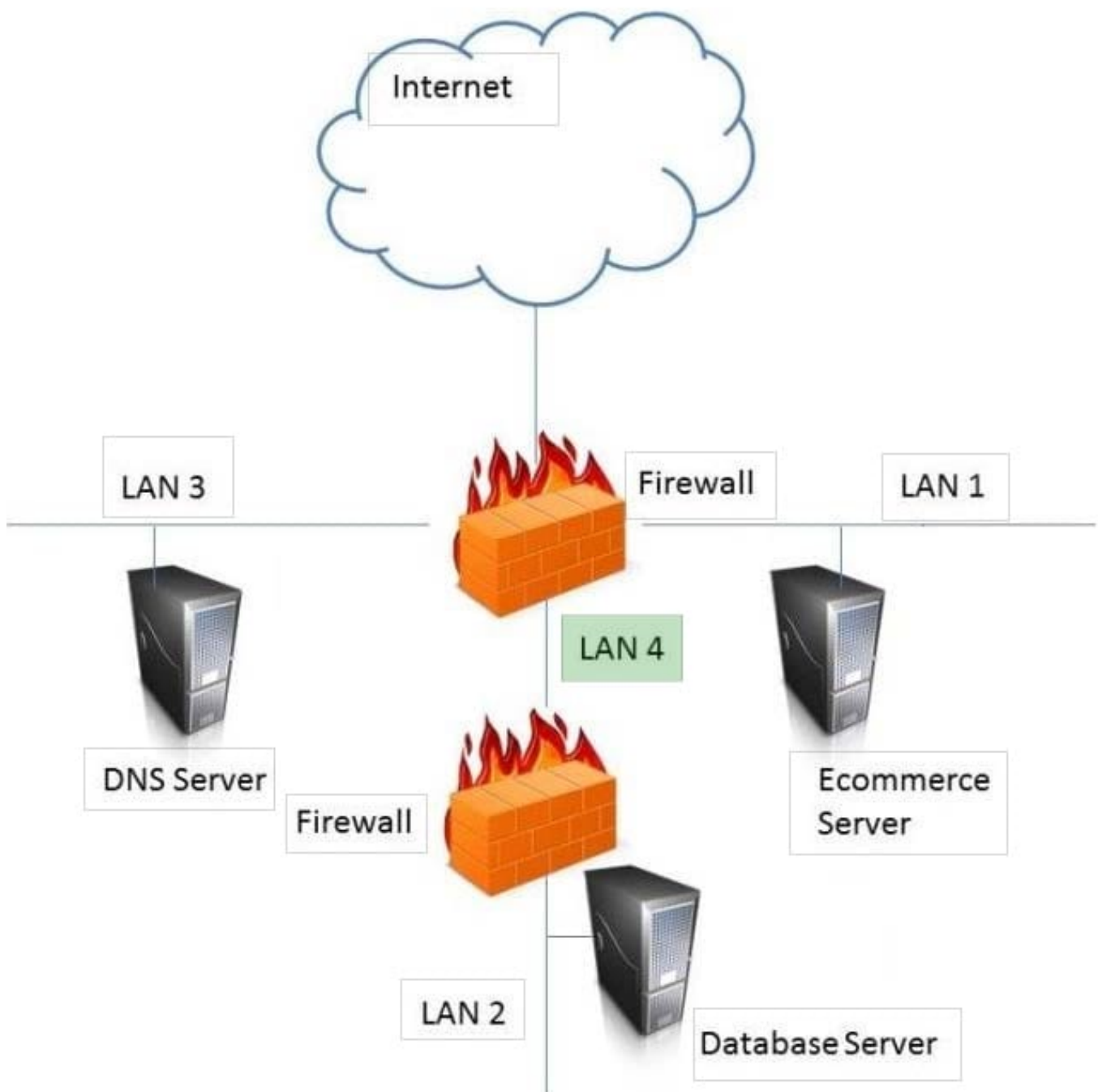
### HOTSPOT

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:



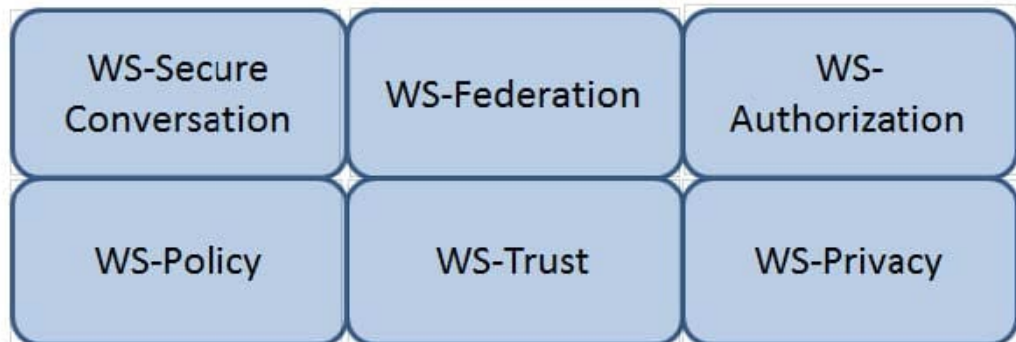
---

#### QUESTION 10

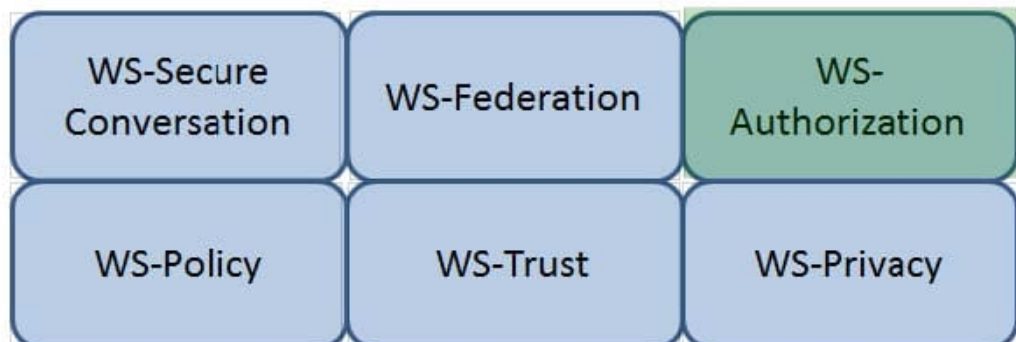
##### HOTSPOT

Which Web Services Security (WS-Security) specification handles the management of security tokens and the underlying policies for granting access? Click on the correct specification in the image below.

Hot Area:



Correct Answer:



---

**QUESTION 11**

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:

Functional Testing Techniques		Input Parameter Selection
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:

Functional Testing Techniques		Input Parameter Selection
	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 12

#### 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