



# CISSP-2018<sup>Q&As</sup>

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.passapply.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



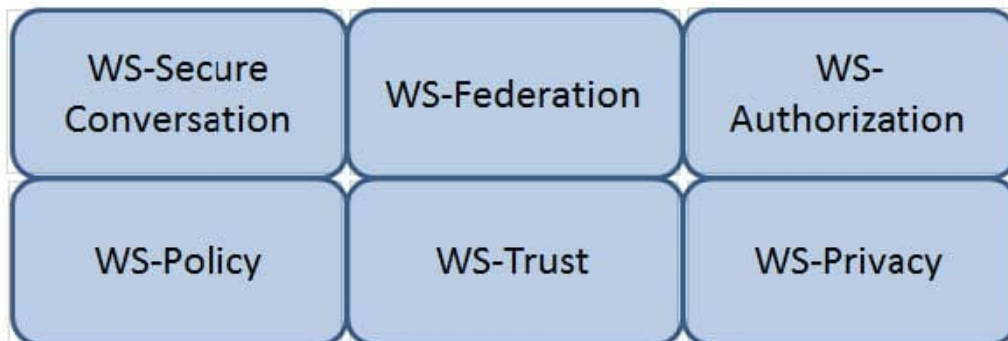


**QUESTION 1**

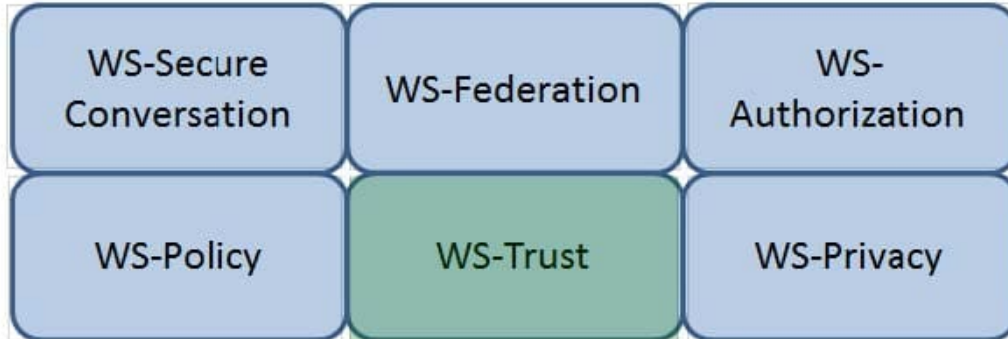
**HOTSPOT**

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 2**

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:

<u>Sequence</u>		<u>Method</u>
1		Overwriting
2		Degaussing
3		Destruction
4		Deleting

Correct Answer:



Sequence


3

2

1

4

Method

Overwriting

Degaussing

Destruction

Deleting

**QUESTION 3**

DRAG DROP

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

Select and Place:

Area

Facilities

Devices

Information

Systems

Technolog

Encryption

Window

Firewall

Authenticati

Correct Answer:

Area


Information

Facilities

Devices

Systems

Technolog

Encryption

Window

Firewall

Authenticati



### QUESTION 4

DRAG DROP

Match the objectives to the assessment questions in the governance domain of Software Assurance Maturity Model (SAMM).

Select and Place:

<b>Secure Architecture</b>		<b>Do you advertise shared security services with guidance for project teams?</b>
<b>Education &amp; Guidance</b>		<b>Are most people tested to ensure a baseline skill- set for secure development practices?</b>
<b>Strategy &amp; Metrics</b>		<b>Does most of the organization know about what's required based on risk ratings?</b>
<b>Vulnerability Management</b>		<b>Are most project teams aware of their security point(s) of contact and response team(s)?</b>

Correct Answer:

<b>Secure Architecture</b>	<b>Do you advertise shared security services with guidance for project teams?</b>
<b>Education &amp; Guidance</b>	<b>Are most people tested to ensure a baseline skill- set for secure development practices?</b>
<b>Strategy &amp; Metrics</b>	<b>Does most of the organization know about what's required based on risk ratings?</b>
<b>Vulnerability Management</b>	<b>Are most project teams aware of their security point(s) of contact and response team(s)?</b>

### QUESTION 5

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		Approve audit budget and resource allocation.
Audit committee		Provide audit oversight.
Compliance officer		Ensure the achievement and maintenance of organizational requirements with applicable certifications.
External auditor		Develop and maintain knowledge and subject-matter expertise relevant to the type of audit.

Correct Answer:

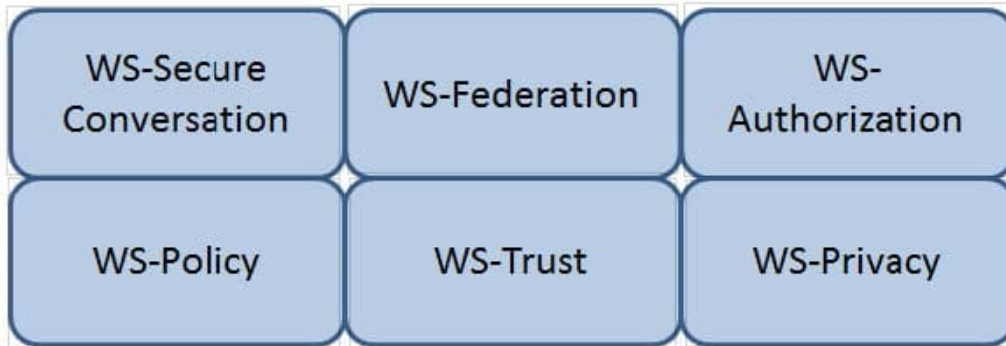
<u>Role</u>		<u>Responsibility</u>
	Executive management	Approve audit budget and resource allocation.
	Audit committee	Provide audit oversight.
	External auditor	Ensure the achievement and maintenance of organizational requirements with applicable certifications.
	Compliance officer	Develop and maintain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

**QUESTION 6**

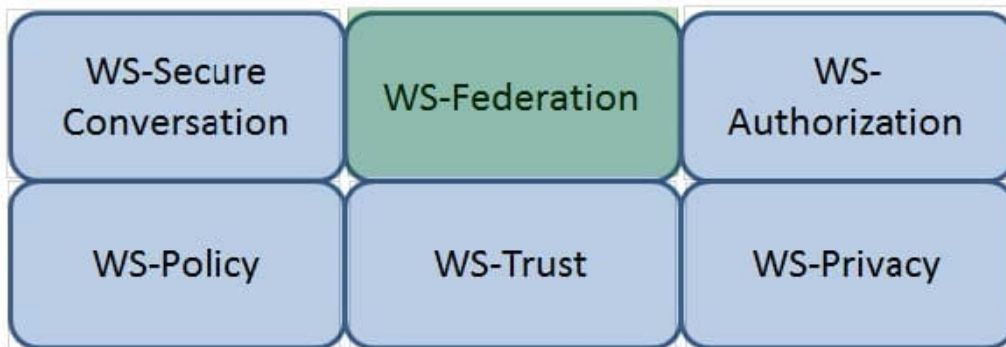
**HOTSPOT**

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:



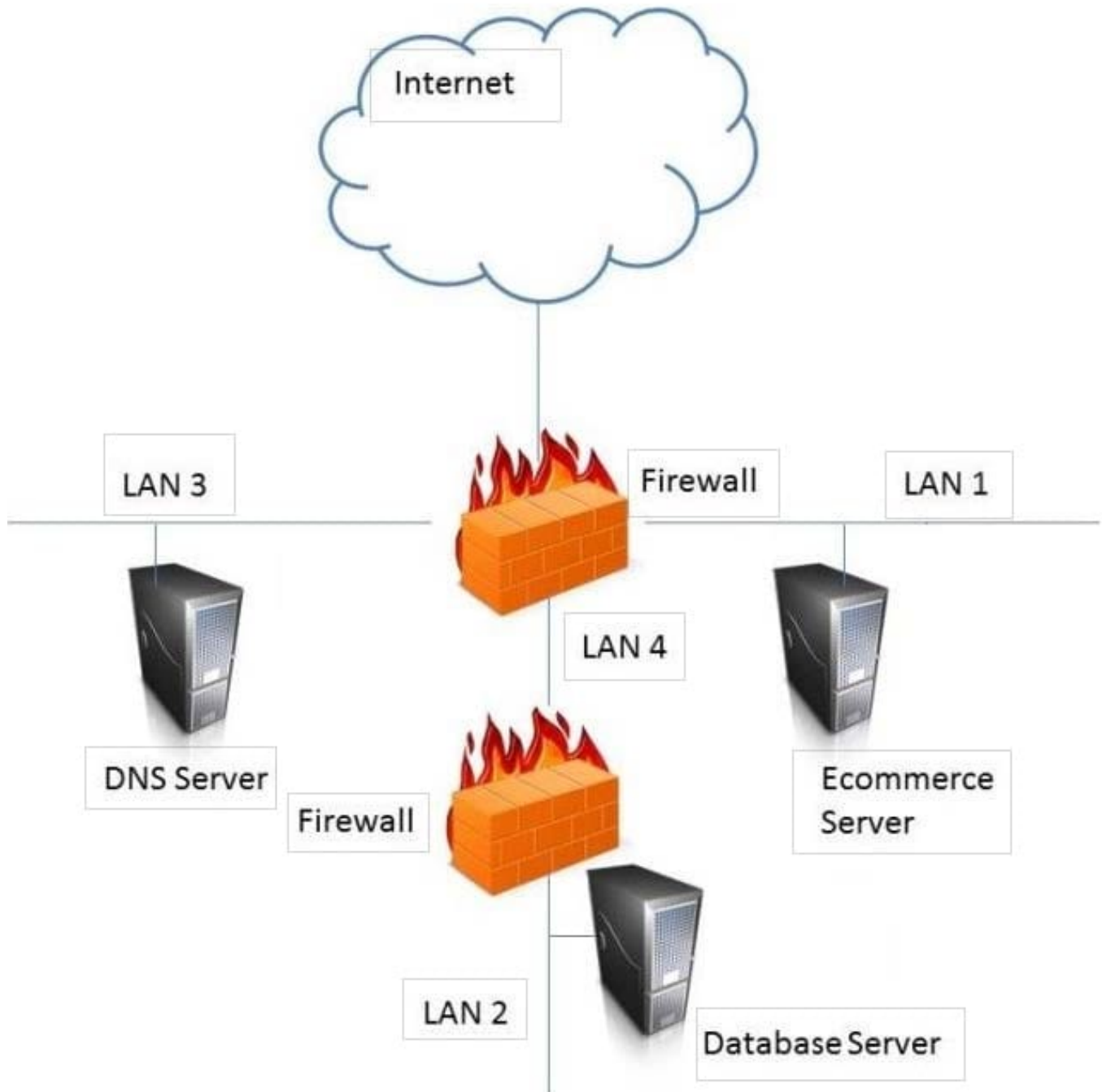
**QUESTION 7**

HOTSPOT



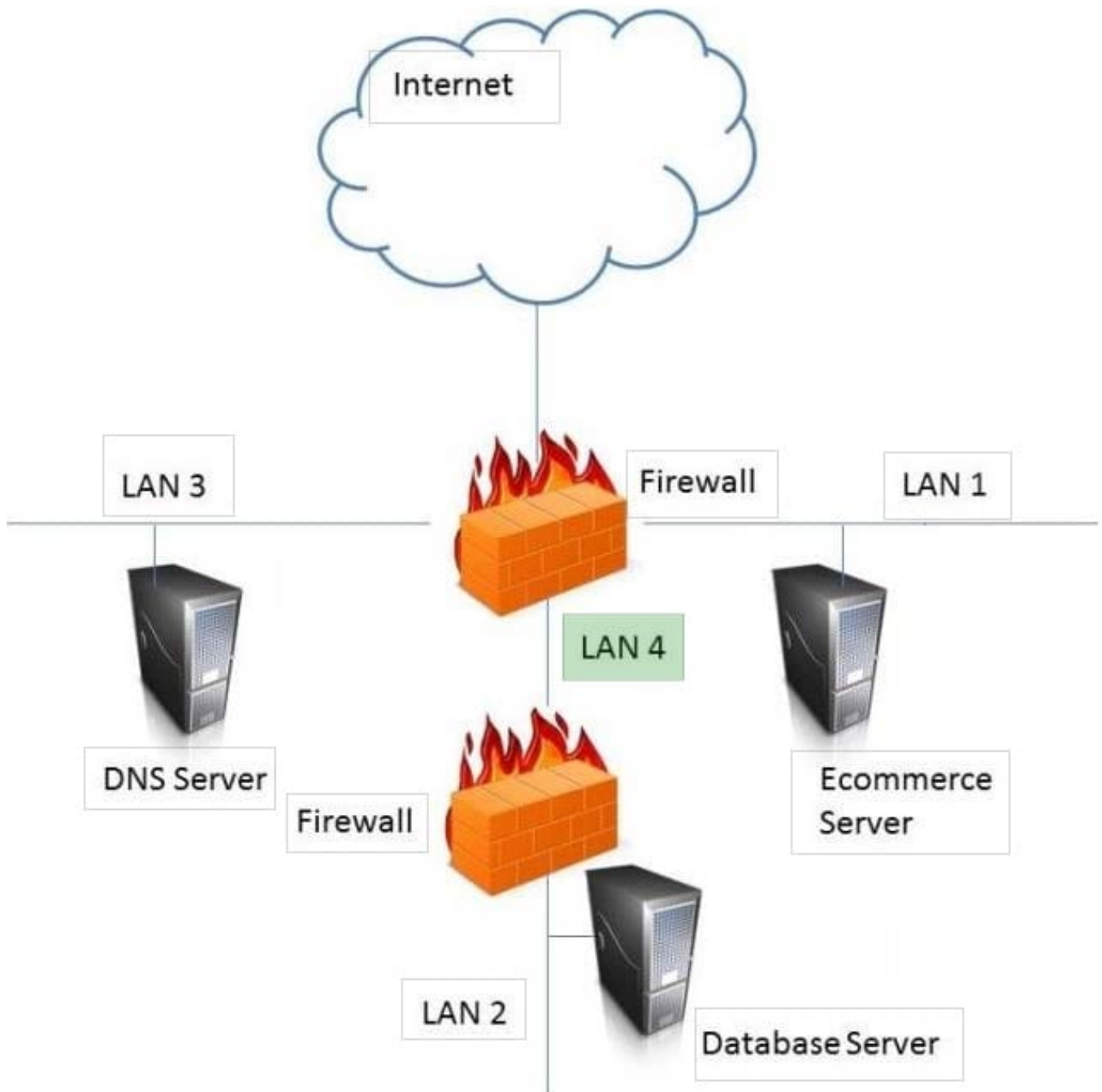
In the network design below, where is the MOST secure Local Area Network (LAN) segment to deploy a Wireless Access Point (WAP) that provides contractors access to the Internet and authorized enterprise services?

Hot Area:



Correct Answer:





**QUESTION 8**

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 9**

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 10**

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

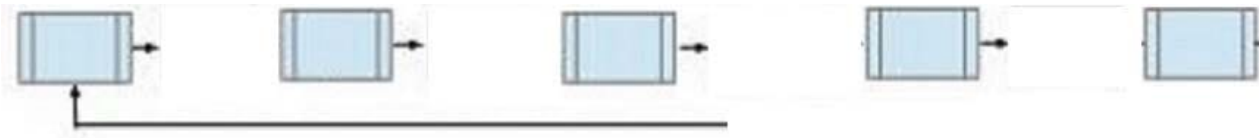
fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.



What is the best approach for the CISO?

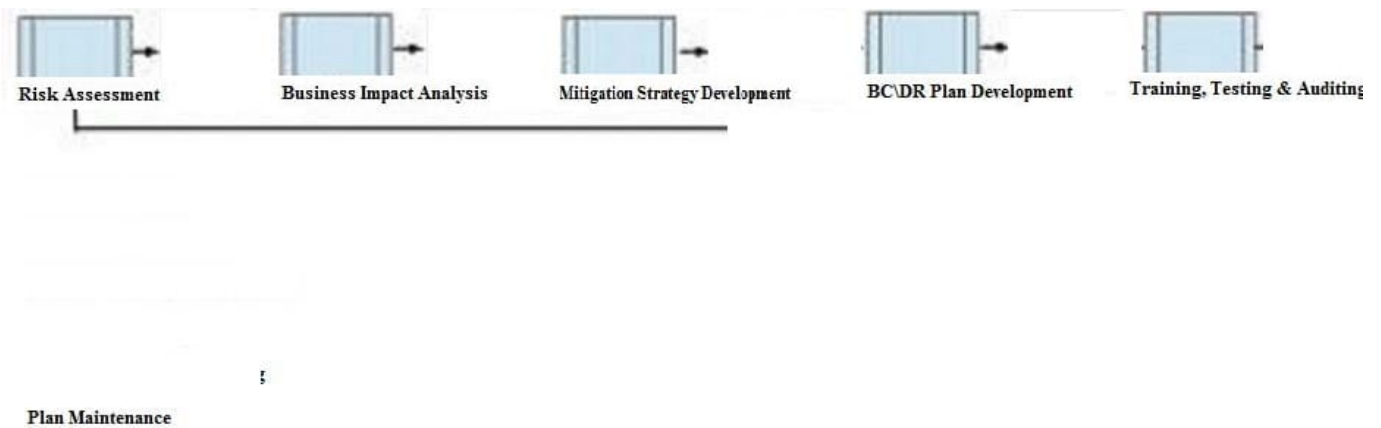
Below are the common phases to creating a Business Continuity/Disaster Recovery (BC/DR) plan. Drag the remaining BC\DR phases to the appropriate corresponding location.

Select and Place:



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

Correct Answer:

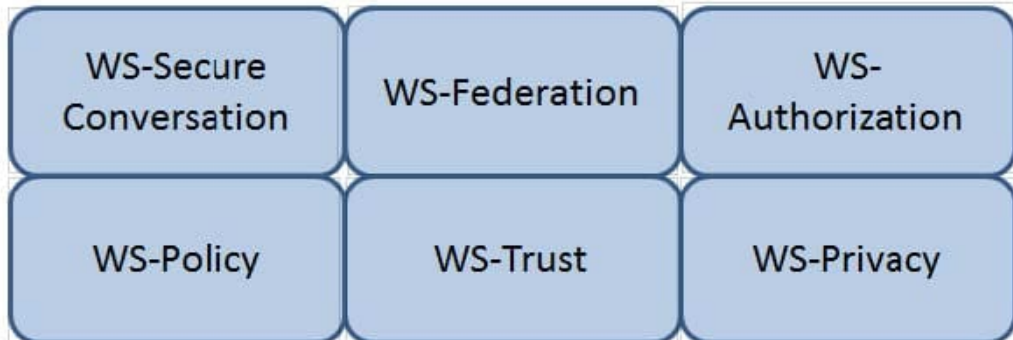


### QUESTION 11

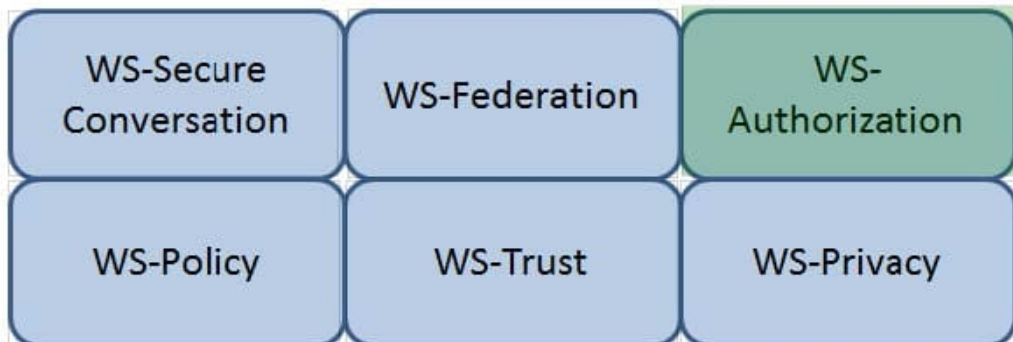
#### HOTSPOT

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 12**

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:

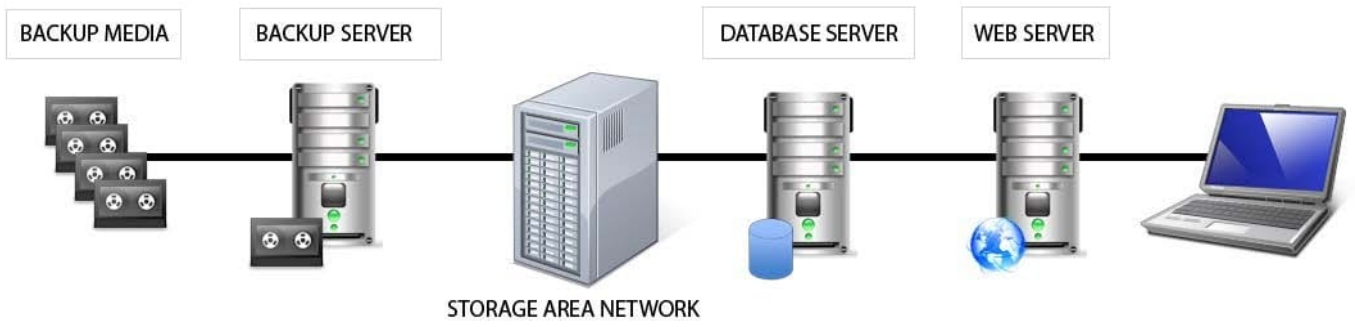
Access Control Type		Example
	Administrative	Labeling of sensitive data
	Logical	Biometrics for authentication
	Technical	Constrained user interface
	Physical	Radio Frequency Identification (RFID) badge

### QUESTION 13

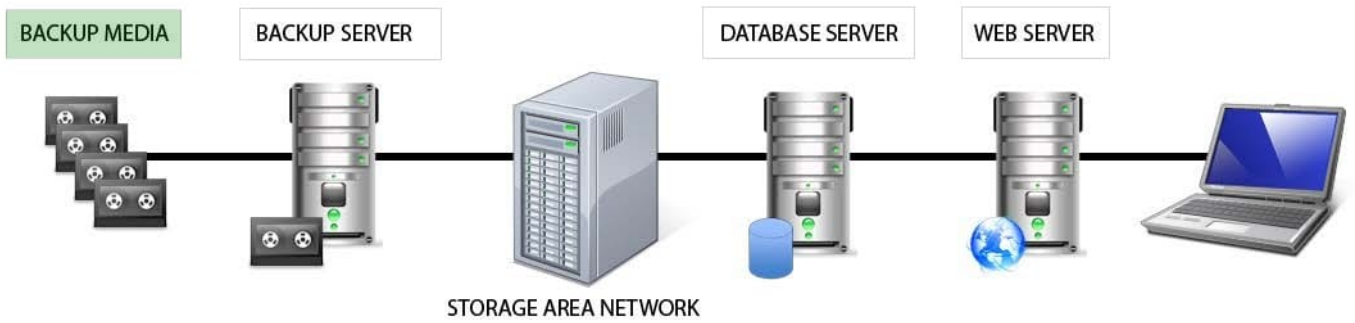
#### HOTSPOT

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 14

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

[Redacted]

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

[Redacted]

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

[Redacted]

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

Risk

[Redacted]

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

Correct Answer:





Security Engineering

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.**

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.**

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

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

**QUESTION 15**

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