



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.pass4itsure.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



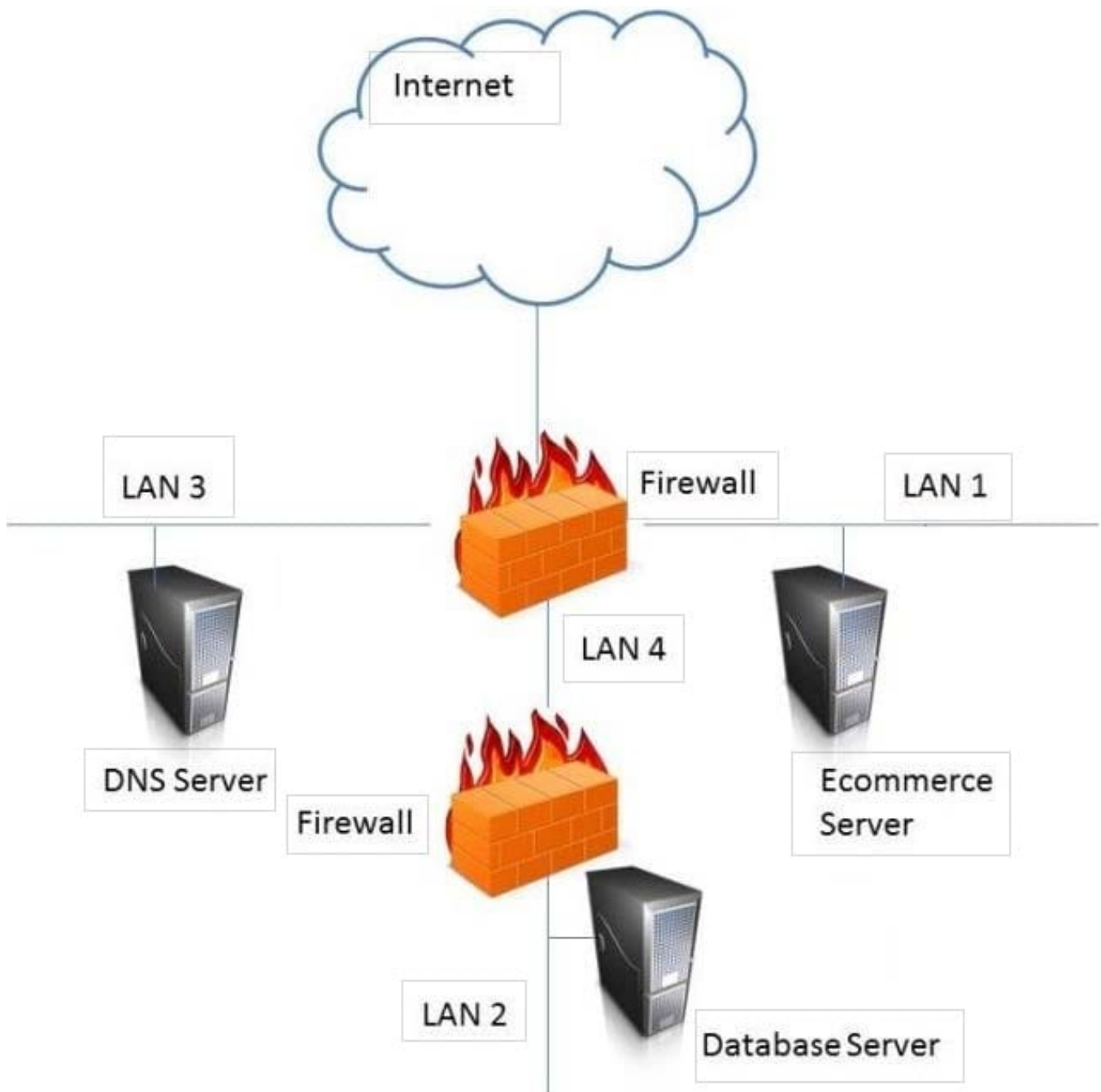


QUESTION 1

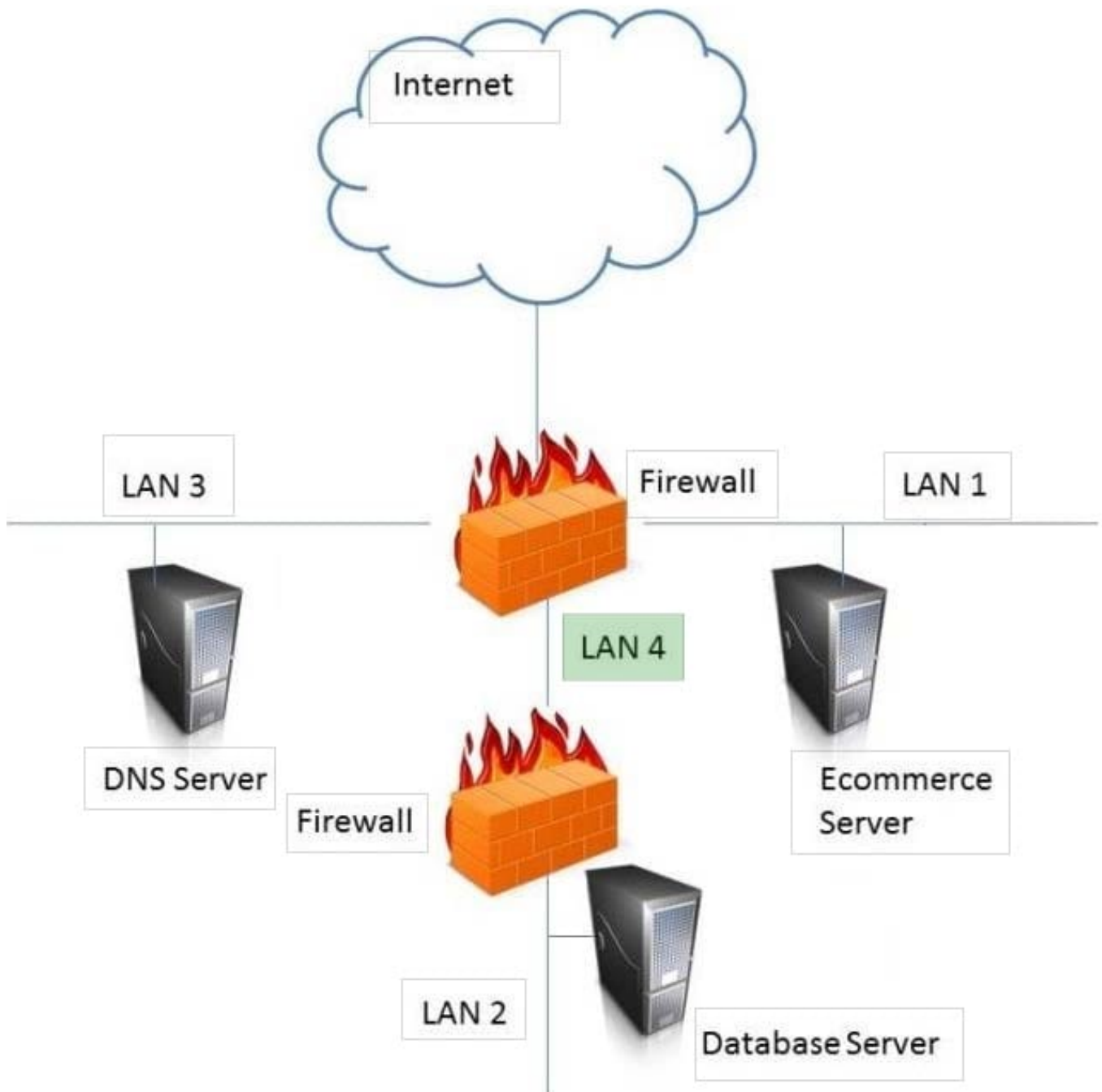
HOTSPOT

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:

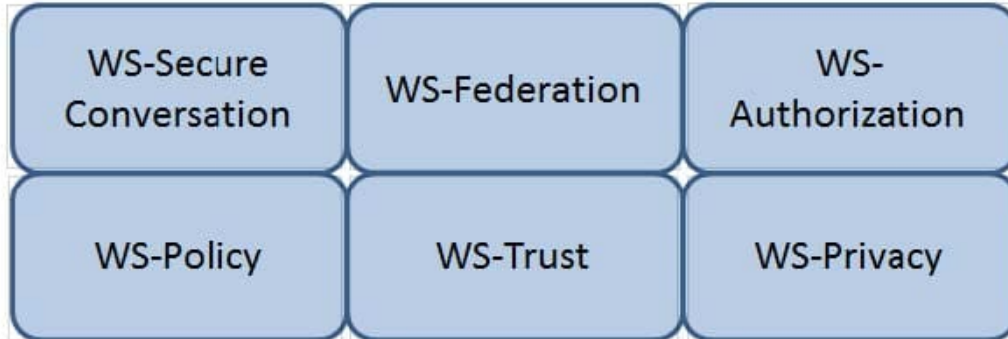


QUESTION 2

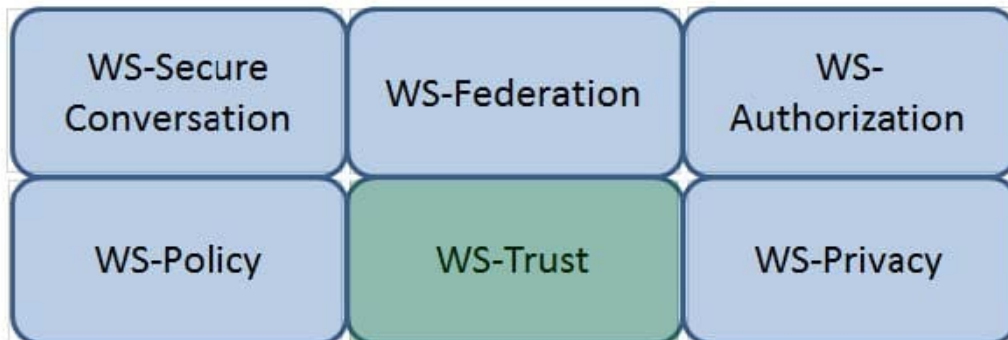
HOTSPOT

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 3

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 4

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 5

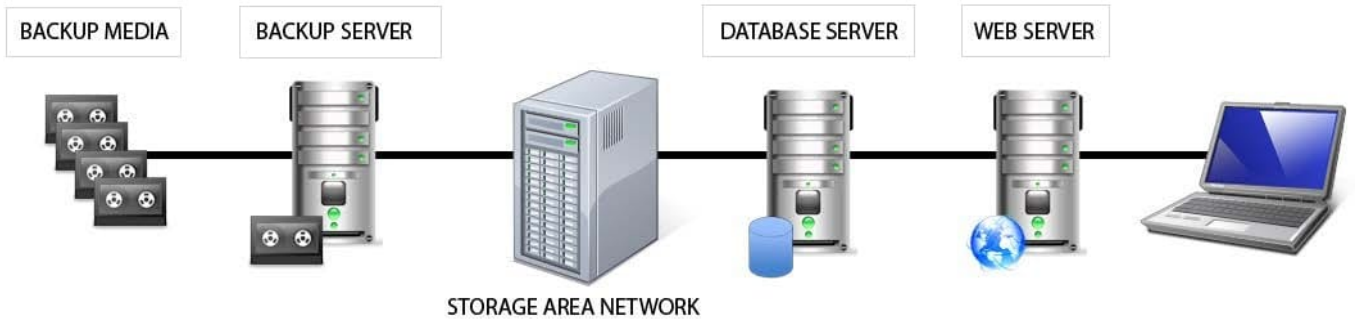
HOTSPOT

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

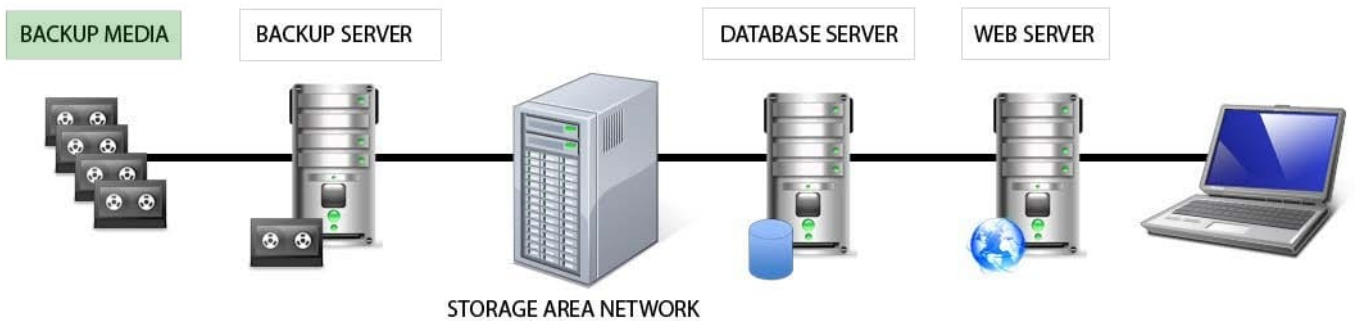


device in the image below.

Hot Area:



Correct Answer:



QUESTION 6

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

- -
 -
 -
- 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 bases on criteria assigned by a custodian

Correct Answer:

Access Control Model

-
-
-
-

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 bases on criteria assigned by a custodian

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

- -
 -
 -
- Overwriting
- Degaussing
- Destruction
- Deleting

Correct Answer:



Sequence

3
2
1
4

Method

Overwriting
Degaussing
Destruction
Deleting

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

Order

	Document the information assets	Step
	Assign a classification level	Step
	Apply the appropriate security markings	Step
	Conduct periodic classification reviews	Step
	Declassify information when appropriate	Step

QUESTION 9

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

State-Based Analysis

[Greyed out]

Input Parameter Selection

Select one input that does not belong to any of the identified partitions.

Equivalence Class Analysis

[Greyed out]

Select inputs that are at the external limits of the domain of valid values.

Decision Table Analysis

[Greyed out]

Select invalid combinations of input values.

Boundary Value Analysis

[Greyed out]

Select unexpected inputs corresponding to each known condition.

Correct Answer:

Functional Testing Techniques

Equivalence Class Analysis

Input Parameter Selection

Select one input that does not belong to any of the identified partitions.

[Empty box]

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 10



DRAG DROP

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

Select and Place:

Event		Order
Disloyal employees		1
User instigated		2
Targeted infiltration		3
Virus infiltrations		4

Correct Answer:

Event		Order
	Disloyal employees	1
	User-instigated	2
	Targeted infiltration	3
	Virus infiltrations	4

QUESTION 11

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

Memorized Secret Token

Out-of-Band Token

Look-up Secret Token

Pre-registered Knowledge Token

Description

A physical or electronic token stores a set of secrets between the claimant and the credential service provider

A physical token that is uniquely addressable and can receive a verifier-selected secret of one-time use

A series of responses to a set of prompts or challenges established by the subscriber and credential service provider during the registration process

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 12

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:

Role

Executive management

Audit committee

Compliance officer

External auditor

Responsibility

Approve audit budget and resource allocation.

Provide audit oversight.

Ensure the achievement and maintenance of organizational requirements with applicable certifications.

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 13

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

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

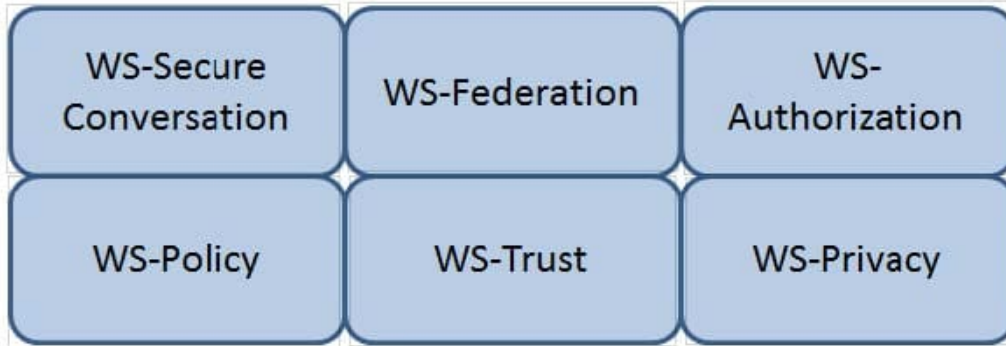
The method used to identify feasible security risk mitigation options and plans.

QUESTION 14

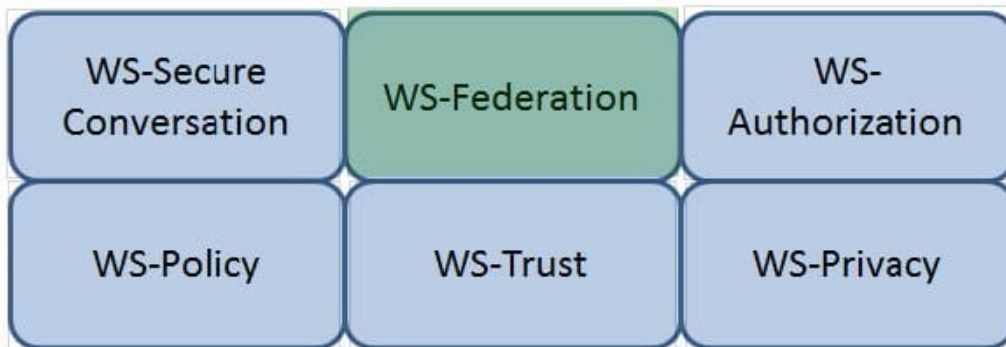
HOTSPOT

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 15

DRAG DROP



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

Select and Place:

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

Correct Answer:

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

[Latest CISSP-2018 Dumps](#)

[CISSP-2018 PDF Dumps](#)

[CISSP-2018 VCE Dumps](#)