

# 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.leads4pass.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

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

- |  |      |
|--|------|
| <b>Document the information assets</b>         | Step |
| <b>Assign a classification level</b>           | Step |
| <b>Apply the appropriate security markings</b> | Step |
| <b>Conduct periodic classification reviews</b> | Step |
| <b>Declassify information when appropriate</b> | Step |

## QUESTION 2

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 based on criteria assigned by a custodian

Correct Answer:

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

## QUESTION 3

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 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:

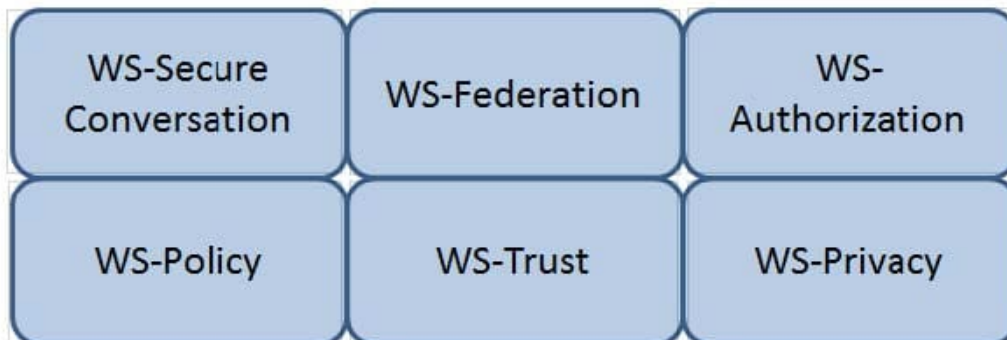
Security Engineering Term		Definition
Risk		A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of
Security Risk Treatment		The method used to identify the confidentiality, 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 5

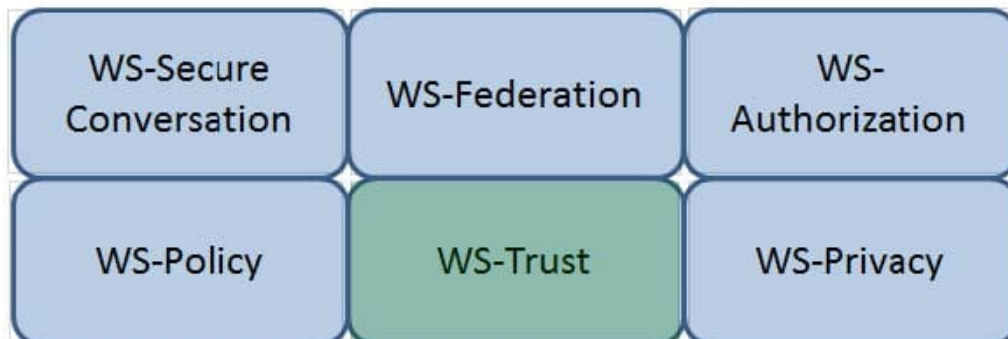
### HOTSPOT

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:



[Latest CISSP-2018 Dumps](#)

[CISSP-2018 Study Guide](#)

[CISSP-2018 Exam Questions](#)