

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

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

Select and Place:

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

Correct Answer:

Security Engineering Term		Definition
Risk	<input type="text"/>	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	<input type="text"/>	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	<input type="text"/>	The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Threat Assessment	<input type="text"/>	The method used to identify feasible security risk mitigation options and plans.

QUESTION 2

DRAG DROP

Place the following information classification steps in sequential order.

Select and Place:

<u>Steps</u>		<u>Order</u>
Declassify information when appropriate		Step
Apply the appropriate security markings		Step
Conduct periodic classification reviews		Step
Assign a classification level		Step
Document the information assets		Step

Correct Answer:

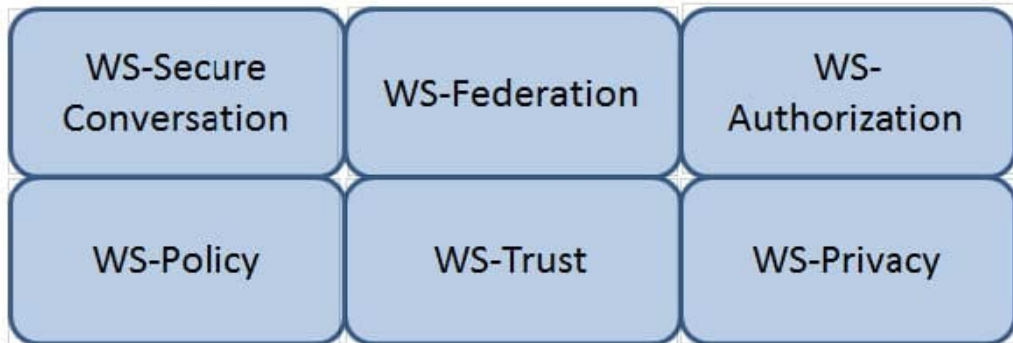
<u>Steps</u>		<u>Order</u>
	Document the information assets	Step
	Assign a classification level	Step
	Apply the appropriate security markings	Step
	Conduct periodic classification reviews	Step
	Declassify information when appropriate	Step

QUESTION 3

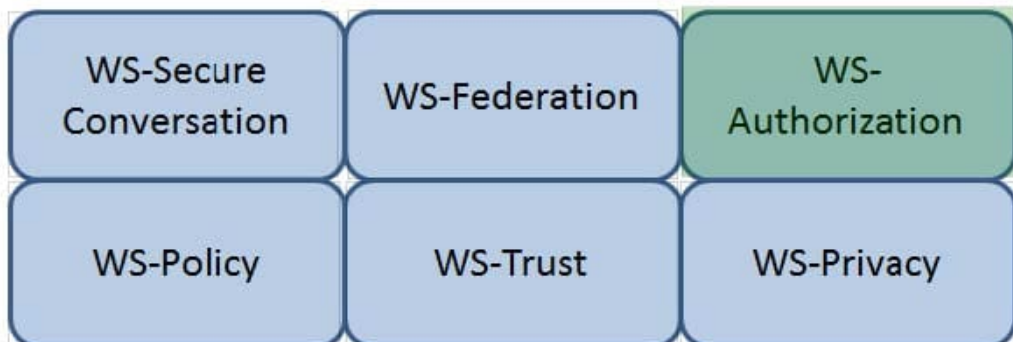
HOTSPOT

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 4

DRAG DROP

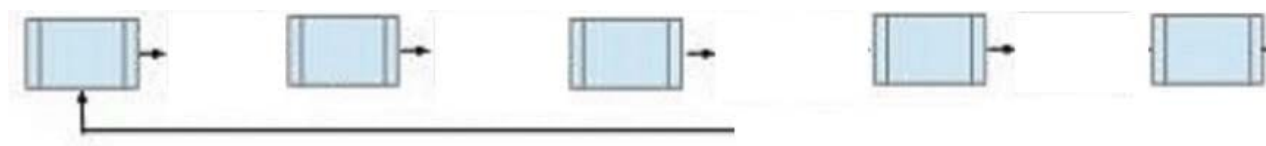
During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is

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?

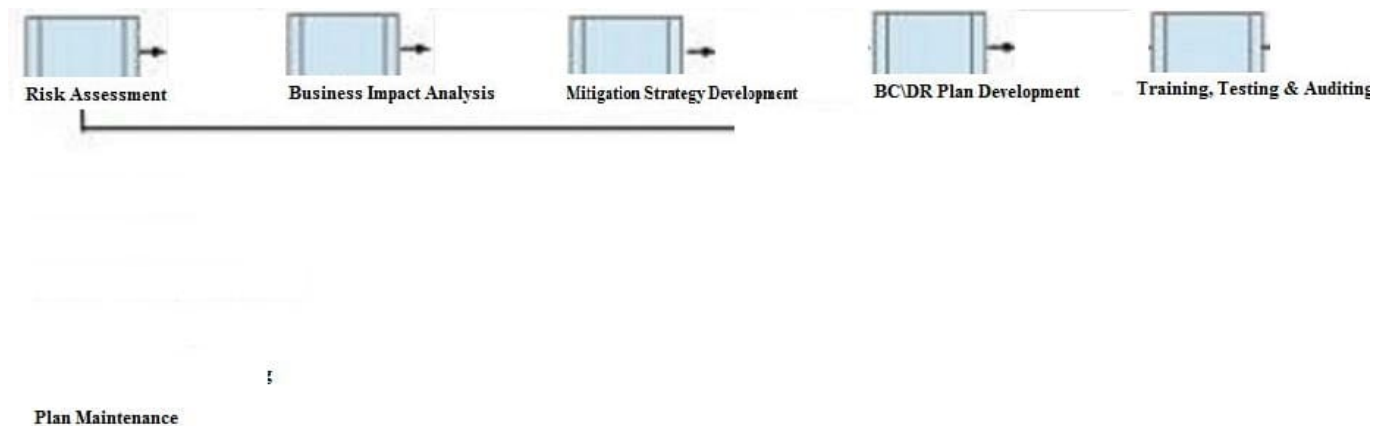
Below are the common phases to creating a Business Continuity/Disaster Recovery (BC/DR) plan. Drag the remaining BC\DR phases to the appropriate corresponding location.

Select and Place:



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

Correct Answer:



QUESTION 5

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