



# 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**

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

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

Input Parameter  
Selection

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 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

Place the following information classification steps in sequential order.

Select and Place:

Steps		Order
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:



Steps

Order

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

**QUESTION 5**

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.

[Latest CISSP-2018 Dumps](#)

[CISSP-2018 VCE Dumps](#)

[CISSP-2018 Practice Test](#)