



# 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.geekcert.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
	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
	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.
	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.

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 2

### 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 3

### 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

## QUESTION 4

### 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

Equivalence Class Analysis

Input Parameter

Selection

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 5

### 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