

# 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

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

Select and Place:

|                          |                      |  |
|--------------------------|----------------------|--|
| Secure Architecture      | <input type="text"/> | Do you advertise shared security services with guidance for project teams?               |
| Education & Guidance     | <input type="text"/> | Are most people tested to ensure a baseline skill- set for secure development practices? |
| Strategy & Metrics       | <input type="text"/> | Does most of the organization know about what's required based on risk ratings?          |
| Vulnerability Management | <input type="text"/> | 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)? |

## QUESTION 2

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 3**

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                 |  | Responsibility  |
|----------------------|--|---|
| Executive management |  | Approve audit budget and resource allocation.   |
| Audit committee      |  | Provide audit oversight.  |
| Compliance officer   |  | Ensure the achievement and maintenance of organizational requirements with applicable certifications. |
| External auditor     |  | Develop and maintain knowledge and subject-matter expertise relevant to the type of audit.            |

Correct Answer:

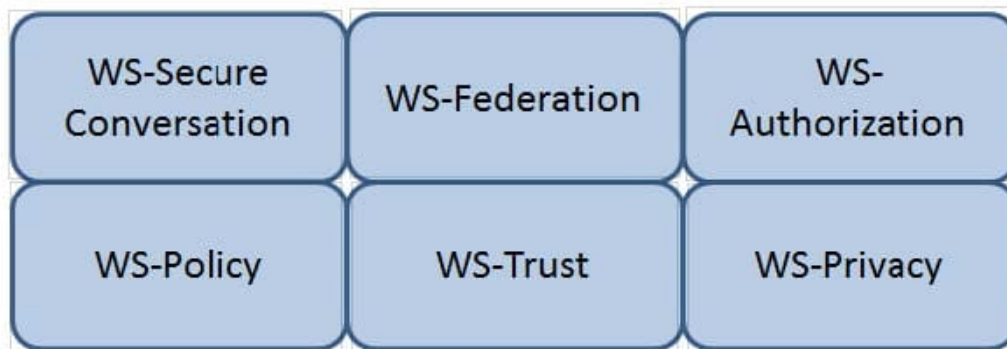
| <u>Role</u>          | <u>Responsibility</u>   |
|----------------------|---|
| Executive management | Approve audit budget and resource allocation.   |
| Audit committee      | Provide audit oversight.  |
| External auditor     | Ensure the achievement and maintenance of organizational requirements with applicable certifications. |
| Compliance officer   | Develop and maintain knowledge and subject-matter expertise relevant to the type of audit.            |

## QUESTION 4

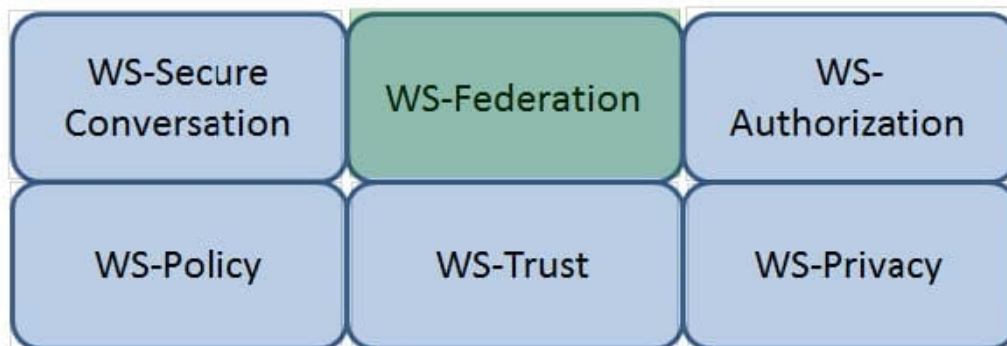
### HOTSPOT

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:



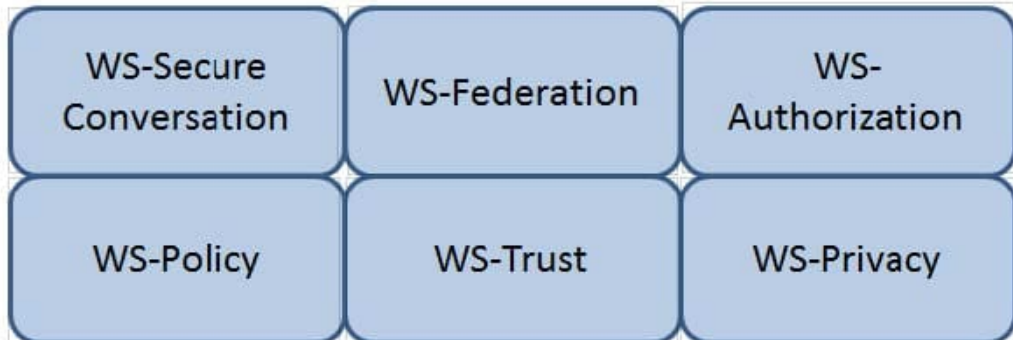
---

## QUESTION 5

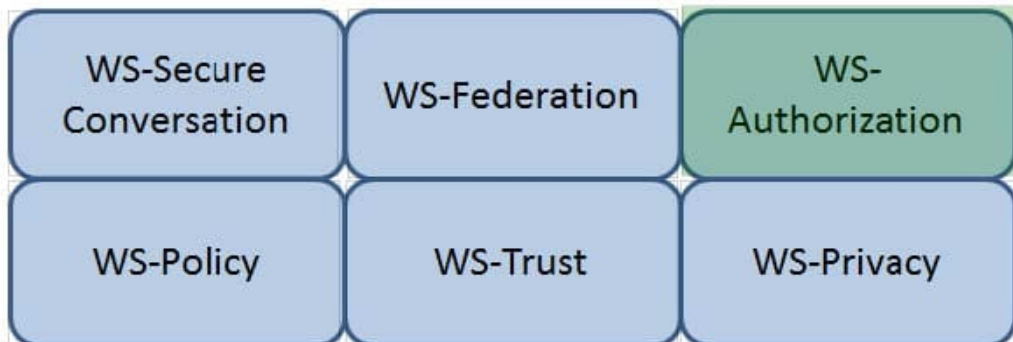
### HOTSPOT

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 6

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 7

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          |  | End user cannot set controls  |
| Discretionary Access Control(DAC) |  | Subject has total control over objects  |
| Role Based Access Control (RBAC)  |  | Dynamically assigns permissions to particular duties based on job function      |
| Rule Based Access Control         |  | Dynamically assigns roles to subjects bases on criteria assigned by a custodian |

Correct Answer:

| Access Control Model |                                   | Restrictions  |
|----------------------|-----------------------------------|---|
|                      | Mandatory Access Control          | End user cannot set controls  |
|                      | Discretionary Access Control(DAC) | Subject has total control over objects  |
|                      | Role Based Access Control (RBAC)  | Dynamically assigns permissions to particular duties based on job function      |
|                      | Rule Based Access Control         | Dynamically assigns roles to subjects bases on criteria assigned by a custodian |

## QUESTION 8

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

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

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

The method used to identify and characterize the dangers anticipated **throughout the life cycle of the system.**

Risk

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 9

DRAG DROP

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

Select and Place:

| <u>Event</u>          |  | <u>Order</u> |
|-----------------------|--|--------------|
| Disloyal employees    |  | 1            |
| User instigated       |  | 2            |
| Targeted infiltration |  | 3            |
| Virus infiltrations   |  | 4            |

Correct Answer:

| <u>Event</u> |                       | <u>Order</u> |
|--------------|-----------------------|--------------|
|              | Disloyal employees    | 1            |
|              | User-instigated       | 2            |
|              | Targeted infiltration | 3            |
|              | Virus infiltrations   | 4            |

## QUESTION 10

DRAG DROP

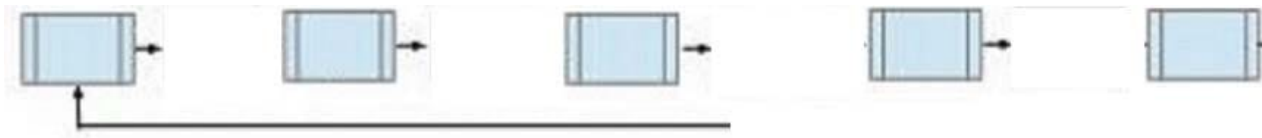
During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is

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:



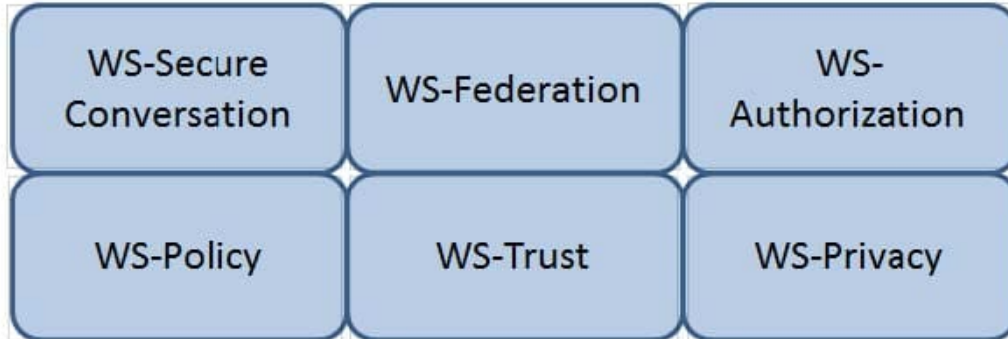
Plan Maintenance

## QUESTION 11

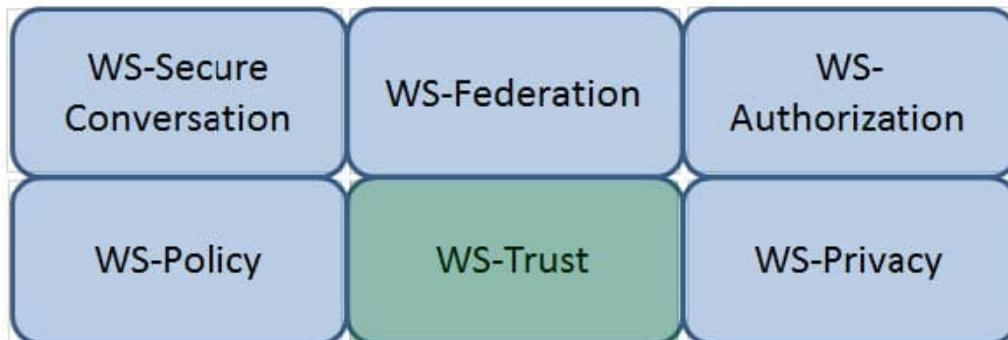
### HOTSPOT

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 12

DRAG DROP

Place the following information classification steps in sequential order.

Select and Place:

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

Correct Answer:

| <u>Steps</u> |  | <u>Order</u> |
|--------------|--|--------------|
|              | <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 13

DRAG DROP

Given the various means to protect physical and logical assets, match the access management area to the technology.

Select and Place:

| Area        |  | Technolog     |
|-------------|--|---------------|
| Facilities  |  | Encryption    |
| Devices     |  | Window        |
| Information |  | Firewall      |
| Systems     |  | Authenticatid |

Correct Answer:

| Area |             | Technolog     |
|------|-------------|---------------|
|      | Information | Encryption    |
|      | Facilities  | Window        |
|      | Devices     | Firewall      |
|      | Systems     | Authenticatid |

## QUESTION 14

DRAG DROP

What is the correct order of steps in an information security assessment?

Place the information security assessment steps on the left next to the numbered boxes on the right in the correct order.

Select and Place:

| <u>Actions</u>              |  | <u>Steps</u> |
|-----------------------------|--|--------------|
| Define the perimeter.       |  | Step 1       |
| Identify the vulnerability. |  | Step 2       |
| Assess the risk.            |  | Step 3       |
| Determine the actions.      |  | Step 4       |

Correct Answer:

| <u>Actions</u> |                             | <u>Steps</u> |
|----------------|-----------------------------|--------------|
|                | Identify the vulnerability. | Step 1       |
|                | Define the perimeter.       | Step 2       |
|                | Assess the risk.            | Step 3       |
|                | Determine the actions.      | Step 4       |

## QUESTION 15

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

[CISSP-2018 PDF Dumps](#)

[CISSP-2018 VCE Dumps](#)

[CISSP-2018 Exam Questions](#)