# 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.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

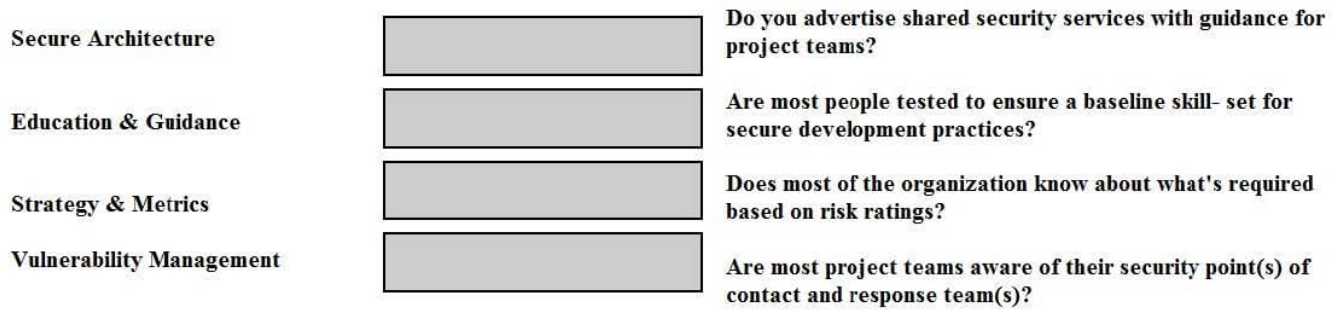
- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

**QUESTION 1**

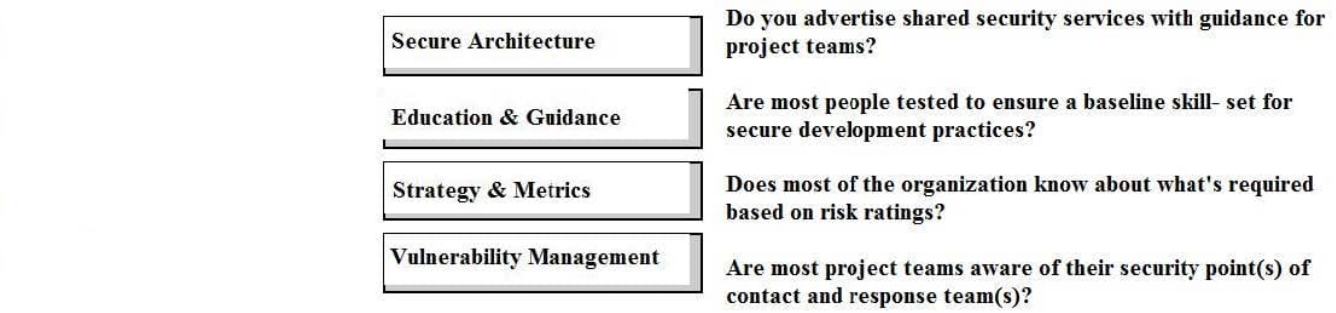
DRAG DROP

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

Select and Place:




Correct Answer:

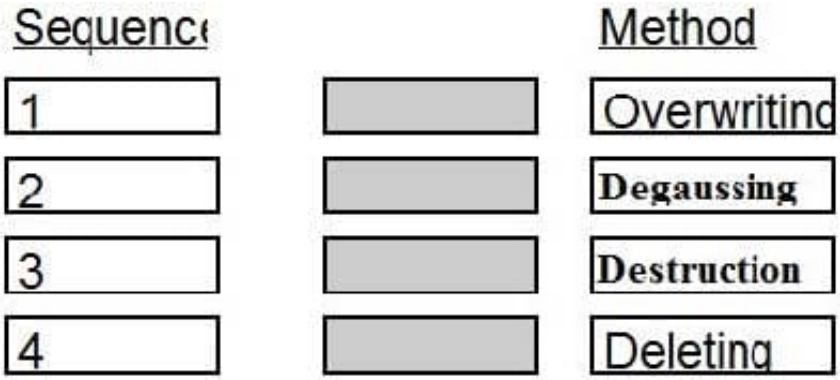



**QUESTION 2**

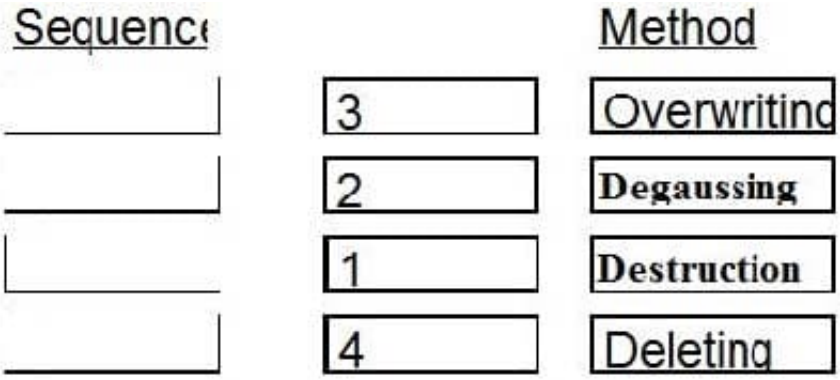
DRAG DROP

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:




Correct Answer:

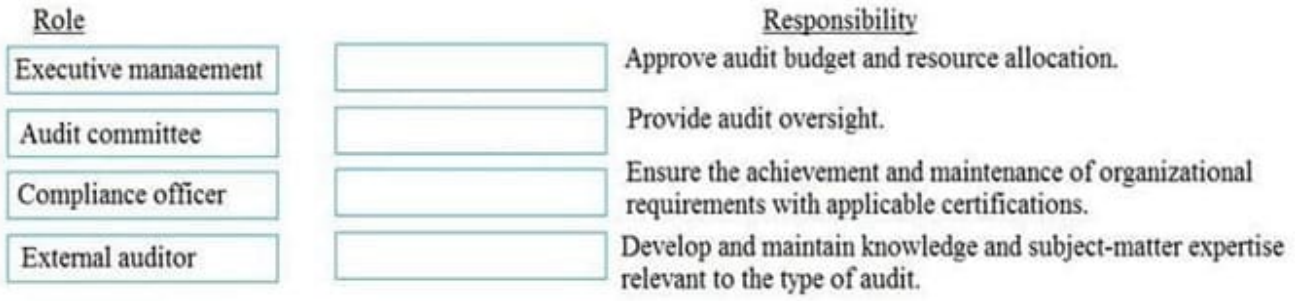



**QUESTION 3**

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:




Correct Answer:

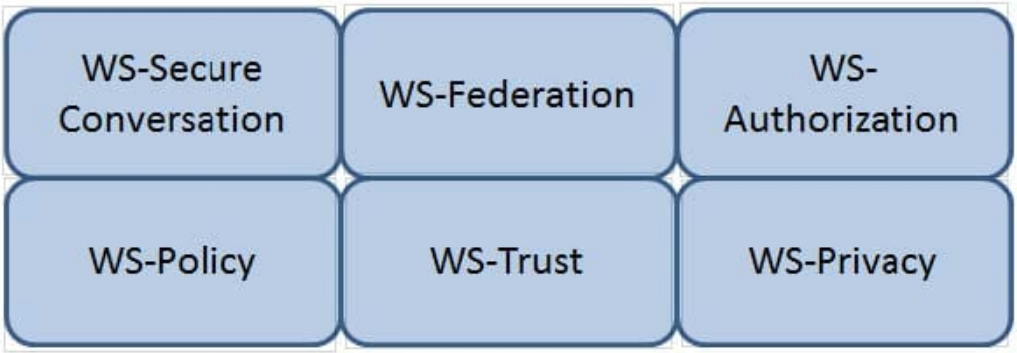
| Role | | Responsibility |
|---|---|---|
| | Executive management | Approve audit budget and resource allocation. |
| | Audit committee | Provide audit oversight. |
| | External auditor | Ensure the achievement and maintenance of organizational requirements with applicable certifications. |
| | Compliance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

**QUESTION 4**

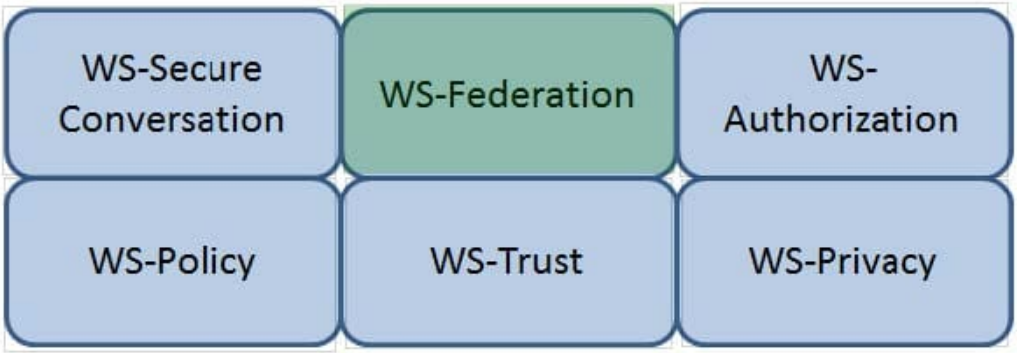
HOTSPOT

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:

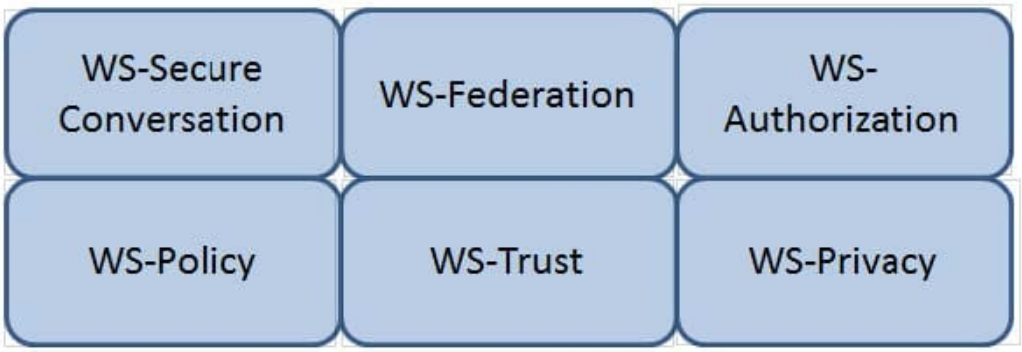



**QUESTION 5**

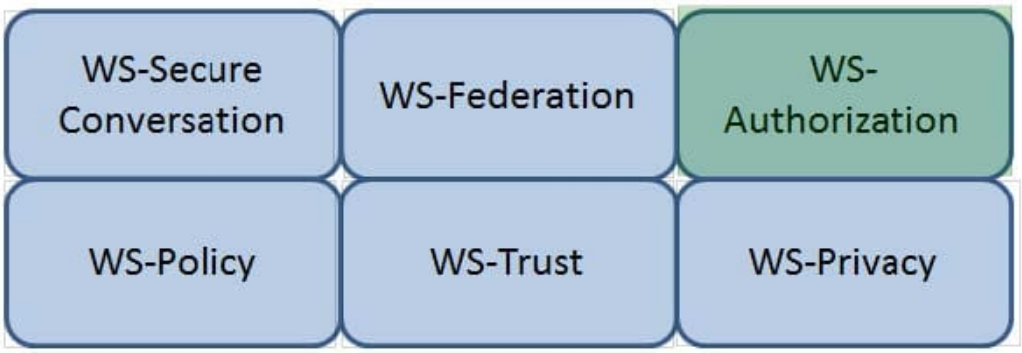
HOTSPOT

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:

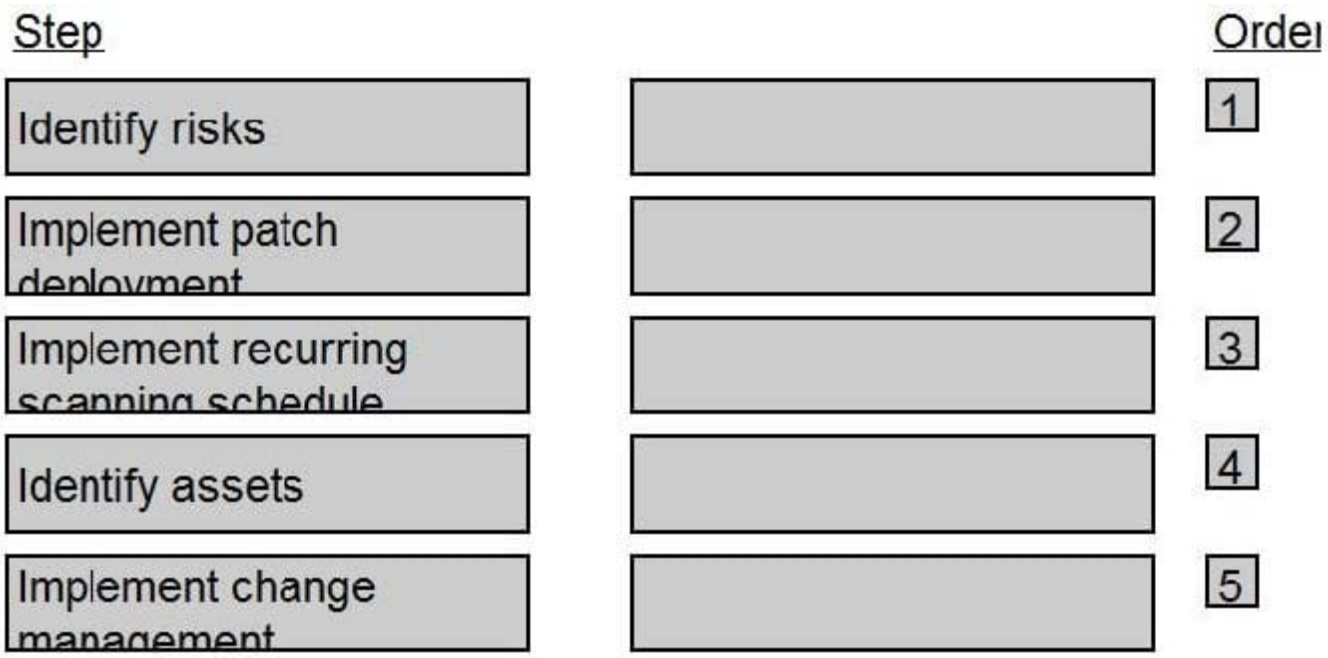



**QUESTION 6**

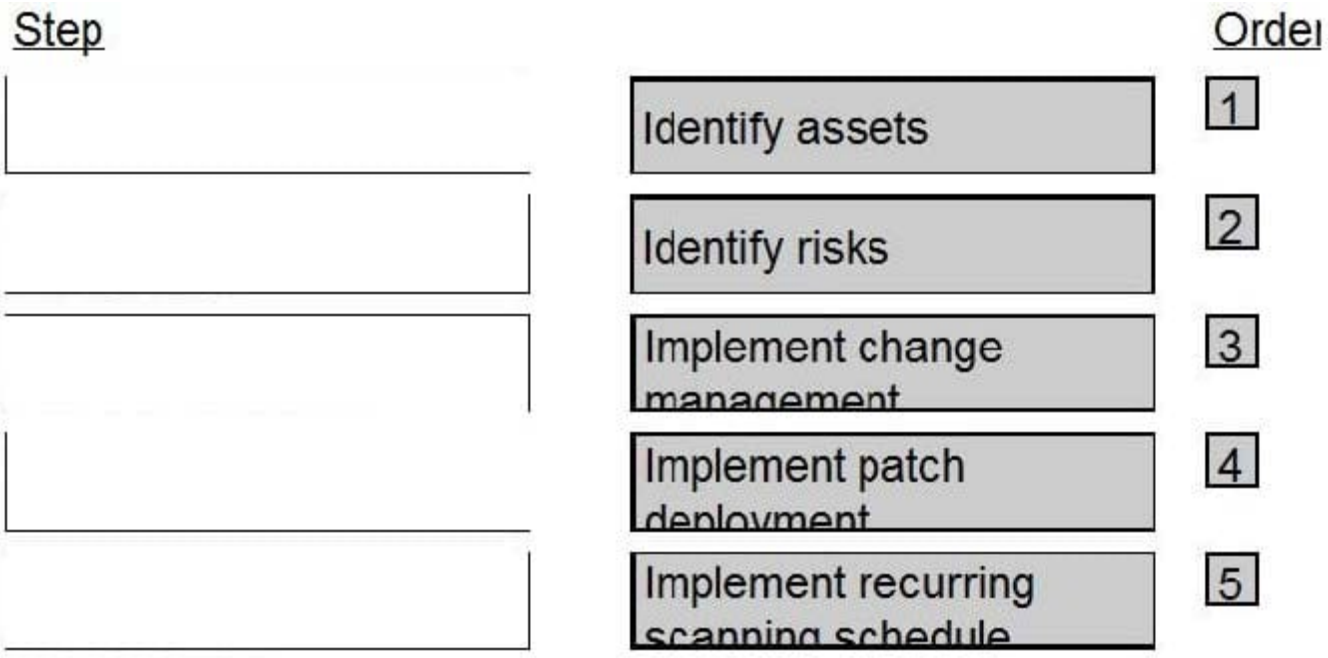
DRAG DROP

Order the below steps to create an effective vulnerability management process.

Select and Place:




Correct Answer:



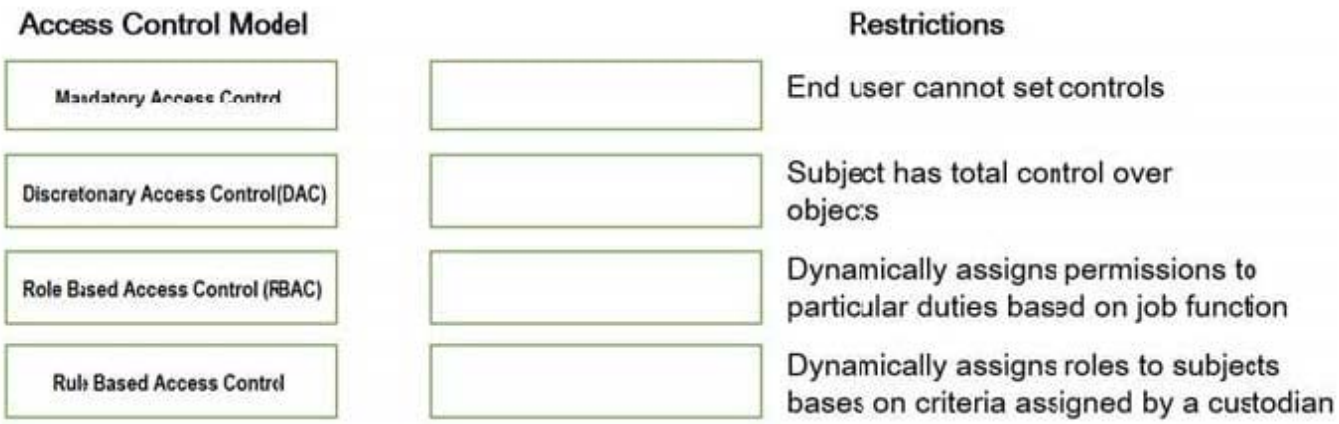

**QUESTION 7**

DRAG DROP

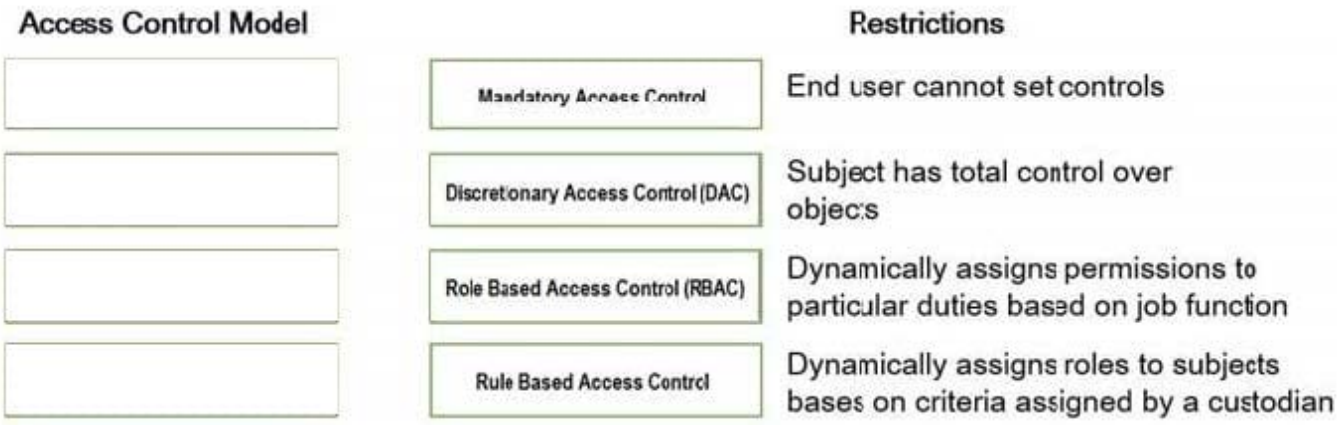
Match the name of access control model with its associated restriction.

Drag each access control model to its appropriate restriction access on the right.

Select and Place:




Correct Answer:

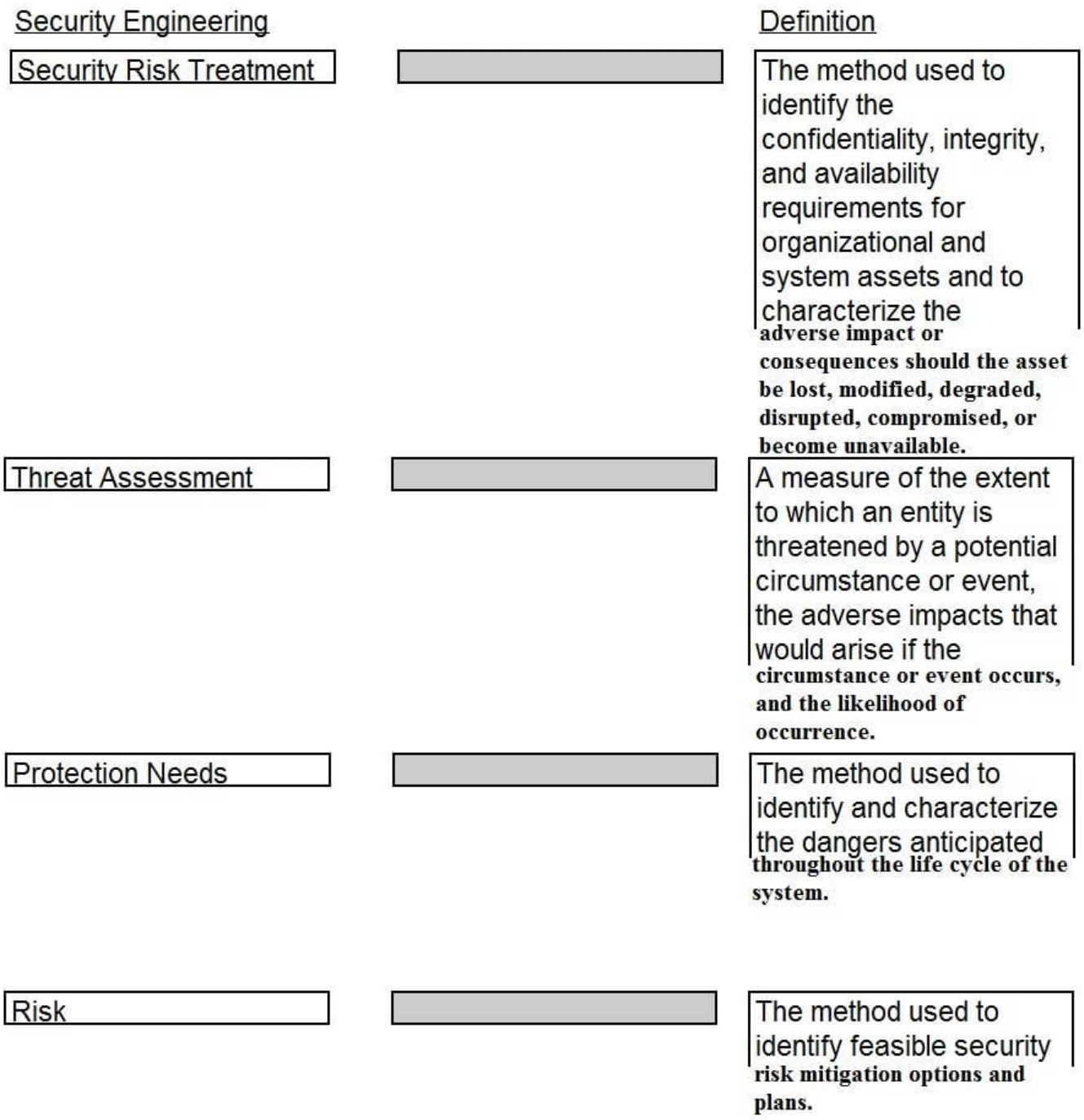



**QUESTION 8**

DRAG DROP

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

Select and Place:




Correct Answer:

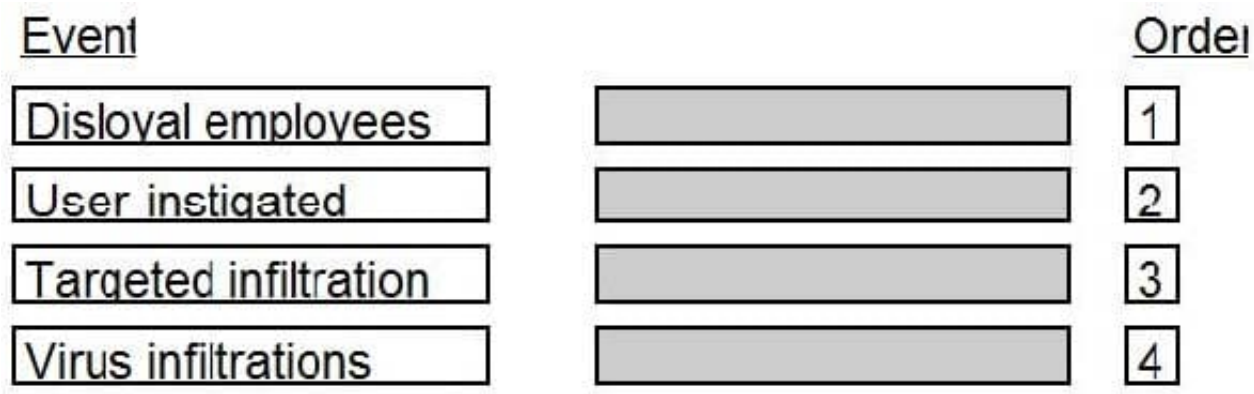
| Security Engineering | | Definition |
|---|---|---|
| | Protection Needs | The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the **adverse impact or consequences should the asset be lost, modified, degraded, 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**

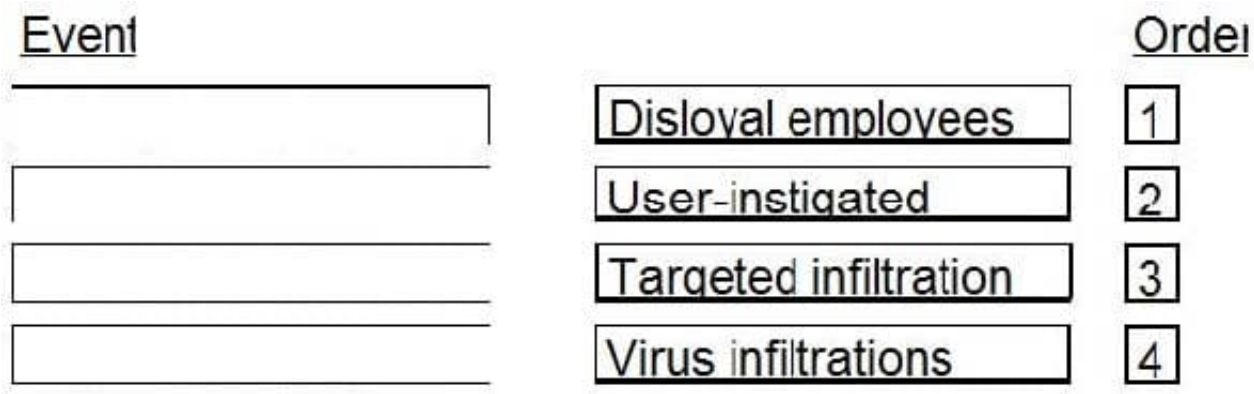
DRAG DROP

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

Select and Place:




Correct Answer:




**QUESTION 10**

DRAG DROP

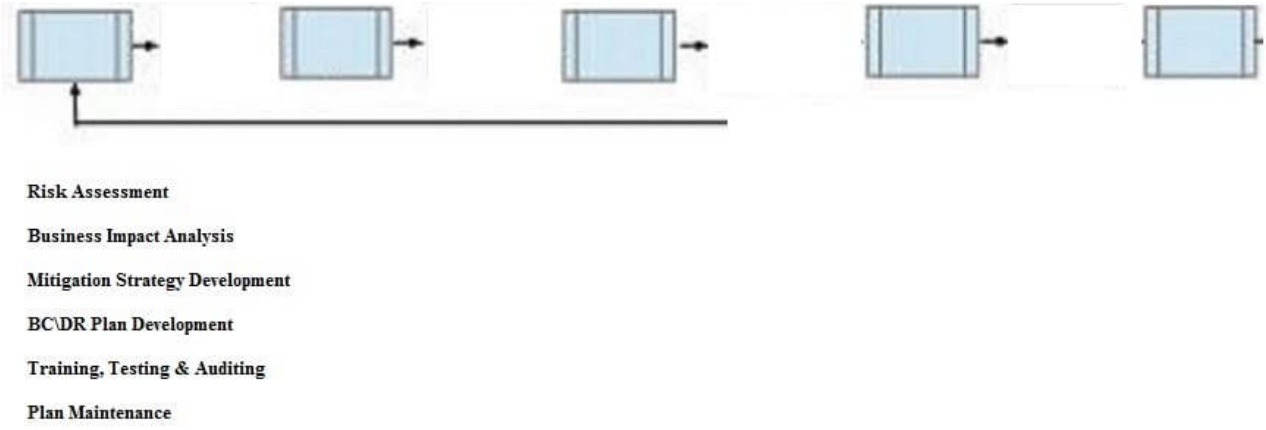
During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is

fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.

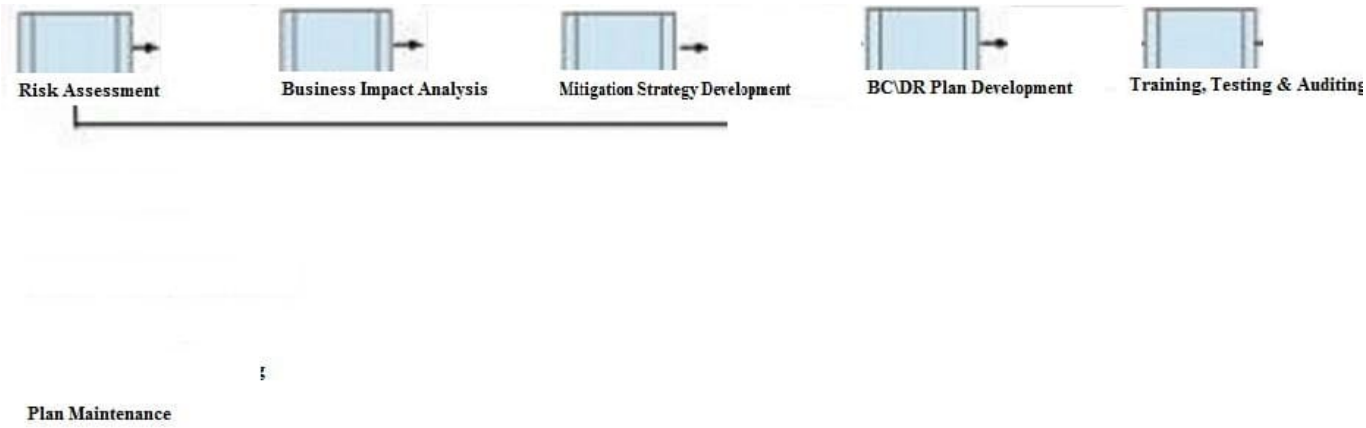
What is the best approach for the CISO?

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:




Correct Answer:

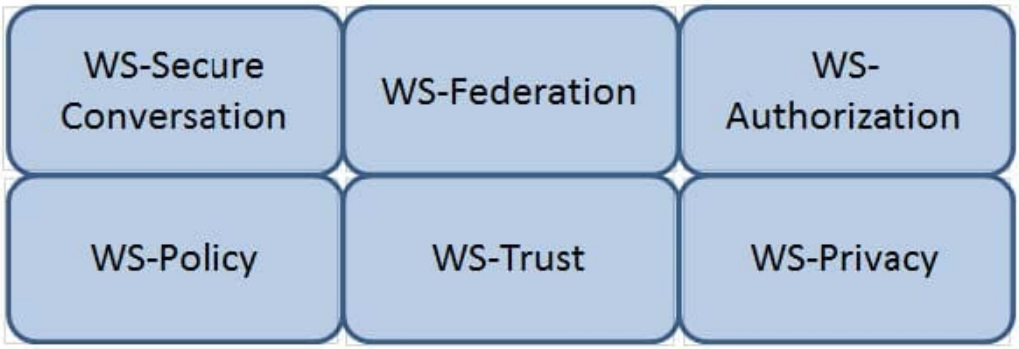



**QUESTION 11**

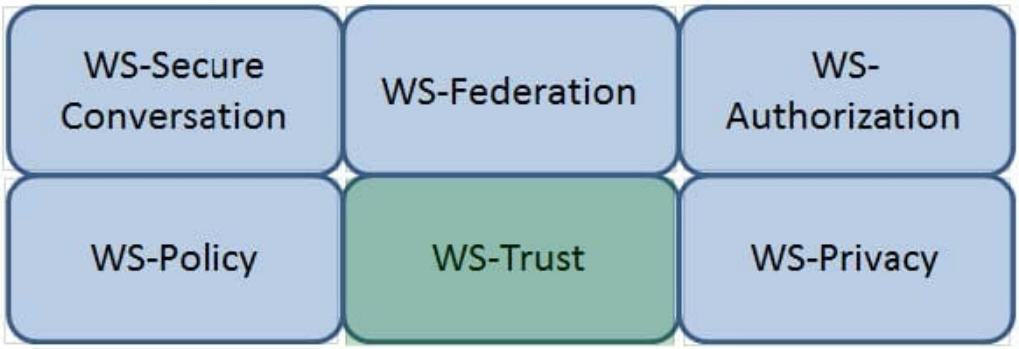
HOTSPOT

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:

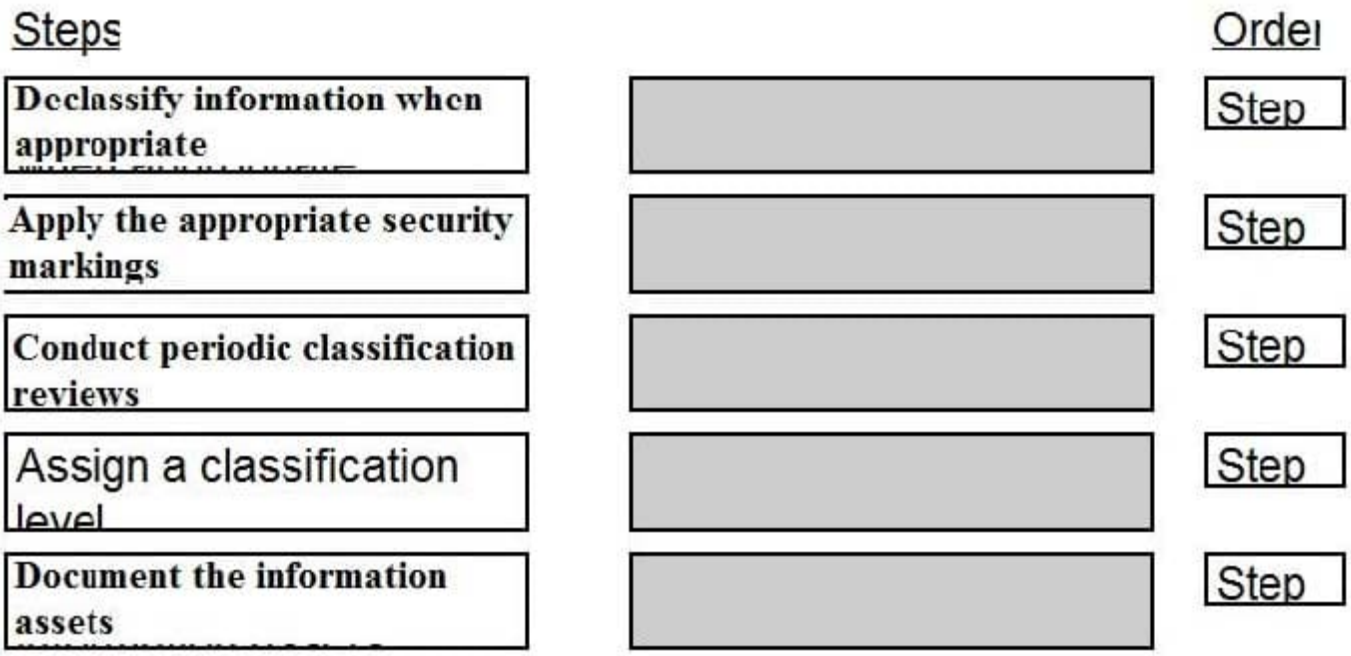



**QUESTION 12**

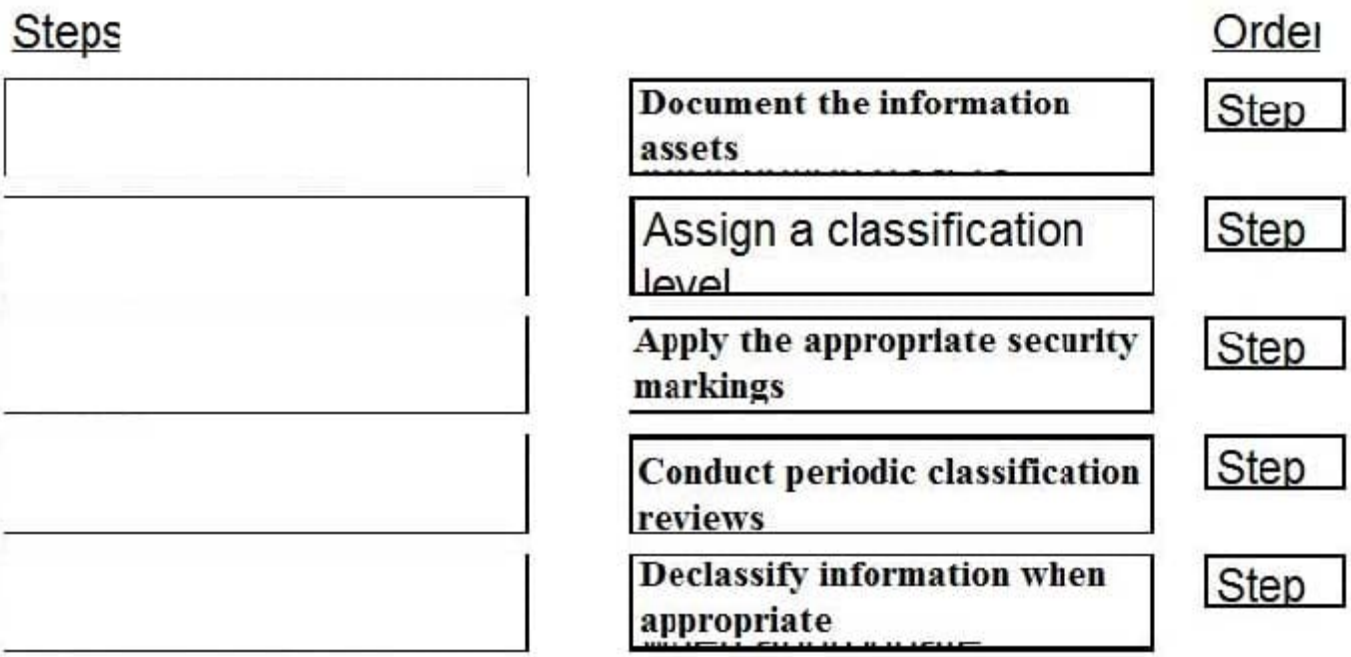
DRAG DROP

Place the following information classification steps in sequential order.

Select and Place:




Correct Answer:

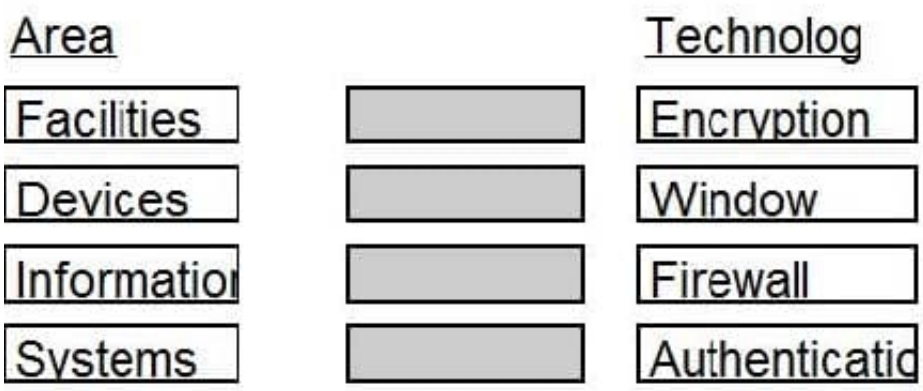



**QUESTION 13**

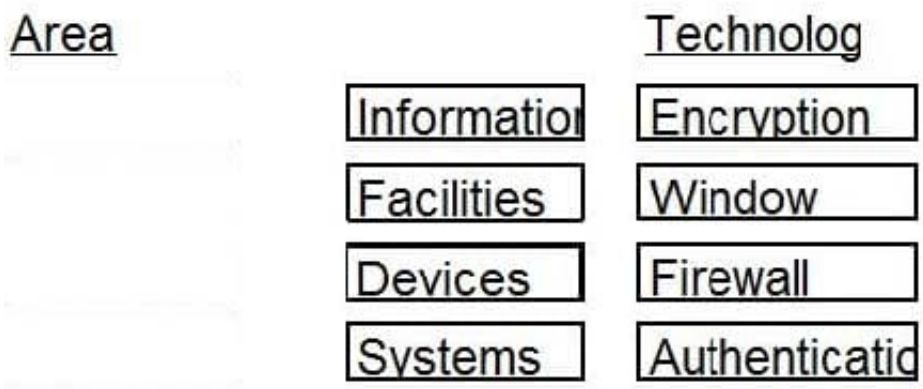
DRAG DROP

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

Select and Place:




Correct Answer:



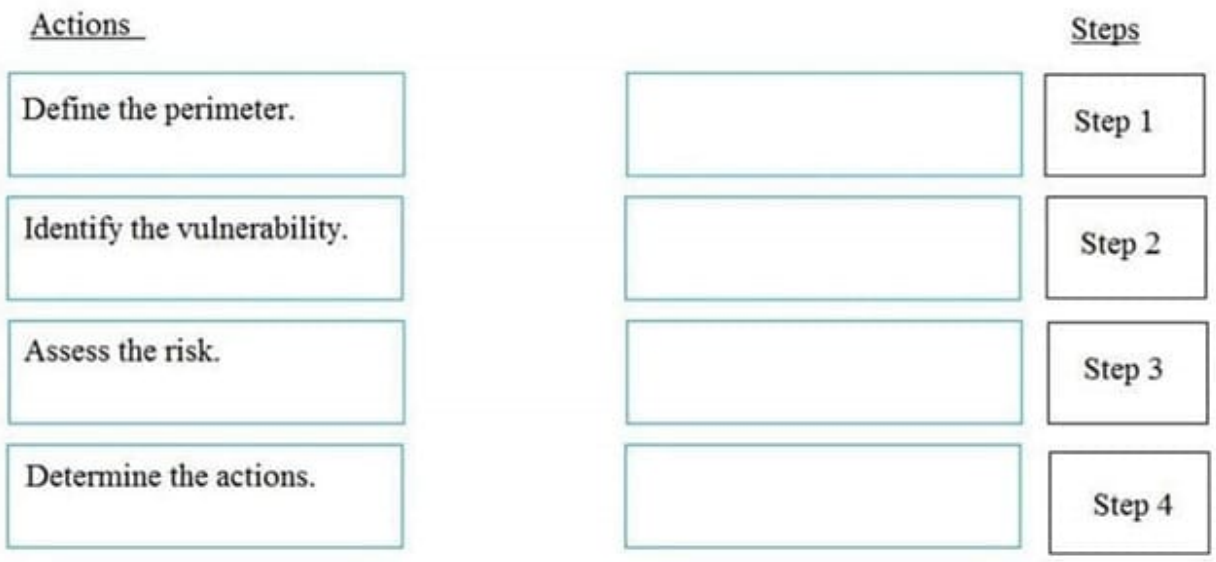

**QUESTION 14**

DRAG DROP

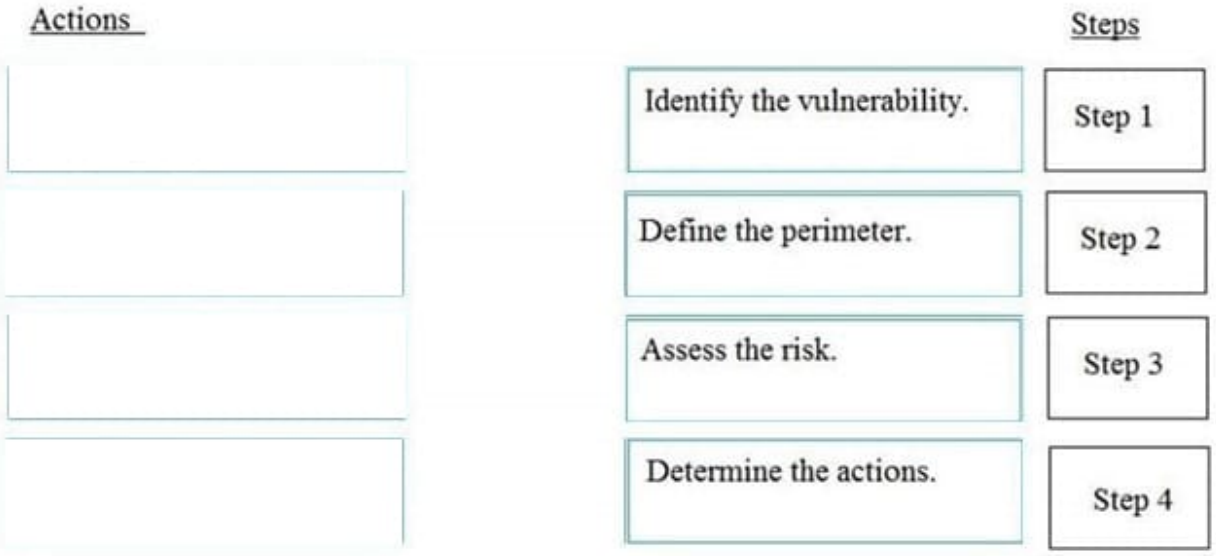
What is the correct order of steps in an information security assessment?

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

Select and Place:




Correct Answer:



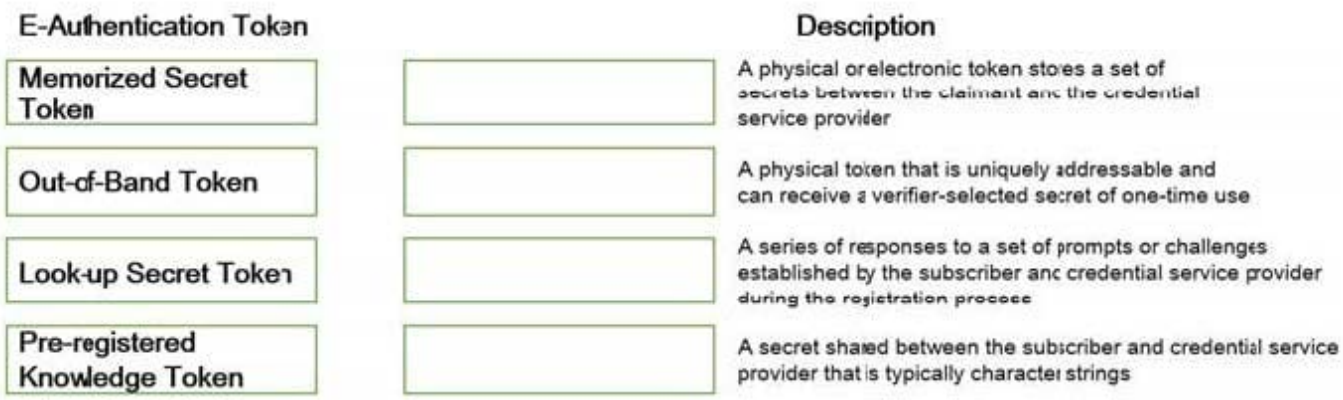

**QUESTION 15**

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:




Correct Answer: