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

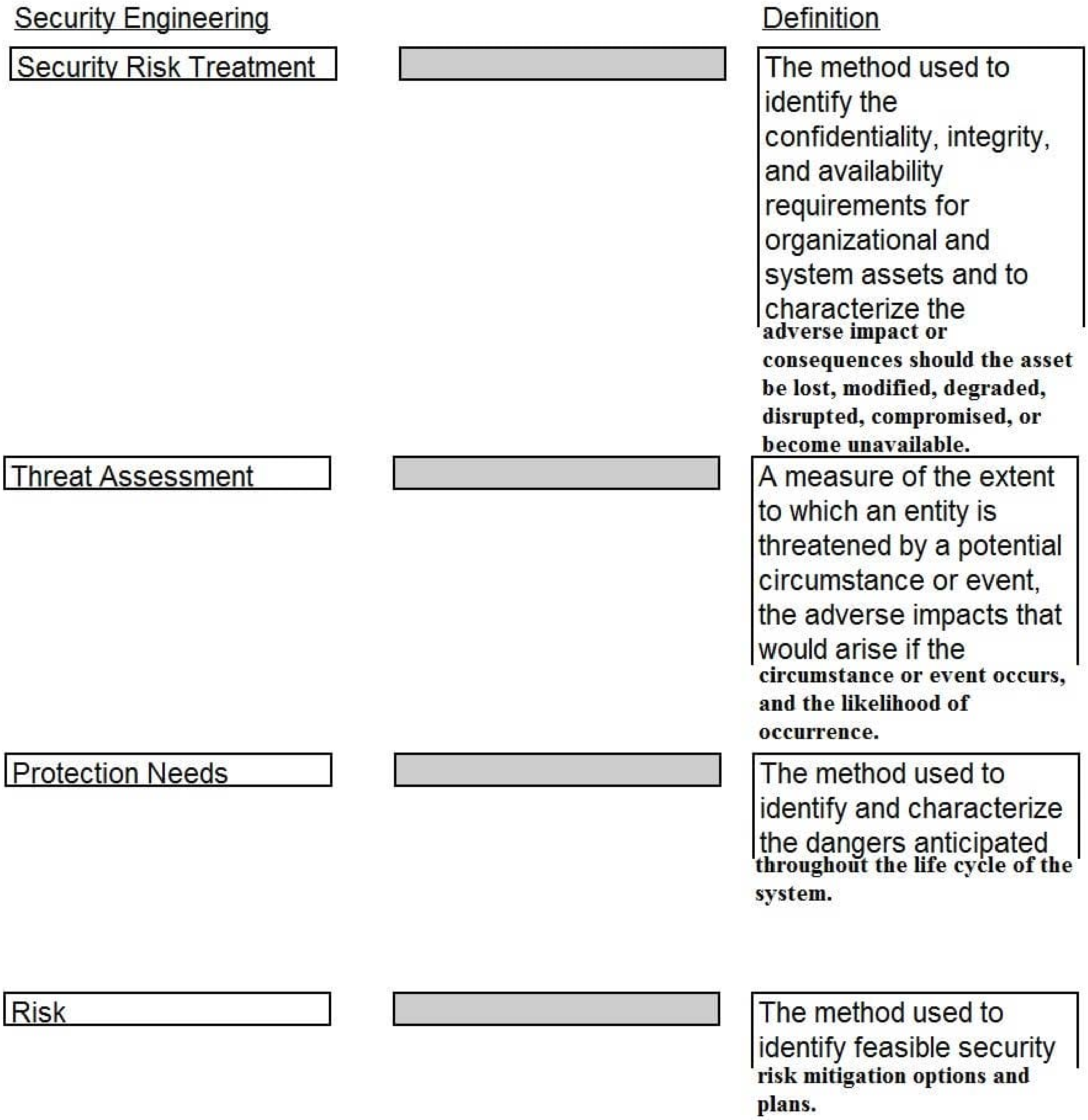
Following Questions and Answers are all new published by ISC Official Exam Center

QUESTION 1

DRAG DROP

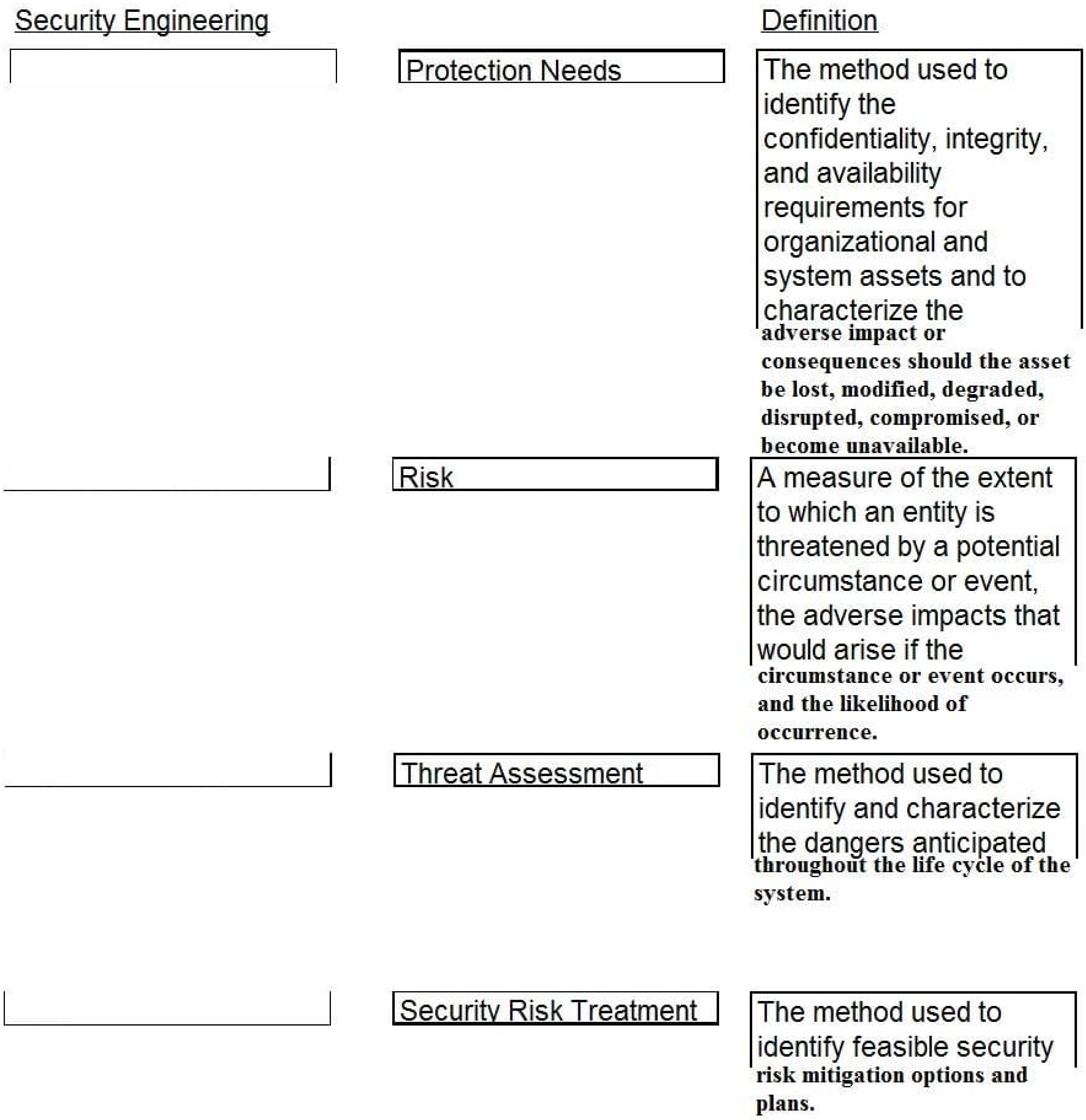
Drag the following Security Engineering terms on the left to the BEST definition on the right.

Select and Place:



Security Engineering		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:



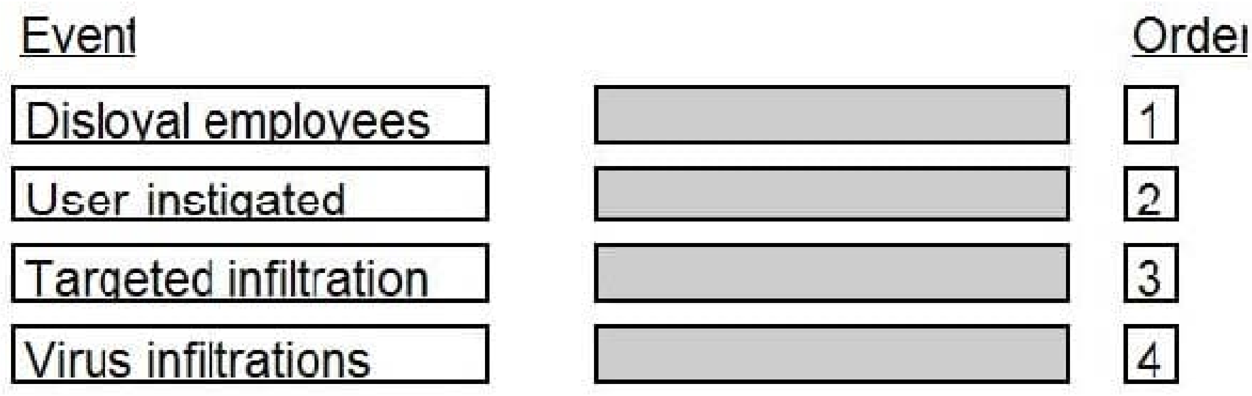
Security Engineering		Definition
	Protection Needs	The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, 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 2

DRAG DROP

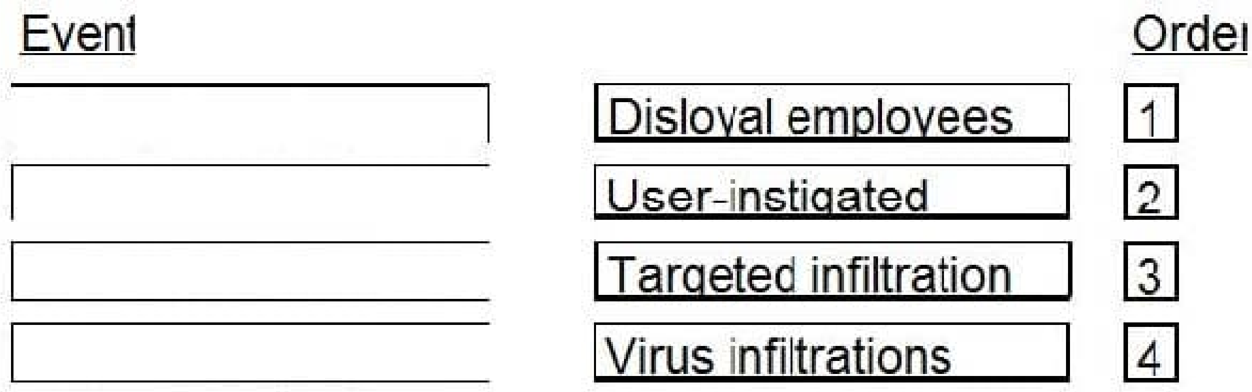
In which order, from MOST to LEAST impacted, does user awareness training reduce the occurrence of the events below?

Select and Place:



Event		Order
Disloyal employees		1
User instigated		2
Targeted infiltration		3
Virus infiltrations		4

Correct Answer:



Event		Order
	Disloyal employees	1
	User-instigated	2
	Targeted infiltration	3
	Virus infiltrations	4

QUESTION 3

DRAG DROP

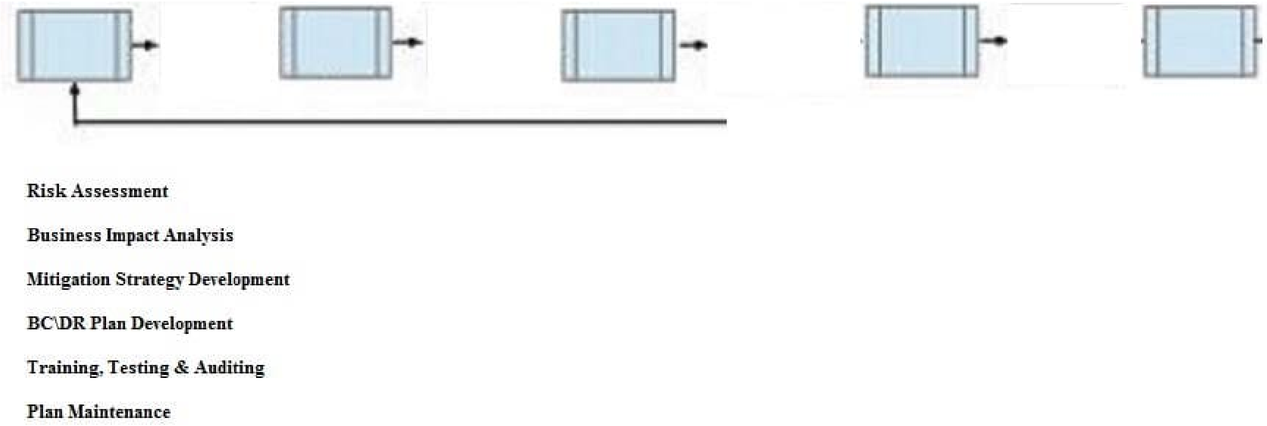
During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is

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

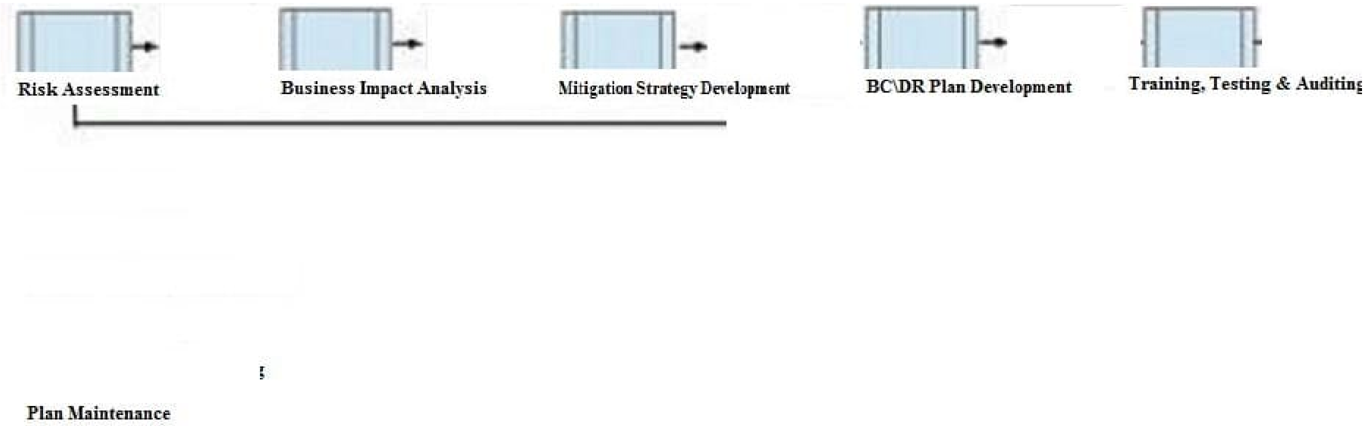
Mitigation Strategy Development

BC\DR Plan Development

Training, Testing & Auditing

Plan Maintenance

Correct Answer:



Risk Assessment

Business Impact Analysis

Mitigation Strategy Development

BC\DR Plan Development

Training, Testing & Auditin

Plan Maintenance

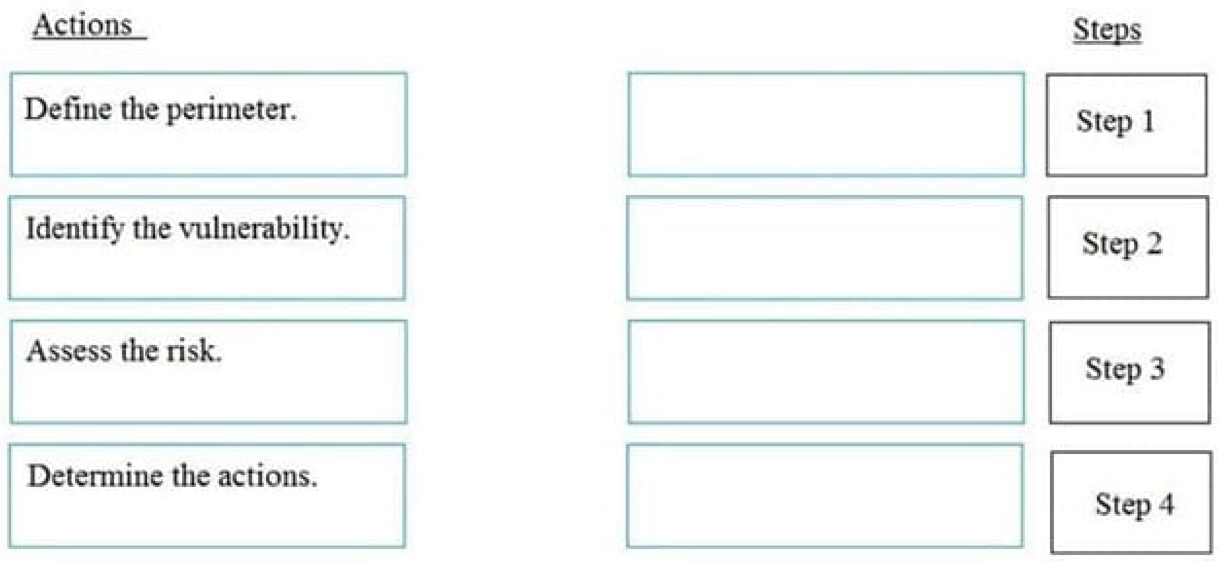
QUESTION 4

DRAG DROP

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

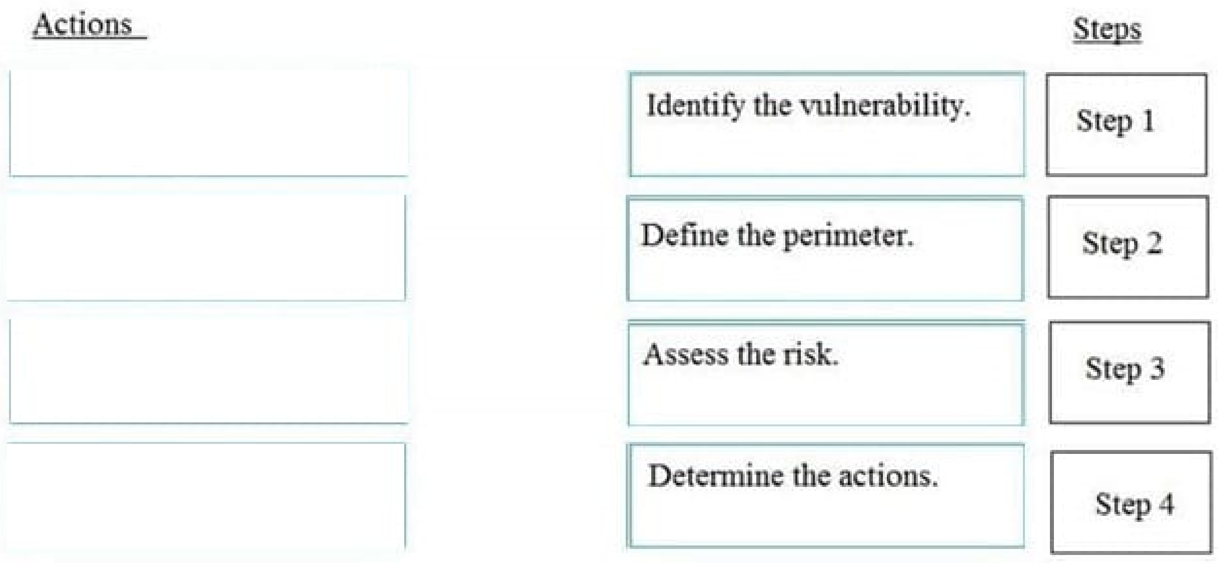
Place the information security assessment steps on the left next to the numbered boxes on the right in the correct order.

Select and Place:



Actions		Steps
Define the perimeter.		Step 1
Identify the vulnerability.		Step 2
Assess the risk.		Step 3
Determine the actions.		Step 4

Correct Answer:



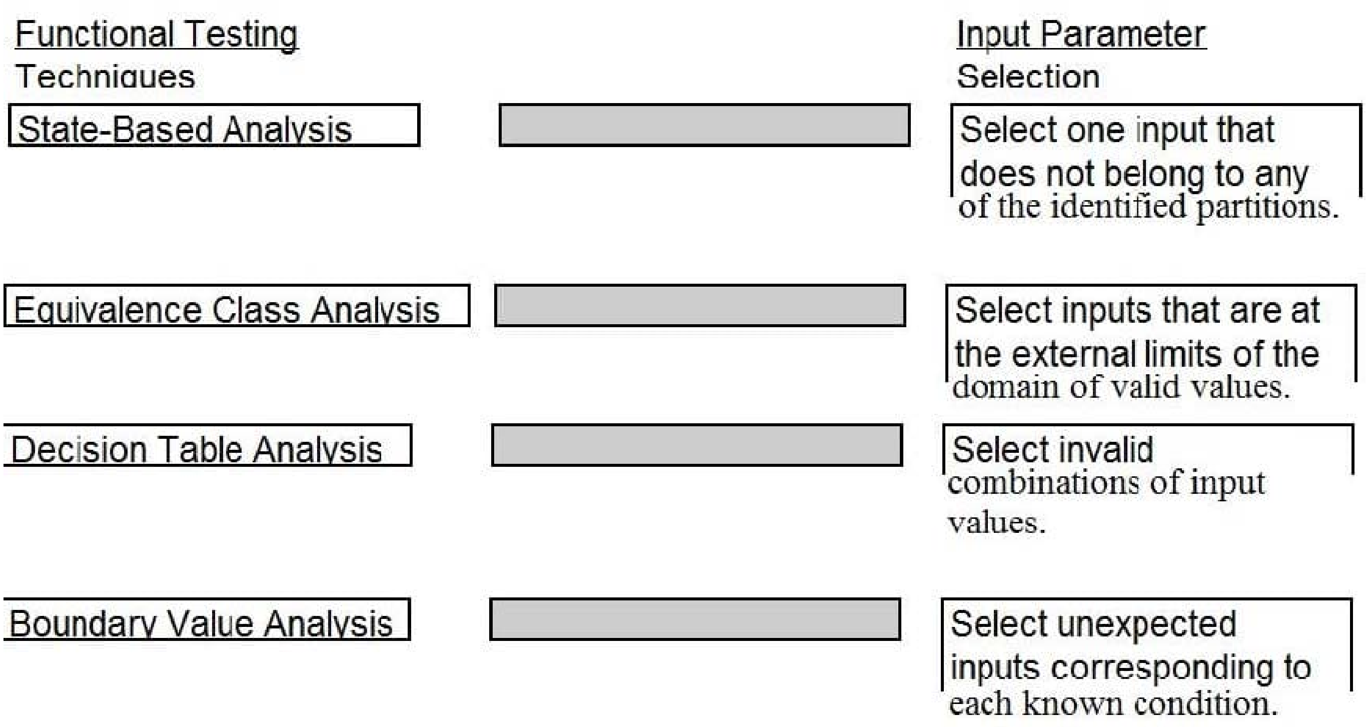
Actions		Steps
	Identify the vulnerability.	Step 1
	Define the perimeter.	Step 2
	Assess the risk.	Step 3
	Determine the actions.	Step 4

QUESTION 5

DRAG DROP

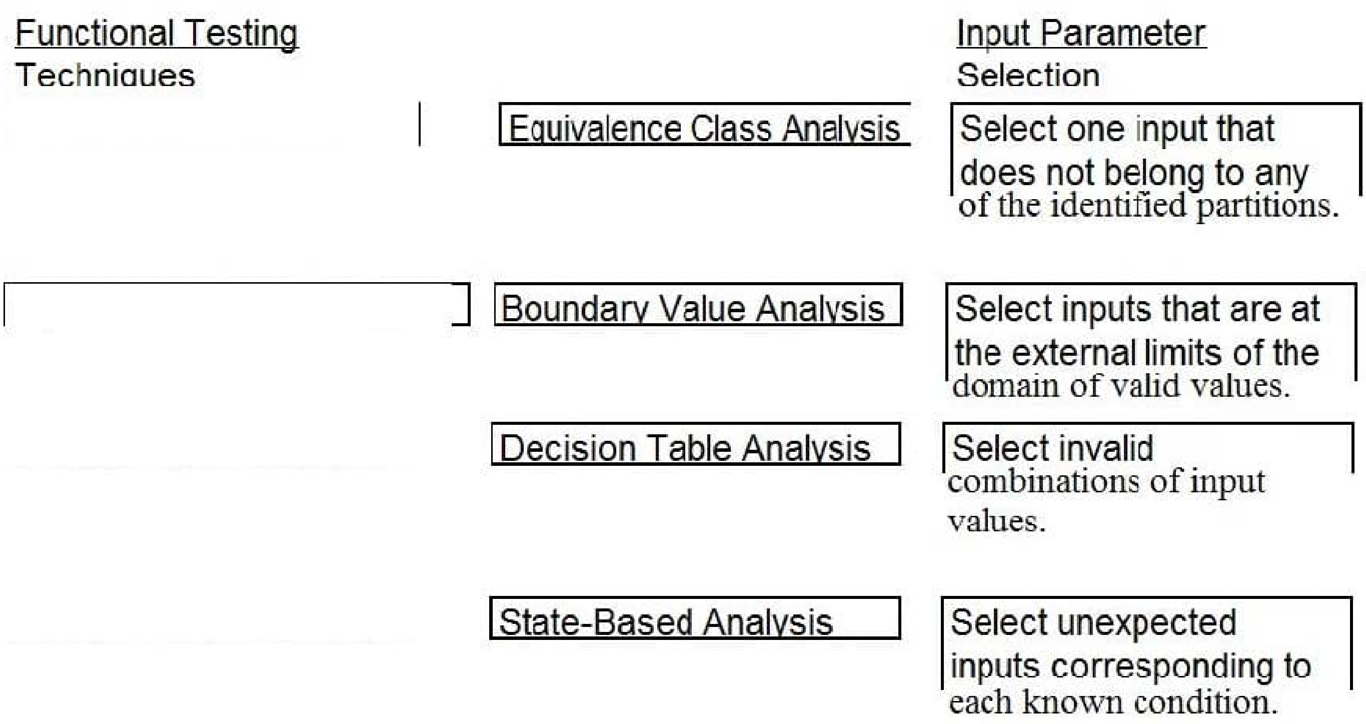
A software security engineer is developing a black box-based test plan that will measure the system\\'s reaction to incorrect or illegal inputs or unexpected operational errors and situations. Match the functional testing techniques on the left with the correct input parameters on the right.

Select and Place:



Functional Testing Techniques		Input Parameter Selection
State-Based Analysis		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:



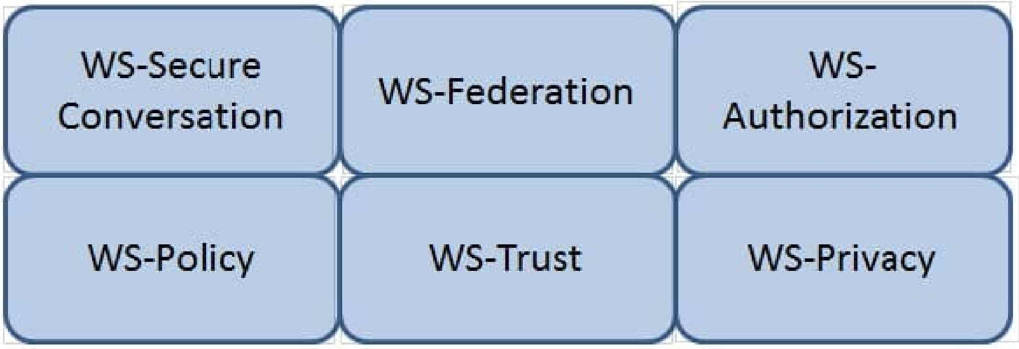
Functional Testing Techniques		Input Parameter Selection
	Equivalence Class Analysis	Select one input that does not belong to any of the identified partitions.
	Boundary Value Analysis	Select inputs that are at the external limits of the domain of valid values.
	Decision Table Analysis	Select invalid combinations of input values.
	State-Based Analysis	Select unexpected inputs corresponding to each known condition.

QUESTION 6

HOTSPOT

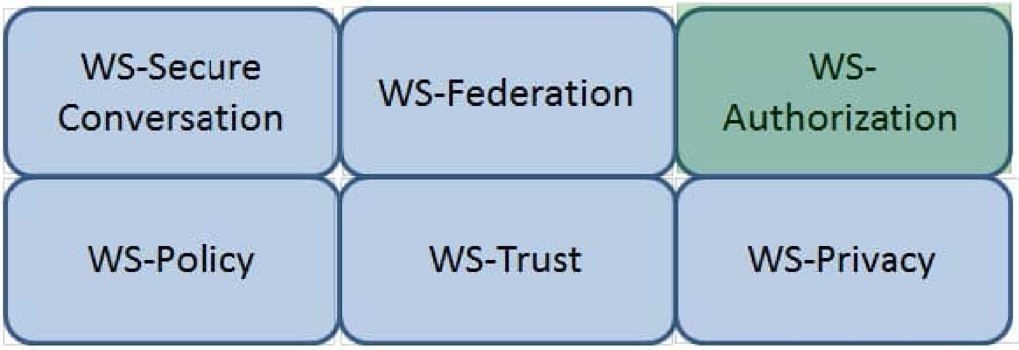
Which Web Services Security (WS-Security) specification handles the management of security tokens and the underlying policies for granting access? Click on the correct specification in the image below.

Hot Area:



WS-Secure Conversation	WS-Federation	WS-Authorization
WS-Policy	WS-Trust	WS-Privacy

Correct Answer:



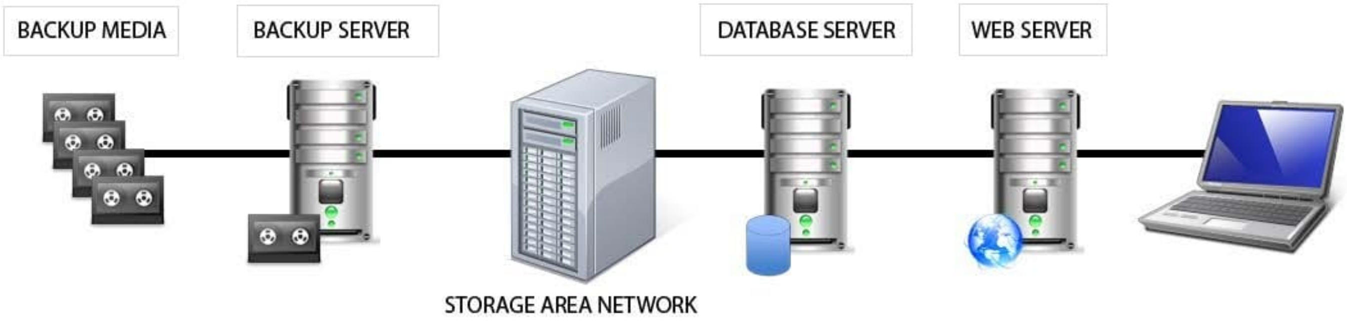
WS-Secure Conversation	WS-Federation	WS-Authorization
WS-Policy	WS-Trust	WS-Privacy

QUESTION 7

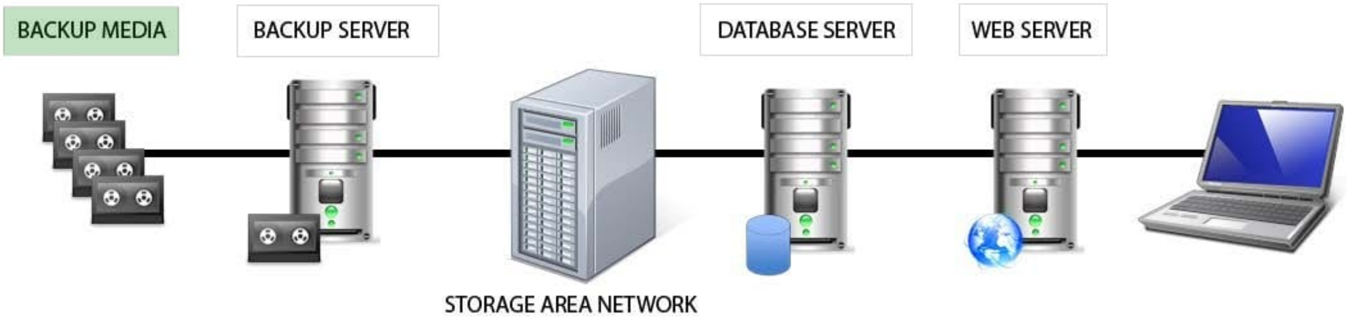
HOTSPOT

Identify the component that MOST likely lacks digital accountability related to information access. Click on the correct device in the image below.

Hot Area:



Correct Answer:

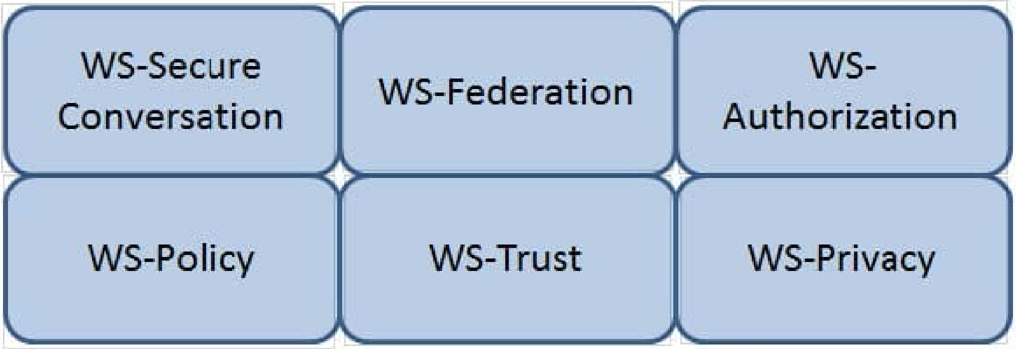


QUESTION 8

HOTSPOT

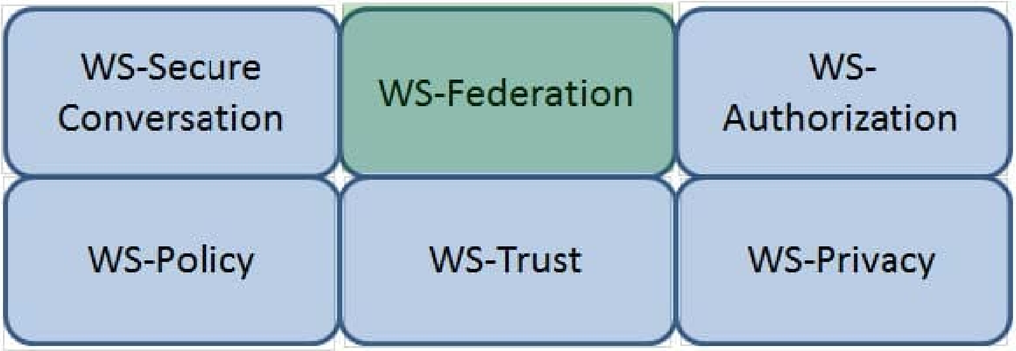
Which Web Services Security (WS-Security) specification maintains a single authenticated identity across multiple dissimilar environments? Click on the correct specification in the image below.

Hot Area:



WS-Secure Conversation	WS-Federation	WS-Authorization
WS-Policy	WS-Trust	WS-Privacy

Correct Answer:



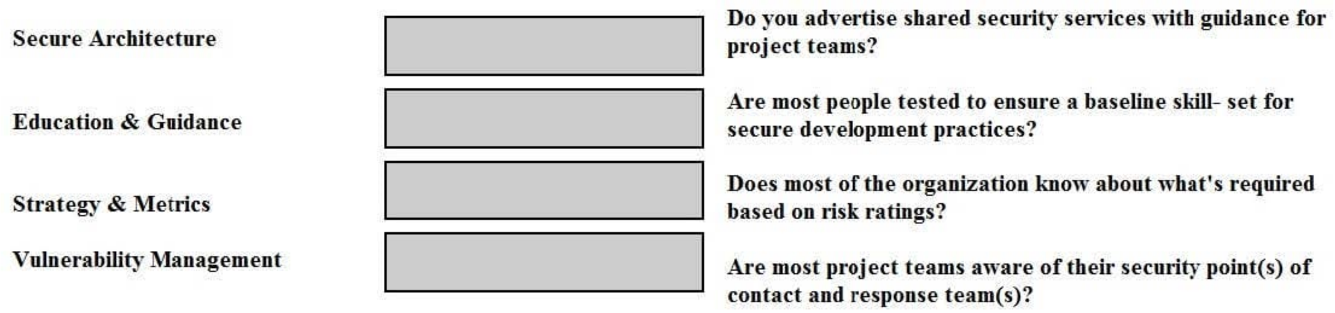
WS-Secure Conversation	**WS-Federation**	WS-Authorization
WS-Policy	WS-Trust	WS-Privacy

QUESTION 9

DRAG DROP

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

Select and Place:



Secure Architecture

Education & Guidance

Strategy & Metrics

Vulnerability Management

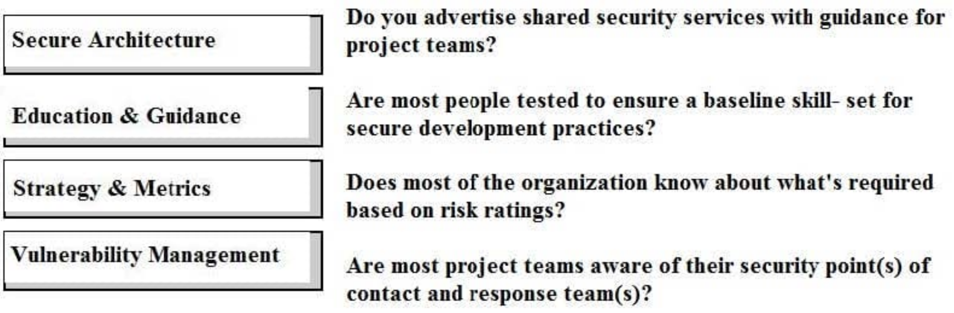
Do you advertise shared security services with guidance for project teams?

Are most people tested to ensure a baseline skill- set for secure development practices?

Does most of the organization know about what's required based on risk ratings?

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)?

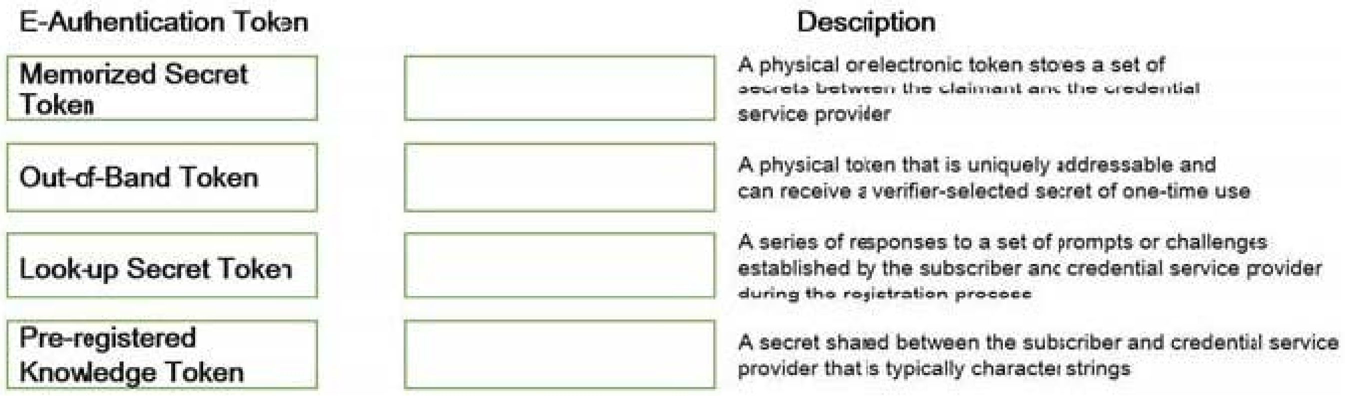
QUESTION 10

DRAG DROP

Match the types of e-authentication tokens to their description.

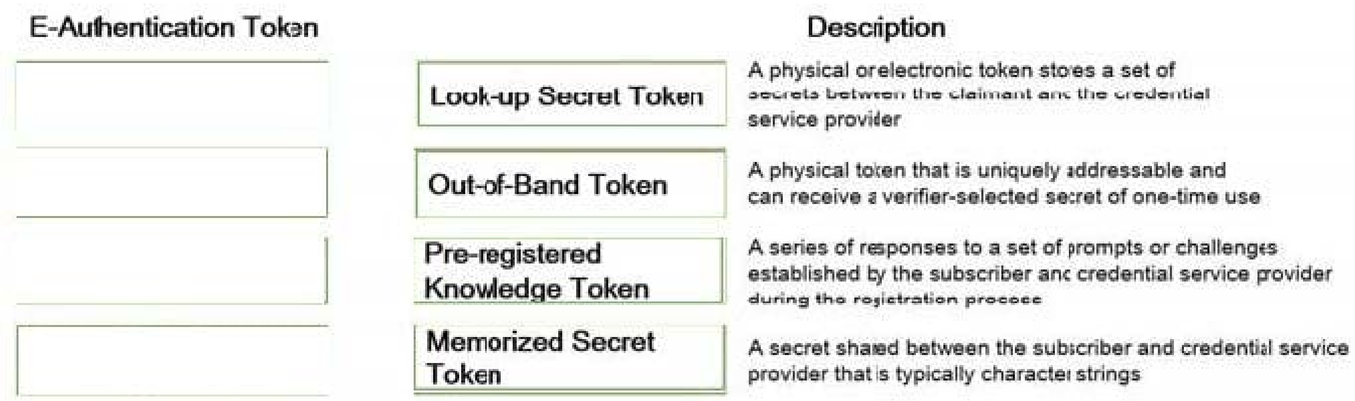
Drag each e-authentication token on the left to its corresponding description on the right.

Select and Place:



E-Authentication Token		Description
Memorized Secret Token		A physical orelectronic 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
Look-up Secret Token		A series of responses to a set of prompts or challenges established by the subscriber and credential service provider during the registration process
Pre-registered Knowledge Token		A secret shared between the subscriber and credential service provider that is typically character strings

Correct Answer:



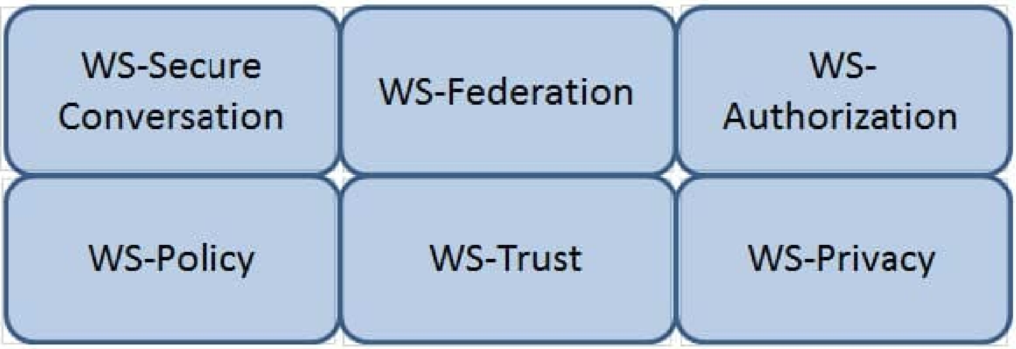
E-Authentication Token		Description
	Look-up Secret Token	A physical orelectronic token stores a set of secrets between the claimant and the credential service provider
	Out-of-Band Token	A physical token that is uniquely addressable and can receive a verifier-selected secret of one-time use
	Pre-registered 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 11

HOTSPOT

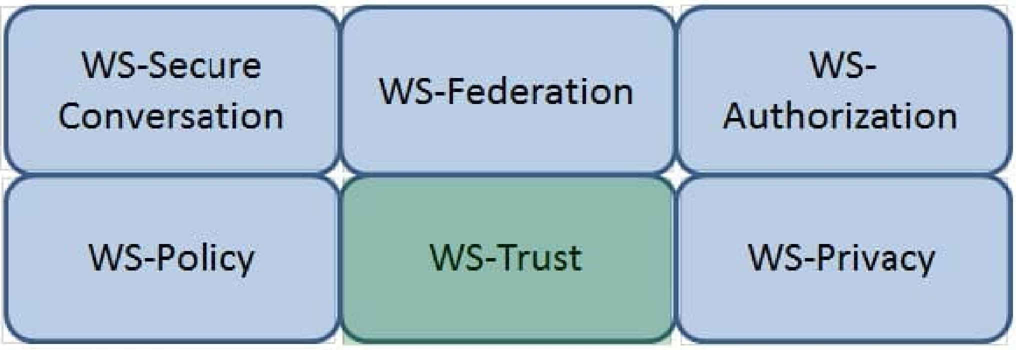
Which Web Services Security (WS-Security) specification negotiates how security tokens will be issued, renewed and validated? Click on the correct specification in the image below.

Hot Area:



WS-Secure Conversation	WS-Federation	WS-Authorization
WS-Policy	WS-Trust	WS-Privacy

Correct Answer:



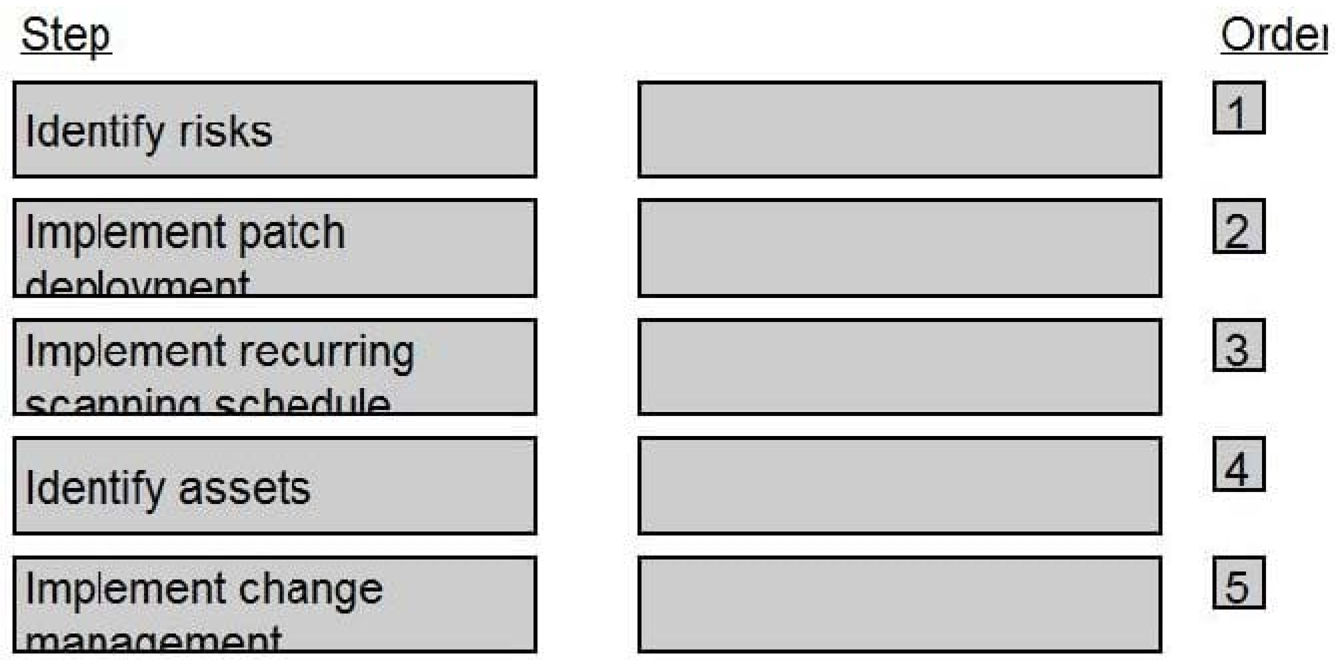
WS-Secure Conversation	WS-Federation	WS-Authorization
WS-Policy	WS-Trust	WS-Privacy

QUESTION 12

DRAG DROP

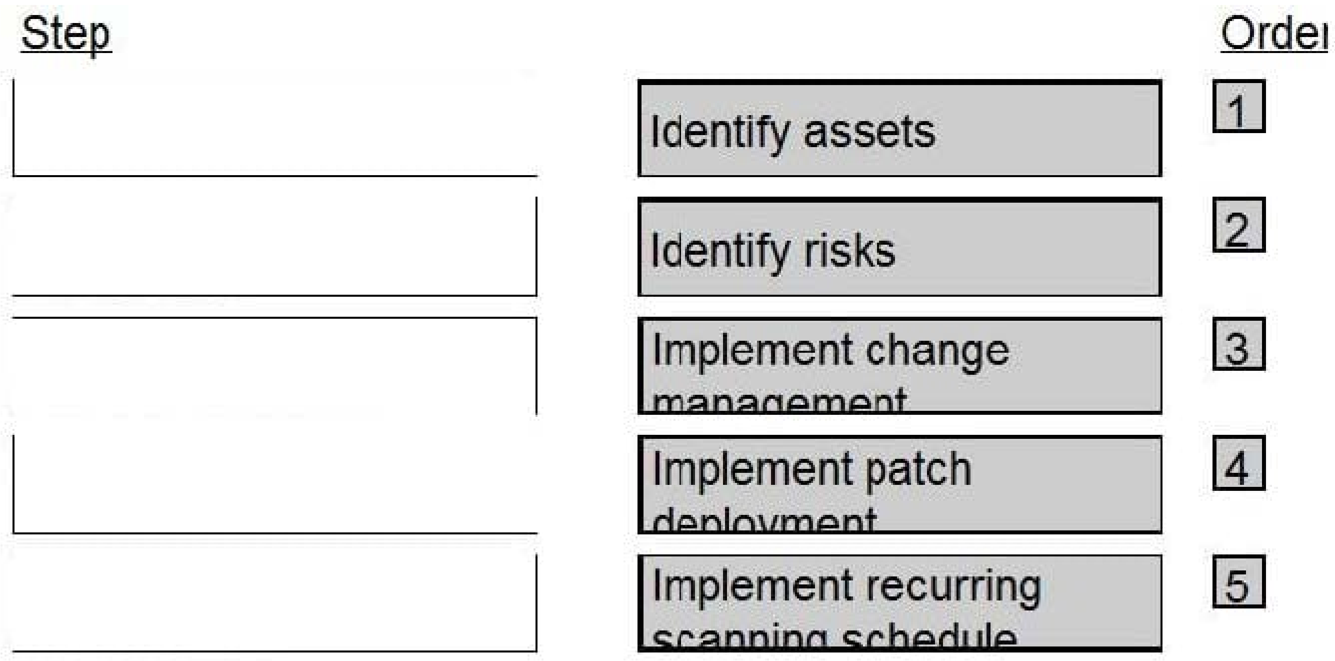
Order the below steps to create an effective vulnerability management process.

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

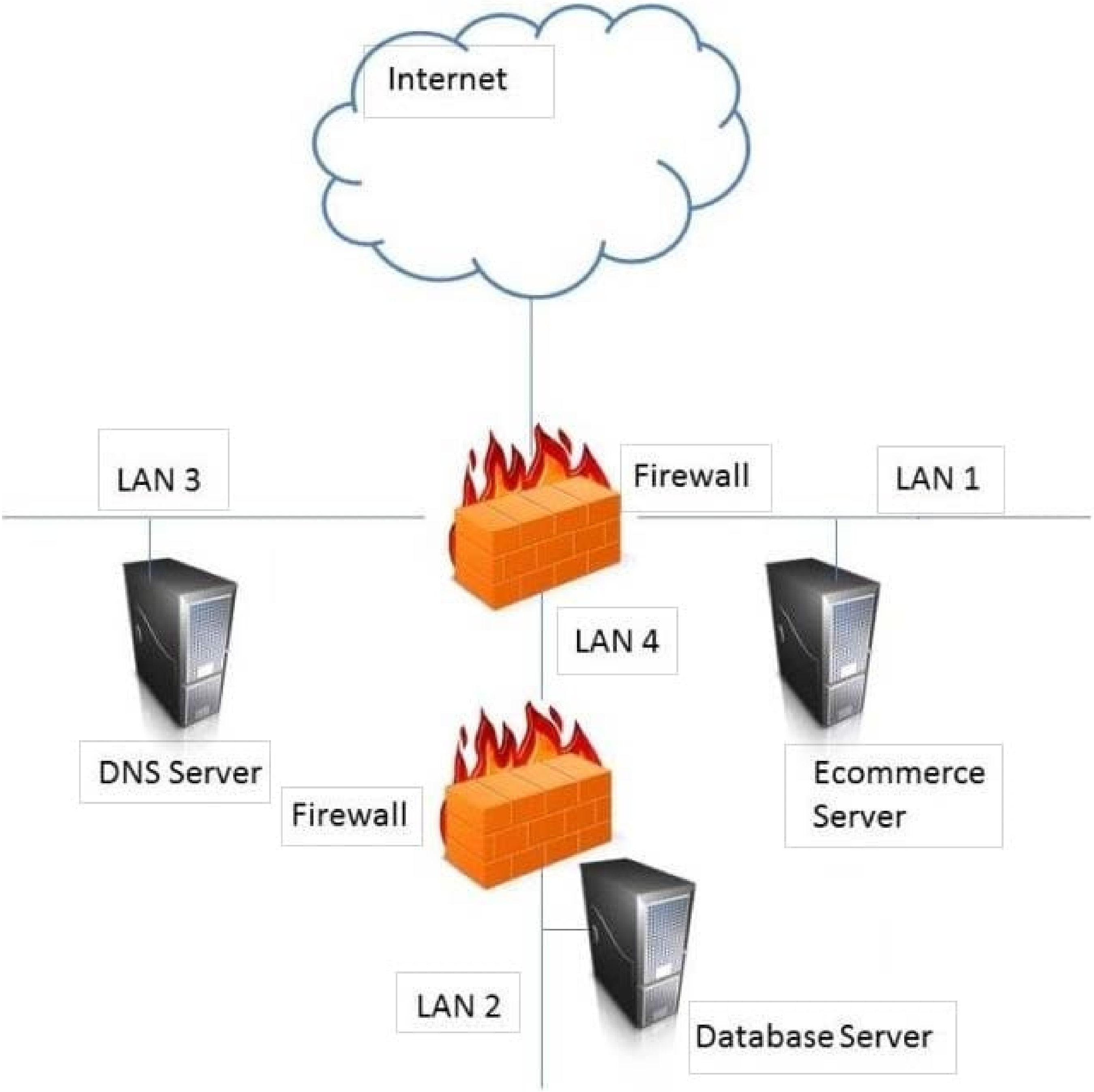
QUESTION 13

HOTSPOT

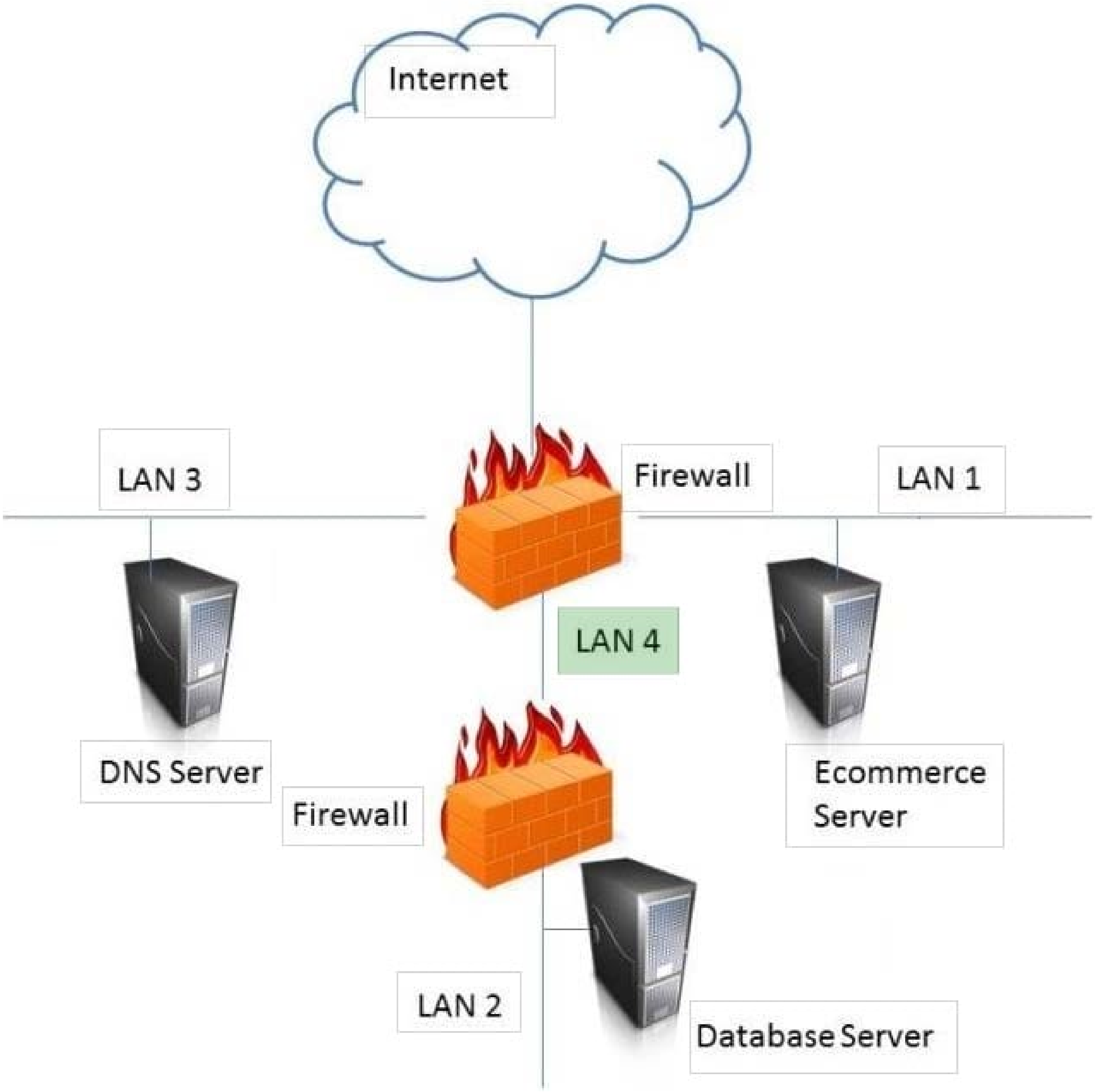
In the network design below, where is the MOST secure Local Area Network (LAN) segment to deploy a Wireless

Access Point (WAP) that provides contractors access to the Internet and authorized enterprise services?

Hot Area:



Correct Answer:



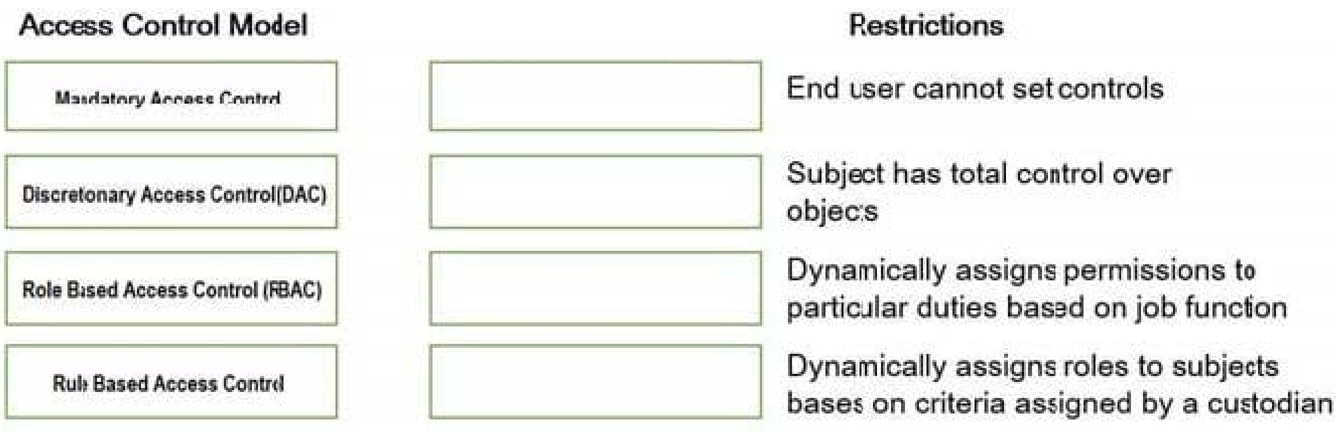
QUESTION 14

DRAG DROP

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

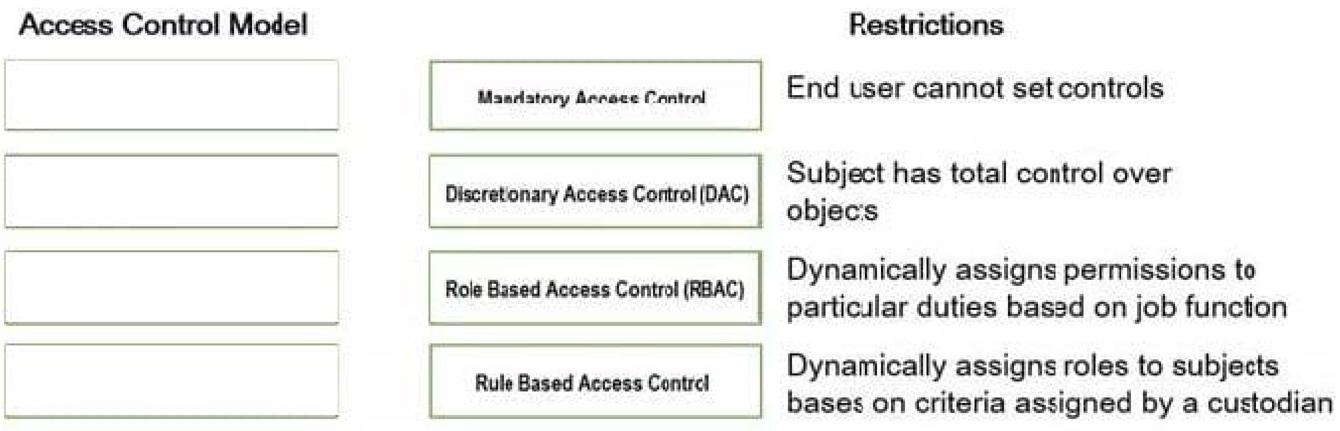
Drag each access control model to its appropriate restriction access on the right.

Select and Place:



Access Control Model		Restrictions
Mandatory Access Control		End user cannot set controls
Discretonary 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:



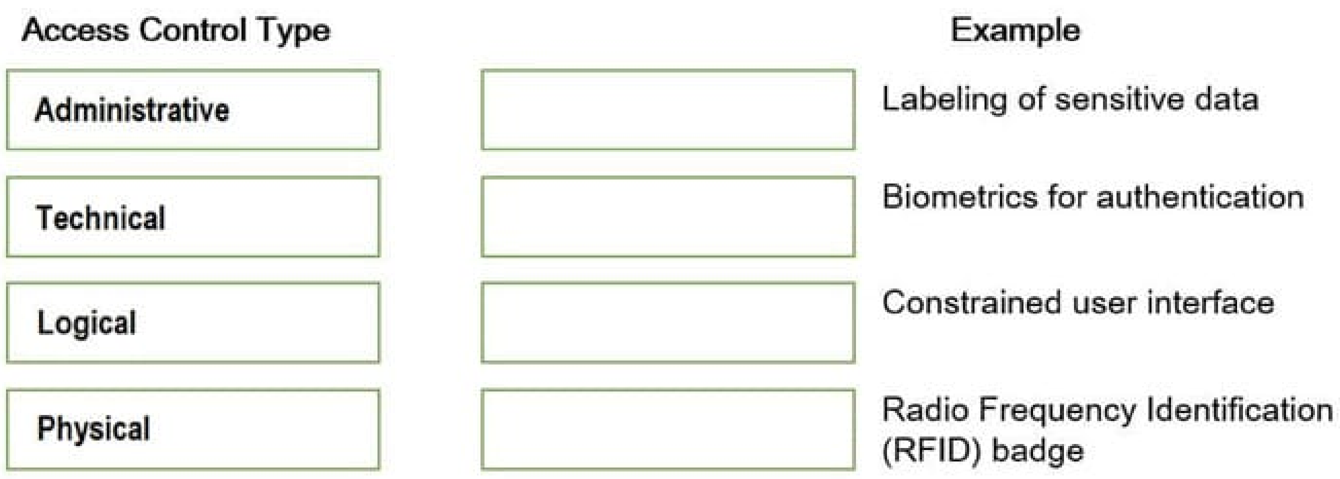
Access Control Model		Restrictions
	Mandatory Access Control	End user cannot set controls
	Discretonary Access Control (DAC)	Subject has total control over objects
	Role Based Access Control (RBAC)	Dynamically assigns permissions to particular duties based on job function
	Rule Based Access Control	Dynamically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

QUESTION 15

DRAG DROP

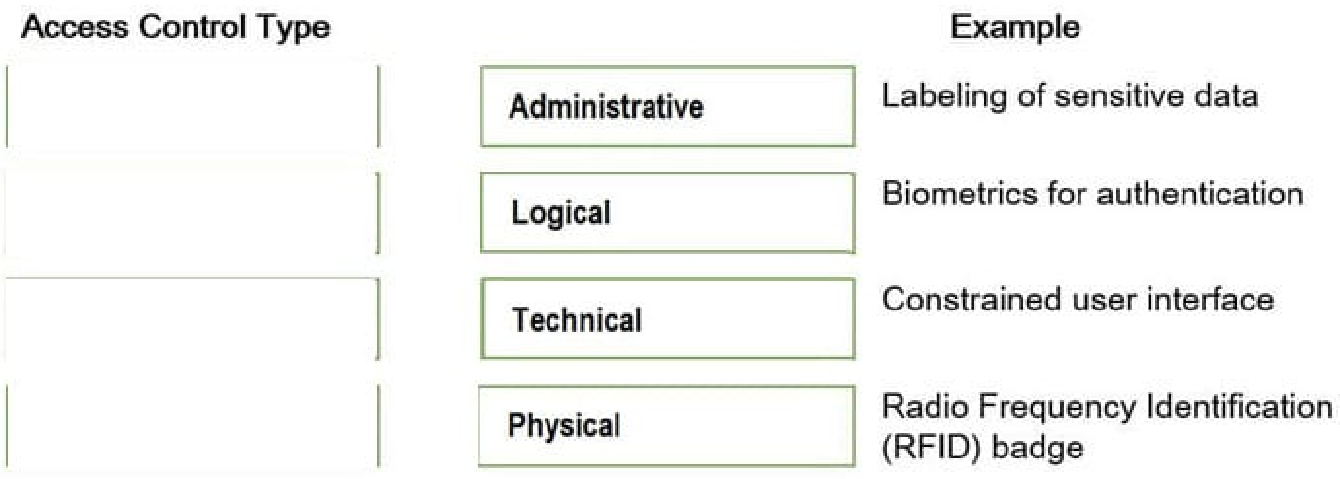
Match the access control type to the example of the control type. Drag each access control type net to its corresponding example.

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

Latest CISSP-2018 Dumps CISSP-2018 Study Guide CISSP-2018 Exam Questions