

Which of the following is NOT a COBIT principle.

Question 3
Not yet answered
Marked out of 1.00
Flag question

Which of the following is NOT a COBIT principle.

Select one:

- ☐ a. Enabling a Holistic Approach
- ☒ b. Compliance Verification
- ☐ c. Meeting Stakeholder Needs
- ☐ d. Applying a Single Integrated Framework

is an action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by A(n) eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that correct action

A(n) _____ is an action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that correct action can be taken.

Select one:

- ☐ Adversary
- ☐ Asset
- ☒ Countermeasure
- ☐ Protocol
- ☐ Attack

What are true about active information gathering? (Select two)

What are true about active information gathering? (Select two)

Select one or more:

- ☐ Google hacking can be used for active information gathering. ~~x~~ P
- ☐ Collecting information about targets using publicly available information. P
- ☒ Port Scanning and OS fingerprinting can be used for active information gathering. A ✓
- ☒ When you have enough information about your targets, you can gather more information about these targets by interacting with them. A ✓

Next page

Bob intercepts an encrypted message and wants to determine what type of algorithm was used to create the message. He first performs a frequency analysis and notes that the frequency of letters in the message closely matches the distribution of letters in the English language. What type of cipher was most likely used to create this message?

Bob intercepts an encrypted message and wants to determine what type of algorithm was used to create the message. He first performs a frequency analysis and notes that the frequency of letters in the message closely matches the distribution of letters in the English language. What type of cipher was most likely used to create this message?

Select one:

- ☐ AES
- ☐ Transposition cipher
- ☐ 3DES
- ☒ Substitution cipher ✓

Match the correct description to the correct management activity

Match the correct description to the correct risk management activity.

Prioritizing threat risk scenarios based on perceived risk ratings. RA

Includes steps such as finding out critical assets and surveying security requirements. RM

Probability and impact is used to calculate the corresponding levels of risk for each threat. RA

Choose...

Choose...
Risk Identification
Risk Evaluation
Risk Analysis
Risk Mitigation
Risk Elimination

Next page

Which of the following feature is NOT standard in a Unified Threat Management (UTM) solution

Which of the following features is NOT standard in a Unified Threat Management (UTM) solution?

Select one:

- ☒ a. Spam Protection ✓
- ☒ b. Firewall ✓
- ☒ c. Content Filtering ✓
- ☒ d. Anti-virus ✓
- ☒ e. Threat Intelligence & Correlation

Which of the following organization is likely to be legally obligated to have business continuity plans

Which of the following organization is likely to be legally obligated to have business continuity plans?

Select one:

- ☐ a. Software Developing Company
- ☐ b. Online Pizza Delivery System
- ☒ c. Micro Finance Organization
- ☐ d. Online Book Store

A preliminary study has identified that a SMB protocol vulnerability in Patient billing system

A preliminary study has identified that a SMB protocol vulnerability in Patient billing system could be exploited by a remote attacker to view critical patient information in the records. John is creating an OCTAVE threat profile for the above scenario. He has identified that the Access should be categorized as Choose..., Actor is an Choose..., motive is Choose... and the outcome is Choose....

(2 Marks)

Choose...

- Choose...
- Physical
- Accidental
- Disclosure
- Outsider
- Fabrication
- Insider
- Modification
- Deliberate
- Network

Next page

Implementing proper accountability measures in an information system supports to achieve; (Select two)

Implementing proper accountability measures in an information system supports to achieve; (Select two)

Select one or more:

- ☒ Deterrence
- ☐ Integrity
- ☐ Confidentiality
- ☐ Authenticity
- ☒ Non-repudiation

Select the correct statement regarding Disaster Recovery & Business Continuity.

Select the correct statement regarding Disaster Recovery & Business Continuity.

Select one:

- ☐ a. None of the given answers are correct
- ☒ b. Disaster Recovery focuses on how to rebuild your processes after a disaster & Business Continuity focuses on maintaining core processes during a disaster
- ☐ c. Business Continuity focuses on how to rebuild your processes after a disaster & Disaster Recovery focuses on maintaining core processes during a disaster
- ☐ d. Business Continuity & Disaster Recovery both focus on how to rebuild your processes after a disaster
- ☐ e. Business Continuity & Disaster Recovery both focus on maintaining core processes during a disaster

Disaster Recovery testing is done in a scheduled periodical manner. so that everyone involved has time to DRP activities.

Disaster Recovery testing is done in a scheduled periodical manner, so that everyone involved has time to pre
DRP activities.

Select one:

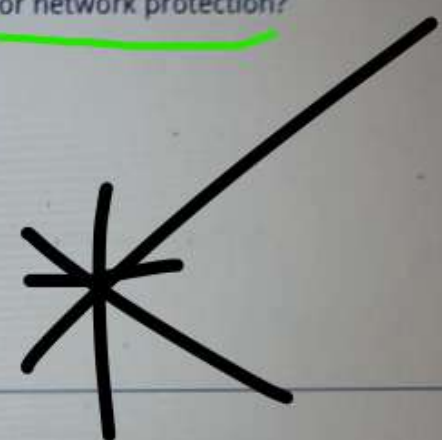
- ☒ True
- ☐ False

Which of me following is NOT a best practice when configuring a firewall for network protection?

Which of the following is NOT a best practice when configuring a firewall for network protection?

Select one:

- ☐ a. Configure all 'deny' statements first
- ☐ b. Configure the 'clean-up' rule
- ☐ c. Configure the rules for return traffic as well
- ☒ d. Configure the 'stealth-mode' rule
- ☐ e. Configure rules in the correct sequence



A _____ represents a potential harm to the system resource.

A _____ represents a potential harm to the system resource.

Select one:

- ☐ phish
- ☒ threat
- ☐ spoof
- ☐ vulnerability

Which of the following is the incorrect statement regarding Digital Signatures?

Which of the following is the incorrect statement regarding Digital Signatures? a

Select one:

- ☒ a. Digital Signatures provide Message Authentication, But does not provide Message Integrity X
- ☐ b. Digital Signatures are based on asymmetric cryptographic algorithms ✓
- ☐ c. Digital Signatures provide Message Authentication.
- ☐ d. Digital Signatures provide both Message Authentication & Integrity
- ☐ e. Digital Signatures provide Message Integrity. ✓

Which of the following is an accurate statement regarding Kerckoffs Principle?

Which of the following is an accurate statement regarding Kerckoff's Principle?

Select one:

- ☒ a. A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the secret key.
- ☐ b. A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of both encryption and decryption algorithms.
- ☐ c. A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the encryption algorithm.
- ☐ d. A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the decryption algorithm.
- ☐ e. None of the above.

All ancient ciphers are based on asymmetry cryptography,

All ancient ciphers are based on asymmetric cryptography.

Select one:

- ☐ True
- ☒ False

Which of the following is NOT an accurate statement about OCTAVE-S?

Which of the following is NOT an accurate statement about OCTAVE-S?

Select one:

- ☐ a. Focuses on critical assets for the organization ✓
- ☐ b. It is a highly flexible risk management framework ✓
- ☒ c. Framework does not need extensive preparation X
- ☐ d. It can be cost be cost effective as it is self-led ✓

Match the given attacks ____ Security service which will be affected by the given scenario

Match the given attacks to the correct security service which will be affected by the given scenario.

A Denial of Service attack has temporarily stopped a web server from receiving client requests.

An internal company report accidentally leaked by an employee through a USB device.

An attacker has deleted the 'syslog' files in a router after completing an attack.

Using an SQL injection command attacker has added a value to an empty cell in a database.

Choose...

- Choose...
- Integrity
- Accountability
- Confidentiality
- Authentication
- Availability

Next page

Recognition by hand writing, voice, typing pattern are examples of

Recognition by hand writing, voice, typing pattern are examples of ____.

Select one:

- ☐ Static biometrics
- ☐ Face recognition
- ☐ Dynamic biometrics
- ☒ Token authentication

Which statement describes the use of keys for encryption?

Which statement describes the use of keys for encryption?

Select one:

- ☒ The sender and receiver must use the same key when using symmetric encryption.
- ☐ The sender and receiver must use the same key when using asymmetric encryption.
- ☐ The sender and receiver must use the same keys for both symmetric and asymmetric encryption.
- ☐ The sender and receiver must use two keys: one for symmetric encryption and another for asymmetric encryption.

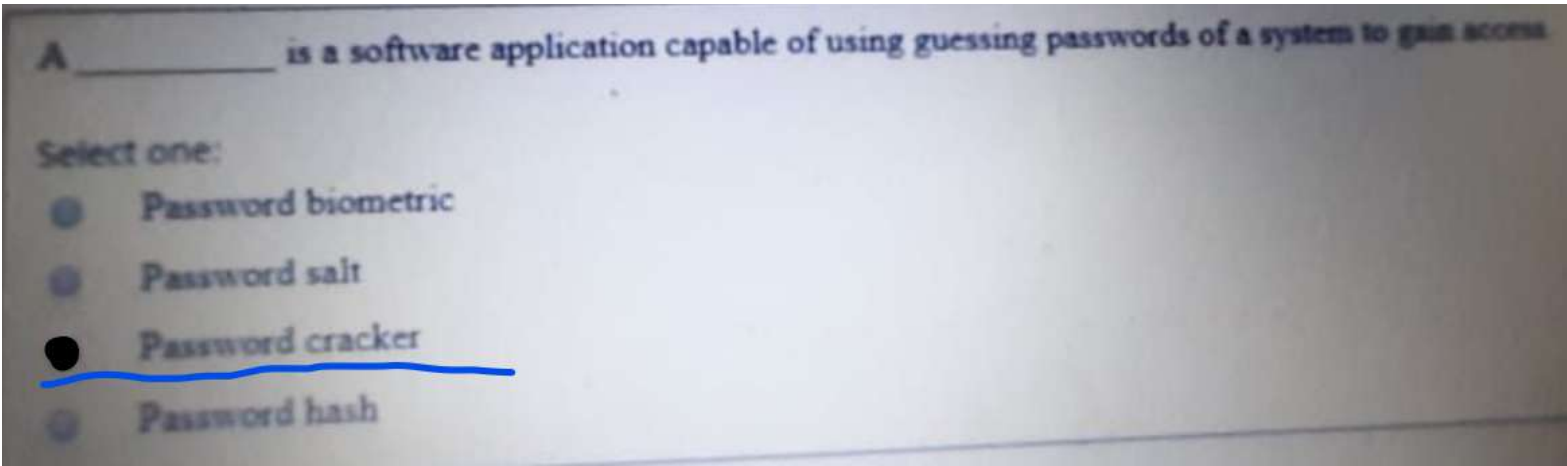
____ assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

____ assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

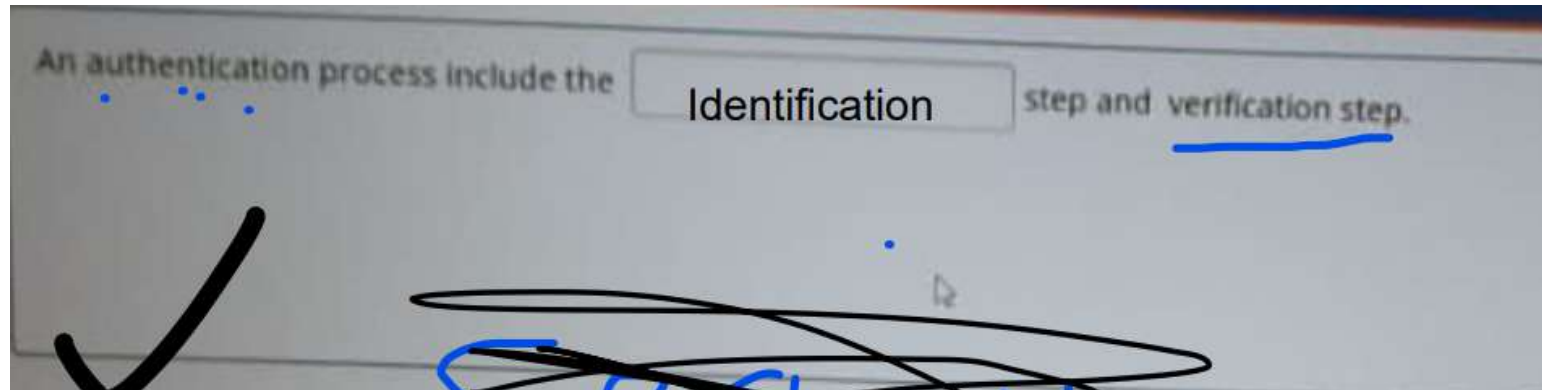
Select one:

- ☐ System integrity
- ☐ Data integrity
- ☐ Authenticity
- ☒ Privacy
- ☐ Availability

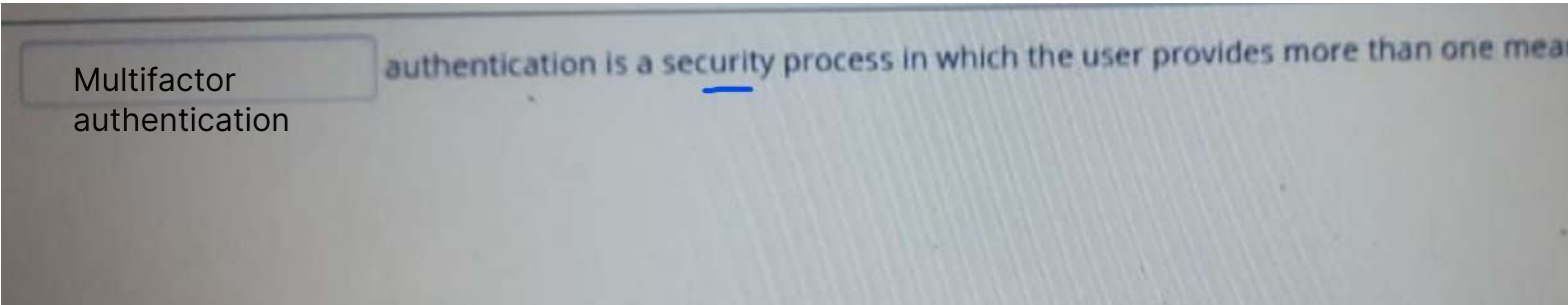
A ____ is a software application capable of using guessing passwords of a system to gain access



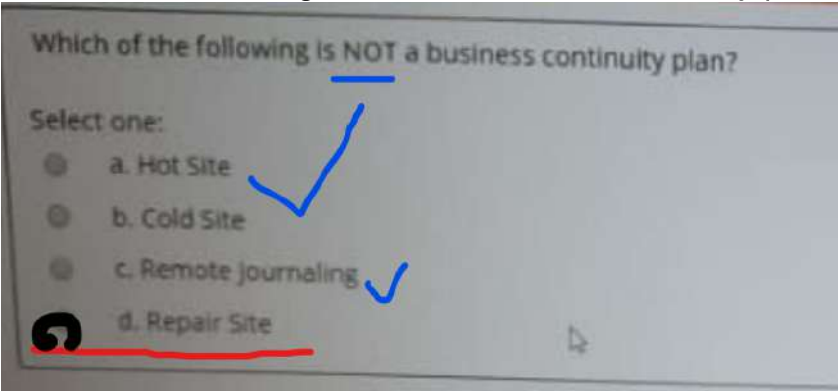
An authentication process include the ____ step and verification step.



authentication is a security process in which the user provides more than one means of Identification.



Which of the following Is NOT a business continuity plan'



Match correct definition with the appropriate disaster Recovery Plan (DRP).

Match correct definition with the appropriate Disaster Recovery Plan (DRP).

Two organizations with similar system configuration agreeing to serve as backup site to each other.

Online transmission of data to backup systems periodically (every few hours) Minimizes loss of data and reduces recovery time.

A site equipped with identical facilities to the original site with system mirroring capability. Data is replicated & backed up immediately. Transparent Recovery.

A site with hardware, software & network installed and compatible to original site.

An empty facility located offsite with required infrastructure ready for installation in the event of a disaster.

Choose...

Choose...

Choose...

New Site

Cold Site

Mutual Backup

Self Backup

Remote Journaling

Hot Site

Mirrored Site

Select the incorrect statement about access control systems.

Select the incorrect statement about access control systems.

Select one:

- ☐ Subjects, objects and access rights are the basic elements of access control systems
- ☒ Access control systems do not depend on inputs coming from other systems such as authentication systems
- ☐ Use to prevent legitimate users from accessing unauthorized resources
- ☐ Implemented based on access control policies such as DAC, MAC and RBAC

_____ and _____ are not administrative controls used in information security. (select two)

_____ and _____ are not administrative controls used in information security. (select two)

Select one or more:

- ☒ Access control list (ACL) ✓
- ☐ Disaster recovery plan
- ☐ Employ hiring procedures
- ☐ Policy
- ☒ Security guards ✓
- ☐ Training and awareness

Complete the description given below

Sri Lanka Institute of Information Technology

Complete the description given below:

Digital certificates are a crucial element in Public Key Infrastructure.

- Purpose of a digital certificate is to validate a users' Public key to a third party.
- In order to do this, a trusted third party known as CA generates a digital certificate with a signature using CA's private key.
- During a digital certificate verification, a user needs to use the public key of the CA.
- However sometimes CAs make certain certificates invalid using a certificate revocation list (CRL).

is an attempt to learn or make use of information from the system that does not affect system resources.

A(n) _____ is an attempt to learn or make use of information from the system that does not affect system resources.

Select one:

- ☐ Denial-of-Service Attack
- ☐ Outside attack
- ☐ Active attack
- ☒ Passive attack
- ☐ Inside attack

A vulnerability cannot exist without a matching threat.

A vulnerability cannot exist without a matching threat.

Select one:

☐ True

☒ False

In Symmetric cryptography sender and the receiver use **the same key** for both encryption and decryption. Therefore, the biggest problem in the setup of symmetric cryptography is **Key Distribution**.

match the appropriate definition to Risk Management steps.

Match the appropriate definition to Risk Management steps.

Risk Management Step	Definition
Risk Analysis	Choose...
Risk Evaluation	Choose...
Risk Control	Choose...

Definitions:

- Action, procedure, device or technique used for protection
- Monitor the effectiveness of risk responses
- Prioritizing the risk levels of calculated risk scenarios
- Identifying the most critical assets of an organization
- Estimation (Calculation) of the risk level of a scenario

Which statement below most accurately reflects the goal of risk mitigation?

Which statement below most accurately reflects the goal of risk mitigation?

Select one:

- ☐ Quantify the impact of potential risks
- ☐ Analyzing and removing all vulnerabilities and threats to security within the organization.
- ☒ Defining the acceptable level of risk the organization can tolerate, then reduce risk to that level.
- ☐ Defining the acceptable level of risk the organization can tolerate, and assigning any costs associated with loss or disruption to a third party such as an insurance carrier.

The shift cipher involves replacing each letter of the alphabet with the letter standing 'n' places further down the alphabet. Complete the equations for the shift cipher.

Open Lanka Institute of Information Technology

The shift cipher involves replacing each letter of the alphabet with the letter standing 'n' places further down the alphabet. Complete the equations for the shift cipher.

Parameters:

- x : plain-text = 21
- y : cipher-text = ?
- k : key = 7

Encryption Equation

$21 = 21 + 7 \text{ mod } 26$

Decryption Equation

$21 = 21 - 7 \text{ mod } 26$

A _____ strategy is one in which the system time to time runs its own password brute force tools to find weak passwords.

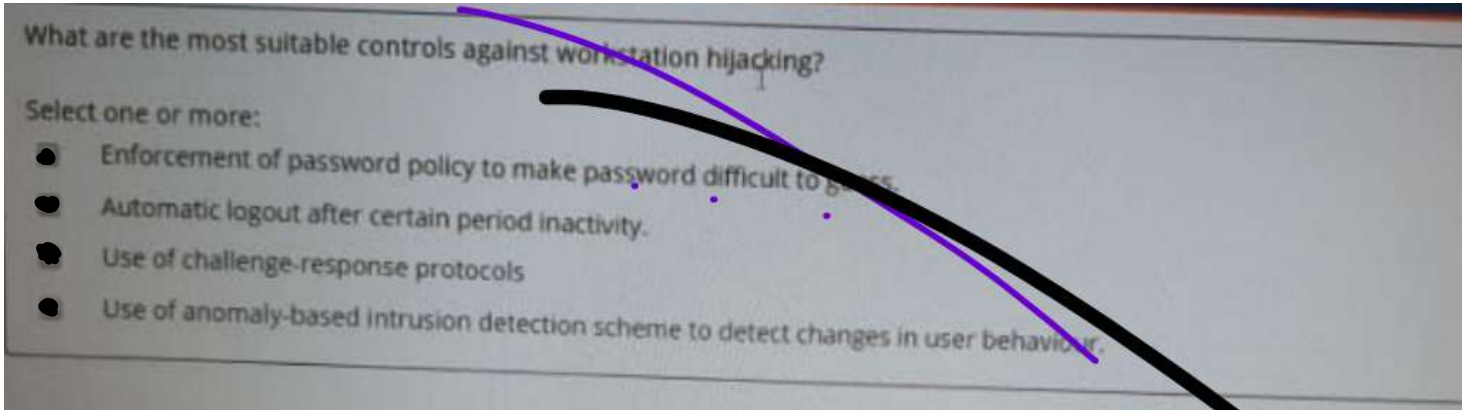
A _____ strategy is one in which the system time to time runs its own password brute force tools to find weak passwords.

Select one:

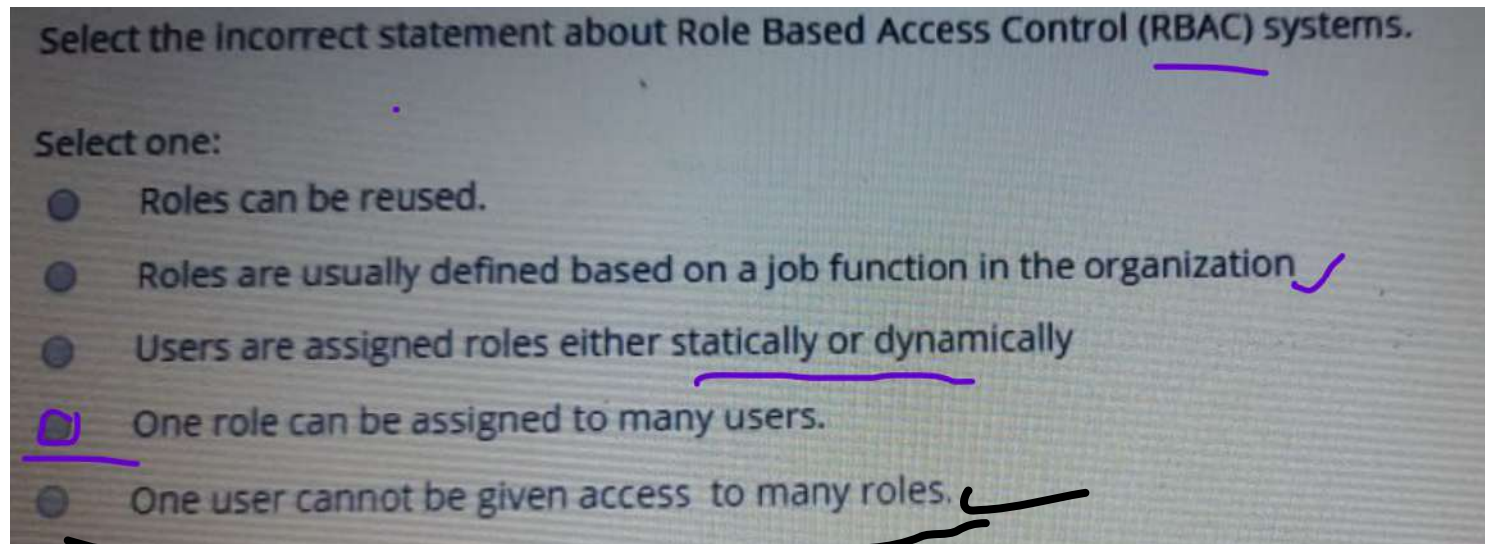
- ☐ Proactive password checking
- ☒ Computer-generated password
- ☐ User education

What are the most suitable controls against workstation hijacking

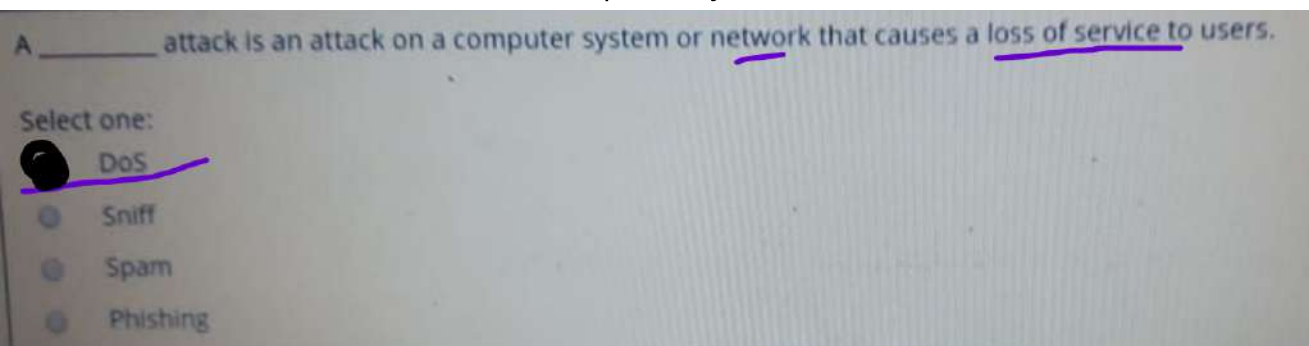
Select one or more:



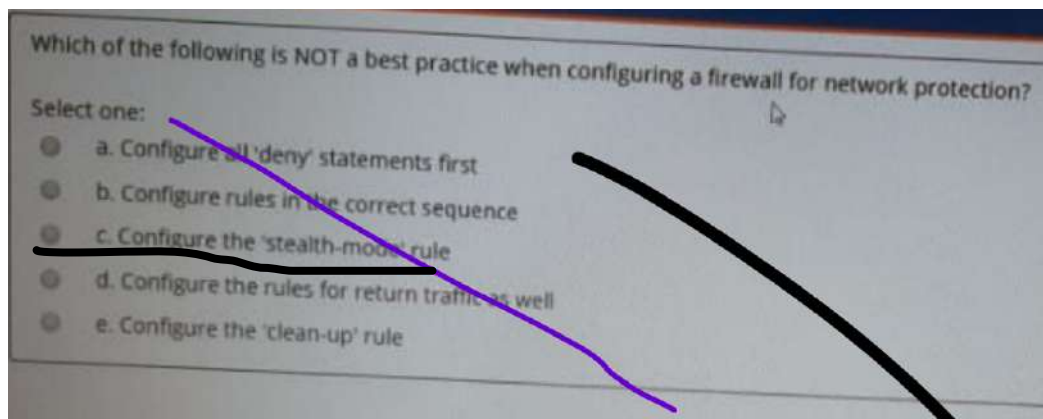
Select the incorrect statement about Role Based Access Control (RBAC) systems.



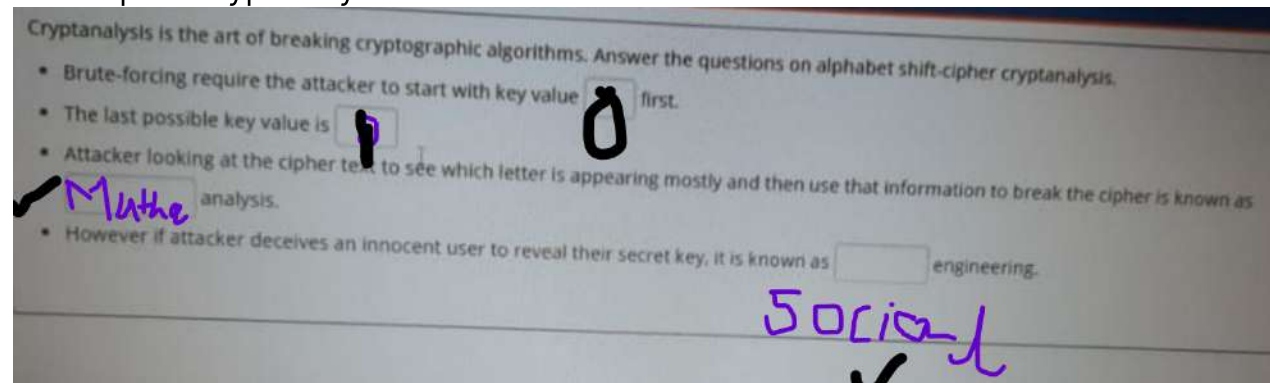
A _____ attack is an attack on a computer system or network that causes a loss of service to users.



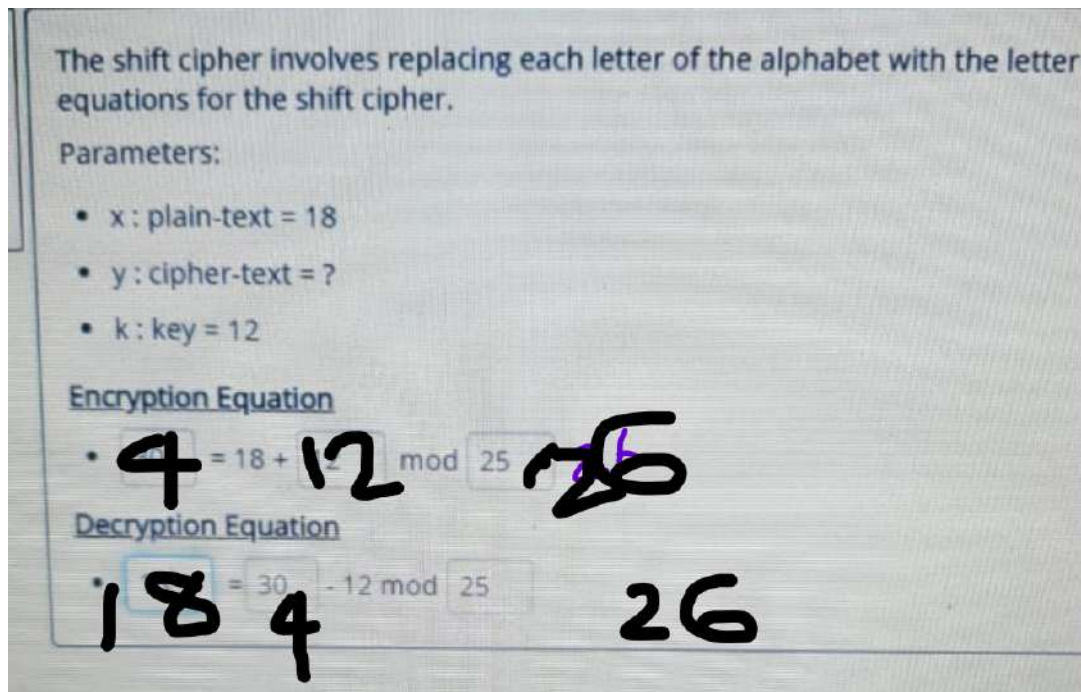
Which of the following is NOT a best practice when configuring a firewall for network protection?



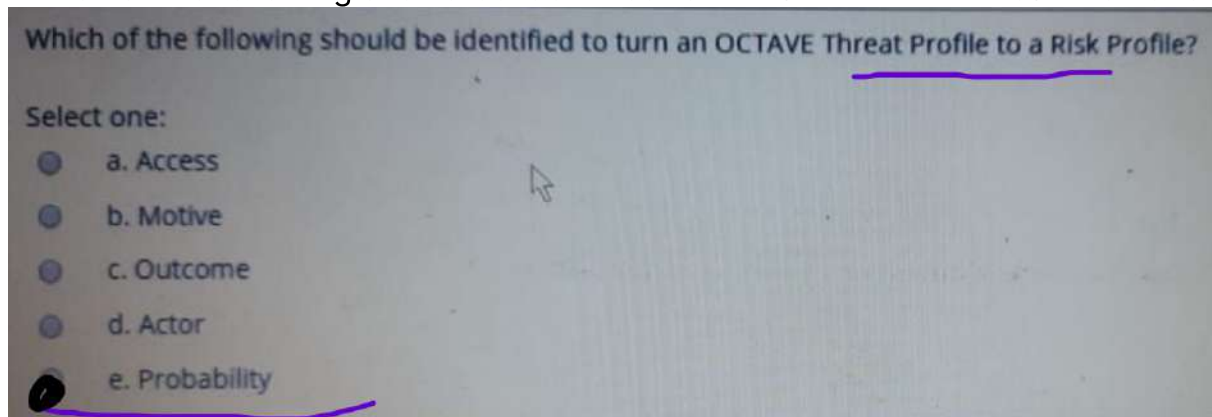
Cryptanalysis is the art of breaking cryptographic algorithm Answer the questions on alphabet shift-cipher cryptanalysis



The shift cipher involves replacing each letter of the alphabet equations for the shift cipher.



Which of the following should be identified to turn an OCTAVE Threat Profile to a Risk Profile?



Which of the following organization is likely to be legally obligated to have business continuity plans?

Which of the following organization is likely to be legally obligated to have business continuity plans?

Select one:

- ☐ a. Online Book Store
- ☐ b. Software Developing Company
- ☒ c. Micro Finance Organization
- ☐ d. Online Pizza Delivery System

Which of the following is NOT a business continuity plan?

Which of the following is NOT a business continuity plan?

Select one:

- ☐ a. Remote Journaling
- ☐ b. Cold Site
- ☐ c. Hot Site
- ☒ d. Repair Site

The shift cipher involves replacing each letter of the alphabet with the letter standing 'n' places further down the alphabet. Complete the equations for the shift cipher.

The shift cipher involves replacing each letter of the alphabet with the letter standing 'n' places further down the alphabet. Complete the equations for the shift cipher.

Parameters:

- x : plain-text = 3
- y : cipher-text = ?
- k : key = 20

Encryption Equation

$23 = 3 + 20 \text{ mod } 26$

Decryption Equation

$3 = 23 - 20 \text{ mod } 26$

Parameters:

- x : plain-text = 6
- y : cipher-text = ?
- k : key = 18

Encryption Equation

$24 = 6 + 18 \text{ mod } 26$

Decryption Equation

$6 = 24 - 18 \text{ mod } 26$

Complete the description given below:

Complete the description given below:

Asymmetric cryptographic algorithms are built based on mathematical problems.

- RSA is a public key algorithm that is built using the integer factorization problem.
- Integer factorization problem is based on finding the prime factors of a given composite number.
- Apart from integer factorization problem, elliptic curve problem is also used to build public key algorithms.

Complete the description given below:

Complete the description given below:

Claude Shannon's confusion principle refers to an encryption operation where the relationship between key and ciphertext is obscured. diffusion principle refers to an encryption operation when one plain-text bit change the entire cipher-text change.

- Data Encryption Standard has an effective key size of 56 bits
- Advanced Encryption Standard has 3 versions depending on the key length

$V1 - 2^{128}$
 $V2 - 2^{192}$
 $V3 - 2^{256}$

What is true about corrective controls?

What is true about corrective controls?

Select one:

- ☒ Designed to find errors or irregularities after they have occurred
- ☐ Designed to discourage errors or irregularities from occurring
- ☐ Intended to discourage potential attackers and send the message that it is better not to attack
- ☐ Updating firewall rules to block an attacking IP address is a corrective control

Which of the following is NOT a COBIT principle.

Which of the following is **NOT** a COBIT principle.

Select one:

- ☒ a. Compliance Verification
- ☐ b. Enabling a Holistic Approach
- ☐ c. Applying a Single Integrated Framework
- ☐ d. Meeting Stakeholder Needs

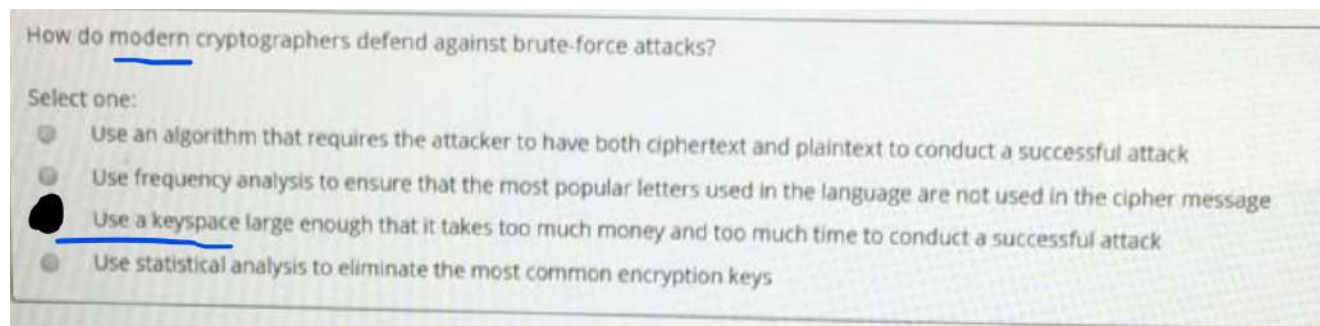
Which component is NOT part of the OCTAVE 'Threat Profile'

Which component is **NOT** part of the OCTAVE 'Threat Profile'?

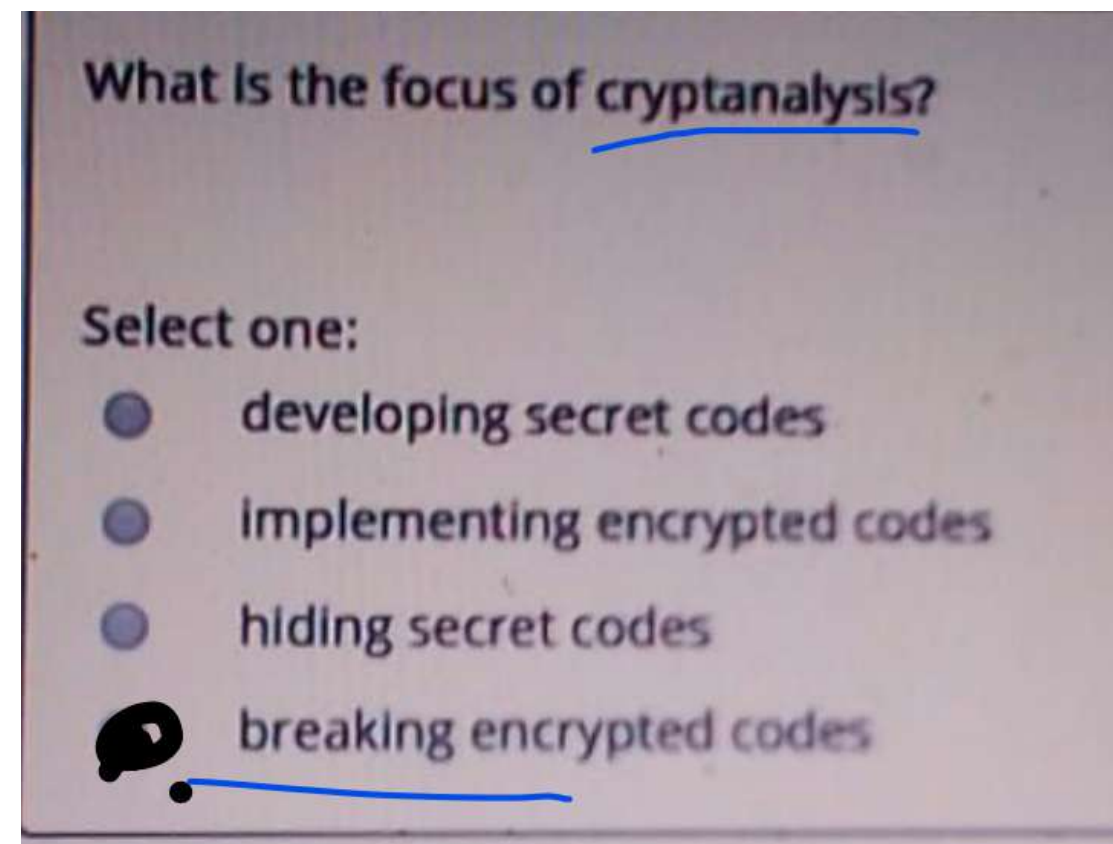
Select one:

- ☐ a. Access
- ☒ b. Control Mechanism
- ☐ c. Actor
- ☐ d. Outcome

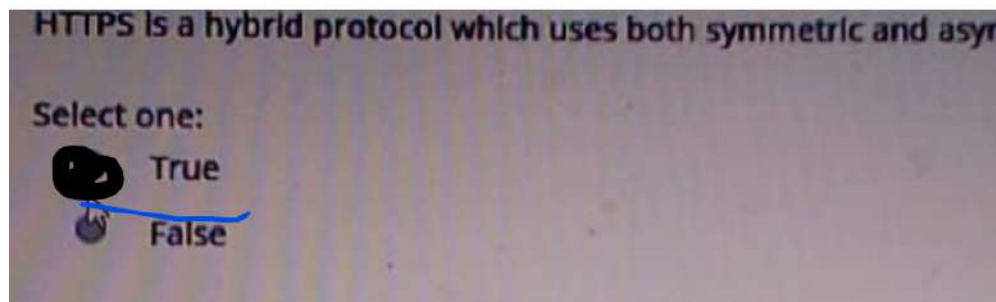
How do modern cryptographers defend against brute force attacks?



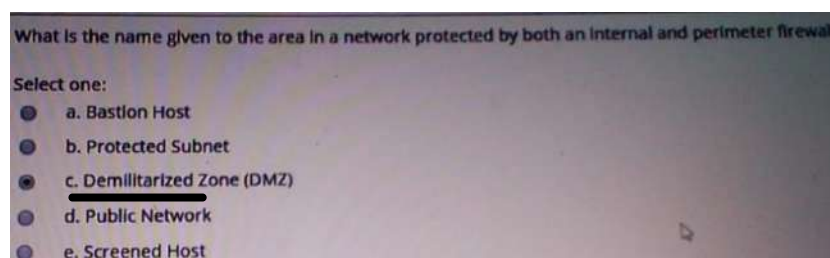
What Is the focus of cryptanalysis?



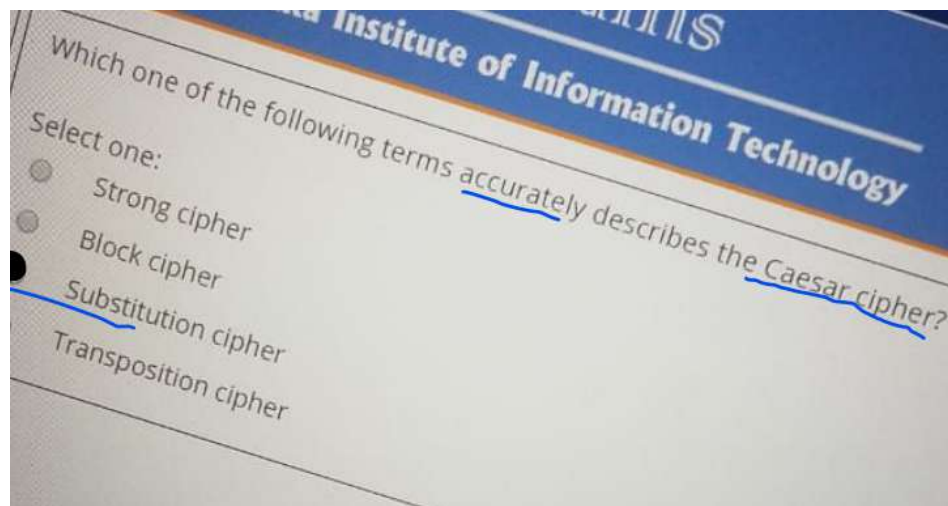
HTTPS is a



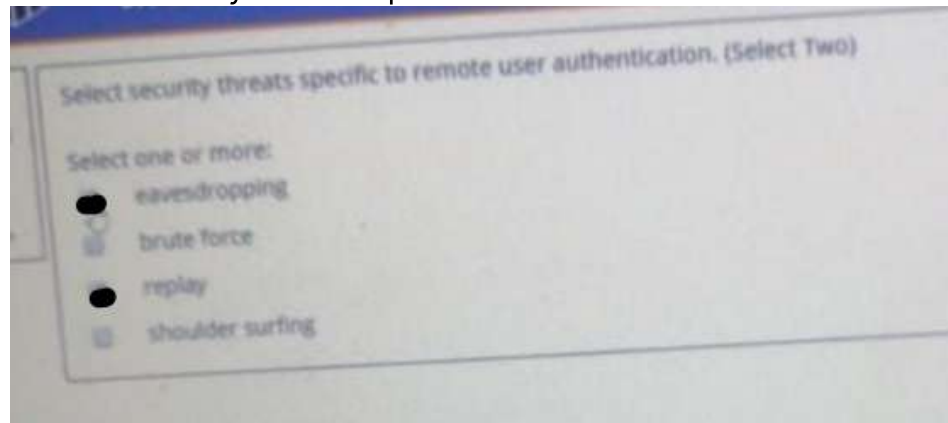
What Is the name given to the area in a network protected by both an internal and perimeter firewall?



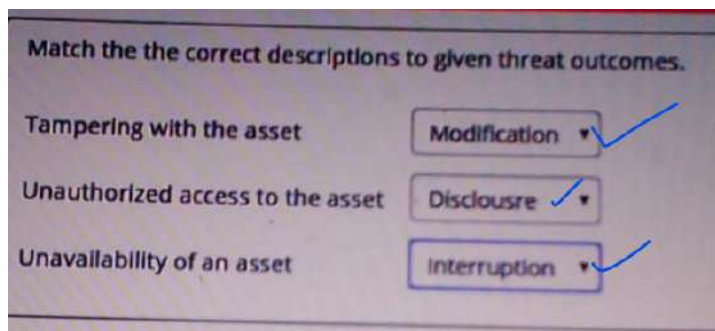
Which one of the following terms accurately describe the caesar cipher?



Select security threats specific to remote user authentication.

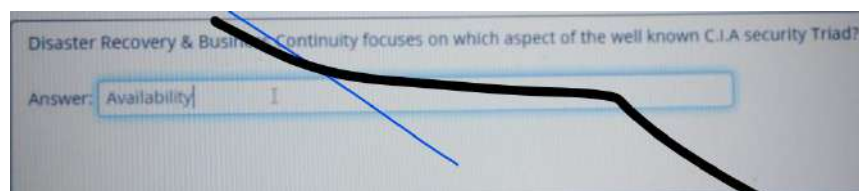


Match the the correct descriptions to given threat outcomes.

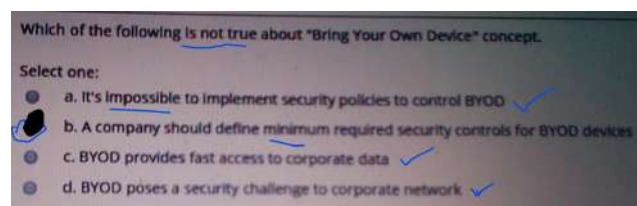


Retina, iris , fingerprint are example of **Physical** bio metrics

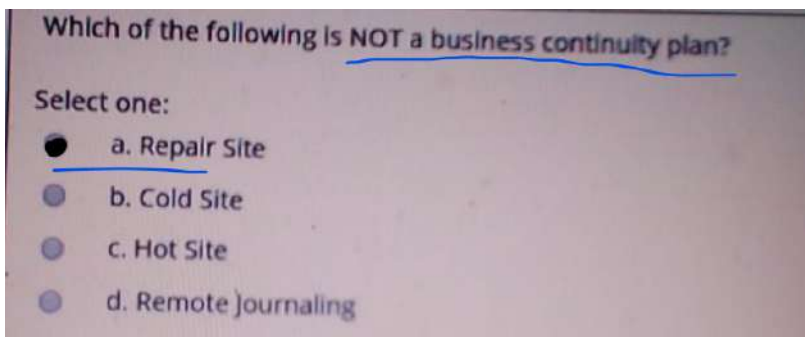
Disaster recovery &



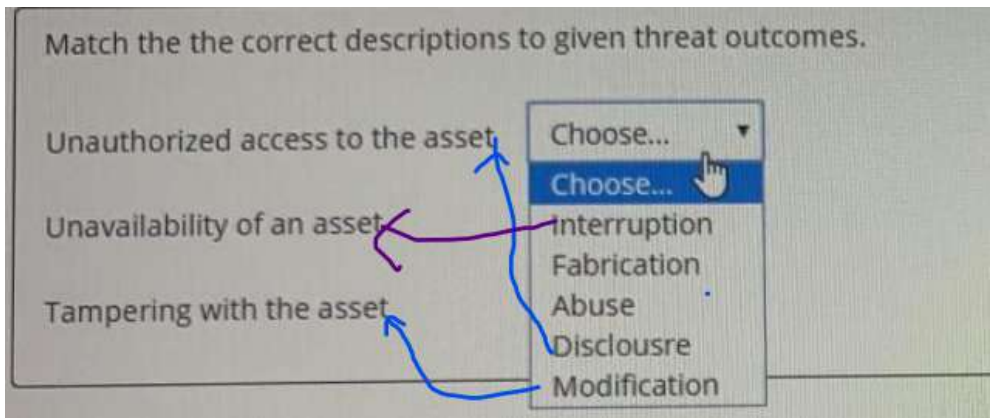
Which of the following Is not true about •Bring Your Own Device• concept.



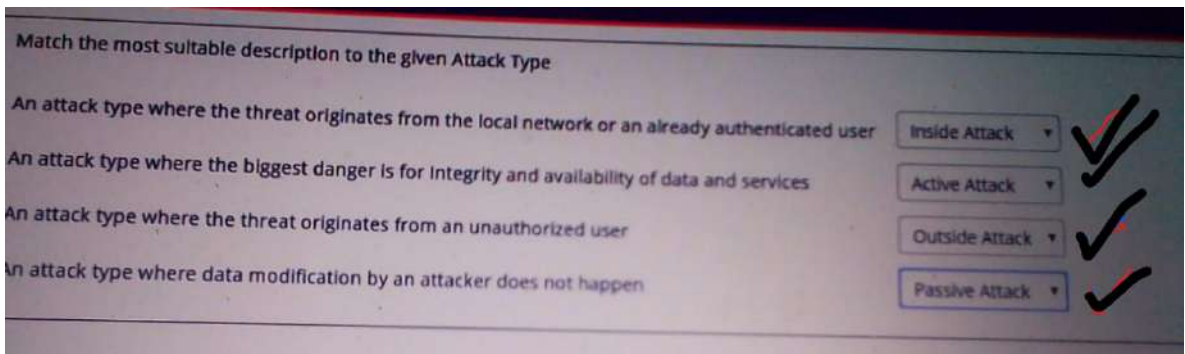
Which of the following is NOT a business continuity plan?



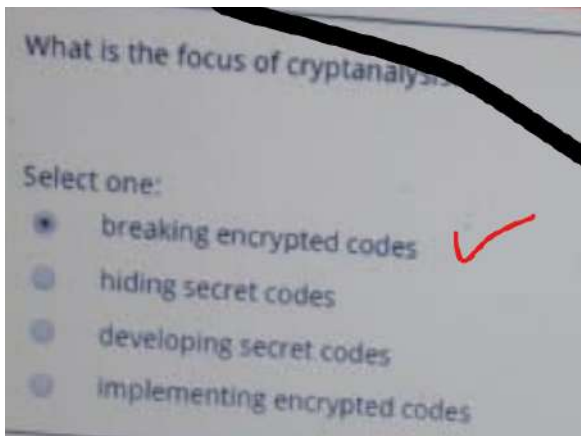
Match the the correct descriptions to given threat outcomes.



Match the most sultable description to the given Attack Type



What is the focus of cryptanalysis



Match the correct description to different phases in Business Continuity Planning (BCP).

Match the correct description to different phases in Business Continuity Planning (BCP).

BC team is identified, roles and responsibilities are assigned. Develop a suitable strategy and action plan and plan activation criteria.

Reviewing & constantly updating/improving the BCP.

Prepare disaster response & recovery procedures. Vendor contracts prepared and recovery resources are purchased. Ensure that recovery team on alert.

Periodically exercise scenarios & produce BC reports & evaluate.

Calculating Impact & Probability for scenarios. Conduct cost-benefit analysis, strategy selection & establish the budget.

Objectives of the BCP are defined and the scope is identified.

Design & Development (Plan) ✓

Maintenance ✓

Implementation (Plan) ✓

Testing ✓

Business/Risk Analysis ✓

Project Initiation

Which of the following features is NOT standard in a Unified Threat Management (UTM) solution?

Which of the following features is NOT standard in a Unified Threat Management (UTM) solution?

Select one:

☒ a. Anti-virus

☐ b. Content Filtering ✓

☐ c. Firewall ✓

☐ d. Spam Protection ✓

☐ e. Threat Intelligence & Correlation ✓

ns

What is true about corrective controls?

Which statement accurately characterizes the evolution of threats to information security?

Which statement accurately characterizes the evolution of threats to information security?

Select one:

☐ Early Internet users often engaged in activities that would harm other users.

☒ Internal threats can cause even greater damage than external threats.

☐ Internet architects planned for data security from the beginning.

☐ Threats have become less sophisticated while the technical knowledge needed by an attacker has grown.

Disaster Recovery testing is done in a scheduled periodical manner, so that everyone involved has time to

Disaster Recovery testing is done in a scheduled periodical manner, so that everyone involved has time to prepare for the DRP activities.

Select one:

☒ True

☐ False

the network administrator

The network administrator for an e-commerce website requires a service that provides a guarantee that legitimate orders are fake. What service provides this type of guarantee?

Select one:

☒ authentication

☐ confidentiality

☐ integrity

☐ nonrepudiation

What are the two main identifiable components needed to calculate 'Risk'?

What are the two main identifiable components needed to calculate 'Risk'?

Select one:

- ☒ a. Impact & Probability of Occurrence
- ☐ b. Probability of Occurrence & Threat
- ☐ c. Impact & Threat
- ☐ d. Threat & Control Level

SLIIT

Sri Lanka Institute of Information Technology has many different stakeholders. Select the most relevant SLIIT (Choose 3).

Select one or more:

- ☒ a. Ministry of Higher Education
- ☐ b. Export Development Board
- ☒ c. University Grants Commission
- ☒ d. Students
- ☐ e. Investment Bankers

Firewall

Read the case study below and answer the questions regarding simple packet filtering.

A firewall is being configured to protect the 192.168.30.0 /24 network. Internal hosts may access all external websites except 100.54.12.124. All external hosts may upload E-mail to 192.168.30.100 and access web pages on 192.168.30.200. All other activity is to be blocked. No connection may be made to the firewall(192.168.30.1) itself.

Complete the first four firewall rules given below.

- Rule 1 - Stealth Rule
- Rule 2 - Blocking the mentioned external website
- Rule 3 & 4 - Allowing all other Web communication

Rule #	Source IP	Source Port	Destination IP	Destination Port	Protocol	Action
1	*	*	192.168.30.1	*	*	Deny
2	192.168.30.0	*	100.54.12.124	*	*	Deny
3	192.168.30.0	*	*	80	TCP	Allow
4	*	80	192.168.30.0	*	TCP	Allow

Note: "*" refers to 'All'