Question 1

Which of the following is an example of a "something you know" authentication factor?

A. User ID
B. Password
C. Fingerprint
D. Iris scan

Feedback :
B is correct. A password is something the user knows and can present as an authentication factor to confirm an identity assertion. A is incorrect because a user ID is an identity assertion, not an authentication factor. C and D are incorrect as they are examples of authentication factors that are something you are, also referred to as "biometrics."

Question 2

Within the organization, who can identify risk?

A. The security manager
B. Any security team member
C. Senior management
D. Anyone

Feedback :

D is correct. Anyone within the organization can identify risk.

Question 3

A vendor sells a particular operating system (OS). In order to deploy the OS securely on different platforms, the vendor publishes several sets of instructions on how to install it, depending on which platform the customer is using. This is an example of a ....

A. Law
B. Procedure
C. Standard
D. Policy

Feedback :

B is correct. This is a set of instructions to perform a particular task, so it is a procedure (several procedures, actually—one for each platform). A is incorrect; the instructions are not a governmental mandate. C is incorrect, because the instructions are particular to a specific product, not accepted throughout the industry. D is incorrect, because the instructions are not particular to a given organization.

Question 4

Of the following, which would probably not be considered a threat?

A. Natural DIsaster
B. Unintentional damage to the system caused by a user
C. A laptop with sensitivie data on it
D. An external attacker trying to gain unauthorized access to the environment

Feedback :

C is correct. A laptop, and the data on it, are assets, not threats. All the other answers are examples of threats, as they all have the potential to cause adverse impact to the organization and the organization's assets.

Question 5

For which of the following assests is integrity probably the most important security aspect?

A. One frame of a streaming video
B. The file that contains passwords used to authenticate users
C. The color scheme of a marketing website
D. Software that checks the spelling of product descriptions for a retail website

Feedback :

B is correct. If a password file is modified, the impact to the environment could be significant; there is a possibility that all authorized users could be denied access, or that anyone (including unauthorized users) could be granted access. The integrity of the password file is probably the most crucial of the four options listed. A is incorrect because one frame of an entire film, if modified, probably would have little to no effect whatsoever on the value of the film to the viewer; a film has thousands (or tens of thousands, or millions) of frames. C is incorrect because a change in marketing material, while significant, is not as crucial as the integrity of the password file described in Answer B. D is incorrect because a typo in a product description is not likely to be as important as the integrity of the password file described in Answer B.

Question 6

Kerpak works in the security office of a medium-sized entertainment company. Kerpak is asked to assess a particular threat, and he suggests that the best way to counter this threat would be to purchase and implement a particular security solution. This is an example of ......

A. Acceptance
B. Avoidance
C. Mitigation
D. Transference

Feedback :

C is correct. Applying a security solution (a type of control) is an example of mitigation. A is incorrect; if Kerpak suggested acceptance, then the threat, and the acceptance of the associated risk, only needs to be documented—no other action is necessary. B is incorrect; if Kerpak suggested avoidance, the course of action would be to cease whatever activity was associated with the threat. D is incorrect; if Kerpak suggested transference, this would involve forming some sort of risk-sharing relationship with an external party, such as an insurance underwriter.

Question 7

The Triffid Corporation publishes a policy that states all personnel will act in a manner that protects health and human safety. The security office is tasked with writing a detailed set of processes on how employees should wear protective gear such a hardhat and gloves when in haradous areas. This detailed set of process is a ......

A. Policy
B. Procedure
C. Standard
D. Law

Feedback :

B is correct. A detailed set of processes used by a specific organization is a procedure. A is incorrect; the policy is the overarching document that requires the procedure be created and implemented. C is incorrect. The procedure is not recognized and implemented throughout the industry; it is used internally.

D is incorrect; the procedure was created by Triffid Corporation, not a governmental body.

Question 8

The city of Grampon wants to know where all its public vehicles (garbage trucks, police cars, etc.) are at all times, so the city has GPS transmitters installed in all the vehicles. What kind of control is this?

A. Administrative
B. Entrenched
C. Physical
D. Technical

Feedback :

D is correct. A GPS unit is part of the IT environment, so this is a technical control. A is incorrect. The GPS unit itself is not a rule or a policy or a process; it is part of the IT environment, so D is a better answer. B is incorrect; "entrenched" is not a term commonly used to describe a particular type of security control, and is used here only as a distractor. C is incorrect; while a GPS unit is a tangible object, it is also part of the IT environment, and it does not interact directly with other physical objects in order to prevent action, so "technical" is a better descriptor, and D is a better answer.

Question 9

The Payment Card Industry (PCI) Council is a committee made up of representatives from major credit card providers (Visa, Mastercard, American Express) in the United States. The PCI Council issues rules that merchants must follow if the merchants choose to accept payment via credit card. These rules describe best practices for securing credit card processing technology, activities for securing credit card information, and how to protect customers' personal data. This set of rules is a _____.

A. Law
B. Policy
C. Standard

D. Procedure

Feedback :

C is correct. This set of rules is known as the Data Security Standard, and it is accepted throughout the industry. A is incorrect, because this set of rules was not issued by a governmental body. B is incorrect, because the set of rules is not a strategic, internal document published by senior leadership of a single organization. D is incorrect, because the set of rules is not internal to a given organization and is not limited to a single activity.

Question 10

Grampon municipal code requires that all companies that operate within city limits will have a set of processes to ensure employees are safe while working with hazardous materials. Triffid Corporation creates a checklist of activities employees must follow while working with hazardous materials inside Grampon city limits. The municipal code is a ______, and the Triffid checklist is a ________.

A. Law, procedure
B. Standard, law
C. Law, standard
D. Policy, law

Feedback :

A is correct. The municipal code was created by a governmental body and is a legal mandate; this is a law. The Triffid checklist is a detailed set of actions which must be used by Triffid employees in specific circumstances; this is a procedure. B and C are incorrect; neither document is recognized throughout the industry, so neither is a standard. D is incorrect; neither document is a strategic internal overview issued by senior management, so neither is a policy.

Question 11

For which of the following systems would the security concept of availability probably be most important?

A. Medical systems that store patient data
B. Retail records of past transactions
C. Online streaming of camera feeds that display historical works of art in museums around the world
D. Medical systems that monitor patient condition in an intensive care unit

Feedback :

D is correct. Information that reflects patient condition is data that necessarily must be kept available in real time, because that data is directly linked to the patients' well-being (and possibly their life). This is, by far, the most important of the options listed. A is incorrect because stored data, while important, is not as critical to patient health as the monitoring function listed in answer D. B is incorrect because retail transactions do not constitute a risk to health and human safety. C is incorrect because displaying artwork does not reflect a risk to health and human safety; also because the loss of online streaming does not actually affect the asset (the artwork in the museum) in any way—the art will still be in the museum, regardless of whether the camera is functioning.

Question 12

A bollard is a post set securely in the ground in order to prevent a vehicle from entering an area or driving past a certain point. Bollards are an example of _______ controls.

A. Physical
B. Administrative
C. Drstic
D. Technical

Feedback :

A is correct. A bollard is a tangible object that prevents a physical act from occurring; this is a physical control. B and D are incorrect because the bollard is a physical control, not administrative or technical. C is incorrect: "drastic" is not a term commonly used to describe a particular type of security control, and is used here only as a distractor.

Question 13

A system that collects transactional information and stores it in a record in order to show which users performed which actions is an example of providing ________.

A. **Non-repudiation**
B. Multifactor authentication
C. Biometrics
D. Privacy

Feedback :

A is correct. Non-repudiation is the concept that users cannot deny they have performed transactions that they did, in fact, conduct. A system that keeps a record of user transactions provides non-repudiation. B and C are incorrect because nothing in the question referred to authentication at all. D is incorrect because non-repudiation does not support privacy (if anything, non-repudiation and privacy are oppositional).

Question 14

A software firewall is an application that runs on a device and prevents specific types of traffic from entering that device. This is a type of ________ control.

A. Physical
B. Administrative
C. Passive
D. **Technical**

Feedback :

D is correct. A software firewall is a technical control, because it is a part of the IT environment. A is incorrect; a software firewall is not a tangible object that protects something. B is incorrect; a software firewall is not a rule or process. Without trying to confuse the issue, a software firewall might incorporate an administrative control: the set of rules which the firewall uses to allow or block particular traffic. However, answer D is a much better way to describe a software firewall. C is incorrect; "passive" is not a term commonly used to describe a particular type of security control, and is used here only as a distractor.

Question 15

In risk management concepts, a(n) __________ is something a security practitioner might need to protect.

A. Vulnerability
B. Asset
C. Threat
D. Likelihood

Feedback :

B is correct. An asset is anything with value, and a security practitioner may need to protect assets. A, C, and D are incorrect because vulnerabilities, threats and likelihood are terms associated with risk concepts, but are not things that a practitioner would protect.

Question 16

Which of the following is an example of a "something you are" authentication factor?

A. A credit card presented to a cash machine
B. Your password and PIN
C. A user ID
D. A photograph of your face

Feedback :

D is correct. A facial photograph is something you are—your appearance. A is incorrect because a credit card is an example of an authentication factor that is something you have. B is incorrect because passwords and PINs are examples of authentication factors that are something you know. C is incorrect because a user ID is an identity assertion, not an authentication factor.

Question 17

All of the following are important ways to practice an organization disaster recovery (DR) effort, which one is the most important?

A. Practice restoring data from backups
B. Facility evacuation drills
C. Desktop/tabletop testing of the plan
D. Running the alternate operating site to determine if it could handle critical functions in times of emergency

Feedback :

B is the only answer that directly addresses health and human safety, which is the paramount concern of all security efforts. All the other answers are good exercises to perform as DR preparation, but B is the correct answer.

Question 18

When should a business continuity plan (BCP) be activated?

A. As soon as possible
B. At the very beginning of a disaster
C. When senior management decides
D. When instructed to do so by regulators

Feedback :

C is correct. A senior manager with the proper authority must initiate the BCP. A is incorrect; this answer has no context—there is no way to know when "as soon as possible" would be. B is incorrect; typically, it is impossible to determine the "beginning" of a disaster. D is incorrect; not all organizations are in regulated industries, and regulators do not supervise disaster response.

Question 19

An attacker outside the organization attempts to gain access to the organization's internal files. This is an example of a(n) ______.

A. **Intrusion**
B. Exploit
C. Disclosure
D. Publication

Feedback :

A is correct. An intrusion is an attempt (successful or otherwise) to gain unauthorized access. B is incorrect; the question does not mention what specific attack or vulnerability was used. C and D are incorrect; the organization did not grant unauthorized access or release the files.

Question 20

You are reviewing log data from a router; there is an entry that shows a user sent traffic through the router at 11:45 am, local time, yesterday. This is an example of a(n) _______.

A. Incident
B. **Event**
C. Attack
D. Threat

Feedback :

An event is any observable occurrence within the IT environment. (Any observable occurrence in a network or system. (Source: NIST SP 800-61 Rev 2) While an event might be part of an incident, attack, or threat, no other information about the event was given in the question, so B is the correct answer.

Question 21

Who approves the incident response policy?

A. (ISC)²
B. Senior management
C. The security manager
D. Investor

Feedback :

B is correct. The organization's senior management are the only entities authorized to accept risk on behalf of the organization, and therefore all organizational policies must be approved by senior management. A is incorrect; (ISC)² has no authority over individual organizations. C is incorrect; the security manager will likely be involved in crafting and implementing the policy, but only senior management can approve it. D is incorrect; investors leave policy review and approval to senior management.

Question 22

True of False? Business continuity planning is a reactive procedure that restores business operations after a disruption occurs.

A. True
B. False

Feedback :

B is correct. Business continuity planning is proactive preparation for restoring operations after disruption. Members from across the organizations participate in the planning to ensure all systems, processes and operations are accounted for in the plan. A is incorrect; business continuity planning is a proactive procedure to prepare for the restoration of operations after disruption.

Question 23

Which of the following is likely to be included in the business continuity plan?

A. **Alternate work areas for personnel affected by a natural disaster**
B. The organization’s strategic security approach
C. Last year’s budge information
D. Log data from all systems

Feedback :

A is correct. The business continuity plan should include provisions for alternate work sites, if the primary site is affected by an interruption, such as a natural disaster. B is incorrect; the organization's strategic security approach should be included in the organization's security policy. C is incorrect; budgetary information is not typically included in the business continuity plan. D is incorrect; log data is not typically included in the business continuity plan.

Question 24

Tekila works for a government agency. All data in the agency is assigned a particular sensitivity level, called a "classification." Every person in the agency is assigned a "clearance" level, which determines the classification of data each person can access.
What is the access control model being implemented in Tekila's agency?

A. **MAC (mandatory access control)**
B. DAC (discretionary access control)
C. RBAC (role-based access control)
D. FAC (formal access control)

Feedback :

This is an example of how MAC can be implemented. A is the correct answer. B is incorrect; in discretionary access control, operational managers are granted authority to determine which personnel have access to assets the manager controls. C is incorrect; in RBAC, personnel might not have clearance levels, and assets might not have classifications. D is incorrect; FAC is not a term used in this context, and is only included here as a distractor.

Question 25

In order for a biometric security to function properly, an authorized person's physiological data must be ______.

A. Broadcast
B. Stored
C. Deleted
D. Modified

Feedback :

B is correct. A biometric security system works by capturing and recording a physiological trait of the authorized person and storing it for comparison whenever that person presents the same trait in the future. A is incorrect; access control information should not be broadcast. C is incorrect; if all biometric data is erased, the data cannot be used for comparison purposes to grant access later. D is incorrect; biometric data should not be modified, or it may become useless for comparison purposes.

Question 26

Handel is a senior manager at Triffid, Inc., and is in charge of implementing a new access control scheme for the company. Handel wants to ensure that operational managers have the utmost personal choice in determining which employees get access to which systems/data. Which method should Handel select?

A. Role-based access control (RBAC)
B. Mandatory access control (MAC)
C. Discretionary access control (DAC)
D. Security policy

Feedback :

DAC gives managers the most choice in determining which employees get access to which assets. C is the correct answer. A and B are incorrect; RBAC and MAC do not offer the same kind of flexibility that DAC does. D is incorrect; "security policy" is too broad and vague to be applicable; C is the better answer.

Question 27

Which of the following roles does not typically require privileged account access?

A. Security administrator
B. Data entry professional
C. System administrator
D. Help Desk technician

Feedback :

B is correct. Data entry professionals do not usually need privileged access. A, C and D are all incorrect; those are roles that typically need privileged access.

Question 28

A human guard monitoring a hidden camera could be considered a ______ control.

A. Detective
B. Preventive
C. Deterrent
D. Logical

Feedback :

A is correct. The guard monitoring the camera can identify anomalous or dangerous activity; this is a detective control. B is incorrect; neither the guard nor the camera is actually preventing any activity before it occurs. C is incorrect; because the attacker is unaware of the guard and the camera, there is no deterrent benefit. D is incorrect; the guard is a physical control.

Question 29

A _____ is a record of something that has occurred.

A. Biometric
B. Law
C. Log
D. Firewall

Feedback :

C is correct. This is a description of a log. A is incorrect; "biometrics" is a term used to describe access control systems that use physiological traits of individuals in order to grant/deny access. B is incorrect; laws are legal mandates. D is incorrect; a firewall is a device for filtering traffic.

Question 30

All of the following are typically perceived as drawbacks to biometric systems, except:

A. Lack of accuracy
B. Potential privacy concerns
C. Retention of physiological data past the point of employment
D. Legality

Feedback :

A is correct. Biometric systems can be extremely accurate, especially when compared with other types of access controls. B, C and D are all potential concerns when using biometric data, so those answers are incorrect in this context.

Question 31

Prachi works as a database administrator for Triffid, Inc. Prachi is allowed to add or delete users, but is not allowed to read or modify the data in the database itself. When Prachi logs onto the system, an access control list (ACL) checks to determine which permissions Prachi has.
In this situation, what is the database?

A. **The object**
B. The rule
C. The subject
D. The site

Feedback :

A is correct. Prachi is manipulating the database, so the database is the object in the subject-object-rule relationship in this case. B and C are incorrect, because the database is the object in this situation. D is incorrect because "site" has no meaning in this context.

Question 32

Which of the following is not an appropriate control to add to privileged accounts?

A. Increased logging
B. Multifactor authentication
C. Increased auditing
D. **Security deposit**

Feedback :

D is correct. We typically do not ask privileged account holders for security deposits. A, B, and C are incorrect; those are appropriate controls to enact for privileged accounts.

Question 33

Prachi works as a database administrator for Triffid, Inc. Prachi is allowed to add or delete users, but is not allowed to read or modify the data in the database itself. When Prachi logs onto the system, an access control list (ACL) checks to determine which permissions Prachi has.
In this situation, what is the ACL?

A. The subject
B. The object
C. The rule
D. The firmware

Feedback :

C is correct. The ACL, in this case, acts as the rule in the subject-object-rule relationship. It determines what Prachi is allowed to do, and what Prachi is not permitted to do. A and B are incorrect, because the ACL is the rule in this case. D is incorrect, because firmware is not typically part of the subject-object-rule relationship, and the ACL is not firmware in any case.

Question 34

Visitors to a secure facility need to be controlled. Controls useful for managing visitors include all of the following except:

A. Sign-in sheet/tracking log
B. Fence
C. Badges that differ from employee badges
D. Receptionist

Feedback :

B is the best answer. A fence is useful for controlling visitors, authorized users and potential intruders. This is the only control listed among the possible answers that is not specific to visitors. A, C and D are all controls that should be used to manage visitors.

Question 35

Which of the following will have the most impact on determining the duration of log retention?

A. Personal preference
B. Applicable laws
C. Industry standards
D. Type of storage media

Feedback :

B is correct. Laws will have the most impact on policies, including log retention periods, because laws cannot be contravened. All the other answers may have some impact on retention periods, but they will never have as much impact as applicable laws.

Question 36

Prachi works as a database administrator for Triffid, Inc. Prachi is allowed to add or delete users, but is not allowed to read or modify the data in the database itself. When Prachi logs onto the system, an access control list (ACL) checks to determine which permissions Prachi has.
In this situation, what is Prachi?

A. The subject
B. The rule
C. The file
D. The object

Feedback :

A is correct. In this situation, Prachi is the subject in the subject-object-rule relationship. Prachi manipulates the database; this makes Prachi the subject. B and D are incorrect, because Prachi is the subject in this situation. C is incorrect, because Prachi is not, and never will be, a file.

Question 37

Which of the following would be considered a logical access control?

A. An iris reader that allows an employee to enter a controlled area
B. A fingerprint reader that allows an employee to enter a controlled area
C. A fingerprint reader that allows an employee to access a laptop computer
D. A chain attached to a laptop computer that connects it to furniture so it cannot be taken

Feedback :

Logical access controls limit who can gain user access to a device/system. C is the correct answer. A, B and D are all physical controls, as they limit physical access to areas and assets.

Question 38

Trina is a security practitioner at Triffid, Inc. Trina has been tasked with selecting a new product to serve as a security control in the environment. After doing some research, Trina selects a particular product. Before that product can be purchased, a manager must review Trina's selection and determine whether to approve the purchase. This is a description of:

A. Two-person integrity
B. Segregation of duties
C. Software
D. Defense in depth

Feedback :

B is correct. Segregation of duties, also called separation of duties, is used to reduce the potential for corruption or fraud within the organization. More than one person must be involved in a given process in order to complete that process. A is incorrect; Trina and the manager are not both required to be present for the transaction. C is incorrect; software is a term used to describe programs and applications. D is incorrect; defense in depth is the use of multiple (and multiple types of) overlapping security controls to protect assets.

Question 39

Larry and Fern both work in the data center. In order to enter the data center to begin their workday, they must both present their own keys (which are different) to the key reader, before the door to the data center opens.
Which security concept is being applied in this situation?

A. Defense in depth
B. Segregation of duties
C. Least privilege
D. Dual control

Feedback :

D is correct. This is an example of dual control, where two people, each with distinct authentication factors, must be present to perform a function. A is incorrect; defense in depth requires multiple controls protecting assets—there is no description of multiple controls in this situation. B is incorrect; in segregation of duties, the parts of a given transaction are split among multiple people, and the task cannot be completed unless each of them takes part. Typically, in segregation of duties, the people involved do not have to take part simultaneously; their actions can be spread over time and distance. This differs from dual control, where both people must be present at the same time. C is incorrect; the situation described in the question does not reduce the permissions of either person involved or limit their capabilities to their job function.

Question 40

At Parvi's place of work, the perimeter of the property is surrounded by a fence; there is a gate with a guard at the entrance. All inner doors only admit personnel with badges, and cameras monitor the hallways. Sensitive data and

media are kept in safes when not in use.
This is an example of:

A. Two-person integrity
B. Segregation of duties
C. Defense in depth
D. Penetration testing

Feedback :

C is correct. Defense in depth is the use of multiple different (and different types of) overlapping controls to provide sufficient security. A and B are incorrect; nothing in the question suggested that two-person integrity or segregation of duties are being used in Parvi's workplace. D is incorrect; this is not a description of penetration testing.

Question 41

To adequately ensure availability for a data center, it is best to plan for both resilience and ________ of the elements in the facility.

A. Uniqueness
B. Destruction
C. Redundancy
D. Hue

Feedback :

C is correct. Availability is enhanced by ensuring that elements of the data center are replicated, in case any given individual element fails. A is incorrect; this is the opposite of redundancy—is any single element is unique, that could become a single point of failure and affect the overall operation. B is incorrect; while secure destruction is worth planning for, that will come at the end of the system life cycle and is not part of ensuring availability. D is incorrect; we generally don't care what color the elements of a data center are.

Question 42

Triffid, Inc., has deployed anti-malware solutions across its internal IT environment. What is an additional task necessary to ensure this control will function properly?

A. Pay all employees a bonus for allowing anti-malware solutions to be run on their systems
B. Update the anti-malware solution regularly
C. Install a monitoring solution to check the anti-malware solution
D. Alert the public that this protective measure has been taken

Feedback :

B is the correct answer. Anti-malware solutions typically work with signatures for known malware; without continual updates, these tools lose their efficacy. A, C and D are incorrect; these measures will not aid in the effectiveness of anti-malware solutions.

Question 43

"Wiring _____" is a common term meaning "a place where wires/conduits are often run, and equipment can be placed, in order to facilitate the use of local networks."

A. Shelf
B. Closet
C. Bracket
D. House

Feedback :

"Wiring closet" is the common term used to described small spaces, typically placed on each floor of a building, where IT infrastructure can be placed. A, C and D are incorrect; these are not common terms used in this manner.

Question 44

Barry wants to upload a series of files to a web-based storage service, so that people Barry has granted authorization can retrieve these files. Which of the following would be Barry's preferred communication protocol if he wanted this activity to be efficient and secure?

A. SMTP (Simple Mail Transfer Protocol)
B. FTP (File Transfer Protocol)
C. SFTP (Secure File Transfer Protocol)
D. SNMP (Simple Network Management Protocol)

Feedback :

C is the correct answer; SFTP is designed specifically for this purpose. A, B and D are incorrect; these protocols are either not efficient or not secure in Barry's intended use.

Question 45

Which of the following is *not* a typical benefit of cloud computing services?

A. Reduced cost of ownership/investment
B. Metered usage
C. Scalability
D. Freedom from legal contraints

Feedback :

D is correct. Moving data/operations into the cloud does not relieve the customer from legal constraints (and may even increase them). A, B and C are all common benefits of cloud services, and are therefore incorrect answers.

Question 46

Gary is an attacker. Gary is able to get access to the communication wire between Dauphine's machine and Linda's machine and can then surveil the traffic between the two when they're communicating. What kind of attack is this?

A. Side channel
B. DDOS
C. On-path
D. Physical

Feedback :

This is a textbook example of an on-path attack, where the attackers insert themselves between communicating parties. C is the correct answer. A is incorrect; a side channel attack is entirely passive, and typically does not include surveilling actual data (it instead surveils operational activity, such as changes in power usage, emissions and so forth). B is incorrect; a DDOS attack involves multiple machines flooding the target to overwhelm the target; Gary is neither shutting down the target nor using multiple devices in the attack. D is incorrect; a physical attack involves tangible materials. An example of a physical attack would be Gary cutting the wire between Linda and Dauphine, so that they could not communicate.

Question 47

The concept that the deployment of multiple types of controls provides better security than using a single type of control.

A. VPN
B. Least privilege
C. Internet
D. Defense in depth

Feedback :

D is correct; defense in depth involves multiple types of controls to provide better security. A is incorrect; a virtual private network protects communication traffic over untrusted media, but does not involve multiple types of controls. B is incorrect; the principle of least privilege is a system of access control. C is incorrect; the internet is an untrusted medium.

Question 48

Which common cloud service model only offers the customer access to a given application?

A. Lunch as a service (LaaS)
B. Infrastructure as a service (IaaS)
C. Platform as a service (PaaS)
D. Software as a service

Feedback :

D is the correct answer. This is a description of how SaaS works. A is incorrect; this is not a common cloud service model. B is incorrect; IaaS offers much more than just access to a given application. C is incorrect; PaaS offers much more than just access to a given application.

Question 49

Inbound traffic from an external source seems to indicate much higher rates of communication than normal, to the point where the internal systems might be overwhelmed. Which security solution can often identify and potentially counter this risk?

A. Firewall
B. Turnstile
C. Anti-malware
D. Badge system

Feedback :

Firewalls can often identify hostile inbound traffic, and potentially counter it. A is the correct answer. B and D are incorrect; these are physical controls and aren't effective in identifying/countering communications attacks. C is incorrect; anti-malware is not typically useful in countering attacks that employ excess traffic as an attack mechanism.

Question 50

A tool that filters inbound traffic to reduce potential threats.

A. NIDS (network-based intrusion detection system)

B. Anti-malware

C. DLP (data loss prevention)

D. Firewall

Feedback :

Firewalls typically filter traffic originating from outside the organization's IT environment. D is the correct answer. A is incorrect; NIDS typically monitor traffic within the production environment. B is incorrect; anti-malware solutions typically identify hostile software. C is incorrect; DLP solutions typically monitor outbound traffic.