Chapter 1

Domain 1: Cloud Concepts, Architecture, and Design

SUBDOMAINS:

- ✓ 1.1 Understand cloud computing concepts
- ✓ 1.2 Describe cloud reference architecture
- ✓ 1.3 Understand security concepts relevant to cloud computing
- ✓ 1.4 Understand design principles of cloud computing
- ✓ 1.5 Evaluate cloud service providers

1. Matthew is reviewing a new cloud service offering that his organization plans to adopt. In this offering, a cloud provider will create virtual server instances under the multitenancy model. Each server instance will be accessible only to Matthew's company. What cloud deployment model is being used?
   - **A.** Hybrid cloud
   - **B.** Public cloud
   - **C.** Private cloud
   - **D.** Community cloud

2. Zeke is responsible for sanitizing a set of solid-state drives (SSDs) removed from servers in his organization's datacenter. The drives will be reused on a different project. Which one of the following sanitization techniques would be most effective?
   - **A.** Cryptographic erasure
   - **B.** Physical destruction
   - **C.** Degaussing
   - **D.** Overwriting

3. Tina would like to use a technology that will allow her to bundle up workloads and easily move them between different operating systems. What technology would best meet this need?
   - **A.** Virtual machines
   - **B.** Serverless computing
   - **C.** Hypervisors
   - **D.** Containers

4. Under the cloud reference architecture, which one of the following activities is not generally part of the responsibilities of a customer?
   - **A.** Monitor services
   - **B.** Prepare systems
   - **C.** Perform business administration
   - **D.** Handle problem reports

5. Seth is helping his organization move their web server cluster to a cloud provider. The goal of this move is to provide the cluster with the ability to grow and shrink based on changing demand. What characteristic of cloud computing is Seth hoping to achieve?
   - **A.** Scalability
   - **B.** On-demand self service
   - **C.** Elasticity
   - **D.** Broad network access

6. Sherry is deploying a zero-trust network architecture for her organization. In this approach, which one of the following characteristics would be least important in validating a login attempt?
   - **A.** User identity
   - **B.** IP address
   - **C.** Geolocation
   - **D.** Nature of requested access

7. Which one of the following hypervisor models is the most resistant to attack?
   - **A.** Type 1
   - **B.** Type 2
   - **C.** Type 3
   - **D.** Type 4

8. Joe is using a virtual server instance running on a public cloud provider and would like to restrict the ports on that server accessible from the internet. What security control would best allow him to meet this need?
   - **A.** Geofencing
   - **B.** Traffic inspection
   - **C.** Network firewall
   - **D.** Network security groups

9. Which one of the following cybersecurity threats is least likely to directly affect an object storage service?
   - **A.** Disk failure
   - **B.** User error
   - **C.** Ransomware
   - **D.** Virus

10. Vince would like to be immediately alerted whenever a user with access to a sensitive cloud service leaves a defined physical area. What type of security control should he implement?
    - **A.** Intrusion prevention system
    - **B.** Geofencing
    - **C.** Firewall rule
    - **D.** Geotagging

11. Which one of the following characteristics is not a component of the standard definition of cloud computing?
    - **A.** Broad network access
    - **B.** Rapid provisioning
    - **C.** Multitenancy
    - **D.** On-demand self service

12. Which one of the following sources provides a set of vendor-neutral design patterns for cloud security?

A. Cloud Security Alliance

B. Amazon Web Services

C. Microsoft

D. $(ISC)^2$

13. Lori is using an API to access sensitive information stored in a cloud service. What cloud secure data lifecycle activity is Lori engaged in?

A. Store

B. Use

C. Destroy

D. Create

14. Helen would like to provision a disk volume in the cloud that is mountable from a server. What cloud capability does she want?

A. Virtualized server

B. Object storage

C. Network capacity

D. Block storage

15. Ben is using the `sudo` command to carry out operations on a Linux server. What type of access is he using?

A. Service access

B. Unauthorized access

C. User access

D. Privileged access

16. Which one of the following cryptographic goals protects against the risks posed when a device is lost or stolen?

A. Nonrepudiation

B. Authentication

C. Integrity

D. Confidentiality

17. Which type of business impact assessment tool is most appropriate when attempting to evaluate the impact of a failure on customer confidence?

A. Quantitative

B. Qualitative

C. Annualized loss expectancy

D. Single loss expectancy

18. Robert is reviewing a system that has been assigned the EAL2 evaluation assurance level under the Common Criteria. What is the highest level of assurance that he may have about the system?

A. It has been functionally tested.

B. It has been structurally tested.

C. It has been formally verified, designed, and tested.

D. It has been semi-formally designed and tested.

19. Jake would like to use a third-party platform to automatically move workloads between cloud service providers. What type of tool would best meet this need?

A. Cloud access service broker

B. Database

C. Virtualization

D. Orchestration

20. Robert is responsible for securing systems used to process credit card information. What security control framework should guide his actions?

A. HIPAA

B. PCI DSS

C. SOX

D. GLBA

21. What type of effort attempts to bring all of an organization's cloud activities under more centralized control?

A. Cloud access service broker

B. Cloud orchestration

C. Cloud governance

D. Cloud migration

22. Chris is designing a cryptographic system for use within his company. The company has 1,000 employees, and they plan to use an asymmetric encryption system. They would like the system to be set up so that any pair of arbitrary users may communicate privately. How many total keys will they need?

A. 500

B. 1,000

C. 2,000

D. 4,950

23. Erin is concerned about the risk that a cloud provider used by her organization will fail, so she is creating a strategy that will combine resources from multiple public cloud providers. What term best describes this strategy?

A. Community cloud

B. Multicloud

C. Private cloud

D. Hybrid cloud

24. Which one of the following would normally be considered an application capability of a cloud service provider?

A. Network capacity

B. Hosted email

C. Block storage

D. Serverless computing

25. What activity are cloud providers able to engage in because not all users will access the full capacity of their service offering simultaneously?

A. Oversubscription

B. Overprovisioning

C. Underprovisioning

D. Undersubscription

26. Brian recently joined an organization that runs the majority of its services on a virtualization platform located in its own datacenter but also leverages an IaaS provider for hosting its web services and an SaaS email system. What term best describes the type of cloud environment this organization uses?

A. Public cloud

B. Dedicated cloud

C. Private cloud

D. Hybrid cloud

27. In an infrastructure as a service (IaaS) environment where a vendor supplies a customer with access to storage services, who is normally responsible for removing sensitive data from drives that are taken out of service?

A. Customer's security team

B. Customer's storage team

C. Customer's vendor management team

D. Vendor

28. Lucca is reviewing his organization's disaster recovery process data and notes that the MTD for the business's main website is two hours. What does he know about the RTO for the site when he does testing and validation?

A. It needs to be less than two hours.

B. It needs to be at least two hours.

C. The MTD is too short and needs to be longer.

D. The RTO is too short and needs to be longer.

29. Alice and Bob would like to use an asymmetric cryptosystem to communicate with each other. They are located in different parts of the country but have exchanged encryption keys by using digital certificates signed by a mutually trusted certificate authority.

When Bob receives an encrypted message from Alice, what key does he use to decrypt the plaintext message's contents?

A. Alice's public key

B. Alice's private key

C. Bob's public key

D. Bob's private key

30. Jen works for an organization that assists other companies in moving their operations from on-premises datacenters to the cloud. Jen's company does not operate their own cloud services but assists in the use of services offered by other organizations. What term best describes the role of Jen's company?

A. Cloud service customer

B. Cloud service partner

C. Cloud service provider

D. Cloud service broker

31. Carla is selecting a hardware security module (HSM) for use by her organization. She is employed by an agency of the U.S. federal government and must ensure that the technology she chooses meets applicable federal standards for cryptographic systems. What publication would best help her determine these requirements?

A. NIST 800-53

B. NIST 800-171

C. Common Criteria

D. FIPS 140-2

32. Ryan is reviewing the design of a new service that will use several offerings from a cloud service provider. The design depends on some unique features offered only by that provider. What should concern Ryan the most about the fact that these service features are not available from other providers?

A. Vendor lock-in

B. Interoperability

C. Auditability

D. Confidentiality

33. Colin is reviewing a system that has been assigned the EAL7 evaluation assurance level under the Common Criteria. What is the highest level of assurance that he may have about the system?

A. It has been functionally tested.

B. It has been methodically tested and checked.

C. It has been methodically designed, tested, and reviewed.

D. It has been formally verified, designed, and tested.

34. Which one of the following technologies provides the capability of creating a distributed, immutable ledger?

A. Quantum computing

B. Blockchain

C. Edge computing

D. Confidential computing

35. Which one of the following systems assurance processes provides an independent third-party evaluation of a system's controls that may be trusted by many different organizations?

A. Planning

B. Definition

C. Verification

D. Accreditation

36. Which one of the following would be considered an example of infrastructure as a service cloud computing?

A. Payroll system managed by a vendor and delivered over the web

B. Application platform managed by a vendor that runs customer code

C. Servers provisioned by customers on a vendor-managed virtualization platform

D. Web-based email service provided by a vendor

37. Which of the following is *not* a factor an organization might use in the cost–benefit analysis when deciding whether to migrate to a cloud environment?

A. Pooled resources in the cloud

B. Shifting from IT investment as capital expenditures to operational expenditures

C. The time savings and efficiencies offered by the cloud service

D. Branding associated with which cloud provider might be selected

38. Barry has a temporary need for massive computing power and is planning to use virtual server instances from a cloud provider for a short period of time. What term best describes the characteristic of Barry's workload?

A. Quantum computing

B. Confidential computing

C. Ephemeral computing

D. Parallel computing

39. You are reviewing a service-level agreement (SLA) and find a provision that guarantees 99.99% uptime for a service you plan to use. What term best describes this type of provision?

A. Availability

B. Security

C. Privacy

D. Resiliency

40. Carlton is selecting a cloud environment for an application run by his organization. He needs an environment where he will have the most control over the application's performance. What service category would be best suited for his needs?

A. SaaS

B. FaaS

C. IaaS

D. PaaS

41. Gavin is looking for guidance on how his organization should approach the evaluation of cloud service providers. What ISO document can help him with this work?

A. ISO 27001

B. ISO 27701

C. ISO 27017

D. ISO 17789

42. Ed has a question about the applicability of PCI DSS requirements to his organization's credit card processing environment. What organization is the regulator in this case?

A. SEC

B. FDA

C. FTC

D. PCI SSC

43. Rick is an application developer who works primarily in Python. He recently decided to evaluate a new service where he provides his Python code to a vendor who then executes it on their server environment. What cloud service category includes this service?

A. SaaS

B. PaaS

C. IaaS

D. CaaS

44. Gordon is developing a business continuity plan for a manufacturing company's IT operations. The company is located in North Dakota and currently evaluating the risk of earthquake. They choose to pursue a risk acceptance strategy. Which one of the following actions is consistent with that strategy?

A. Purchasing earthquake insurance

B. Relocating the datacenter to a safer area

C. Documenting the decision-making process

D. Reengineering the facility to withstand the shock of an earthquake

45. Matthew is a data scientist looking to apply machine learning and artificial intelligence techniques in his organization. He is developing an application that will analyze a potential customer and develop an estimate of how likely it is that they will make a purchase. What type of analytic technique is he using?

A. Optimal analytics

B. Descriptive analytics

C. Prescriptive analytics

D. Predictive analytics

46. Which one of the following statements correctly describes resource pooling?

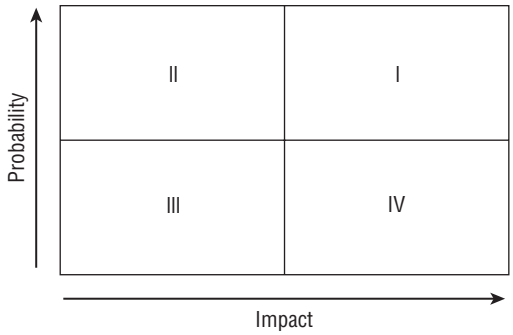
A. Resource pooling allows customers to add computing resources as needed.

B. Resource pooling allows the cloud provider to achieve economies of scale.

C. Resource pooling allows customers to remove computing resources as needed.

D. Resource pooling allows customers to provision resources without service provider interaction.

47. The Domer Industries risk assessment team recently conducted a qualitative risk assessment and developed a matrix similar to the one shown here. Which quadrant contains the risks that require the most immediate attention?



A. I

B. II

C. III

D. IV

48. Which one of the following types of agreements is the most formal document that contains expectations about availability and other performance parameters between a service provider and a customer?

A. Service-level agreement (SLA)

B. Operational-level agreement (OLA)

C. Memorandum of understanding (MOU)

D. Statement of work (SOW)

49. Bianca is preparing for her organization's move to a cloud computing environment. She is concerned that issues may arise during the change and would like to ensure that they can revert back to their on-premises environment in the case of a problem. What consideration is Bianca concerned about?

A. Reversibility

B. Portability

C. Regulatory

D. Resiliency

50. Which one of the following organizations is not known for producing cloud security guidance?

A. SANS Institute

B. FBI

C. Cloud Security Alliance

D. Microsoft

51. Vince is using a new cloud service provider and is charged for each CPU that he uses, every bit of data transferred over the network, and every GB of disk space allocated. What characteristic of cloud services does this describe?

A. Elasticity

B. On-demand self service

C. Scalability

D. Measured service

52. Who is responsible for performing scheduled maintenance of server operating systems in a PaaS environment?

A. The customer.

B. Both the customer and the service provider.

C. No operating system maintenance is necessary in a PaaS environment.

D. The service provider.

53. When considering a move from a traditional on-premises environment to the cloud, organizations often calculate a return on investment. Which one of the following factors should you expect to contribute the most to this calculation?

A. Utility costs

B. Licensing fees

C. Security expenses

D. Executive compensation

54. Devon is using an IaaS environment and would like to provision storage that will be used as a disk attached to a server instance. What type of storage should he use?

A. Archival storage

B. Block storage

C. Object storage

D. Database storage

55. During a system audit, Casey notices that the private key for her organization's web server has been stored in a public Amazon S3 storage bucket for more than a year. What should she do?

A. Remove the key from the bucket.

B. Notify all customers that their data may have been exposed.

C. Request a new certificate using a new key.

D. Nothing, because the private key should be accessible for validation.

56. Glenda would like to conduct a disaster recovery test and is seeking a test that will allow a review of the plan with no disruption to normal information system activities and as minimal a commitment of time as possible. What type of test should she choose?

A. Tabletop exercise

B. Parallel test

C. Full interruption test

D. Checklist review

57. Mark is considering replacing his organization's customer relationship management (CRM) solution with a new product that is available in the cloud. This new solution is completely managed by the vendor, and Mark's company will not have to write any code or manage any physical resources. What type of cloud solution is Mark considering?

A. IaaS

B. CaaS

C. PaaS

D. SaaS

58. Ben has been tasked with identifying security controls for systems covered by his organization's information classification system. Why might Ben choose to use a security baseline?

A. They apply in all circumstances, allowing consistent security controls.

B. They are approved by industry standards bodies, preventing liability.

C. They provide a good starting point that can be tailored to organizational needs.

D. They ensure that systems are always in a secure state.

59. What approach to technology management integrates the three components of technology management shown in this illustration?

A. Agile

B. Lean

C. DevOps

D. ITIL

60. Stacey is configuring a PaaS service for use in her organization. She would like to get SSH access to the servers that will be executing her code and contacts the vendor to request this access. What response should she expect?

A. Immediate approval of the request.

B. Immediate denial of the request.

C. The vendor will likely request more information before granting the request.

D. The vendor will likely ask for executive-level approval of the request.

61. Tom enables an application firewall provided by his cloud infrastructure as a service provider that is designed to block many types of application attacks. When viewed from a risk management perspective, what metric is Tom attempting to lower by implementing this countermeasure?

A. Impact

B. RPO

C. MTO

D. Likelihood

62. Lisa wants to integrate with a cloud identity provider that uses OAuth 2.0, and she wants to select an appropriate authentication framework. Which of the following best suits her needs?

A. OpenID Connect

B. SAML

C. RADIUS

D. Kerberos

63. Elise is helping her organization prepare to evaluate and adopt a new cloud-based human resource management (HRM) system vendor. What would be the most appropriate minimum security standard for her to require of possible vendors?

A. Compliance with all laws and regulations

B. Handling information in the same manner the organization would

C. Elimination of all identified security risks

D. Compliance with the vendor's own policies

64. Fran's company is considering purchasing a web-based email service from a vendor and eliminating its own email server environment as a cost-saving measure. What type of cloud computing environment is Fran's company considering?

A. SaaS

B. IaaS

C. CaaS

D. PaaS

65. Carl is deploying a set of video sensors that will be placed in remote locations as part of a research project. Due to connectivity limitations, he would like to perform as much image processing and computation as possible on the device itself before sending results back to the cloud for further analysis. What computing model would best meet his needs?

A. Serverless computing

B. Edge computing

C. IaaS computing

D. SaaS computing

66. Ben is working on integrating a federated identity management system and needs to exchange authentication and authorization information for browser-based single sign-on. What technology is his best option?

A. HTML

B. XACML

C. SAML

D. SPML

67. Bert is considering the use of an infrastructure as a service cloud computing partner to provide virtual servers. Which one of the following would be a vendor responsibility in this scenario?

A. Maintaining the hypervisor

B. Managing operating system security settings

C. Maintaining the host firewall

D. Configuring server access control

68. Nuno's company is outsourcing its email system to a cloud service provider who will provide web-based email access to employees of Nuno's company. What cloud service category is being used?

A. PaaS

B. IaaS

C. SaaS

D. FaaS

69. What software development methodology is most closely linked to the DevSecOps approach?

A. Waterfall

B. Spiral

C. Agile

D. Modified waterfall

70. Bailey is concerned that users around her organization are using a variety of cloud services and would like to enforce security policies consistently across those services. What security control would be best suited for her needs?

A. DRM

B. IPS

C. CASB

D. DLP

71. Roger recently accepted a new position as a security professional at a company that runs its entire IT infrastructure within an IaaS environment. Which one of the following would most likely be the responsibility of Roger's firm?

A. Configuring accessible network ports

B. Applying hypervisor updates

C. Patching operating systems

D. Wiping drives prior to disposal

72. In which cloud computing model does a customer share computing infrastructure with other customers of the cloud vendor where one customer may not know the other's identity?

A. Public cloud

B. Private cloud

C. Community cloud

D. Shared cloud

73. Kristen wants to use multiple processing sites for her data, but does not want to pay for a full datacenter. Which of the following options would you recommend as her best option if she wants to be able to quickly migrate portions of her custom application environment to the facilities in multiple countries without having to wait to ship or acquire hardware?

A. A cloud PaaS vendor

B. A hosted datacenter provider

C. A cloud IaaS vendor

D. A datacenter vendor that provides rack, power, and remote hands services

74. Which one of the following statements about cloud networking is *not* correct?

A. Security groups are the equivalent of network firewall rules.

B. IaaS networking is not configurable.

C. PaaS and SaaS networking are managed by the cloud service provider.

D. Customers may connect to cloud service provider networks using a VPN.

75. Darcy's organization is deploying serverless computing technology to better meet the needs of developers and users. In a serverless model, who is normally responsible for configuring operating system security controls?

A. Software developer

B. Cybersecurity professional

C. Cloud architect

D. Vendor

76. What is the international standard that provides guidance for the creation of an organizational information security management system (ISMS)?

A. NIST SP 800-53

B. PCI DSS

C. ISO 27001

D. NIST SP 800-37

77. You are the security subject matter expert (SME) for an organization considering a transition from a traditional IT enterprise environment into a hosted cloud provider's datacenter. One of the challenges you're facing is whether your current applications in the on-premises environment will function properly with the provider's hosted systems and tools. This is a(n) _____ issue.

A. Interoperability

B. Portability

C. Stability

D. Security

78. Mike is conducting a business impact assessment of his organization's potential move to the cloud. He is concerned about the ability to shift workloads between cloud vendors as needs change. What term best describes Mike's concern?

A. Resiliency

B. Regulatory

C. Reversibility

D. Portability

79. Which one of the following statements is correct?

A. Services that are scalable are also elastic.

B. There is no relationship between elasticity and scalability.

C. Services that are elastic are also scalable.

D. Services that are either elastic or scalable are both elastic and scalable.

80. From a customer perspective, all of the following are benefits of infrastructure as a service (IaaS) cloud services *except* _____.

A. Reduced cost of ownership

B. Reduced energy costs

C. Metered usage

D. Reduced overhead of administering the operating system (OS) in the cloud environment

81. Encryption is an essential tool for affording security to cloud-based operations. While it is possible to encrypt every system, piece of data, and transaction that takes place on the cloud, why might that not be the optimum choice for an organization?

A. Key length variances don't provide any actual additional security.

B. It would cause additional processing overhead and time delay.

C. It might result in vendor lockout.

D. The data subjects might be upset by this.

82. _____ is an example of due care, and _____ is an example of due diligence.

A. Privacy data security policy; auditing the controls dictated by the privacy data security policy

B. The European Union General Data Protection Regulation (GDPR); the Gramm–Leach–Bliley Act (GLBA)

C. Locks on doors; turnstiles

D. Perimeter defenses; internal defenses

83. Which one of the following is a critical component for confidential computing environments?

A. TEE

B. TPM

C. HSM

D. PKI

84. Which one of the following programs provides a general certification process for computing hardware that might be used in a government environment?

A. FedRAMP

B. NIST 800-53

C. Common Criteria

D. FIPS 140-2

85. In a Lightweight Directory Access Protocol (LDAP) environment, each entry in a directory server is identified by a _____.

A. Domain name (DN)

B. Distinguished name (DN)

C. Directory name (DN)

D. Default name (DN)

86. Which one of the following cloud building block technologies is best suited for storing data that is structured into related tables?

A. Storage

B. Networking

C. Databases

D. Virtualization

87. You are concerned about protecting sensitive data while it is stored in memory on a server. What emerging technology is designed to assist with this work?

A. Quantum computing

B. Confidential computing

C. Edge computing

D. Fog computing

88. Your organization has migrated into a platform as a service (PaaS) configuration. A network administrator within the cloud provider has accessed your data and sold a list of your users to a competitor. Who is required to make data breach notifications in accordance with all applicable laws?

A. The network admin responsible

B. The cloud provider

C. The regulators overseeing your deployment

D. Your organization

89. If an organization wants to retain the *most* control of their assets in the cloud, which service and deployment model combination should they choose?

A. Platform as a service (PaaS), community

B. Infrastructure as a service (IaaS), hybrid

C. Software as a service (SaaS), public

D. Infrastructure as a service (IaaS), private

90. Henry's company has deployed an extensive IoT infrastructure for building monitoring that includes environmental controls, occupancy sensors, and a variety of other sensors and controllers that help manage the building. Which of the following security concerns should Henry report as the most critical in his analysis of the IoT deployment?

A. There is a lack of local storage space for security logs, which is common to IoT devices.

B. The IoT devices may not have a separate administrative interface, allowing anybody on the same network to attempt to log in to them and making brute-force attacks possible.

C. The IoT devices may not support strong encryption for communications, exposing the log and sensor data to interception on the network.

D. The long-term support and patching model for the IoT devices may create security and operational risk for the organization.

91. In what cloud computing model does the customer build a cloud computing environment in their own datacenter or build an environment in another datacenter that is for the customer's exclusive use?

A. Public cloud

B. Private cloud

C. Hybrid cloud

D. Shared cloud

92. What cloud computing component is most susceptible to an escape attack?

A. Hypervisor

B. Hardware security module

C. Trusted platform module

D. Database

93. Steve is concerned that users of his organization's cloud environment may be sending sensitive information over HTTPS connections. What technology would best help him detect this activity?

A. Traffic inspection

B. Port blocking

C. Patching

D. Geofencing

94. Which one of the following disaster recovery approaches is generally the most cost-effective for an organization?

A. Hot site

B. Cloud site

C. Cold site

D. Warm site

95. An essential element of access management, _____ is the practice of confirming that an individual is who they claim to be.

A. Authentication

B. Authorization

C. Nonrepudiation

D. Regression

96. Which one of the following cloud service categories places the most security responsibility with the cloud service provider?

A. SaaS

B. PaaS

C. FaaS

D. IaaS

97. Alice and Bob are using a symmetric encryption algorithm to exchange sensitive information. How many total encryption keys are necessary for this communication?

A. 1

B. 2

C. 3

D. 4

98. Mike and Renee would like to use an asymmetric cryptosystem to communicate with each other. They are located in different parts of the country but have exchanged encryption keys by using digital certificates signed by a mutually trusted certificate authority.

When Mike receives Renee's digital certificate, what key does he use to verify the authenticity of the certificate?

A. Renee's public key

B. Renee's private key

C. CA's public key

D. CA's private key

99. What computing technology, if fully developed, has the potential to undermine the security of modern encryption algorithms?

A. Confidential computing

B. Ephemeral computing

C. Quantum computing

D. Parallel computing

100. What is usually considered the difference between business continuity (BC) efforts and disaster recovery (DR) efforts?

A. BC involves a recovery time objective (RTO), and DR involves a recovery point objective (RPO).

B. BC is for events caused by humans (like arson or theft), whereas DR is for natural disasters.

C. BC is about maintaining critical functions during a disruption of normal operations, and DR is about recovering to normal operations after a disruption.

D. BC involves protecting human assets (personnel, staff, users), whereas DR is about protecting property (assets, data).