

SY0-701^{Q&As}

CompTIA Security+ 2024

Pass CompTIA SY0-701 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/sy0-701.html>

100% Passing Guarantee
100% Money Back Assurance

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

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



QUESTION 1

Which of the following is the most common data loss path for an air-gapped network?

- A. Bastion host
- B. Unsecured Bluetooth
- C. Unpatched OS
- D. Removable devices

Correct Answer: D

An air-gapped network is a network that is physically isolated from other networks, such as the internet, to prevent unauthorized access and data leakage. However, an air-gapped network can still be compromised by removable devices, such as USB drives, CDs, DVDs, or external hard drives, that are used to transfer data between the air-gapped network and other networks. Removable devices can carry malware, spyware, or other malicious code that can infect the air-gapped network or exfiltrate data from it. Therefore, removable devices are the most common data loss path for an air-gapped network.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 9: Network Security, page 449 1

QUESTION 2

A bank insists all of its vendors must prevent data loss on stolen laptops. Which of the following strategies is the bank requiring?

- A. Encryption at rest
- B. Masking
- C. Data classification
- D. Permission restrictions

Correct Answer: A

Encryption at rest is a strategy that protects data stored on a device, such as a laptop, by converting it into an unreadable format that can only be accessed with a decryption key or password. Encryption at rest can prevent data loss on stolen laptops by preventing unauthorized access to the data, even if the device is physically compromised. Encryption at rest can also help comply with data privacy regulations and standards that require data protection. Masking, data classification, and permission restrictions are other strategies that can help protect data, but they may not be sufficient or applicable for data stored on laptops. Masking is a technique that obscures sensitive data elements, such as credit card numbers, with random characters or symbols, but it is usually used for data in transit or in use, not at rest. Data classification is a process that assigns labels to data based on its sensitivity and business impact, but it does not protect the data itself. Permission restrictions are rules that define who can access, modify, or delete data, but they may not prevent unauthorized access if the laptop is stolen and the security controls are bypassed.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 17-18, 372-373

QUESTION 3

A company is planning a disaster recovery site and needs to ensure that a single natural disaster would not result in the complete loss of regulated backup data. Which of the following should the company consider?

- A. Geographic dispersion
- B. Platform diversity
- C. Hot site
- D. Load balancing

Correct Answer: A

Geographic dispersion is the practice of having backup data stored in different locations that are far enough apart to minimize the risk of a single natural disaster affecting both sites. This ensures that the company can recover its regulated data in case of a disaster at the primary site. Platform diversity, hot site, and load balancing are not directly related to the protection of backup data from natural disasters. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 449; Disaster Recovery Planning: Geographic Diversity

QUESTION 4

A client asked a security company to provide a document outlining the project, the cost, and the completion time frame. Which of the following documents should the company provide to the client?

- A. MSA
- B. SLA
- C. BPA
- D. SOW

Correct Answer: D

An ISOW is a document that outlines the project, the cost, and the completion time frame for a security company to provide a service to a client. ISOW stands for Information Security Operations Work, and it is a type of contract that specifies the scope, deliverables, milestones, and payment terms of a security project. An ISOW is usually used for one-time or short-term projects that have a clear and defined objective and outcome. For example, an ISOW can be used for a security assessment, a penetration test, a security audit, or a security training. The other options are not correct because they are not documents that outline the project, the cost, and the completion time frame for a security company to provide a service to a client. A MSA is a master service agreement, which is a type of contract that establishes the general terms and conditions for a long-term or ongoing relationship between a security company and a client. A MSA does not specify the details of each individual project, but rather sets the framework for future projects that will be governed by separate statements of work (SOWs). A SLA is a service level agreement, which is a type of contract that defines the quality and performance standards for a security service provided by a security company to a client. A SLA usually includes the metrics, targets, responsibilities, and penalties for measuring and ensuring the service level. A BPA is a business partnership agreement, which is a type of contract that establishes the roles and expectations for a strategic alliance between two or more security companies that collaborate to provide a joint service to a client. A BPA usually covers the objectives, benefits, risks, and obligations of the partnership.

References: CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 387. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 8.2: Compliance and Controls, video: Contracts and Agreements (5:12).

QUESTION 5

A company needs to provide administrative access to internal resources while minimizing the traffic allowed through the security boundary. Which of the following methods is most secure?

- A. Implementing a bastion host
- B. Deploying a perimeter network
- C. Installing a WAF
- D. Utilizing single sign-on

Correct Answer: A

A bastion host is a special-purpose server that is designed to withstand attacks and provide secure access to internal resources. A bastion host is usually placed on the edge of a network, acting as a gateway or proxy to the internal network. A bastion host can be configured to allow only certain types of traffic, such as SSH or HTTP, and block all other traffic. A bastion host can also run security software such as firewalls, intrusion detection systems, and antivirus programs to monitor and filter incoming and outgoing traffic. A bastion host can provide administrative access to internal resources by requiring strong authentication and encryption, and by logging all activities for auditing purposes¹². A bastion host is the most secure method among the given options because it minimizes the traffic allowed through the security boundary and provides a single point of control and defense. A bastion host can also isolate the internal network from direct exposure to the internet or other untrusted networks, reducing the attack surface and the risk of compromise³. Deploying a perimeter network is not the correct answer, because a perimeter network is a network segment that separates the internal network from the external network. A perimeter network usually hosts public-facing services such as web servers, email servers, or DNS servers that need to be accessible from the internet. A perimeter network does not provide administrative access to internal resources, but rather protects them from unauthorized access. A perimeter network can also increase the complexity and cost of network management and security⁴. Installing a WAF is not the correct answer, because a WAF is a security tool that protects web applications from common web-based attacks by monitoring, filtering, and blocking HTTP traffic. A WAF can prevent attacks such as cross-site scripting, SQL injection, or file inclusion, among others. A WAF does not provide administrative access to internal resources, but rather protects them from web application vulnerabilities. A WAF is also not a comprehensive solution for network security, as it only operates at the application layer and does not protect against other types of attacks or threats⁵. Utilizing single sign-on is not the correct answer, because single sign-on is a method of authentication that allows users to access multiple sites, services, or applications with one username and password. Single sign-on can simplify the sign-in process for users and reduce the number of passwords they have to remember and manage. Single sign-on does not provide administrative access to internal resources, but rather enables access to various resources that the user is authorized to use. Single sign-on can also introduce security risks if the user's credentials are compromised or if the single sign-on provider is breached⁶.

References: 1: Bastion host - Wikipedia, 2: 14 Best Practices to Secure SSH Bastion Host - goteleport.com, 3: The Importance Of Bastion Hosts In Network Security, 4: What is the network perimeter? | Cloudflare, 5: What is a WAF? | Web Application Firewall explained, 6: [What is single sign-on (SSO)? - Definition from WhatIs.com]

[SY0-701 PDF Dumps](#)

[SY0-701 Practice Test](#)

[SY0-701 Braindumps](#)