

# SY0-701<sup>Q&As</sup>

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

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 2

A company is developing a critical system for the government and storing project information on a fileshare. Which of the following describes how this data will most likely be classified? (Select two).

- A. Private
- B. Confidential
- C. Public
- D. Operational
- E. Urgent
- F. Restricted

Correct Answer: BF

Data classification is the process of assigning labels to data based on its sensitivity and business impact. Different organizations and sectors may have different data classification schemes, but a common one is the following1:

Public: Data that can be freely disclosed to anyone without any harm or risk. Private: Data that is intended for internal use only and may cause some harm or risk if disclosed.

Confidential: Data that is intended for authorized use only and may cause significant harm or risk if disclosed.

Restricted: Data that is intended for very limited use only and may cause severe harm or risk if disclosed.

In this scenario, the company is developing a critical system for the government and storing project information on a fileshare. This data is likely to be classified as confidential and restricted, because it is not meant for public or private use,

and it may cause serious damage to national security or public safety if disclosed. The government may also have specific requirements or regulations for handling such data, such as encryption, access control, and auditing.

References: 1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17 2: Data Classification Practices: Final Project Description Released

---

### QUESTION 3

Several universities are participating in a collaborative research project and need to share compute and storage resources. Which of the following cloud deployment strategies would BEST meet this need?

- A. Community
- B. Private
- C. Public
- D. Hybrid

Correct Answer: A

Community cloud storage is a variation of the private cloud storage model, which offers cloud solutions for specific businesses or communities. In this model, cloud storage providers offer their cloud architecture, software and other development tools to meet the requirements of the community. A community cloud in computing is a collaborative effort in which infrastructure is shared between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally.

---

### QUESTION 4

An employee receives a text message from an unknown number claiming to be the company's Chief Executive Officer and asking the employee to purchase several gift cards. Which of the following types of attacks does this describe?

- A. Vishing
- B. Smishing
- C. Pretexting
- D. Phishing

Correct Answer: B

Smishing is a type of phishing attack that uses text messages or common messaging apps to trick victims into clicking on malicious links or providing personal information. The scenario in the question describes a smishing attack that uses pretexting, which is a form of social engineering that involves impersonating someone else to gain trust or access. The unknown number claims to be the company's CEO and asks the employee to purchase gift cards, which is a common scam tactic. Vishing is a similar type of attack that uses phone calls or voicemails, while phishing is a broader term that covers any email-based attack. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 771; Smishing vs. Phishing: Understanding the Differences

### QUESTION 5

Which of the following is the most likely to be used to document risks, responsible parties, and thresholds?

- A. Risk tolerance
- B. Risk transfer
- C. Risk register
- D. Risk analysis

Correct Answer: C

A risk register is a document that records and tracks the risks associated with a project, system, or organization. A risk register typically includes information such as the risk description, the risk owner, the risk probability, the risk impact, the risk level, the risk response strategy, and the risk status. A risk register can help identify, assess, prioritize, monitor, and control risks, as well as communicate them to relevant stakeholders. A risk register can also help document the risk tolerance and thresholds of an organization, which are the acceptable levels of risk exposure and the criteria for escalating or mitigating risks.

References: CompTIA Security+ Certification Exam Objectives, Domain 5.1: Explain the importance of policies, plans, and procedures related to organizational security. CompTIA Security+ Study Guide (SY0-701), Chapter 5: Governance, Risk, and Compliance, page 211. CompTIA Security+ Certification Guide, Chapter 2: Risk Management, page 33. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 4.

---

### QUESTION 6

After an audit, an administrator discovers all users have access to confidential data on a file server. Which of the following should the administrator use to restrict access to the data quickly?

- A. Group Policy
- B. Content filtering
- C. Data loss prevention
- D. Access control lists

Correct Answer: D

Access control lists (ACLs) are rules that specify which users or groups can access which resources on a file server. They can help restrict access to confidential data by granting or denying permissions based on the identity or role of the user. In this case, the administrator can use ACLs to quickly modify the access rights of the users and prevent them from accessing the data they are not authorized to see.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308 1

---

### QUESTION 7

Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?

- A. Compensating control
- B. Network segmentation
- C. Transfer of risk
- D. SNMP traps

Correct Answer: A

A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or a weakness that cannot be resolved by the primary control. A compensating control does not prevent or eliminate the vulnerability or weakness, but it can reduce the likelihood or impact of an attack. A host-based firewall on a legacy Linux system that allows connections from only specific internal IP addresses is an example of a compensating control, as it can limit the exposure of the system to potential threats from external or unauthorized sources. A host-based firewall is a software application that monitors and filters the incoming and outgoing network traffic on a single host, based on a set of rules or policies. A legacy Linux system is an older version of the Linux operating system that may not be compatible with the latest security updates or patches, and may have known vulnerabilities or weaknesses that could be exploited by attackers.

References: Security Controls -SY0-601 CompTIA Security+ : 5.1, Security Controls -CompTIA Security+ SY0-501 -5.7, CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 240. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

---

## QUESTION 8

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 9**

After a recent vulnerability scan, a security engineer needs to harden the routers within the corporate network. Which of the following is the most appropriate to disable?

- A. Console access
- B. Routing protocols
- C. VLANs
- D. Web-based administration

Correct Answer: D

Web-based administration is a feature that allows users to configure and manage routers through a web browser interface. While this feature can provide convenience and ease of use, it can also pose a security risk, especially if the web interface is exposed to the internet or uses weak authentication or encryption methods. Web-based administration can be exploited by attackers to gain unauthorized access to the router's settings, firmware, or data, or to launch attacks such as cross-site scripting (XSS) or cross-site request forgery (CSRF). Therefore, disabling web-based administration is a good practice to harden the routers within the corporate network. Console access, routing protocols, and VLANs are other features that can be configured on routers, but they are not the most appropriate to disable for hardening purposes. Console access is a physical connection to the router that requires direct access to the device, which can be secured by locking the router in a cabinet or using a strong password. Routing protocols are essential for routers to exchange routing information and maintain network connectivity, and they can be secured by using authentication or encryption mechanisms. VLANs are logical segments of a network that can enhance network performance and security by isolating traffic and devices, and they can be secured by using VLAN access control lists (VACLs) or private VLANs (PVLANS).

References: CCNA SEC: Router Hardening Your Router's Security Stinks: Here's How to Fix It

**QUESTION 10**

Several users have opened tickets with the help desk. The help desk has reassigned the tickets to a security analyst for further review. The security analyst reviews the following metrics:

Hostname	Normal CPU utilization %	Current CPU utilization %	Normal network connections	Current network connections
Accounting-PC	22%	48%	12	66
HR-PC	35%	55%	15	57
IT-PC	78%	98%	25	92
Sales-PC	28%	50%	20	56
Manager-PC	21%	44%	18	49

Which of the following is MOST likely the result of the security analyst's review?

- A. The ISP is dropping outbound connections
- B. The user of the Sales-PC fell for a phishing attack
- C. Corporate PCs have been turned into a botnet
- D. An on-path attack is taking place between PCs and the router

Correct Answer: C

The metrics show a significant increase in both CPU utilization and network connections for all the listed PCs compared to their normal values. This could indicate that the machines are being used for unauthorized activities. The current CPU utilization of all the PCs is significantly higher than the normal CPU utilization. This indicates that the PCs are running a lot of processes, which is a common symptom of a botnet infection. The number of current network connections for all the PCs is also significantly higher than the normal number of network connections. This is another common symptom of a botnet infection. A botnet is a network of computers that have been infected with malware and controlled by a remote attacker. The attacker can use the botnet to carry out a variety of malicious activities, such as sending spam, launching DDoS attacks, or stealing data.

---

#### QUESTION 11

Which of the following methods to secure credit card data is best to use when a requirement is to see only the last four numbers on a credit card?

- A. Encryption
- B. Hashing
- C. Masking
- D. Tokenization

Correct Answer: C

Masking is a method to secure credit card data that involves replacing some or all of the digits with symbols, such as asterisks, dashes, or Xs, while leaving some of the original digits visible. Masking is best to use when a requirement is to see only the last four numbers on a credit card, as it can prevent unauthorized access to the full card number, while still allowing identification and verification of the cardholder. Masking does not alter the original data, unlike encryption, hashing, or tokenization, which use algorithms to transform the data into different formats.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2: Compliance and Operational Security, page 721. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 2: Compliance and Operational Security, page 722.

---

#### QUESTION 12

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 13

Which of the following would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed?

- A. A full inventory of all hardware and software
- B. Documentation of system classifications
- C. A list of system owners and their departments
- D. Third-party risk assessment documentation

Correct Answer: A

A full inventory of all hardware and software is essential for measuring the overall risk to an organization when a new vulnerability is disclosed, because it allows the security analyst to identify which systems are affected by the vulnerability and prioritize the remediation efforts. Without a full inventory, the security analyst may miss some vulnerable systems or waste time and resources on irrelevant ones. Documentation of system classifications, a list of system owners and their departments, and third-party risk assessment documentation are all useful for risk management, but they are not sufficient to measure the impact of a new vulnerability. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1221; Risk Assessment and Analysis Methods: Qualitative and Quantitative3

---

### QUESTION 14

Which of the following vulnerabilities is exploited when an attacker overwrites a register with a malicious address?

- A. VM escape
- B. SQL injection
- C. Buffer overflow
- D. Race condition

Correct Answer: C

A buffer overflow is a vulnerability that occurs when an application writes more data to a memory buffer than it can hold, causing the excess data to overwrite adjacent memory locations. A register is a small storage area in the CPU that holds temporary data or instructions. An attacker can exploit a buffer overflow to overwrite a register with a malicious address that points to a shellcode, which is a piece of code that gives the attacker control over the system. By doing so, the attacker can bypass the normal execution flow of the application and execute arbitrary commands.

References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 2: Threats, Attacks, and Vulnerabilities, Section 2.3: Application Attacks, Page 76 1; Buffer Overflows - CompTIA Security+ SY0-701 - 2.3 2

---

**QUESTION 15**

A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team. Which of the following best describes the threat actor in the CISO's report?

- A. Insider threat
- B. Hactivist
- C. Nation-state
- D. Organized crime

Correct Answer: D

Ransomware-as-a-service is a type of cybercrime where hackers sell or rent ransomware tools or services to other criminals who use them to launch attacks and extort money from victims. This is a typical example of organized crime, which is a group of criminals who work together to conduct illegal activities for profit. Organized crime is different from other types of threat actors, such as insider threats, hactivists, or nation-states, who may have different motives, methods, or targets.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 17 1

[Latest SY0-701 Dumps](#)

[SY0-701 VCE Dumps](#)

[SY0-701 Exam Questions](#)