RC0-C02$^{\text{Q\&As}}$

CompTIA Advanced Security Practitioner (CASP) Recertification Exam for Continuing Education

QUESTION 1

Joe, the Chief Executive Officer (CEO), was an Information security professor and a Subject Matter Expert for over 20 years. He has designed a network defense method which he says is significantly better than prominent international standards. He has recommended that the company use his cryptographic method. Which of the following methodologies should be adopted?

A. The company should develop an in-house solution and keep the algorithm a secret.

B. The company should use the CEO\\'s encryption scheme.

C. The company should use a mixture of both systems to meet minimum standards.

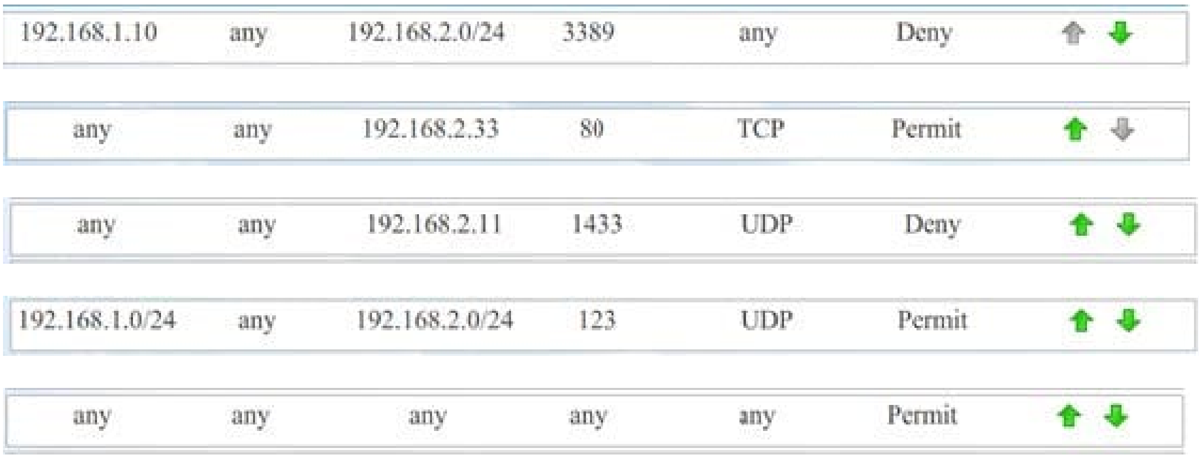
D. The company should use the method recommended by other respected information security organizations.

Correct Answer: D

In this question, we have one person\\'s opinion about the best way to secure the network. His method may be more secure than other systems. However, for consensus of opinion, it is better to use the method recommended by other respected information security organizations. If the CEO\\'s methods were the best methods, it is likely that the other respected information security organizations would have thought about them and would be using them. In other words, the methods recommended by other respected information security organizations are probably the best methods. Furthermore, if the company\\'s systems need to communicate with external systems, the systems will need to use a `standard\\' method otherwise the external system may not be able to decipher the communications from the company\\'s systems.

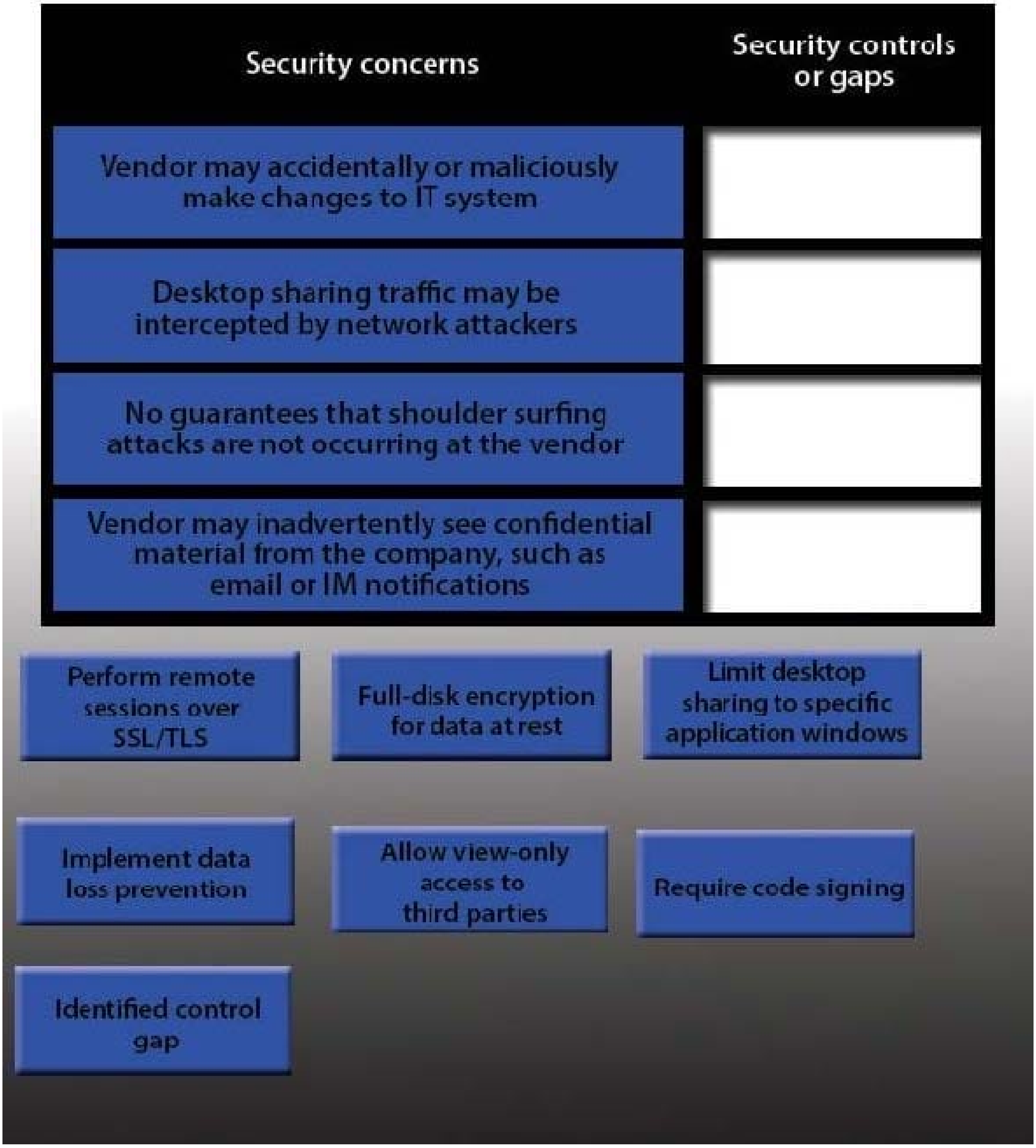
QUESTION 2

IT staff within a company often conduct remote desktop sharing sessions with vendors to troubleshoot vendor product-related issues. Drag and drop the following security controls to match the associated security concern. Options may be used once or not at all.



192.168.1.10	any	192.168.2.0/24	3389	any	Deny	⬆ ⬇
any	any	192.168.2.33	80	TCP	Permit	⬆ ⬇
any	any	192.168.2.11	1433	UDP	Deny	⬆ ⬇
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	⬆ ⬇
any	any	any	any	any	Permit	⬆ ⬇

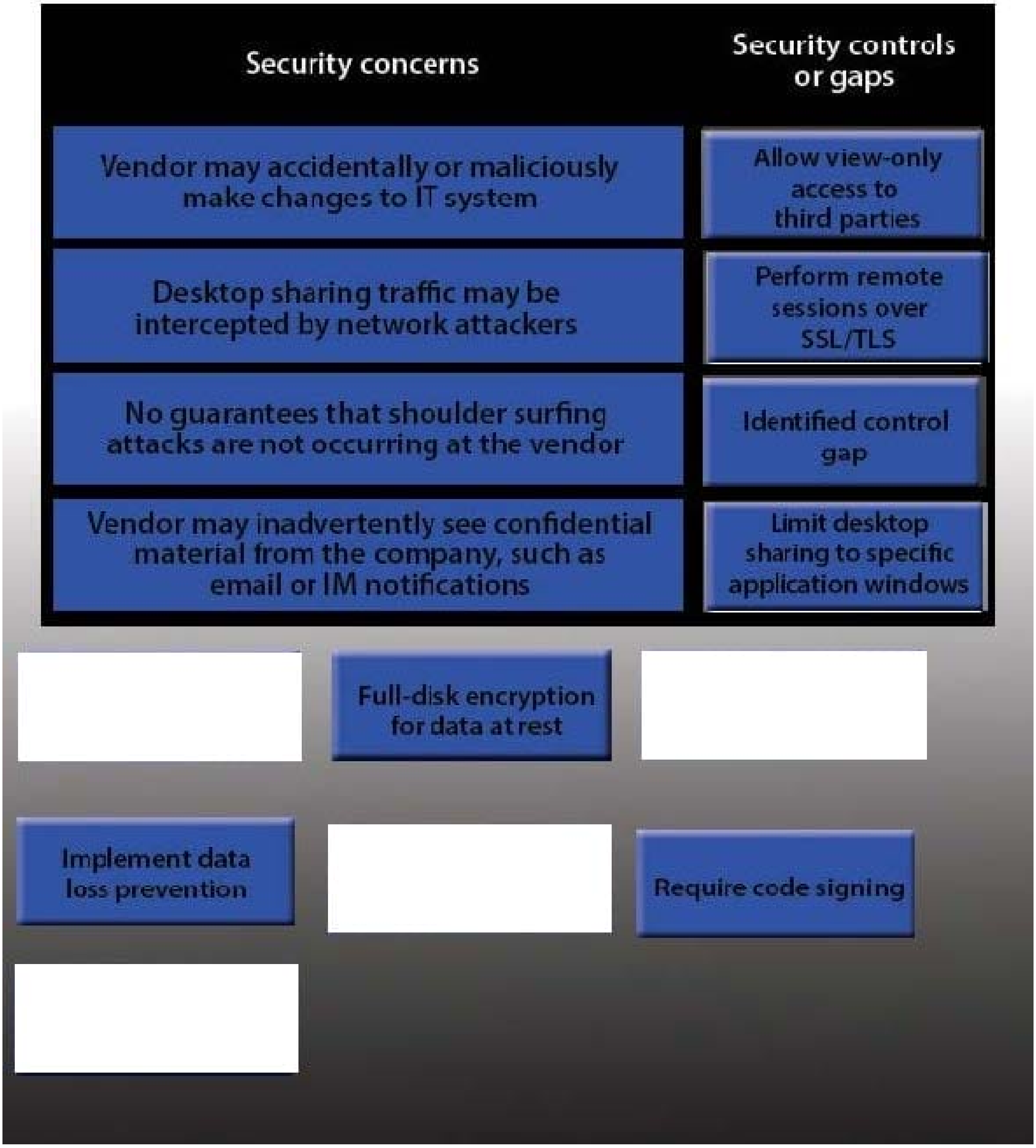
Select and Place:



Security concerns	Security controls or gaps
Vendor may accidentally or maliciously make changes to IT system	
Desktop sharing traffic may be intercepted by network attackers	
No guarantees that shoulder surfing attacks are not occurring at the vendor	
Vendor may inadvertently see confidential material from the company, such as email or IM notifications	

- Perform remote sessions over SSL/TLS
- Full-disk encryption for data at rest
- Limit desktop sharing to specific application windows
- Implement data loss prevention
- Allow view-only access to third parties
- Require code signing
- Identified control gap

Correct Answer:



Security concerns	Security controls or gaps
Vendor may accidentally or maliciously make changes to IT system	Allow view-only access to third parties
Desktop sharing traffic may be intercepted by network attackers	Perform remote sessions over SSL/TLS
No guarantees that shoulder surfing attacks are not occurring at the vendor	Identified control gap
Vendor may inadvertently see confidential material from the company, such as email or IM notifications	Limit desktop sharing to specific application windows

Full-disk encryption for data at rest

Implement data loss prevention

Require code signing

Vendor may accidentally or maliciously make changes to the IT system Allow view-only access.

With view-only access, the third party can view the desktop but cannot interact with it. In other words, they cannot control the keyboard or mouse to make any changes.

Desktop sharing traffic may be intercepted by network attackers Use SSL for remote sessions.

SSL (Secure Sockets Layer) encrypts data in transit between computers. If an attacker intercepted the traffic, the data would be encrypted and therefore unreadable to the attacker.

No guarantees that shoulder surfing attacks are not occurring at the vendor Identified control gap.

Shoulder surfing is where someone else gains information by looking at your computer screen. This should be identified as a risk. A control gap occurs when there are either insufficient or no actions taken to avoid or mitigate a significant risk.

Vendor may inadvertently see confidential material from the company such as email and IMs Limit desktop session to certain windows.

The easiest way to prevent a third party from viewing your emails and IMs is to close the email and IM application windows for the duration of the desktop sharing session.

QUESTION 3

After reviewing a company\\'s NAS configuration and file system access logs, the auditor is advising the security administrator to implement additional security controls on the NFS export. The security administrator decides to remove the no_root_squash directive from the export and add the nosuid directive. Which of the following is true about the security controls implemented by the security administrator?

A. The newly implemented security controls are in place to ensure that NFS encryption can only be controlled by the root user.

B. Removing the no_root_squash directive grants the root user remote NFS read/write access to important files owned by root on the NAS.

C. Users with root access on remote NFS client computers can always use the SU command to modify other user\\'s files on the NAS.

D. Adding the nosuid directive disables regular users from accessing files owned by the root user over NFS even after using the SU command.

Correct Answer: C

If a user has root access, the user can log in with a non-root access account and then use the SU (Switch User) command to perform functions that require root access such as modifying other user\\'s files on the NAS.

By default, NFS shares change the root user to the nfsnobody user, an unprivileged user account. In this way, all root-created files are owned by nfsnobody, which prevents uploading of programs with the setuid bit set. If no_root_squash is

used, remote root users are able to change any file on the shared file system and leave trojaned applications for other users to inadvertently execute.

Some unix programs are called "suid" programs: They set the id of the person running them to whomever is the owner of the file. If a file is owned by root and is suid, then the program will execute as root, so that they can perform operations

that only root is allowed to do. Using the nosuid option is a good idea and you should consider using this with all NFS mounted disks. It means that the server\\'s root user cannot make a suid-root program on the file system, log in to the client

as a normal user and then use the suid-root program to become root on the client too.

QUESTION 4

A well-known retailer has experienced a massive credit card breach. The retailer had gone through an audit and had been presented with a potential problem on their network. Vendors were authenticating directly to the retailer\\'s AD servers, and an improper firewall rule allowed pivoting from the AD server to the DMZ where credit card servers were kept. The firewall rule was needed for an internal application that was developed, which presents risk. The retailer determined that because the vendors were required to have site to site VPN\\'s no other security action was taken.

To prove to the retailer the monetary value of this risk, which of the following type of calculations is needed?

A. Residual Risk calculation

B. A cost/benefit analysis

C. Quantitative Risk Analysis

D. Qualitative Risk Analysis

Correct Answer: C

Performing quantitative risk analysis focuses on assessing the probability of risk with a metric measurement which is usually a numerical value based on money or time.

QUESTION 5

Which of the following technologies prevents an unauthorized HBA from viewing iSCSI target information?

A. Deduplication

B. Data snapshots

C. LUN masking

D. Storage multipaths

Correct Answer: C

A logical unit number (LUN) is a unique identifier that designates individual hard disk devices or grouped devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the management of block storage arrays shared over a storage area network (SAN).

LUN masking subdivides access to a given port. Then, even if several LUNs are accessed through the same port, the server masks can be set to limit each server\\'s access to the appropriate LUNs. LUN masking is typically conducted at the host bus adapter (HBA) or switch level.

RC0-C02 PDF Dumps RC0-C02 VCE Dumps RC0-C02 Practice Test