CAS-002Q&As

CompTIA Advanced Security Practitioner Exam

Pass CompTIA CAS-002 Exam with 100% Guarantee

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

https://www.pass2lead.com/cas-002.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 team is established to create a secure connection between software packages in order to list employee\\'s remaining or unused benefits on their paycheck stubs. Which of the following business roles would be MOST effective on this team?

A. Network Administrator, Database Administrator, Programmers

B. Network Administrator, Emergency Response Team, Human Resources

C. Finance Officer, Human Resources, Security Administrator

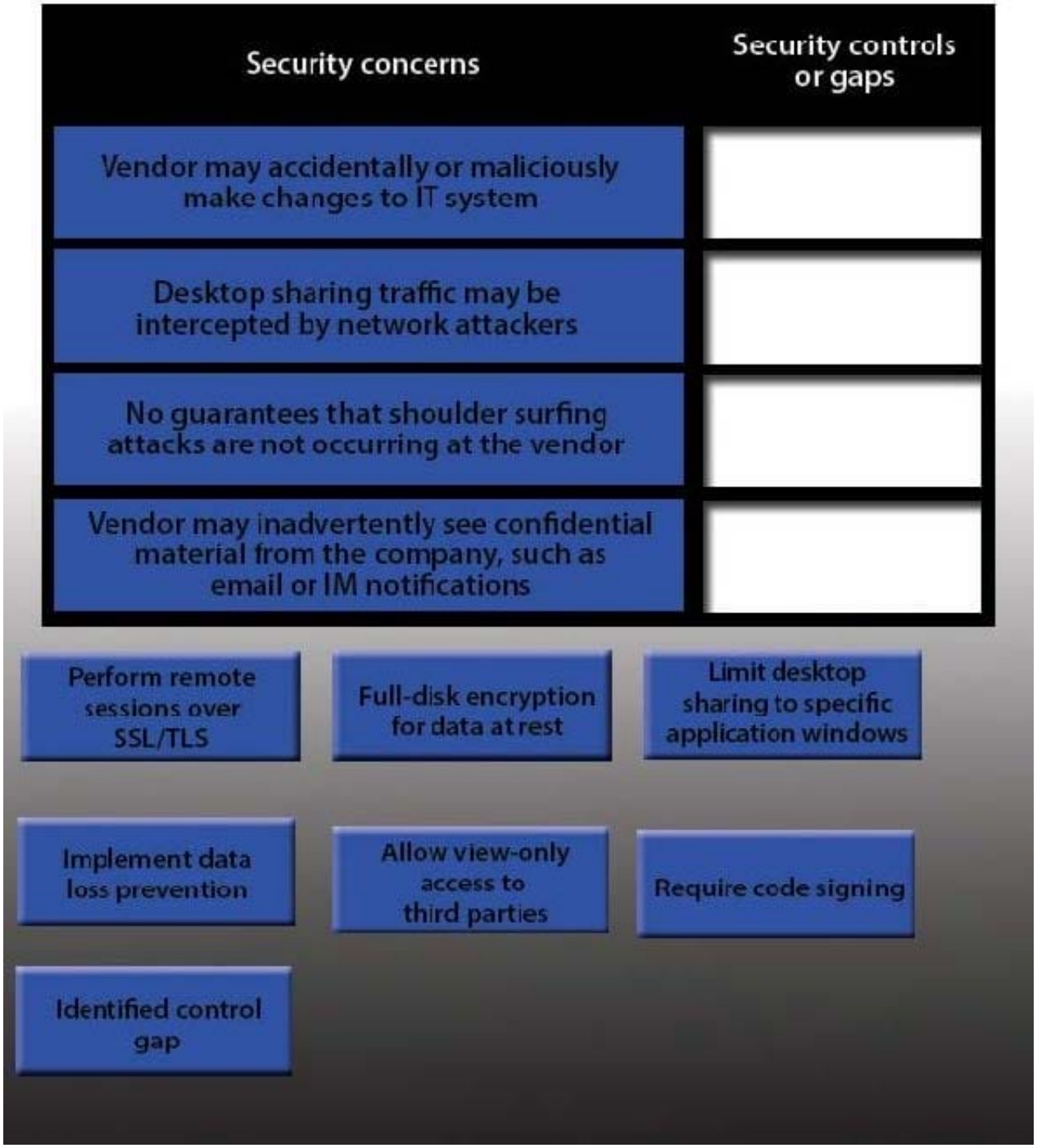
D. Database Administrator, Facilities Manager, Physical Security Manager

Correct Answer: C

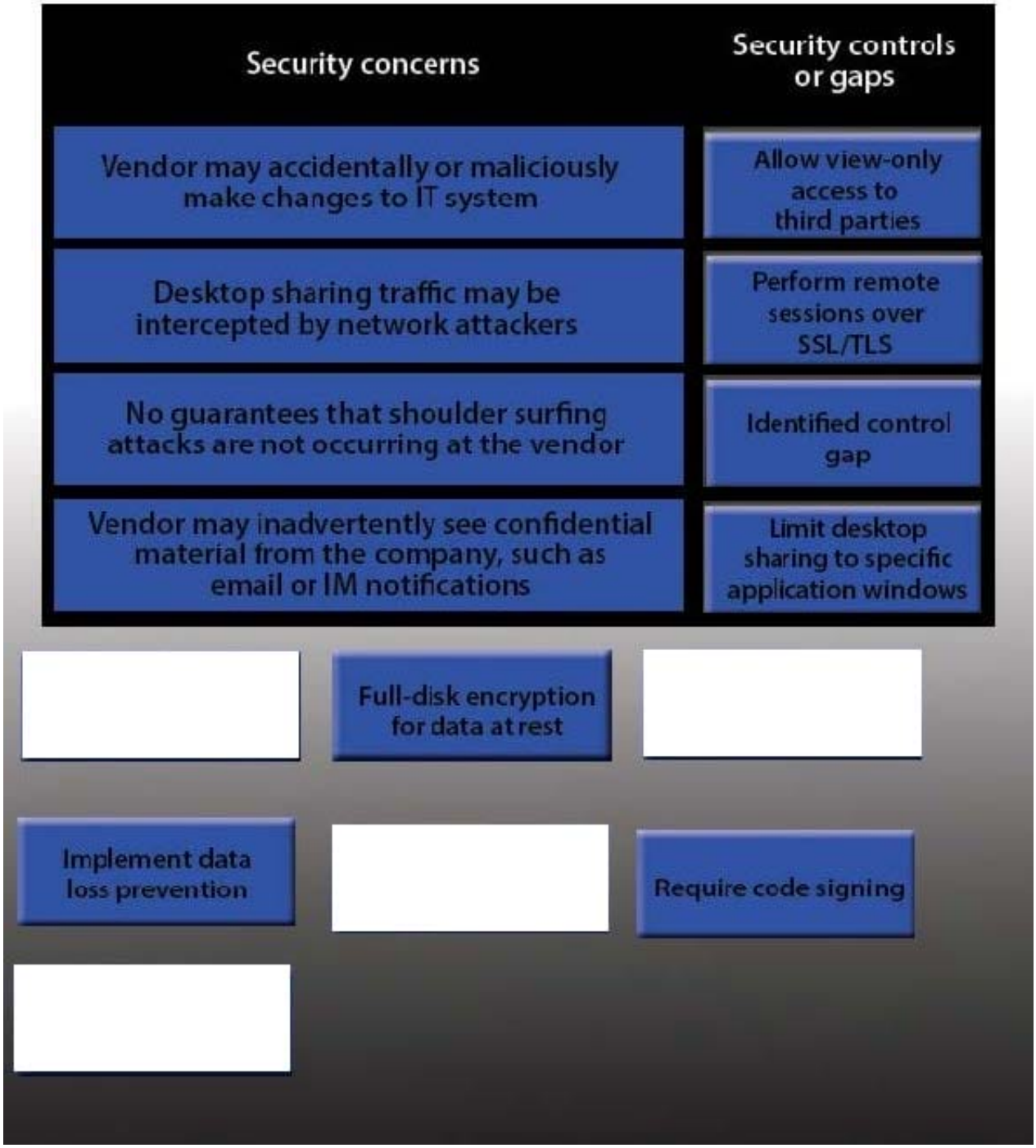
QUESTION 2

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.

Select and Place:



Correct Answer:



QUESTION 3

An investigator wants to collect the most volatile data first in an incident to preserve the data that runs the highest risk of being lost. After memory, which of the following BEST represents the remaining order of volatility that the investigator should follow?

A. File system information, swap files, network processes, system processes and raw disk blocks.

B. Raw disk blocks, network processes, system processes, swap files and file system information.

C. System processes, network processes, file system information, swap files and raw disk blocks.

D. Raw disk blocks, swap files, network processes, system processes, and file system information.

Correct Answer: C

QUESTION 4

An external penetration tester compromised one of the client organization\\'s authentication servers and retrieved the password database. Which of the following methods allows the penetration tester to MOST efficiently use any obtained administrative credentials on the client organization\\'s other systems, without impacting the integrity of any of the systems?

A. Use the pass the hash technique

B. Use rainbow tables to crack the passwords

C. Use the existing access to change the password

D. Use social engineering to obtain the actual password

Correct Answer: A

QUESTION 5

Which of the following is true about an unauthenticated SAMLv2 transaction?

A. The browser asks the SP for a resource. The SP provides the browser with an XHTML format. The browser asks the IdP to validate the user, and then provides the XHTML back to the SP for access.

B. The browser asks the IdP for a resource. The IdP provides the browser with an XHTML format. The browser asks the SP to validate the user, and then provides the XHTML to the IdP for access.

C. The browser asks the IdP to validate the user. The IdP sends an XHTML form to the SP and a cookie to the browser. The browser asks for a resource to the SP, which verifies the cookie and XHTML format for access.

D. The browser asks the SP to validate the user. The SP sends an XHTML form to the IdP. The IdP provides the XHTML form back to the SP, and then the browser asks the SP for a resource.

Correct Answer: A