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

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

Pass CompTIA RC0-C02 Exam with 100% Guarantee

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

QUESTION 1

Ann is testing the robustness of a marketing website through an intercepting proxy. She has intercepted the following HTTP request:

POST /login.aspx HTTP/1.1

Host: comptia.org

Content-type: text/html

txtUsername=annandtxtPassword=annandalreadyLoggedIn=falseandsubmit=true

Which of the following should Ann perform to test whether the website is susceptible to a simple authentication bypass?

A. Remove all of the post data and change the request to /login.aspx from POST to GET

B. Attempt to brute force all usernames and passwords using a password cracker

C. Remove the txtPassword post data and change alreadyLoggedIn from false to true

D. Remove the txtUsername and txtPassword post data and toggle submit from true to false

Correct Answer: C

The text "txtUsername=annandtxtPassword=ann" is an attempted login using a username of `ann\\' and also a password of `ann\\'.

The text "alreadyLoggedIn=false" is saying that Ann is not already logged in. To test whether we can bypass the authentication, we can attempt the login without the password and we can see if we can bypass the `alreadyloggedin\\' check by

changing alreadyLoggedIn from false to true. If we are able to log in, then we have bypassed the authentication check.

QUESTION 2

A security manager has received the following email from the Chief Financial Officer (CFO):

"While I am concerned about the security of the proprietary financial data in our ERP application, we have had a lot of turnover in the accounting group and I am having a difficult time meeting our monthly performance targets. As things

currently stand, we do not allow employees to work from home but this is something I am willing to allow so we can get back on track. What should we do first to securely enable this capability for my group?"

Based on the information provided, which of the following would be the MOST appropriate response to the CFO?

A. Remote access to the ERP tool introduces additional security vulnerabilities and should not be allowed.

B. Allow VNC access to corporate desktops from personal computers for the users working from home.

C. Allow terminal services access from personal computers after the CFO provides a list of the users working from home.

D. Work with the executive management team to revise policies before allowing any remote access.

Correct Answer: D

The Chief Financial Officer (CFO) wants to change company policy to allow employees to work from home. Before the new policy is implemented, the relevant documented company policies should be updated to reflect the new policy. Company policies are rarely defined by a single person in a company; they are usually defined by executive management. Therefore, you should work with the executive management team to revise the policies.

QUESTION 3

A company receives an e-discovery request for the Chief Information Officer\\'s (CIO\\'s) email data. The storage administrator reports that the data retention policy relevant to their industry only requires one year of email data. However the storage administrator also reports that there are three years of email data on the server and five years of email data on backup tapes. How many years of data MUST the company legally provide?

A. 1

B. 2

C. 3

D. 5

Correct Answer: D

QUESTION 4

A manufacturer is planning to build a segregated network. There are requirements to segregate development and test infrastructure from production and the need to support multiple entry points into the network depending on the service

being accessed. There are also strict rules in place to only permit user access from within the same zone. Currently, the following access requirements have been identified:

Developers have the ability to perform technical validation of development applications.

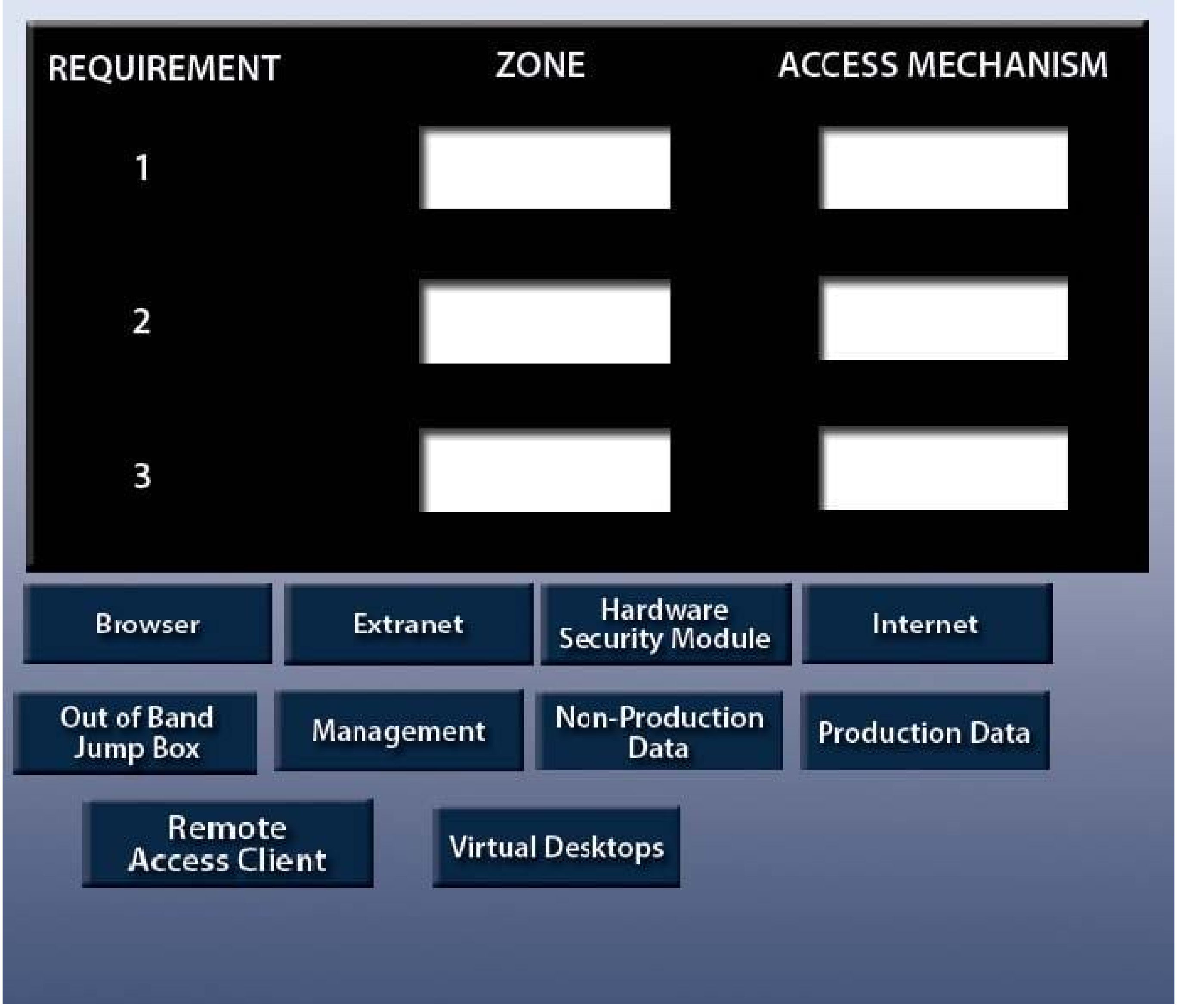
End users have the ability to access internal web applications.

Third-party vendors have the ability to support applications.

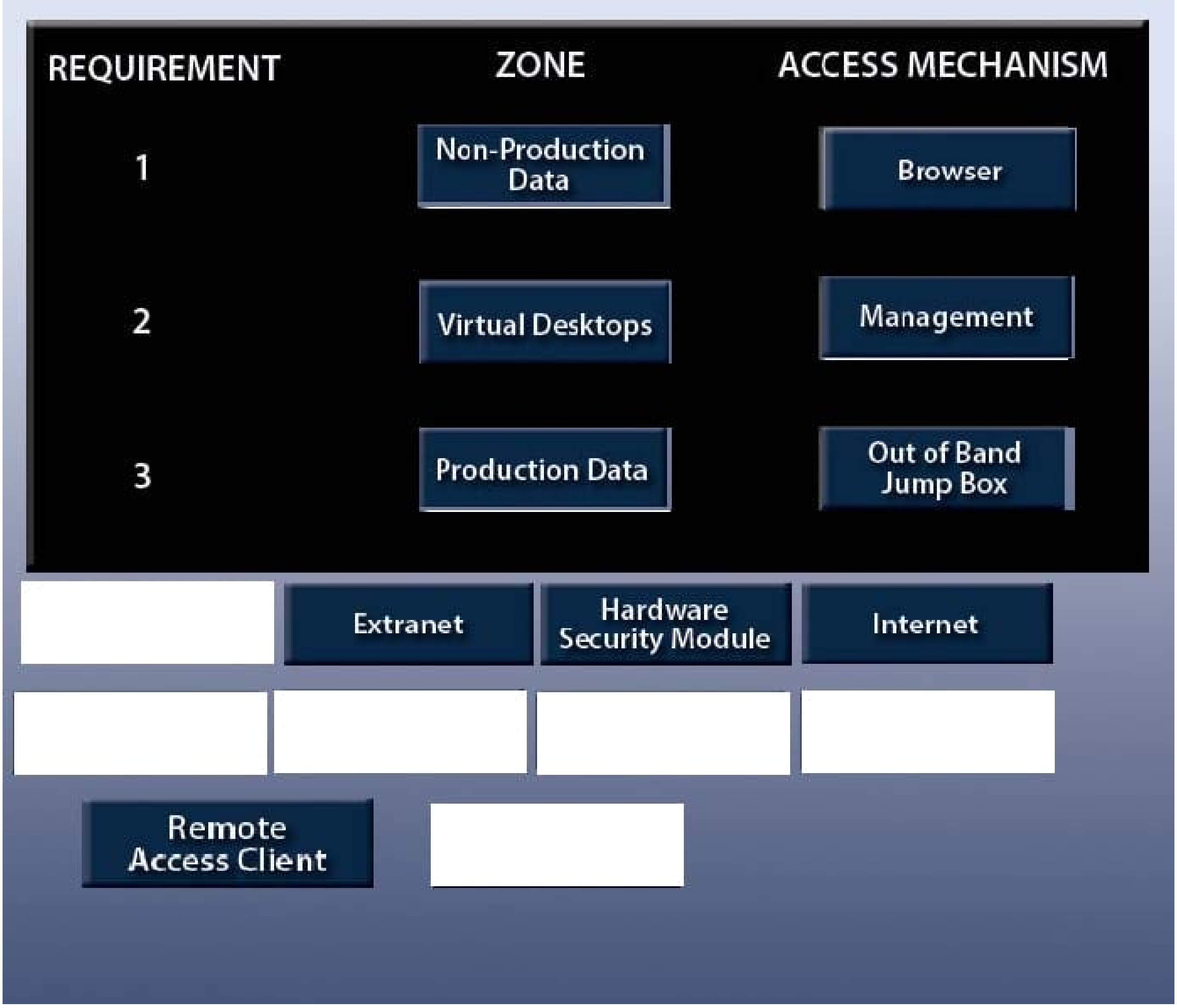
In order to meet segregation and access requirements, drag and drop the appropriate network zone that the user would be accessing and the access mechanism to meet the above criteria. Options may be used once or not at all. All

placeholders must be filled.

Select and Place:



Correct Answer:



QUESTION 5

A security policy states that all applications on the network must have a password length of eight characters. There are three legacy applications on the network that cannot meet this policy. One system will be upgraded in six months, and two are not expected to be upgraded or removed from the network. Which of the following processes should be followed?

A. Establish a risk matrix

B. Inherit the risk for six months

C. Provide a business justification to avoid the risk

D. Provide a business justification for a risk exception

Correct Answer: D

The Exception Request must include:

A description of the non-compliance.

The anticipated length of non-compliance (2-year maximum). The proposed assessment of risk associated with non-compliance. The proposed plan for managing the risk associated with non-compliance. The proposed metrics for evaluating

the success of risk management (if risk is significant). The proposed review date to evaluate progress toward compliance. An endorsement of the request by the appropriate Information Trustee (VP or Dean).