Calendar

Question 1

Correct

Mark 2.00 out of 2.00

⚑ Flag question

A user is asked to perform a risk analysis of a company. The user asks for the company asset database that contains a list of all equipment.The user uses this information as part of a risk analysis. Which type of risk analysis could be performed?

Select one:

○ exposure factor

○ qualitative

⦿ quantitative   ✔

○ hardware

Refer to curriculum topic: 6.2.1
Physical items can be assigned a value for quantitative analysis.

The correct answer is: quantitative

Question 2

Correct

Mark 2.00 out of 2.00

⚑ Flag question

A user needs to add redundancy to the routers in a company. What are the three options the user can use? (Choose three.)

Select one or more:

☐ RAID

☑ GLBP   ✔

☐ STP

☐ IPFIX

☑ VRRP   ✔

☑ HSRP   ✔

Refer to curriculum topic: 6.2.3
Three protocols that provide default gateway redundancy include VRRP, GLBP, and HSRP.

The correct answers are: HSRP, VRRP, GLBP

Question 3

Correct

Mark 2.00 out of 2.00

⚐ Flag question

A user was hired by a company to provide a highly available network infrastructure. The user wants to build redundancy into the network in case of a switch failure, but wants to prevent Layer 2 looping. What would the user implement in the network?

Select one:

○ HSRP

○ VRRP

○ GLBP

⦿ Spanning Tree Protocol ✓

Refer to curriculum topic: 6.2.3

Loops and duplicate frames cause poor performance in a switched network. The Spanning Tree Protocol (STP) provides a loop-free path through the switch network.

The correct answer is: Spanning Tree Protocol

Question 4

Correct

Mark 2.00 out of 2.00

⚐ Flag question

A user is asked to evaluate the security posture of a company. The user looks at past attempts to break into the company and evaluates the threats and exposures to create a report. Which type of risk analysis could the user perform?

Select one:

⦿ qualitative ✓

○ opinion

○ subjective

○ objective

Refer to curriculum topic: 6.2.1

Two approaches to risk analysis are quantitative and qualitative. Qualitative analysis is based on opinions and scenarios.

The correct answer is: qualitative

Question 5

Correct

Mark 2.00 out of 2.00

⚑ Flag question

A company is concerned with traffic that flows through the network. There is a concern that there may be malware that exists that is not being blocked or eradicated by antivirus. What technology can be put in place to detect potential malware traffic on the network?

Select one:

○ IPS

◉ IDS ✔

○ firewall

○ NAC

Refer to curriculum topic: 6.3.2

A passive system that can analyze traffic is needed to detect malware on the network and send alerts.

The correct answer is: IDS

Question 6

Correct

Mark 2.00 out of 2.00

⚑ Flag question

A user is purchasing a new server for the company data center. The user wants disk striping with parity on three disks. Which RAID level should the user implement?

Select one:

◉ 5 ✔

○ 0

○ 1+0

○ 1

Refer to curriculum topic: 6.2.3

RAID 5 striping with parity would be the best choice.

The correct answer is: 5

Question 7

Correct

Mark 2.00 out of 2.00

⚐ Flag question

A user is evaluating the network infrastructure of a company. The user noted many redundant systems and devices in place, but no overall evaluation of the network. In a report, the user emphasized the methods and configurations needed as a whole to make the network fault tolerant. What is the type of design the user is stressing?

Select one:

⦿ resilient ✔

◯ availability

◯ comprehensive

◯ spanning tree

Refer to curriculum topic: 6.2.4

In order to deploy a resilient design, it is critical to understand the needs of a business and then incorporate redundancy to address those needs.

The correct answer is: resilient

Question 8

Correct

Mark 2.00 out of 2.00

⚐ Flag question

A user was hired as the new security officer. One of the first projects was to take inventory of the company assets and create a comprehensive database. Which three pieces of information would the user want to capture in an asset database? (Choose three.)

Select one or more:

☑ operating systems ✔

☐ groups

☐ passwords

☑ hardware network devices ✔

☐ users

☑ workstations ✔

Refer to curriculum topic: 6.2.1

A security breach has happened at a major corporation. The incident team has responded and executed their incident response plan. During which phase are lessons learned applied?

Select one:

- ○ recovery
- ⦿ post-incident ✔
- ○ analyze
- ○ detection
- ○ containment
- ○ preparation

Refer to curriculum topic: 6.3.1
One of the key aspects of an incident response plan is to look at how monitoring can be improved and management can help minimize the impact on business. This usually occurs after the incident has been handled.

The correct answer is: post-incident

A user is running a routine audit of the server hardware in the company data center. Several servers are using single drives to host operating systems and multiple types of attached storage solutions for storing data. The user wants to offer a better solution to provide fault tolerance during a drive failure. Which solution is best?

Select one:

- ○ offsite backup
- ○ tape backup
- ○ UPS
- ⦿ RAID ✔

Refer to curriculum topic: 6.2.3

Question 11

Correct

Mark 2.00 out of 2.00

⚑ Flag question

A user is a consultant who is hired to prepare a report to Congress as to which industries should be required to maintain five nine availability. Which three industries should the user include in a report? (Choose three.)

Select one or more:

- ☐ food service
- ☑ public safety ✔
- ☐ education
- ☑ healthcare ✔
- ☑ finance ✔
- ☐ retail

Refer to curriculum topic: 6.1.1

Industries that are critical to everyday life like financial, healthcare, and public safety should have systems that are available 99.999% of the time (the five nines principle).

The correct answers are: finance, healthcare, public safety

Question 12

Correct

Mark 2.00 out of 2.00

⚑ Flag question

A team has been asked to create an incident response plan for security incidents. In what phase of an incident response plan does the team get management approval of the plan?

Select one:

- ○ containment
- ○ post-incident
- ⦿ preparation ✔
- ○ analysis
- ○ recovery
- ○ detection

Question 13

Correct

Mark 2.00 out of 2.00

⚑ Flag question

A user is redesigning a network for a small company and wants to ensure security at a reasonable price. The user deploys a new application-aware firewall with intrusion detection capabilities on the ISP connection. The user installs a second firewall to separate the company network from the public network. Additionally, the user installs an IPS on the internal network of the company. What approach is the user implementing?

Select one:

○ attack based

◉ layered ✔

○ risk based

○ structured

Refer to curriculum topic: 6.2.2
Using different defenses at various points of the network creates a layered approach.

The correct answer is: layered

Question 14

Correct

Mark 2.00 out of 2.00

⚑ Flag question

A user has completed a six month project to identify all data locations and catalog the location. The next step is to classify the data and produce some criteria on data sensitivity. Which two steps can the user take to classify the data? (Choose two.)

Select one or more:

☐ Determine how often data is backed up.

☐ Treat all the data the same.

☑ Identify sensitivity of the data. ✔

☐ Determine permissions for the data.

☑ Establish the owner of the data. ✔

☐ Determine the user of the data.

Refer to curriculum topic: 6.2.1
Categorizing data is a process of determining first who owns the data then determining the sensitivity of the data.

Question 15

Correct

Mark 2.00 out of 2.00

⚑ Flag question

A user is asked to evaluate the data center to improve availability for customers. The user notices that there is only one ISP connection, some of the equipment is out of warranty, there are no spare parts, and no one was monitoring the UPS which was tripped twice in one month. Which three deficiencies in high availability has the user identified? (Choose three.)

Select one or more:

- ☐ failure to prevent security incidents
- ☐ failure to protect against poor maintenance
- ☑ failure to design for reliability ✔
- ☑ failure to detect errors as they occur ✔
- ☑ single points of failure ✔
- ☐ failure to identify management issues

Refer to curriculum topic: 6.1.1
A data center needs to be designed from the outset for high availability with no single points of failure.

The correct answers are: single points of failure, failure to detect errors as they occur, failure to design for reliability

---

Question 16

Correct

Mark 2.00 out of 2.00

⚑ Flag question

A user is asked to create a disaster recovery plan for a company. The user needs to have a few questions answered by management to proceed. Which three questions should the user ask management as part of the process of creating the plan? (Choose three.)

Select one or more:

- ☑ Who is responsible for the process ✔
- ☑ Where does the individual perform the process? ✔
- ☐ How long does the process take?
- ☑ What is the process? ✔
- ☐ Can the individual perform the process?
- ☐ Does the process require approval?

Refer to curriculum topic: 6.4.1

Question **17**

Correct

Mark 2.00 out of 2.00

⚐ Flag question

The CEO of a company is concerned that if a data breach should occur and customer data is exposed, the company could be sued. The CEO makes the decision to buy insurance for the company. What type of risk mitigation is the CEO implementing?

Select one:

○ avoidance

○ mitigation

○ reduction

● transference ✔

Refer to curriculum topic: 6.2.1
Buying insurance transfers the risk to a third party.

The correct answer is: transference