**Data Recovery & Backups**

1.Question 1

Question

**What options are available for storing backups, physically?**On-site onlyOff-site onlyBoth on-site and off-siteThere's no need to store physical backups anymore

**Ans:3**

**Correct**

Nice job! You can either backup data to another system located on-site, or the backups can be sent to a remote system off-site. Ideally, these two would be combined to balance efficiency and risk.

2.Question 2

Question

**What are some ways you can make your backups more space-efficient? Check all that apply.**

Use full backups only

Use compression

**Correct**

That's exactly right! Compression reduces the overall size required to store the backup data, making it more efficient. Incremental backups only store the data that's changed, as opposed to all data or files, making it more efficient, too.

Use encryption

Use incremental backups

**Correct**

That's exactly right! Compression reduces the overall size required to store the backup data, making it more efficient. Incremental backups only store the data that's changed, as opposed to all data or files, making it more efficient, too.

**Ans:2,4**

**Correct**

Great, you got all the right answers.

3.Question 3

Question

**Which of these are part of the five primary elements that make up a post-mortem report? Check all that apply.**

A summary

**Correct**

Excellent! The report would include (1) a summary; (2) a detailed timeline of events; (3) an analysis of the root cause; (4) an explanation of steps taken for resolution and recovery; and (5) recommendations to prevent a similar event from occurring again.

Backup procedures

A timeline

**Correct**

Excellent! The report would include (1) a summary; (2) a detailed timeline of events; (3) an analysis of the root cause; (4) an explanation of steps taken for resolution and recovery; and (5) recommendations to prevent a similar event from occurring again.

Resolution and recovery steps

**Correct**

Excellent! The report would include (1) a summary; (2) a detailed timeline of events; (3) an analysis of the root cause; (4) an explanation of steps taken for resolution and recovery; and (5) recommendations to prevent a similar event from occurring again.

A root cause description

**Correct**

Excellent! The report would include (1) a summary; (2) a detailed timeline of events; (3) an analysis of the root cause; (4) an explanation of steps taken for resolution and recovery; and (5) recommendations to prevent a similar event from occurring again.

Recommended future action items

**Correct**

Excellent! The report would include (1) a summary; (2) a detailed timeline of events; (3) an analysis of the root cause; (4) an explanation of steps taken for resolution and recovery; and (5) recommendations to prevent a similar event from occurring again.

**Ans:1,3,4**

**Correct**

Great, you got all the right answers.

4.Question 4

Question

**The unthinkable happens and disaster strikes, crippling your network. You implement your disaster plan, but it doesn't go smoothly. You decide to investigate. What is a commom term in the IT community for this investigation?**After-outage analysisPost-mortemPost-disaster inquiryRecovery inspection probe

**Ans:2**

**Correct**

You nailed it! Imagine that something did go wrong with your systems, and you had to use your disaster plan. A post-mortem is a way for you to document any problems you discovered along the way and how to fix them.

5.Question 5

Question

**What are advantages of on-site backups? Check all that apply.**

Data is more secure because of less outbound traffic.

**Correct**

Well done! The more traffic going out of the network, even for backups, the higher the risk of data being intercepted. On-site backups reduce this vulnerability.

There is less bandwidth usage.

Data is safe in case of disaster.

There is quicker data access.

**Correct**

Well done! One advantage of on-site backup solutions is that the data is physically very close, which makes accessing the data much quicker.

**Ans:1,2,4**

6.Question 6

Question

**What is the standard medium for long-term archival backup data storage?**Optical disksMagnetic tapesFloppy disksUSB drives

**Ans:2**

**Correct**

Right on! Tape storage is slow but cheap, and has become the standard medium for archival backups.

7.Question 7

Question

**Which type of backup only saves the parts of data that have changed within files since the last backup took place?**Incremental backupDifferential backupsComplete backupRAID array

**Ans:1**

**Correct**

Woohoo! An incremental backup is when only the data that’s changed in files is backed up. This is even more efficient in terms of both disk space and time required when compared to differential backups.

8.Question 8

Question

**Cloud services are the ideal backup option for user files. Which of these is not one of today's popular cloud storage platforms?**Apple iCloudDropboxGoogle DriveRsync

**Ans:4**

**Correct**

You got it! Rsync is a command line tool used to compress and transfer files from one computer to another. While it is often used for backup, it's not a cloud service.

9.Question 9

Question

**You are performing a network risk assessment to develop your disaster recovery plan. Which of these are examples of detection measures? Check all that apply.**

Testing your own (and users') knowledge and readiness for disaster

**Correct**

Awesome! Alerts and monitoring are only useful if everyone knows how to respond to them! Make sure you perform regular disaster tests.

Using an alert system for outages

**Correct**

Awesome! If uptime and availability is important for your organization, make sure you have a comprehensive system in place that can quickly detect and alert you to service outages.

Monitoring system testing

**Correct**

Awesome! You absolutely need to test your monitoring and alert systems. Simulate the conditions your monitoring systems are designed to catch. Make sure the detection thresholds actually fire the alerts like they’re supposed to.

Conducting regular, automated backups

**Ans:1,2,3**

**Correct**

Great, you got all the right answers.

10.Question 10

Question

**What are some of the purposes of a post-mortem? Check all that apply.**

To understand the cause of mistakes and how to prevent them

**Correct**

Great work! The intention of a post-mortem is to understand the root cause of why the mistakes happened and how to prevent them from happening again.

To foster a culture where it's OK to make mistakes

To learn from and adapt processes for higher efficiency

**Correct**

Great work! The content in the post-mortem report might trigger a thought for some other team and make them realize they have a similar problem in their infrastructure. You may also identify areas that could be improved that are the responsibility of teams that weren’t involved in the incident.

To shame and punish mistakes

**Ans:1.2.3**