Question 1) Your payroll application writes employee salary information into DynamoDB table. You are getting an error with certain data and would like to verify the entered in the DynamoDB table to confirm that the data written was correct. How can you do this? (Choose 2)

a) By connecting the SQL client to your DynamoDB table and view the data from the table.
b) DynamoDB tables stores data as JSON documents in S3. The S3 documents can be downloaded and verified.
c) By using the AWS Command Line Interface (CLI) tools to query the DynamoDB table's data.
d) By using the DynamoDB exported into CSV.
e) By using the AWS Console to view the DynamoDB table's data.

Question 2) How AWS charges for using VPC?

a) VPC is charges are based on number of internet gateways
b) VPC is charged based on the number of subnet in it
c) VPC is charged based on the number of VPN hours
d) No additional charges for VPC, you pay only for the resources inside the VPC

Question 3) How an EC2 instance running within your VPC can be secured?

a) Using internet gateway
b) Using ACLs
c) Using security groups
d) Using policies

Question 4) True/false. We can perform peering between VPCs of different regions.

a) True
b) False

Question 5) What is the maximum visibility timeout in SQS?

a) 12 hours
b) 30 days
c) 1 day
d) 1 hour

Question 6) Does AWS provide the ability to group SQS messages into batches?

a) Yes
b) No

Question 7) In SQS, there is a possibility to receive a previously received message again?

a) Yes
b) No

Question 8) Does Amazon SWF ensure that a task is assigned only once and is never duplicated?

a) Yes
b) No

Question 9) What is the main difference between SWF and SQS?

a) SWF presents a push based API, and Amazon SQS offers a pull based API
b) Both offer a message oriented API
c) SWF presents a task oriented API and Amazon SQS offers a message oriented API
d) SWF presents a message oriented API and Amazon SQS offers task oriented API

Question 10) The system at your organisation experienced down time. During the troubleshooting process it was found that system administrator mistakenly terminated production EC2 instances. What measures should be taken in order to avoid similar situation in the future?

a) EC2 instances termination should only be authorised by leveraging EC2 termination protection and MFA
b) Create an IAM user and apply an IAM role which prevents users from terminating the instances

----

Answer Keys:

1. C & E	6. B
2. D	7. A
3. C	8. A
4. B	9. C
5. A	10. B