Quiz M2

1. What is the benefit of elasticity in the cloud?

- Reduce the time that it takes to make new IT resources available to developers from weeks to minutes.
- Create systems that scale to the required capacity based on changes in demand.
- Minimize storage requirements by reducing logging and auditing activities.
- Trade fixed expense for variable expense.

2. What is the pricing model that AWS customers can use to pay for resources on an as-needed basis?

- Pay as you go
- Pay as you reserve
- Pay as you decommission
- Pay as you buy

3. What is one method that a company could use to ensure high availability during a security attack?

- Resource monitoring
- Access control
- Regular audits
- Automatic scaling

4. Which security principle addresses monitoring, alerting, and auditing actions and changes to the environment in real time?

- ○ Enable traceability.
- ○ Apply the principle of least privilege.
- ○ Protect data in transit and at rest.
- ○ Secure all layers.

5. What is a best practice for automation that can assist with providing a reliable and repeatable secure infrastructure?

- ○ Use detective controls.
- ○ Implement infrastructure as code.
- ○ Use encryption and access controls.
- ○ Implement a log management solution.

6. Which options are characteristics of the principle of least privilege? (Select TWO.)

- ☐ Monitor actions and changes.
- ☐ Use different AWS services.
- ☐ Grant access only as needed.
- ☐ Use encryption and access controls.
- ☐ Enforce separation of duties.

7. Which options are security principles that are based on the security pillar of the AWS Well-Architected Framework? (Select THREE.)

- [ ] Automate security best practices.
- [ ] Protect data in transit and data at rest.
- [ ] Use automatic scaling.
- [ ] Prepare for security events.
- [ ] Democratize advanced technologies.
- [ ] Design your systems for high availability.

8. Security and compliance are shared responsibilities between AWS and the customer. What is an AWS responsibility?

- ( ) Managing application software
- ( ) Configuring security groups
- ( ) Managing customer data
- ( ) Patching network infrastructure

9. What are customer security responsibilities according to the AWS shared responsibility model? (Select TWO.)

- [ ] Managing customer data
- [ ] Maintaining the physical hardware
- [ ] Managing account credentials and policies
- [ ] Maintaining the network infrastructure and virtualization of the infrastructure
- [ ] Maintaining any hypervisor used on instances

10. Who is responsible to operate, manage, and control security OF the cloud, according to the AWS shared responsibility model?

- ( ) Customer
- ( ) AWS
- ( ) Managed services organization (MSO)
- ( ) Managed service provider (MSP)