Section-Based – Security, Compliance, and Governance for AI Solutions(AIF-C01)

!!BEST OF LUCK!!

Ques 1: A healthcare organization is in the process of migrating its patient management system to AWS. As part of their compliance and due diligence efforts, they must ensure that all AWS services and solutions they plan to use comply with various healthcare regulations, such as HIPAA and HITRUST. The organization also works with independent software vendors (ISVs) who need to verify compliance with the AWS services they intend to integrate. The organization must obtain security and compliance documentation from AWS to meet these regulatory requirements and demonstrate compliance to auditors.

Which AWS service can this organization access the necessary security and compliance reports?

a) Amazon Macie

b) AWS CloudTrail

c) AWS Security Hub

d) AWS Artifact

Ans: AWS Artifact

Ques 2: A research institution has deployed a generative AI solution within its system. The compliance team must guarantee that the solution adheres to the necessary standards to protect the confidentiality, integrity, and availability of the data accessed by the AI. This is particularly important as the institution handles sensitive federal research data.

Which standards will ensure the solution meets US government regulatory requirements?

a) Payment card industry data security standard (PCI-DSS)

b) Health Insurance Portability and Accountability Act (HIPAA)

c) National Institute of Standards and Technology (NIST)

d) Federal Risk and Authorization Management Program (FedRAMP)

Ans: National Institute of Standards and Technology (NIST)

Ques 3: A company has deployed a machine learning model for fraud detection in its e-commerce platform. The model has been running in production for several months. The company wants to ensure that it continues to perform accurately and reliably.

Which AWS services or features should the company use to monitor the model's performance and incorporate human review when necessary? (Select TWO.)

a) Amazon Bedrock

b) Amazon SageMaker Ground Truth

c) Amazon SageMaker Data Wrangler

d) Amazon A2I (Amazon Augmented AI)

e) Amazon SageMaker Model Monitor

Ans: Amazon A2I (Amazon Augmented AI) & Amazon SageMaker Model Monitor

Ques 4: A data science team is working on a computer vision project that involves training a deep learning model using a large dataset of labeled images.

Which of the following best practices should the team follow to ensure the security and integrity of its training data? (Select TWO.)

a) Implement role-based access controls to restrict data access to authorized personnel only.

b) Conduct exploratory data analysis to identify and remove outliers and anomalies.

c) Leverage versioning and audit trails to track changes to the dataset.

d) Perform data normalization to standardize the image formats and dimensions.

e) Use cryptographic hashing techniques to verify the authenticity of the data.

Ans: Implement role-based access controls to restrict data access to authorized personnel only & Use cryptographic hashing techniques to verify the authenticity of the data.

Ques 5: A technology firm is implementing a new generative AI model for customer interactions and needs to ensure the system's security against various vulnerabilities.

The ML security team is tasked with identifying the most critical security vulnerabilities that could impact the AI model's performance and integrity. The team also considered configuring AWS Snowball to optimize data transfer speeds during training.

Which vulnerabilities should the firm prioritize? (Select THREE.)

a) Overreliance on AI capabilities

b) Prompt Injection

c) Model theft

d) Training data poisoning

e) Excessive agency

f) Model denial of service

Ans: Prompt Injection & Training data poisoning & Model denial of service

Ques 6: A cloud security engineer is tasked with securing machine learning (ML) workloads in an AWS environment. The engineer needs to ensure that only specific applications and services can access Amazon SageMaker and Amazon RDS resources. These applications require controlled and limited access to these services to maintain security and minimize the risk of unauthorized access.

Which AWS service or feature can the engineer use to grant and manage these permissions effectively?

a) AWS Security Token Service (STS)

b) AWS Secrets Manager

c) AWS Identity and Access Management (IAM)

d) VPC Endpoint Policy

Ans: AWS Identity and Access Management (IAM)

Ques 7: A company relies heavily on machine learning models for personalized recommendations and fraud detection. The company stores sensitive data in Amazon S3 buckets and needs a solution that automatically discovers, classifies, and protects this sensitive data.

Which of the following is the MOST suitable for this use case?

a) Amazon Kinesis

b) Amazon Inspector

c) Amazon GuardDuty

d) Amazon Macie

Ans: Amazon Macie

Ques 8: An AI startup uses generative AI models to create personalized content. The company develops and deploys these models using Amazon SageMaker, Amazon Bedrock, and Amazon Q Business. Following the AWS Generative AI Security Scoping Matrix to strengthen governance and compliance, the team wants to audit AWS Service API activity related to generative AI workloads due to recent concerns about unauthorized access to sensitive training data and model parameters.

Which of the following services can help the startup audit AWS Service API activity related to generative AI workloads?

a) AWS Trusted Advisor

b) AWS Config

c) AWS CloudTrail

d) Amazon Inspector

Ans: AWS CloudTrail

Ques 9: An AI Specialist implements AI models to optimize a company's network operations. To comply with industry standards, the specialist must document the models' training and performance details for auditing purposes.

What AWS service can help the company fulfill this need?

a) Amazon SageMaker Model Monitor

b) Amazon SageMaker Model Cards

c) AWS Config

d) AWS CloudTrail

Ans: Amazon SageMaker Model Cards

Ques 10: A financial institution must ensure that data transferred from Amazon S3 to an Amazon SageMaker instance for training machine

learning models does not leave the AWS network, adhering to strict compliance requirements.

Which AWS Service will meet this requirement most effectively?

a) Amazon VPC Gateway Endpoint

b) Amazon CloudFront Distribution

c) Amazon S3 Transfer Acceleration

d) Amazon S3 Access Point

Ans: Amazon VPC Gateway Endpoint

Ques 11: A biotech company uses machine learning (ML) models on AWS to analyze sensitive genomic data. Before continuing its research, the company must review AWS's adherence to industry data security and regulatory compliance regulations.

Which service can provide this information?

a) Amazon Inspector

b) AWS Config

c) AWS Artifact

d) AWS Trusted Advisor

Ans: AWS Artifact

Ques 12: A healthcare organization is developing an AI-driven diagnostic application leveraging Amazon Bedrock. The application is deployed within a VPC that must comply with strict data privacy regulations. These regulations prohibit any internet connectivity to or from the VPC.

What AWS service or feature will satisfy these objectives?

a) Internet gateway

b) AWS PrivateLink

c) Amazon S3 VPC Endpoint

d) AWS Direct Connect

Ans: AWS PrivateLink

Ques 13: A company is developing a new AI-driven application that must comply with various industry standards and regulations. To ensure compliance, they need to access and review AWS's compliance documentation and agreements.

Which of the following should be used to obtain these documents?

a) AWS CloudTrail

b) AWS Audit Manager

c) AWS Artifact

d) AWS Config

Ans: AWS Artifact

Ques 14: A company has deployed a generative AI application using Amazon SageMaker. They must log and audit all API activities for compliance and security, including interactions with Amazon S3 and DynamoDB.

Which AWS service should the company use to achieve this?

a) AWS Audit Manager

b) Amazon CloudWatch Logs

c) AWS Config

d) AWS CloudTrail

Ans: AWS CloudTrail

Ques 15: A data scientist uses Amazon SageMaker for a machine learning project to classify images of plant species. The datasets need to be securely stored, easily accessible for training, and efficiently managed throughout the project.

Which of the following would you use to store and manage your dataset for this machine learning project?

a) Amazon S3

b) AWS Snowcone

c) Amazon EFS

d) Amazon Fsx

Ans: Amazon S3