🛡️ Domain 2: Security and Compliance (30%)

📌 Task Statement 2.1 – Understand the AWS Shared Responsibility Model

🔷 **AWS is responsible for "Security OF the Cloud":**

- **Physical security** of data centers (e.g., controlled access, surveillance).
- **Hardware, networking, and virtualization layer** (e.g., EC2 hypervisors).
- **Patch management** for AWS-managed services (e.g., RDS, DynamoDB, Lambda).
- **Secure global infrastructure**, including the backbone network and Availability Zones.

🔶 **Customers are responsible for "Security IN the Cloud":**

- **Data protection**: Encrypt data at rest and in transit (KMS, SSE, TLS).
- **IAM configuration**: Manage users, roles, groups, MFA, and permissions using least privilege.
- **OS (Operating System) patching and hardening**: EC2 and container instances.
- **Network security controls**: Use Security Groups, NACLs, VPNs, routing tables, etc.
- **Application-layer security**: Secure app logic, validate inputs, classify data.
- **Monitoring and incident response**: Enable logging, auditing, and alerts.

✅ **Key takeaway**: AWS secures the platform and infrastructure. You must secure everything you deploy — from access control to encryption and app security.

📌 Task Statement 2.2 – Understand AWS Cloud Security, Governance & Compliance Concepts

🔐 **IAM Core Components:**

- **IAM Users**: Identities for humans or applications with long-term credentials.
- **IAM Groups**: Logical user collections for shared permissions.
- **IAM Roles**: Temporary access identities (EC2, Lambda, federated users, cross-account).
- **IAM Policies**: JSON-based documents defining allowed/denied actions.

🔐 **Types of IAM Policies:**

- **Identity-based**: Attached to users, groups, or roles.
- **Resource-based**: Attached directly to resources (e.g., S3 bucket policies).
- **Permissions boundaries**: Limit maximum permissions for IAM identities.
- **Service Control Policies (SCPs)**: Guardrails for AWS Organizations.

🔐 **Governance Best Practices:**

- **Apply least privilege**: Only grant what is absolutely necessary.
- **Enable MFA**: For root and privileged accounts.
- **Use roles over long-term credentials**: Prefer instance profiles and temporary tokens.
- **Rotate access keys** regularly.
- **Use IAM Access Analyzer** to detect unintended access or sharing.

🌍 **AWS Global Compliance:**

AWS supports global compliance by offering:

- Audited services/infrastructure that align with key standards:
- **ISO**: 27001 (ISMS), 27017 (cloud security), 27018 (data privacy)
- **SOC Reports**: SOC 1, SOC 2, SOC 3
- **PCI DSS Level 1**: Card payment processing
- **HIPAA / HITECH**: Healthcare data protection
- **FedRAMP (Moderate & High)**: U.S. government workloads
- **GDPR**: AWS acts as a data processor, customer retains data control

✅ **Compliance Support:**

- **AWS Artifact**: Access compliance documents and audit reports.
- **AWS Config**: Track resource compliance continuously.
- **AWS Security Hub**: Aggregates findings and performs compliance checks.
- **Shared Responsibility Reminder**: AWS handles infra security; you must configure services correctly to stay compliant.

📌 Task Statement 2.3 – Identify AWS Access Management Capabilities

🔑 **Key IAM Capabilities:**

- **Authentication**: Users sign in with credentials, federated identities via SAML/OIDC.
- **Authorization**: IAM Policies control which actions and resources are allowed.
- **Temporary Access**: IAM Roles with STS (Security Token Service) for short-lived credentials.
- **Federated Access**: Integration with corporate identity providers (IdPs).
- **Organizations & SCPs**: Centralized governance across accounts.
- **Access Analyzer**: Finds resources shared externally or overly permissive access.
- **MFA & credential rotation**: For enhanced account security.

✅ **Best Practice Summary**:

- Enforce least privilege, enable MFA, monitor and rotate keys, prefer roles over users, and utilize Access Analyzer.

📌 Task Statement 2.4 – Identify Resources and Components for Security

📝 AWS Logging Tools

- **AWS CloudTrail**: Records all **API calls** (management + data events) for **auditing**, **security investigations**, and **compliance**.
- **CloudWatch**: Monitors **metrics**, **logs**, and **events**. Supports **CloudWatch Alarms** to trigger notifications or automated actions.
- **AWS Config**: Continuously tracks **resource configurations** and **changes**. Enables **compliance auditing** (e.g., block public S3 buckets).

🛡️ Threat Detection & Vulnerability Management

- **GuardDuty**: Uses CloudTrail, **VPC flow logs**, and **DNS logs** to detect **suspicious activity** like reconnaissance or anomalous API behavior.
- **Inspector**: Scans EC2 and containers for **OS vulnerabilities** and **CIS benchmark compliance**.
- **Security Hub**: Centralizes findings from GuardDuty, Inspector, Macie, and others. Performs **compliance checks** (e.g., **CIS**, **PCI DSS**).
- **Macie**: Uses **ML** to classify **sensitive data** in S3 (e.g., **PII**, financial data) and detect potential **data leaks**.

🚨 Incident Response Best Practices

- Enable **CloudTrail** + **Config** for full audit visibility.
- Use **CloudWatch Alarms** / **Security Hub** for real-time alerts.
- Review **GuardDuty findings** regularly and respond promptly.
- Create **incident runbooks** for common security issues.
- Maintain a defined **incident response team** with clear roles.

🔐 **Encryption and Key Management:**

Encryption at Rest:

- **SSE-S3 (Server-Side Encryption with Amazon S3-Managed Keys):** AWS automatically encrypts S3 objects using keys managed by AWS.

- **SSE-KMS (Server-Side Encryption with AWS Key Management Service):** S3 objects are encrypted using customer master keys (CMKs) managed by AWS KMS, allowing more control over key lifecycle and access.

- **SSE-C (Server-Side Encryption with Customer-Provided Keys):** Customers provide and manage encryption keys; AWS uses them to encrypt/decrypt S3 objects but does not store the keys.

- **EBS encryption:** Elastic Block Store (EBS) volumes used by EC2 instances can be encrypted using AWS KMS-managed keys, securing data at the block storage level.

- Enable encryption on **RDS (Relational Database Service)**, **Redshift** (data warehousing), and **DynamoDB** (NoSQL database) to protect databases at rest.

Encryption in Transit:

- Use **TLS (Transport Layer Security)** / **SSL (Secure Sockets Layer)** protocols to encrypt data as it moves across networks, ensuring confidentiality and integrity.

- Services like **Elastic Load Balancer (ELB)** and **API Gateway** support HTTPS endpoints, enforcing encrypted communication between clients and AWS services.

AWS Key Management Service (KMS):

- Centralized service for **creation**, **storage**, **rotation**, and **management** of cryptographic keys.

- Supports **Customer Master Keys (CMKs)** which can be **AWS-managed** (AWS handles lifecycle) or **customer-managed** (full customer control over policies, rotation).

- Seamlessly integrates with AWS services for automatic encryption/decryption operations without exposing keys.

- Supports **grants** — fine-grained permissions on keys, enabling controlled, temporary access to keys for specific tasks or users.

🔐 **Network Security Components:**

Security Groups

- Stateful firewalls attached to EC2 instances.
- Control inbound/outbound traffic based on IP, port, protocol.

Network ACLs (NACLs)

- Stateless, subnet-level firewalls.
- Rules evaluated in order, applied to inbound and outbound traffic.

VPC Flow Logs

- Capture IP traffic flow to/from network interfaces.
- Useful for forensics, troubleshooting, and identifying suspicious behavior.

VPN & Direct Connect

- Secure hybrid connectivity options.
- VPN: Encrypts traffic over public internet using IPsec.
- Direct Connect: Dedicated private links between on-premises and AWS.

AWS Shield

- Standard: Always-on DDoS protection at no extra cost.
- Advanced: 24/7 response team, cost protection, enhanced detection.

AWS WAF

- Protects web apps from XSS, SQL injection, and other Layer 7 threats.
- Supports custom rules, rate limiting, managed rule groups.

CHATGPT AWS EMULATE EXAM PROMPT.

Prompt: I'm preparing for the **AWS Cloud Practitioner Exam.CLF-C02.**
Your job is to emulate the AWS Exam.
I need you to create questions on **Domain 2: Security & compliance** from the AWS exam.
Do one question at a time, don't reveal the answer till I ask.
Ensure it's the **same difficulty as the exam** to thoroughly prepare me to ace it.
Pleasure ensures the difficulty of the exam as I must ace it. (ensure the difficulty is the same as the exam).

Domain 2 AWS Exam resource topics/documentation task link.

Domain 2: Security and Compliance (30%)

- **Task Statement 2.1** – *Understand the AWS shared responsibility model*
- **Task Statement 2.2** – *Understand AWS Cloud security, governance & compliance concepts*
- **Task Statement 2.3** – *Identify AWS access management capabilities*
- **Task Statement 2.4** – *Identify components and resources for security*

https://d1.awsstatic.com/training-and-certification/docs-cloud-practitioner/AWS-Certified-Cloud-Practitioner_Exam-Guide.pdf?utm_source=chatgpt.com