**Session 1: AWS Cloud Platform & Services**

**1. Compare and contrast AWS IaaS, PaaS, and SaaS offerings with real-world examples. How would you decide which model best fits a financial services company migrating from on-premises?**

* **IaaS (Infrastructure as a Service):** Provides virtualized computing resources like EC2, EBS, and VPC. Example: Hosting core banking applications on EC2 for full control over OS and security.
* **PaaS (Platform as a Service):** Offers managed platforms for app development, such as AWS Elastic Beanstalk or Lambda. Example: Deploying APIs for payment processing without managing servers.
* **SaaS (Software as a Service):** Delivers ready-to-use applications like Amazon WorkMail or QuickSight. Example: Using QuickSight for financial analytics. **Decision:** For a financial services company, IaaS is ideal for legacy migration requiring control and compliance, while PaaS suits new microservices-based apps. SaaS can be used for productivity tools.

**2. Evaluate the integration of AWS services (EC2, S3, RDS, Lambda, VPC) to design a scalable e-commerce architecture. Provide a high-level diagram to support your answer.**

* **EC2:** Hosts web servers and application logic.
* **S3:** Stores product images and static content.
* **RDS:** Manages transactional data for orders and customers.
* **Lambda:** Handles serverless tasks like image processing or notifications.
* **VPC:** Provides secure networking and isolation. This architecture ensures scalability, security, and cost efficiency.  
  *(I can create a neat diagram for you—would you like me to generate one?)*

**3. Explain how AWS Shared Responsibility Model affects compliance requirements when deploying workloads in regulated industries like healthcare or banking.**

AWS operates under a shared responsibility model:

* **AWS Responsibility:** Security *of* the cloud (physical infrastructure, networking, hardware).
* **Customer Responsibility:** Security *in* the cloud (data encryption, IAM policies, compliance configurations). For regulated industries, customers must implement HIPAA or PCI DSS controls, configure encryption, and maintain audit logs. AWS provides compliance-ready services, but ultimate responsibility for data governance lies with the customer.

**Session 2: Edge Locations & CloudFront**

**4. Explain how CloudFront edge locations improve performance for a video streaming platform. What metrics would you monitor to evaluate its effectiveness?**

CloudFront caches content at edge locations closer to users, reducing latency and improving streaming quality. Metrics to monitor:

* **Cache Hit Ratio**
* **Latency**
* **Throughput**
* **Error Rates** These metrics ensure optimal performance and user experience globally.

**5. Propose a content delivery strategy using CloudFront for a global e-learning platform with users across North America, Europe, and Asia. How would you handle regional restrictions (geo-blocking) and caching policies?**

Strategy:

* Use **CloudFront distributions** with multiple edge locations for low latency.
* Implement **geo-restriction policies** to block content in restricted regions.
* Configure **cache behaviors** for static assets (long TTL) and dynamic content (short TTL).
* Integrate with **Lambda@Edge** for custom logic like authentication or localization.

**6. Analyze how CloudFront integrates with AWS Shield, WAF, and Route 53 to provide a secure and resilient content delivery solution.**

* **AWS Shield:** Protects against DDoS attacks.
* **AWS WAF:** Filters malicious traffic using custom rules.
* **Route 53:** Provides DNS-based routing and failover. Together, these services ensure high availability, security, and performance for global content delivery.