Risk Assessment

Risk Category	Potential Risk	Impact	Mitigation Strategy
Operational Risks	Scalability Bottlenecks	Performance issues during peak traffic.	Implement auto-scaling with ECS and load balancing with ALB.
	Lack of Monitoring & Incident Response	Delayed response to system failures.	Enable AWS CloudWatch, centralized logging (ELK Stack), and automated alerts.

Risk Category	Potential Risk	Impact	Mitigation Strategy
Third-Party Risks	KYC Provider Downtime	User onboarding disruptions.	Implement fallback providers (e.g., alternate KYC services), enable manual verification.
	CMS or API Rate Limits	Throttling may slow down content delivery.	Implement caching (Redis), optimize API calls, and establish rate limit agreements.
	Dependency on External Payment Providers	Payment processing failures or delays.	Implement redundant payment providers and automatic retry mechanisms.

Risk Category	Potential Risk	Impact	Mitigation Strategy
Compliance Risks	KYC & AML Non-Compliance	Fines, legal action, business restrictions.	Automate KYC with Jumio, AML with AWS Fraud Detector, maintain audit logs.
	GDPR/CCPA Violations	Legal penalties, reputational damage.	Implement data anonymization, right-to-forget policies, and compliance tracking.

Risk Category	Potential Risk	Impact	Mitigation Strategy
Security Risks	Data Breaches	Unauthorized access to sensitive user data.	Implement encryption (AES-256), IAM policies, AWS WAF, and security audits.
	Account Takeover	Users may fall victim to phishing attacks.	Enforce MFA (TOTP, FIDO2), anomaly detection with AWS Cognito, and user education.
	API Abuse & DDoS Attacks	Service disruption, potential downtime.	Rate limiting via API Gateway, AWS Shield, and WAF.

	Insider Threats	Unauthorized actions by internal users.	Implement least-privilege IAM policies and activity logging with AWS CloudTrail.