D	
Reg. Number:	

Continuous Assessment Test (CAT) – II OCTOBER 2025

Programme	:	B.Tech. Computer Science and Engineering	Semester	:	Fall Semester 2025-26
Course Code & Course Title	:	BCSE355L- Cloud Architecture Design	Class Number	:	CH2025260101059 CH2025260101054 CH2025260101057 CH2025260101058 CH2025260101060 CH2025260101055 CH2025260101062
Faculty	:	Dr. K. Palani Thanaraj Dr. Priyaadharshini M Dr. Priyadarshini R Dr. Om Kumar C U Dr. Selvam D Dr. Sandosh S Dr. Parvathy A K	Slot	· :	F1+TF1
Duration	:	1 hour 30 minutes	Max. Mark		50

General Instructions:

- Write only your registration number on the question paper in the box provided and do not write other information
- Only non-programmable calculator without storage is permitted

Answer all questions

		Answer all questions			
Q. No	Sub Sec.	Description	Marks	СО	BT Level
1		A social media analytics startup manages a PostgreSQL database that records millions of daily user interactions. The database needs to efficiently handle heavy write operations from user activity, while also supporting complex read-heavy analytics queries that must not degrade the performance of the write operations. The team wants to ensure: • Read operations can scale independently from writes. • Data remains consistent across multiple copies of the database despite possible delays in updates. • Backup and recovery processes do not interrupt ongoing user activity. • The system can continue serving requests if the main database becomes unavailable. a) Propose an AWS-based architecture that addresses the need for separating read and write workloads. Illustrate the mechanism that keeps the different database instances in sync, and how this improves both performance and availability. [5 Marks] b) Analyse how backups can be integrated into this architecture without burdening the primary database, how synchronization	10	4	K4

delays are handled, the scalability limits regarding multiple instances, and what happens during a failure of the primary system. [5 Marks] Assume that you are an AWS solutions architect tasked with designing a secure and compliant logging solution for a multinational corporation operating in multiple AWS regions. The corporation requires operating in multiple AWS regions of a segregation. Specific needs for real-time monitoring, cross-region log aggregation. a) Design and justify a centralized, multi-account logging architecture that ensures tamper-proof, immutable logs while architecture that ensures tamper-proof, famultiple of specific and propose a resilient, cross-region log aggregation. Sharksl adhering to the principle of least privilege. [5 Marksl] ashering to the principle of least privilege. [5 Marksl] Shucket for long-term retention and analysis. [5 Marks] Sbucket for long-term retention and analysis. [6 Marks] Sbucket for long-term retention and analysis. [6 Marks] Sbucket for long-term retention and analysis. [7 Marks] Sbucket for long-term retention and analysis. [7 Marks] Sbucket for long-term retention and analysis. [8 Marks] Sbecauth the following concerns: a long-term retention and analysis. [8 Marks] Sbecauth the following concerns: b No multi-account structure is in place, making it difficult to isolate production from development. b Roll substances and segregated, causing lack of visibility into cost centers. b No multi-account structure is in place, making it difficult to isolate production from development. b Roll substances a		L. Ja			
Assume that you are an AWS solutions architect tasked with designing a Assume that you are an AWS solution for a multinational corporation secure and compliant logging solution for a multinational corporation specific needs for real-time monitoring, cross-region log aggregation. specific needs for real-time monitoring, cross-region log aggregation architecture that ensures tamper-proof, immutable logs while architecture that ensures tamper-proof, immutable logs was stratedy. State the proof of a production, staging, and development) are deployed under a single AWS account. A recent internal audit revealed the following concerns: Root account is frequently used for daily operations. IAM users have broad AdministratorAccess policies without restrictions. No multi-account structure is in place, making it difficult to isolate production from development. Billing reports are not segregated, causing lack of visibility into cost centers. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy in a material proof that the proof of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clea		timits regarding multiple			
Assume that you are an AWS solutions architect tasked with designing a system. [5 Marks] Assume that you are an AWS solution for a multinational corporation secure and compliant logging solution for a multinational corporation operating in multiple AWS regions. The corporation requires operating in the complex of the corporation operating in the complex of the co		delays are handled, the scalability infinite of the primary			
Assume that you are an AWS solutions architect tasked with coapse. Assume that you are an AWS solutions architect tasked with coapse. Assume that you are an AWS solution for a multinational corporation secure and compliant logging solution for a multinational corporation requires operating in multiple AWS regions. The corporation requires operating in multiple AWS regions. The corporation requires operating in multiple AWS regions. The corporation requires operating in multiple AWS regions are solved and propose a centralized, multi-account logging architecture that ensures tamper-proof, immutable logs while architecture that ensures required to validate strategy. Justify the technical mechanisms required to validate strategy. Account structure is in place, making it difficult to isolate production from development. Billing reports are not segregated, causing lack of visibility into cost centers. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, Cloud Trail, and centralized logging. Clear billin		Instances and what happens			
operating in multiple AWS regions. The corporations operating in multiple AWS regions. The corporations operating in multiple AWS regions. The corporation of the comprehensive auditing of all API calls across its AWS accounts, with comprehensive auditing of all API calls across-region log aggregation. Specific needs for real-time monitoring, cross-region log aggregation architecture that ensures tamper-proof, immutable logs while architecture that ensures tamper-proof, immutable logs from disparate geographical regions into a single, centralized logs from disparate geographical regions into a single, centralized logs from disparate geographical regions into a single, centralized logs from disparate geographical regions into a single, centralized logs from disparate geographical regions into a single, centralized logs from disparate geographical regions into a single, centralized logs from development. • IAM users have broad AdministratorAccess policies without restrictions. • No multi-account structure is in place, making it difficult to isolate production from development. • Billing reports are not segregated, causing lack of visibility into cost centers. • No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: • Secure handling of root and IAM accounts. • Implementation of a multi-account strategy using AWS Organizations. • Use of Service Control Policies (SCPs) to enforce least privilege. • Enabling MFA, CloudTrail, and centralized logging. • Clear billing segregation and cost optimization across teams/projects. a) Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] b) Justify how your approach improves security, cost m		Cuctom 13 Marks			
operating in multiple AWS regions. The corporations operating in multiple AWS regions. The corporations operating in multiple AWS regions. The corporation of the comprehensive auditing of all API calls across its AWS accounts, with comprehensive auditing of all API calls across-region log aggregation. Specific needs for real-time monitoring, cross-region log aggregation architecture that ensures tamper-proof, immutable logs while architecture that ensures tamper-proof, immutable logs from disparate geographical regions into a single, centralized logs from disparate geographical regions into a single, centralized logs from disparate geographical regions into a single, centralized logs from disparate geographical regions into a single, centralized logs from disparate geographical regions into a single, centralized logs from disparate geographical regions into a single, centralized logs from development. **A start-up organization manages customer transactions on AWS.** A start-up organization manages customer transactions on AWS.** A start-up organization from development. **Billing reports are not segregated, causing lack of visibility into cost centers. **No centralized logging or monitoring is implemented for security events. **Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: **Secure handling of root and IAM accounts.** **Implementation of a multi-account strategy using AWS Organizations.** **Use of Service Control Policies (SCPs) to enforce least privilege.** **Enabling MFA, CloudTrail, and centralized logging.** **Clear billing segregation and cost optimization across teams/projects. **Propose with an illustration a detailed AWS Account Management strategy addressing the requirements.** **Soft in personal finance company is building a digital		Assume that you are an AWS solutions architect tasks			
comprehensive auditing of all API calls across its AWS account specific needs for real-time monitoring, cross-region log aggregation. specific needs for real-time monitoring, cross-region log aggregation. a) Design and justify a centralized, multi-account logging architecture that ensures tamper-proof, immutable logs while architecture that ensures the provided to validate strategy. Justify the technical mechanisms required to validate strategy. A start-up organization manages customer transactions on AWS. I AM users have broad AdministratorAccess policies without restrictions. No multi-account structure is in place, making it difficult to isolate production from development. Billing reports are not segregated, causing lack of visibility into cost centers. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. Propose with an illustra					
specific needs for real-time monitoring, cross-region log aggregation a) Design and justify a centralized, multi-account architecture that ensures tamper-proof, immutable logs while architecture that ensures that ensures that ensures that ensures that ensures the following concerns: No mutti-account structure is in place, making it difficult to isolate production from development. Billing reports are not segregated, causing lack of visibility into cost centers. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Scure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. Soff in personal finance company is building a digital wallet and online		I charating in multiple 12			
specific needs for tearnistify a centralized, multi-account architecture that ensures tamper-proof, immutable logs while architecture that ensures tamper-proof, immutable logs from disparate geographical regions into a single, centralized logs from disparate geographical regions into a single, centralized logs from disparate geographical regions into a single, centralized system of the following concerns: A start-up organization manages customer transactions on AWS. A start-up organization manages customer transactions on AWS. A start-up organization manages customer transactions on AWS. Currently, all workloads (production, staging, and development) are deployed under a single AWS account. A recent internal audit revealed the following concerns: Root account is frequently used for daily operations. IAM users have broad AdministratorAccess policies without restrictions. No multi-account structure is in place, making it difficult to isolate production from development. Billing reports are not segregated, causing lack of visibility into cost centers. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] Bustify how your approach improves security, cost management, and compliance. [5 marks]		comprehensive auditing of all API calls across its region log aggregation.			1/5
a posign and places architecture that ensures tamper-proof, immulator architecture that ensures tamper-proof, immulator architecture that ensures adhering to the principle of least privilege. [5 Marks] adhering to the principle of least privilege. [5 Marks] Be Evaluate and propose a resilient, cross-region log aggregation by Evaluate and propose a resilient, cross-region log aggregation disparate geographical regions into a single, centralized logs from disparate geographical regions into a single, centralized logs from disparate geographical regions into a single, centralized logs from disparate geographical regions into a single, centralized logs from disparate geographical regions into a single, centralized deployed under a single AWS account. A recent internal audit revealed the following concerns: Root account is frequently used for daily operations. IAM users have broad AdministratorAccess policies without restrictions. No multi-account structure is in place, making it difficult to isolate production from development. Billing reports are not segregated, causing lack of visibility into cost centers. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] Bustify how your approach improves security, cost management, and compliance. [5 marks]		energific needs for real-time monitoring, cross-region tog logging	10	1	K5
archtecture and entropies of least privilege. [5 Mains] adhering to the principle of least privilege logs aggregation b) Evaluate and propose a resilient, cross-region log aggregation b) Evaluate and propose a resilient, cross-region log aggregation b) Evaluate and propose a resilient, cross-region log aggregation b) Evaluate and propose a resilient, cross-region log aggregation b) Evaluate and propose a resilient, cross-region log aggregation b) Evaluate and propose a resilient, cross-region log aggregation b) Evaluate and propose a resilient, cross-region log aggregation b) Evaluate and propose a resilient, cross-region log aggregation b) Evaluate and propose a resilient, cross-region log aggregation b) Evaluate and propose a resilient, cross-region log aggregation b) contralized logging customer transactions on AWS. A start-up organization wangement strategy that ensures: No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] D) Justify how your approach improves security, cost management, and compliance. [5 marks]		a) Design and Justily			
adhering to the pintopose a resilient, cross-region to validate strategy. Justify the technical mechanisms required to validate strategy and sangle, centralized logs from disparate geographical regions into a single, centralized on AWS. A start-up organization manages customer transactions on AWS. A start-up organization manages customer transactions on AWS. A start-up organization and sangle, and development) are currently all workloads (production, staging, and development) are deployed under a single AWS account structure is in place, making it difficult to isolate production from development. Billing reports are not segregated, causing lack of visibility into cost centers. No centralized logging or monitoring is implemented for security events. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. Serial personal finance company is building a digital wallet and online	2	architecture that ensures tamper-ploof, hards			
b) Evaluate and propose strategy. Justify the technical mechanisms required to design the strategy. Justify the technical mechanisms required to design does from disparate geographical regions into a single, centralized logs from disparate geographical regions into a single, centralized S3 bucket for long-term retention and analysis. [5 Marks] A start-up organization manages customer transactions on AWS. A start-up organization manages customer transactions on AWS. Currently, all workloads (production, staging, and development) are deployed under a single AWS account. A recent internal audit revealed the following concerns: Root account is frequently used for daily operations. I AM users have broad AdministratorAccess policies without restrictions. No multi-account structure is in place, making it difficult to isolate production from development. Billing reports are not segregated, causing lack of visibility into cost centers. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. a) Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] Justify how your approach improves security, cost management, and compliance. [5 marks]					
logs from disparate geographical regions into a single start geographical regions into a single start geographical regions into a single start porganization manages customer transactions on AWS. A start-up organization manages customer transactions on AWS. Currently, all workloads (production, staging, and development) are deployed under a single AWS account. A recent internal audit revealed the following concerns: Root account is frequently used for daily operations. IAM users have broad AdministratorAccess policies without restrictions. No multi-account structure is in place, making it difficult to isolate production from development. Billing reports are not segregated, causing lack of visibility into cost centers. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. a) Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] Justify how your approach improves security, cost management, and compliance. [5 marks]					
So bucket for long-term retention and analysis. [5 Marks] So bucket for long-term retention and analysis. [5 Marks] So bucket for long-term retention and analysis. [5 Marks] So bucket for long-term retention and analysis. [5 Marks] So bucket for long-term retention and analysis. [5 Marks] So bushet for long-term retention and analysis. [5 Marks] So bushet for long-term retention and analysis. [5 Marks] So bushet for long-term retention and analysis. [5 Marks] So bushet for long-term retention and analysis. [5 Marks] So bushet for long-term retention and analysis. [5 Marks] A start-up organization manages customer transactions on AWS. A start-up organization and detailed for security retents. A start-up organization for development. Billing reports are not segregated, causing lack of visibility into cost centers. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] Justify how your approach improves security, cost management, and compliance. [5 marks] SoFi a personal finance company is building a digital wallet and online		strategy, Justily and a single, some into a suigio,			
A start-up organization manages customer transactions on Awo. A start-up organization manages customer transactions on Awo. Currently, all workloads (production, staging, and development) are deployed under a single AWS account. A recent internal audit revealed the following concerns: Root account is frequently used for daily operations. • IAM users have broad AdministratorAccess policies without restrictions. • No multi-account structure is in place, making it difficult to isolate production from development. • Billing reports are not segregated, causing lack of visibility into cost centers. • No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: • Secure handling of root and IAM accounts. • Implementation of a multi-account strategy using AWS Organizations. • Use of Service Control Policies (SCPs) to enforce least privilege. • Enabling MFA, CloudTrail, and centralized logging. • Clear billing segregation and cost optimization across teams/projects. a) Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] b) Justify how your approach improves security, cost management, and compliance. [5 marks]		1 - re from disparate goods 1 - 1 reis [5 Marks]		-	
A start-up organization lineages Currently, all workloads (production, staging, and development) are Currently, all workloads (production, staging, and development) are deployed under a single AWS account. A recent internal audit revealed the following concerns: Root account is frequently used for daily operations. IAM users have broad AdministratorAccess policies without restrictions. No multi-account structure is in place, making it difficult to isolate production from development. Billing reports are not segregated, causing lack of visibility into cost centers. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] Justify how your approach improves security, cost management, and compliance. [5 marks] SoFi a personal finance company is building a digital wallet and online		S3 bucket for long-term transactions on AWB.			
Currently, all Workholds AwS account. A recent internal audit revealed deployed under a single AWS account. A recent internal audit revealed the following concerns: Root account is frequently used for daily operations. IAM users have broad AdministratorAccess policies without restrictions. No multi-account structure is in place, making it difficult to isolate production from development. Billing reports are not segregated, causing lack of visibility into cost centers. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] Justify how your approach improves security, cost management, and compliance. [5 marks]		A start-up organization manages and development) are			
deployed under a single Arro active the following concerns: Root account is frequently used for daily operations. IAM users have broad AdministratorAccess policies without restrictions. No multi-account structure is in place, making it difficult to isolate production from development. Billing reports are not segregated, causing lack of visibility into cost centers. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] b) Justify how your approach improves security, cost management, and compliance. [5 marks]		Currently, all workloads (production, stagging, A recent internal audit revealed			
the following concerns: Root account is frequently used for daily operations. IAM users have broad AdministratorAccess policies without restrictions. No multi-account structure is in place, making it difficult to isolate production from development. Billing reports are not segregated, causing lack of visibility into cost centers. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] b) Justify how your approach improves security, cost management, and compliance. [5 marks]		deployed under a single AWS assume			
 IAM users have broad Administration to the restrictions. No multi-account structure is in place, making it difficult to isolate production from development. Billing reports are not segregated, causing lack of visibility into cost centers. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. a) Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] b) Justify how your approach improves security, cost management, and compliance. [5 marks] SoFi a personal finance company is building a digital wallet and online 		the following concerns:			
restrictions. No multi-account structure is in place, making it difficult to isolate production from development. Billing reports are not segregated, causing lack of visibility into cost centers. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] Justify how your approach improves security, cost management, and compliance. [5 marks]		Root account is frequently used to daily operation.			
 No multi-account structure is in place, making it different isolate production from development. Billing reports are not segregated, causing lack of visibility into cost centers. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. a) Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] b) Justify how your approach improves security, cost management, and compliance. [5 marks] SoFi a personal finance company is building a digital wallet and online 				3	
isolate production from development. Billing reports are not segregated, causing lack of visibility into cost centers. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] Justify how your approach improves security, cost management, and compliance. [5 marks]		restrictions.			
 Billing reports are not segregated, causing lates of the cost centers. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. a) Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] b) Justify how your approach improves security, cost management, and compliance. [5 marks] SoFi a personal finance company is building a digital wallet and online 					
cost centers. No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] Distify how your approach improves security, cost management, and compliance. [5 marks]		isolate production from development			1
No centralized logging or monitoring is implemented for security events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] Justify how your approach improves security, cost management, and compliance. [5 marks] SoFi a personal finance company is building a digital wallet and online					1
events. Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] Distify how your approach improves security, cost management, and compliance. [5 marks] SoFi a personal finance company is building a digital wallet and online		cost centers.			
Management has asked you, as the AWS Cloud Administrator, to design a robust AWS Account Management strategy that ensures: • Secure handling of root and IAM accounts. • Implementation of a multi-account strategy using AWS Organizations. • Use of Service Control Policies (SCPs) to enforce least privilege. • Enabling MFA, CloudTrail, and centralized logging. • Clear billing segregation and cost optimization across teams/projects. a) Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] b) Justify how your approach improves security, cost management, and compliance. [5 marks]					***
 a robust AWS Account Management strategy that the strategy of the str	•	events.	10	2	K4
 Secure handling of root and IAM accounts. Implementation of a multi-account strategy using AWS Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. a) Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] b) Justify how your approach improves security, cost management, and compliance. [5 marks] SoFi a personal finance company is building a digital wallet and online 	3	Management has asked you, as the strategy that ensures:			Į į
 Implementation of a multi-account strategy using PWO Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. a) Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] b) Justify how your approach improves security, cost management, and compliance. [5 marks] SoFi a personal finance company is building a digital wallet and online 		a robust AWS Account ividing of root and IAM accounts.			
Organizations. Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. a) Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] b) Justify how your approach improves security, cost management, and compliance. [5 marks] SoFi a personal finance company is building a digital wallet and online		Secure nanding of foot and 22 Secure nanding of a multi-account strategy using AWS The secure nanding of the secure nanding o			
 Use of Service Control Policies (SCPs) to enforce least privilege. Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. a) Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] b) Justify how your approach improves security, cost management, and compliance. [5 marks] SoFi a personal finance company is building a digital wallet and online 		• Implementation of a main asset			
 Enabling MFA, CloudTrail, and centralized logging. Clear billing segregation and cost optimization across teams/projects. a) Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] b) Justify how your approach improves security, cost management, and compliance. [5 marks] SoFi a personal finance company is building a digital wallet and online 		Organizations. Ly of Service Control Policies (SCPs) to enforce least privilege.			100 m
Clear billing segregation and cost optimization across teams/projects. a) Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] b) Justify how your approach improves security, cost management, and compliance. [5 marks] SoFi a personal finance company is building a digital wallet and online		Use of Service Country I and centralized logging.			
teams/projects. a) Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] b) Justify how your approach improves security, cost management, and compliance. [5 marks] SoFi a personal finance company is building a digital wallet and online		• Enabling IVIFA, Cloud Itali, and cost optimization across			
a) Propose with an illustration a detailed AWS Account Management strategy addressing the requirements. [5 marks] b) Justify how your approach improves security, cost management, and compliance. [5 marks] SoFi a personal finance company is building a digital wallet and online					
Management strategy addressing the requirements. [5 marks] b) Justify how your approach improves security, cost management, and compliance. [5 marks] SoFi a personal finance company is building a digital wallet and online		teams/projects.			¥1
[5 marks] b) Justify how your approach improves security, cost management, and compliance. [5 marks] SoFi a personal finance company is building a digital wallet and online		Management strategy addressing the requirements.			
b) Justify how your approach improves security, cost management, and compliance. [5 marks] SoFi a personal finance company is building a digital wallet and online					
and compliance. [5 marks] SoFi a personal finance company is building a digital wallet and online		b) Justify how your approach improves security, cost management,			
SoFi a personal finance company is building a digital wallet and online					
payment platform on AWS. Their application runs on Application Load		SoFi a personal finance company is building a digital wallet and online			
	4	payment platform on AWS. Their application runs on Application Load			

	Balancer (ALB) with Amazon EC2, customer transaction data is stored in Amazon RDS, and financial records are archived in Amazon S3. The company is concerned about: 1. Large-scale DDoS attacks during peak transaction hours. 2. Data confidentiality and compliance with PCI DSS and RBI (Reserve Bank of India) regulations. As the cloud security architect: a) Design a defense strategy with an illustration using suitable service to ensure high availability and continuous protection against DDoS attacks on the fintech application. Justify why this solution is suitable for a financial platform. [5 Marks] b) Explain how AWS Key Management Service (KMS) can be used to secure customer financial data in RDS and S3, focusing on key rotation, auditability, and access control. Show how this	10	2	K4
5	supports fintech regulatory compliance. [5 Marks] A rapidly growing e-commerce startup, EcomKart, relies heavily on AWS for its backend infrastructure, including multiple database services like Amazon RDS for transactional data, DynamoDB for session management, and Redshift for analytics. Over the last quarter, EcomKart has observed a significant and unexpected surge in its AWS database billing, impacting its profitability targets. The CFO has tasked your team with identifying the root causes and proposing a sustainable cost optimization strategy. a) Analyze the potential cost drivers for EcomKart's increasing database expenses across Amazon RDS, DynamoDB, and Redshift. Show a sample financial breakdown highlighting the distribution of costs. [3 Marks] b) Propose specific metrics and AWS tools that would be essential for a detailed cost audit to pinpoint the primary areas of expenditure with justification. [4 Marks] c) Based on your audit findings, recommend and justify a prioritized set of three distinct cost optimization strategies for EcomKart, considering both short-term impact and long-term sustainability. For each strategy, discuss potential trade-offs and how you would monitor their effectiveness. [3 Marks]		3	K4