Component	Very Small Customers (1-2 accounts)	Small Customers (3-5 accounts/apps)	Medium Customers (6-15 accounts/apps)	Large Customers (15+ accounts/apps)
Foundation	AWS Organizations only	AWS Control Tower	AWS Control Tower	AWS Control Tower with custom extensions
Account Structure	- Management account - 1 workload account	- Management account - Log archive account - Audit account - 1+ workload accounts	- Management account - Log archive account - Audit account - Shared services account - Separate Dev, Test, Prod accounts - Separate business unit/app accounts	- Management account - Log archive account - Audit account - Security account - Shared services account - Network account - Separate Dev, Test, Stage, Prod accounts - Separate business unit/department/app accounts
Organizational Structure	Minimal AWS Organizations structure: - Root - Workloads OU	Basic AWS Organizations structure: - Root - Core OU (Log, Audit) - Workloads OU	More complex OU structure: - Root - Core OU (Log, Audit, Shared Services) - Prod OU - Non-Prod OU - Sandbox OU	Comprehensive OU structure: - Root - Infrastructure OU (Core, Network, Security) - Prod OU (by business unit) - Non-Prod OU (by business unit) - Sandbox OU - Suspended OU
Guardrails	- Basic SCPs - Manual AWS Config rules	- Basic SCPs - Control Tower mandatory guardrails - Few selected strongly recommended guardrails	- SCPs for each OU - All Control Tower guardrails - Custom AWS Config rules - Tag policies	- Granular SCPs for each OU - All Control Tower guardrails - Extensive custom AWS Config rules - Custom Lambda functions for advanced policies - Comprehensive tag policies and enforcement
Access Management	- IAM users and groups - Basic IAM policies	- AWS IAM Identity Center - Basic permission sets - Local user management	- AWS IAM Identity Center - Integration with customer's identity provider (e.g., Azure AD) - Custom permission sets - Attribute-based access control (ABAC)	- AWS IAM Identity Center - Integration with enterprise identity management - Fine-grained permission sets - Advanced ABAC - Custom IAM policies and roles - Automated access reviews
Networking	- Simple VPC setup - Basic VPN for on-	- Basic VPC setup - AWS Transit Gateway for	- Hub-and-spoke with AWS Transit Gateway	- Complex architecture with Transit Gateway

Component	Very Small Customers (1-2 accounts)	Small Customers (3-5 accounts/apps)	Medium Customers (6-15 accounts/apps)	Large Customers (15+ accounts/apps)
	premises connectivity (if needed)	inter-VPC connectivity - Simple Direct Connect or VPN for on-premises connectivity	- Shared services VPC - Transit Gateway Network Manager - AWS Network Firewall - Direct Connect with backup VPN	- Multiple Transit Gateways for isolation - SD-WAN integration - AWS Network Firewall and Gateway Load Balancer - AWS WAF and Shield Advanced - Global Accelerator for optimized routing - Multiple Direct Connect connections with redundancy
Automation	- Simple CloudFormation templates - Basic AWS CLI scripts	- Basic CloudFormation templates - AWS Systems Manager for patching and maintenance	- CloudFormation StackSets - AWS Systems Manager for config management - Basic CI/CD pipelines for infrastructure	- Control Tower Account Factory for Terraform (AFT) - Custom account vending machine - Advanced CI/CD pipelines for infrastructure and applications - AWS Systems Manager for comprehensive ops management - Custom automation runbooks
Security	- GuardDuty (optional) - Basic IAM policies - Manual security checks	- GuardDuty - Basic IAM policies - AWS Security Hub (basic features) - Amazon Inspector for vulnerability assessments	- GuardDuty with automated remediation - Security Hub with custom actions - Network Firewall - AWS Config advanced queries - Amazon Detective for security investigations - AWS Certificate Manager for SSL/TLS management	- GuardDuty with custom threat detection - Security Hub with multi-account aggregation - Network Firewall with complex rule sets - WAF with custom rules and managed rule sets - AWS Macie for sensitive data discovery - AWS KMS for centralized key management - Third-party security tool integration (e.g., Splunk, CrowdStrike)
Monitoring and Logging	- Basic CloudWatch alarms - CloudTrail enabled in management account	- Basic CloudWatch dashboards - CloudTrail logs in central account - Simple SNS/SES alerting	- Enhanced CloudWatch dashboards and alarms - CloudTrail logs with organization trail - Log aggregation in	- Comprehensive monitoring with CloudWatch, CloudTrail, and X-Ray - Centralized logging with Kinesis Data Firehose - Advanced log analytics with

Component	Very Small Customers (1-2 accounts)	Small Customers (3-5 accounts/apps)	Medium Customers (6-15 accounts/apps)	Large Customers (15+ accounts/apps)
			centralized account - Basic log analytics with Athena	Elasticsearch Service - Custom metrics and logs collection - Integration with enterprise monitoring tools (e.g., Datadog, New Relic)
Cost Management	- AWS Budgets (basic) - Cost Explorer (basic usage)	- AWS Budgets and Cost Explorer - Basic cost allocation tags	- AWS Budgets and Cost Explorer - Detailed tagging strategy - AWS Cost and Usage Report - Savings Plans for compute savings	- AWS Budgets and Cost Explorer with customizations - Comprehensive tagging strategy and enforcement - Savings Plans and Reserved Instances optimization - Detailed cost allocation and chargeback model - Integration with FinOps platforms (e.g., CloudHealth, Cloudability)
Compliance and Governance	- Manual compliance checks - AWS Artifact for accessing compliance reports	- Basic AWS Config rules - Manual compliance reporting - AWS Artifact for accessing compliance reports	- Custom AWS Config rules - AWS Audit Manager for assessments - Automated compliance reporting - Integration with GRC tools	- Extensive custom AWS Config rules - AWS Audit Manager with custom frameworks - Continuous compliance monitoring and remediation - Custom dashboards for compliance status - Integration with enterprise GRC platforms
Data Management	- Basic S3 bucket policies - Manual backups	- Basic S3 bucket policies - Simple backup strategy with AWS Backup	- S3 bucket policies and access points - AWS Backup with cross-region and cross-account strategies - Basic data lifecycle management	- Complex S3 bucket policies, access points, and lens - AWS Backup with advanced features and custom scripts - Comprehensive data lifecycle and archival strategies - Data catalog and classification using AWS Glue and Macie - Data lakes with Lake Formation
Disaster Recovery	- Basic backup strategy - Single-region deployment	- Basic backup and restore strategy - Single-region deployments	- Multi-region backup strategy - Pilot light or warm standby for critical applications	- Multi-region active-active deployments - Advanced DR strategies (e.g., hot standby, multi-site active-active)

Component	Very Small Customers (1-2 accounts)	Small Customers (3-5 accounts/apps)	Medium Customers (6-15 accounts/apps)	Large Customers (15+ accounts/apps)
			- Basic disaster recovery runbooks	- Automated failover and failback procedures - Regular DR testing and simulation exercises