KOAN

NZISM AWS

Prepared For: NZ Government

By: Koan Limited

Table of Contents

AWS Five Pillars of Well Architected Review (WAR)

AWS Configuration principles are observed including the root user is secured, account contact information is set, AWS CloudTrail and CloudWatch used.

Operational Excellence

- Workload health metrics and defined, collected and analyzed
- Internal resource trained for operational enablement
- Deployments are tested in staging and validated with test cases before prod deployment
- Solution components emit information allowing operators to understand state to enable troubleshooting operational events
- Code assets are version controlled

Security

- Identity and Access Management Principles are observed including access requirements defined, grant least privileges, and AWS Session Manager access to systems
- Networking - security groups are tightly coupled, internet access is encrypted using HTTPS/TLS, data stores are in private subnets.
- Operations- cryptographic keys are managed securely, procedures in place.

Performance Efficiency

- Majority of workloads are lambda.
- AWS API Integration official AWS SDKs are used to call AWS API Endpoints

Reliability

- Deployment is automated using Infrastructure as Code (IaC) CDK.
- Availability requirements are defined including recovery time objective (RTO) and recovery point objective (RPO) for individual node and availability zone disruptions.
- Autoscaling solutions are implemented including AWS S3, AWS CloudFront, AWS Auto Scaling and AWS Lambda.

Cost Optimization

- Total Cost of Ownership (TCO) analysis cost modelling is done along side Return on Investment (ROI).

AWS Operational Best Practices

Manage Cloud Access

1. Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions, EMR clusters, EC2 instances, RDS instances, S3 cannot be publicly accessed
2. Ports are restricted on EC2 Security Groups and EC2 instances deployed within VPCs.
3. Ensure AWS Systems Manager (SSM) documents are not public
4. Only allow authorized users, processes, and devices access to S3

AWS Identity and Access Management (IAM)

5. Enable multi-factor authentication (MFA) for all IAM users and hardware MFA for root
6. Check root user has no access keys attached to their AWS IAM role.
7. Identities/credentials are managed using an organizational IAM password policy.
8. Incorporate the principles of least privilege and separation of duties with access permissions

Restrict Access using Security Groups

9. EC2 Security Groups manage network access with stateful filtering of ingress and egress
10. Security group restricts remote access to AWS resources.

Encryption at Rest

11. Ensure encryption is used by default as sensitive data may exist.
12. Encryption is enabled for AWS CloudTrail, CloudWatch Log Groups
13. Enable encryption for AWS EBS volumes, EFS, S3 buckets, RDS instances and snapshots
14. Use AWS KMS with AWS Secrets Manager

Encrypt Data in Transit

15. Ensure ELBs are configured with SSL or HTTPS listeners and ALBs redirects requests to HTTPS
16. RDS instances require TLS/SSL encryption to connect to SQL clients.
17. Classic ELB SSL listeners are using a custom security policy.
18. S3 buckets require requests to use Secure Socket Layer (SSL)

Auditing

19. Consolidated logging and monitoring are properly used within the AWS environment
20. Configure CloudTrail with CloudWatch Logs to monitor trail logs and be notified of activity
21. Use AWS CloudTrail in non-repudiation by recording AWS Console actions and API calls
22. Enable Amazon RDS logging and use a minimum duration of event log data is retained

23. Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs.
24. Enable AWS WAF (V2) logging on regional and global web ACLs
25. API Gateway logging displays view of users who have accessed the API

AWS Web Application Firewall

26. AWS WAF is enabled on Load Balancers to help protect web applications

Ensure Network Integrity

27. AWS Systems Manager to provide detailed system configurations
28. Network integrity is protected by ensuring X509 certificates are issues by AWS ACM
29. Load Balancing activity is a central point of communication within an environment.

AWS Key Management Service

30. Key material is stored in AWS KMS, and the backing key is rotated and tied to key ID of CMK
31. At least one KMS Customer Master Key (CMK) has been defined for each data classification

Vulnerabilities Checking

32. Enable rules to help with identification and documentation of EC2 vulnerabilities
33. Patch Baselines configured in Patch Manager, auto-approval of critical security patches
34. RDS minor upgrades managed automatically

Monitor Cybersecurity

35. Use AWS GuardDuty to monitor / detect cybersecurity events with threat intelligence feeds
36. Use AWS SecurityHub to monitor unauthorized personnel, connections, devices
37. Use the collection of S3 data events to help in detecting any anomalous activity

Business Continuity

38. Enable cross-zone load balancing for ELBs to maintain capacity and availability
39. Multi-AZ support in RDS provides enhanced availability and durability for database instances

AWS Backup Plan

40. Use the backup feature of Amazon RDS to create backups of databases and transaction logs
41. Enable data back-up processes to ensure RDS instances, DynamoDB tables, EBS volumes, EFS are part of an AWS Backup Plan. Use S3 bucket versioning.
42. Enable automatic backups, AWS ElastiCache creates a backup of the cluster on a daily basis
43. Ensure where applicable Amazon RDS instances have deletion protection enabled.

About Koan

Tuakiri | Koan is an AWS and software development consultancy based in Wellington and Palmerston North. Koan has been building and deploying secure, compliant, enterprise applications for Global and New Zealand customers for 20 years.

Whāinga | Our objective is to foster trusted partnerships with our customers. From our experience collaboration is the most effective way of adding value and delivering successful outcomes for our customers. We are an AWS Advanced Tier Partner registered on the AWS Partner Network (APN).

We have a team of senior AWS certified practitioners, all with specific knowledge and areas in areas we work in. This enables Koan to:

- Provide AWS specialist services across SMBs, commercial and Government departments
- Provide AWS services including Well Architected Reviews (WAR), Cloud Adoption Framework
- AWS Migrations - take our customers on a successful digital transformation journey from migrating legacy systems and workloads into the cloud
- AWS Managed Service Provider (MSP) Offerings – manage the ongoing weekly/daily issues associated with maintaining an AWS environment
- AWS Modernization – modernise medium to large scale applications from heritage lift and shift AWS deployments into serverless cloud native scalable applications.
- Cloud Native / Servlerless saves business time and effort in terms of Devops and costs around Managed Kubernetes services.
- Greenfields – scope, architect and build new applications
- Provide a specific set of services that are strategically focused and security first
- Provide DevOps and DevSecOps services to manage, deploy, backup and maintain AWS based applications, including EKS and ECS.
- Provide software development services, DBAs, senior developers with a wide range of skillsets across multiple stacks (being given the focus is Node and AWS)
- Focus on helping our customers to deliver business & transformational change that delivers strategic business outcomes
- Gain a firm understanding of your data and its quality. We believe data is key to effectively managing any business
- Provide specialist AWS integrated Data Analytics, Data Lake/Warehouses, Machine Learning
- Engage trusted advisors and consultants who can build partnerships with customers Determining how best to add value to our customers business'.

Our model provides a wrap-around support for our team and customers as required so that success is shared in a collaborative manner.

Business Details and Contact

Term	Detail
Trading name:	Koan Limited
Physical / postal address:	Level 2, 40 Lady Elizabeth Lane. Wellington Central, Wellington, New Zealand
Business website:	www.koan.co.nz
Type of entity (legal status):	Limited Liability Company
Registration number (NZBN):	6077527
Country of residence:	New Zealand
GST registration number:	120-563-114
Ownership	100% ownership Aotearoa, New Zealand

Item	Detail
Contact person:	Gareth Lawrence
Position:	Managing Director
Mobile number:	021 132 3991
Email address:	gareth@koan.co.nz