About Koan

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.

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 Select 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 Kurbenetes services.
- 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 which is why we put it at the centre of all our enquiries
- 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.

Operational Best Practices for NZISM

Manage Cloud Access

1. Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions, EMR clusters, EC2 instances, RDS instances, Redshift Clusters, S3 cannot be publicly accessed
2. Manage access to resources in the AWS Cloud by ensuring common ports are restricted on EC2 Security Groups.
3. Ensuring Amazon ES Domains are within an AWS VPC
4. Deploy EC2 instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC.
5. Ensure AWS Systems Manager (SSM) documents are not public
6. Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to S3

AWS Identity and Access Management (IAM)

7. Enable multi-factor authentication (MFA) for all IAM users and hardware MFA is enabled for the root user.
8. Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role.
9. The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. Check for IAM passwords and access keys that are not used for a specified time period
10. Incorporate the principles of least privilege and separation of duties with access permissions and authorizations

Restrict Access using Security Groups

11. EC2 Security Groups manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources.
12. Restrict all the traffic on the default security group restricts remote access to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on resources restricts remote access.

Encryption at Rest

13. Because sensitive data may exist and to help protect data at rest, ensuring encryption is used by default where applicable.
14. Encryption is enabled for AWS CloudTrail trails and CloudWatch Log Groups

15. Ensure that encryption is enabled for AWS EBS volumes, AWS EFS, AWS S3 buckets, RDS instances, RDS snapshots
16. Ensure encryption is enabled for API Gateway stage's cache
17. ensure encryption with AWS KMS is enabled for AWS Secrets Manager secrets

Encrypt Data in Transit

18. Ensure ELBs are configured with SSL or HTTPS listeners and ALBs redirects HTTP requests to HTTPS
19. Ensure Redshift clusters require TLS/SSL encryption to connect to SQL clients.
20. ensure that Classic ELB SSL listeners are using a custom security policy.
21. Ensure that S3 buckets require requests to use Secure Socket Layer (SSL)

Auditing

22. Ensure consolidated logging and monitoring are properly used within the AWS environment
23. Configure CloudTrail with CloudWatch Logs to monitor trail logs and be notified when specific activity occurs
24. Use AWS CloudTrail in non-repudiation by recording AWS Console actions and API calls
25. Ensure a minimum duration of event log data is retained for log groups to help with troubleshooting and forensics investigation
26. Enable Amazon RDS logging
27. Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs.
28. Enable AWS WAF (V2) logging on regional and global web ACLs
29. VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in VPCs
30. API Gateway logging displays detailed views of users who and the way they accessed the API

AWS Web Application Firewall

31. Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications

Ensure Network Integrity

32. Use AWS Systems Manager to provide detailed system configurations
33. Network integrity is protected by ensuring X509 certificates are issued by AWS ACM
34. Elastic Load Balancing activity is a central point of communication within an environment

AWS Key Management Service

35. AWS KMS enables customers to rotate the backing key, which is key material stored in AWS KMS and is tied to the key ID of the CMK

36. At least one KMS Customer Master Key (CMK) has been defined for each distinct data classification, and the CMK(s) are being used to encrypt all data stored at that classification.

Vulnerabilities Checking

37. Enable rule to help with identification and documentation of EC2 vulnerabilities
38. Patch Baselines for Windows and/or Linux have been configured in Patch Manager, including auto-approval of critical security patches within 2 days of release.

Monitor Cybersecurity

39. Use Amazon GuardDuty to help monitor and detect potential cybersecurity events by using threat intelligence feeds
40. Use AWS Security Hub to monitor unauthorized personnel, connections, devices, and software.
41. Use the collection of S3 data events to help in detecting any anomalous activity

Business Continuity

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

AWS Backup Plan

44. The backup feature of Amazon RDS creates backups of your databases and transaction logs
45. To enable data back-up processes ensure RDS instances, DynamoDB tables, EBS volumes, EFS are part of an AWS Backup Plan
46. When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis
47. Ensure Amazon RDS instances have deletion protection enabled.
48. Ensure Amazon Redshift clusters have automated snapshots
49. S3 bucket versioning helps keep multiple variants of an object in the same S3 bucket

Our Business:

Tem	Detail
Trading name:	Koan Limited
Physical address:	7th Floor, Aviation House, 12 Johnston Street, Wellington 6011
Postal address:	565 Featherston Street, Palmerston North
Registered office:	565 Featherston Street Palmerston North
Business website:	www.koan.co.nz
Type of entity (legal status):	Limited Liability Company
Registration number:	6077527
Country of residence:	New Zealand
GST registration number:	120-563-114

Our Point of Contact

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