

KEMENTERIAN PENDIDIKAN

MOE ENTERPRISE CLOUD (MEC)

**PROGRAM CAKNA MYGOVCLOUD@CFA 2026 BERSAMA PENTADBIR PROJEK
PENGGUNA GOVERNMENT HYBRID CLOUD (GHC)**

Shahrul Faizal Selamat

Unit Pengurusan Pengkomputeran Awan
Seksyen Pusat Data, Pengkomputeran Awan dan Emel
Bahagian Pengurusan Maklumat
Kementerian Pendidikan

PENGENALAN



KEMENTERIAN PENDIDIKAN

1

Dasar Cloud First

Transformasi digital sektor awam Malaysia melalui Dasar Pengkomputeran Awan Negara (Cloud First Policy)

2

Pemodenan ICT KPM

Keperluan KPM memodenkan infrastruktur ICT bagi menyokong ekosistem pendidikan negara

3

Bermula April 2022

Perjalanan pengkomputeran awan KPM bermula dengan projek pertama - Aplikasi Online SPM Result

4

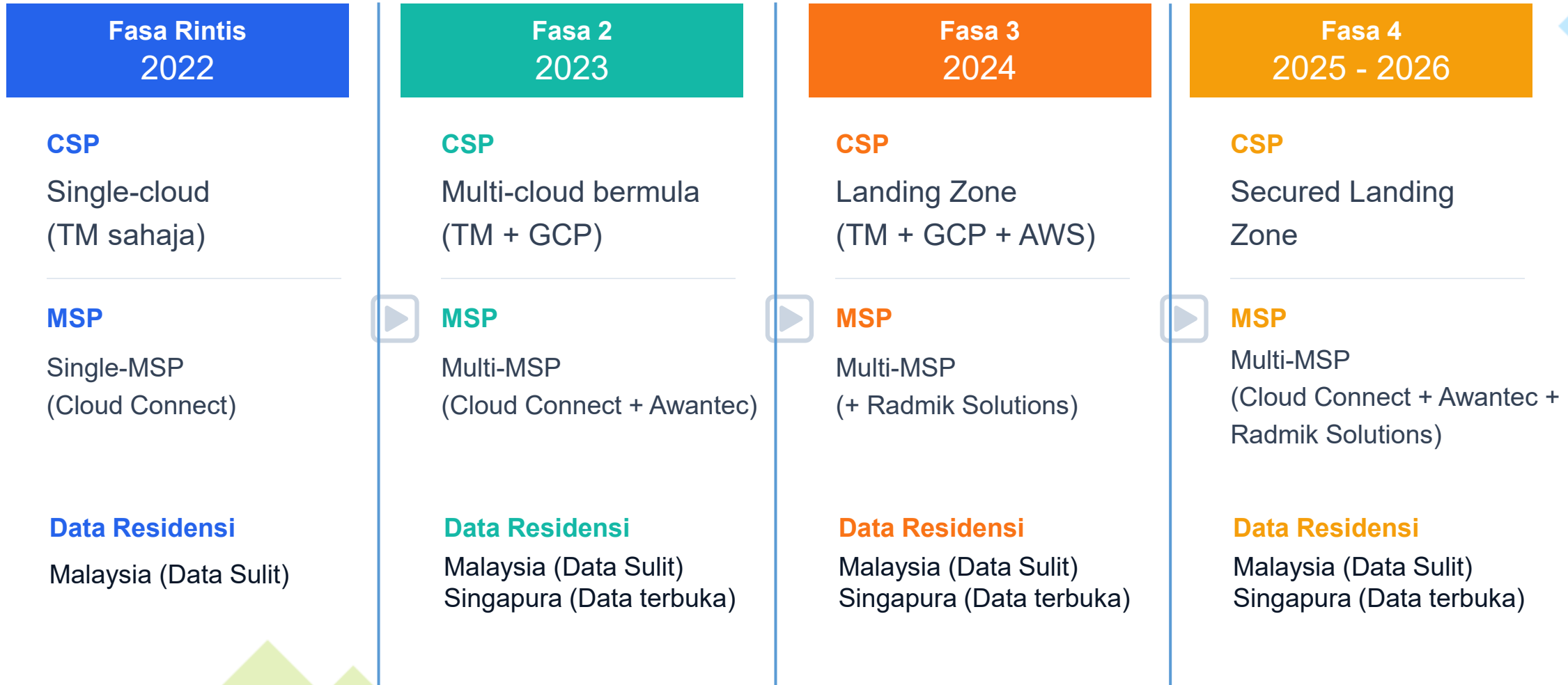
10 Projek Sehingga Kini

Kini telah berkembang kepada 10 projek merangkumi 30 sistem yang digunakan secara pentadbiran (PdT) serta Pengajaran dan Pembelajaran (PdP) di KPM.

GARIS MASA PENGKOMPUTERAN AWAN KPM



KEMENTERIAN PENDIDIKAN



PORTFOLIO PROJEK



KEMENTERIAN PENDIDIKAN

10

Projek
Keseluruhan
5 Tamat | 5 Aktif

RM47M

Jumlah Nilai
Kontrak
Sejak 2022

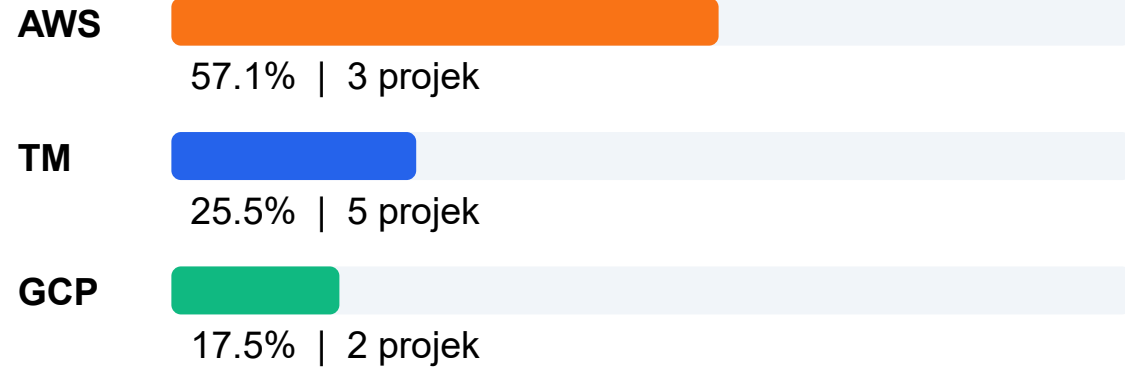
3

Cloud Service
Provider
AWS | TM | GCP

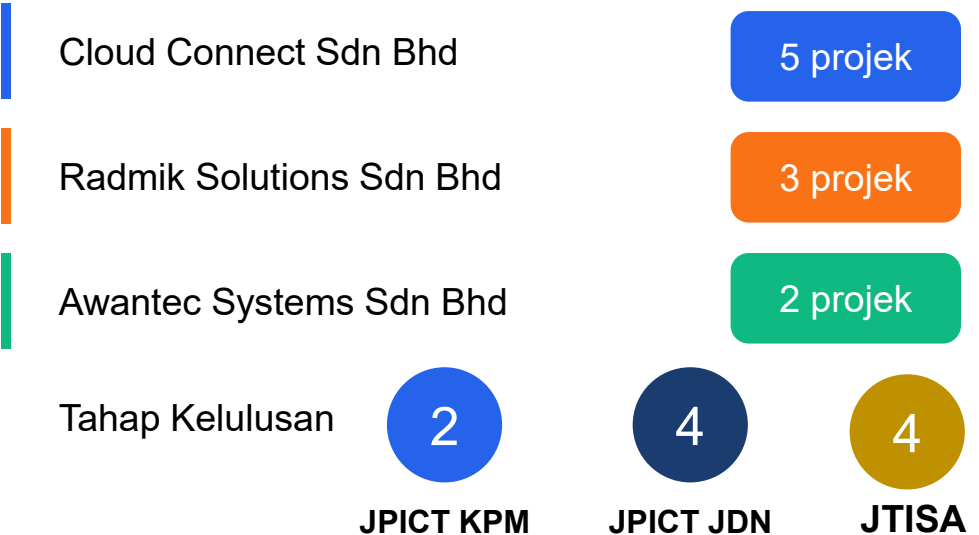
3

Managed Service
Provider
Cloud Connect | Radmik | Awantec

Pecahan CSP (Nilai)



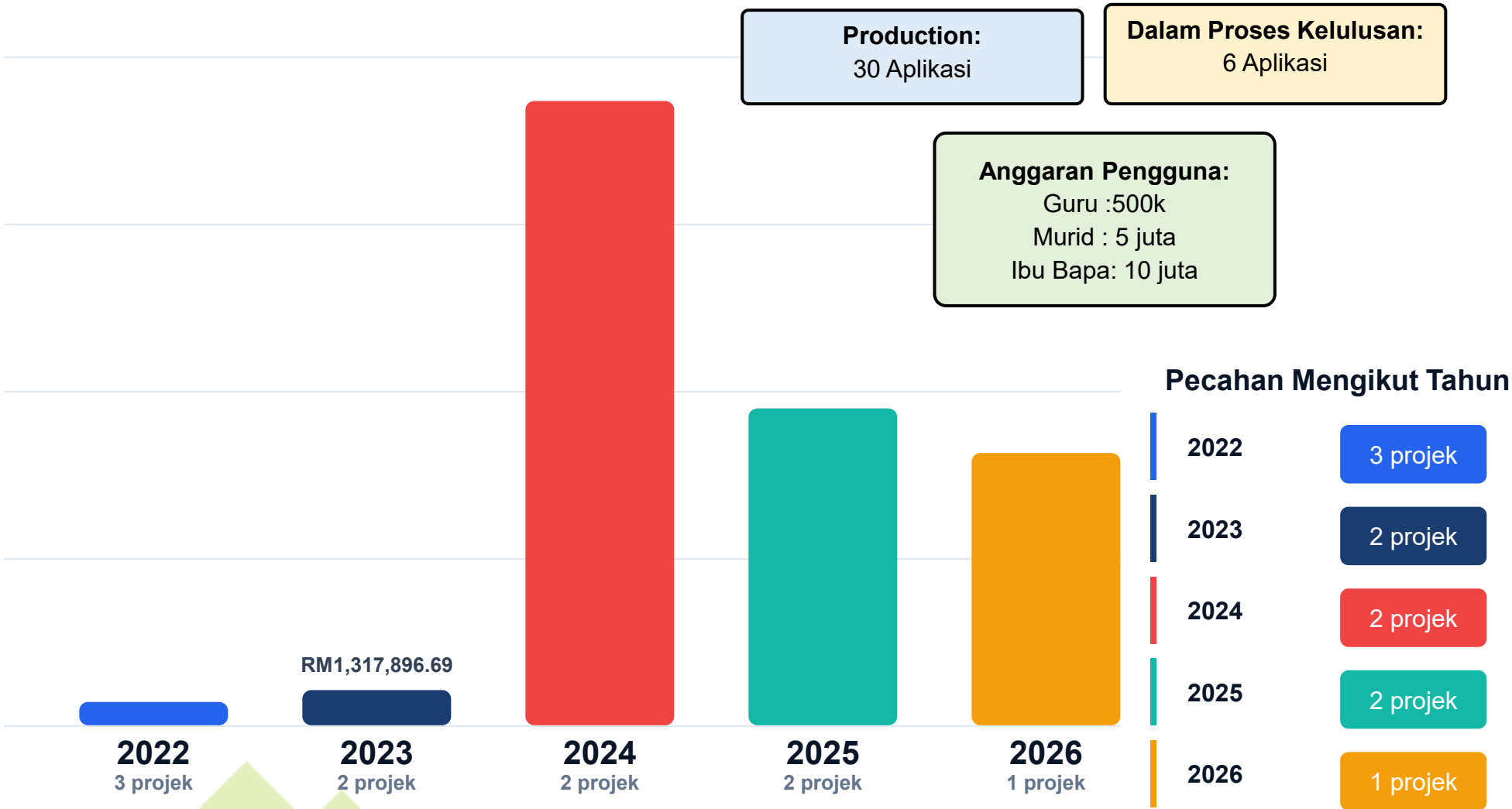
Pecahan MSP



PORTFOLIO PROJEK



KEMENTERIAN PENDIDIKAN



ISU DAN CABARAN



KEMENTERIAN PENDIDIKAN

1 Migrasi Data Legasi

Migrasi data dari sistem legasi (*legacy systems*) ke persekitaran awan.

2 Keserasian Aplikasi

Isu keserasian aplikasi sedia ada dengan platform awan berbeza (AWS/GCP/TM).

3 Multi-Cloud

Koordinasi dan pengurusan persekitaran multi-cloud (3 CSP berbeza) — kompleksiti operasi

4 Proses Kelulusan

Proses kelulusan (BAKAT/JPICT KPM / JTISA) memerlukan masa yang panjang

5 Perolehan & Kontrak

Proses perolehan secara manual dan pengurusan kontrak yang kompleks..

6 Pengoptimuman Kos

Memastikan kos penggunaan cloud berada pada tahap yang optimum.

7 Klasifikasi Data

Penentuan klasifikasi data bagi residensi data.

8 Kemahiran Teknikal

Keperluan latihan teknikal untuk pentadbir cloud KPM.

9 Keselamatan Siber

Pengurusan dan pematuhan keselamatan siber.

PENAMBAHBAIKAN



KEMENTERIAN PENDIDIKAN



Pewujudan Unit Pengurusan Pengkomputeran Awan

Pewujudan unit baharu bagi menguruskan perolehan dan kontrak cloud di KPM.



Pegawai Pengelas

Melantik pegawai pengelas bagi setiap bahagian di KPM..



Penggunaan Agentic AI

Menggunakan AI bagi menyelesaikan isu keserasian aplikasi sedia ada dengan platform awan. Cth: AWS Kiro, AWS Transform.



MOE Cloud Sandbox

Penyediaan Cloud Sandbox bagi pelaksanaan Proof of Concept (POC) dan pengujian aplikasi di cloud.



Secured Landing Zone

Pembangunan secured landing zone berdasarkan MOE Enterprise Cloud (MEC) Framework bagi setiap cloud platform.

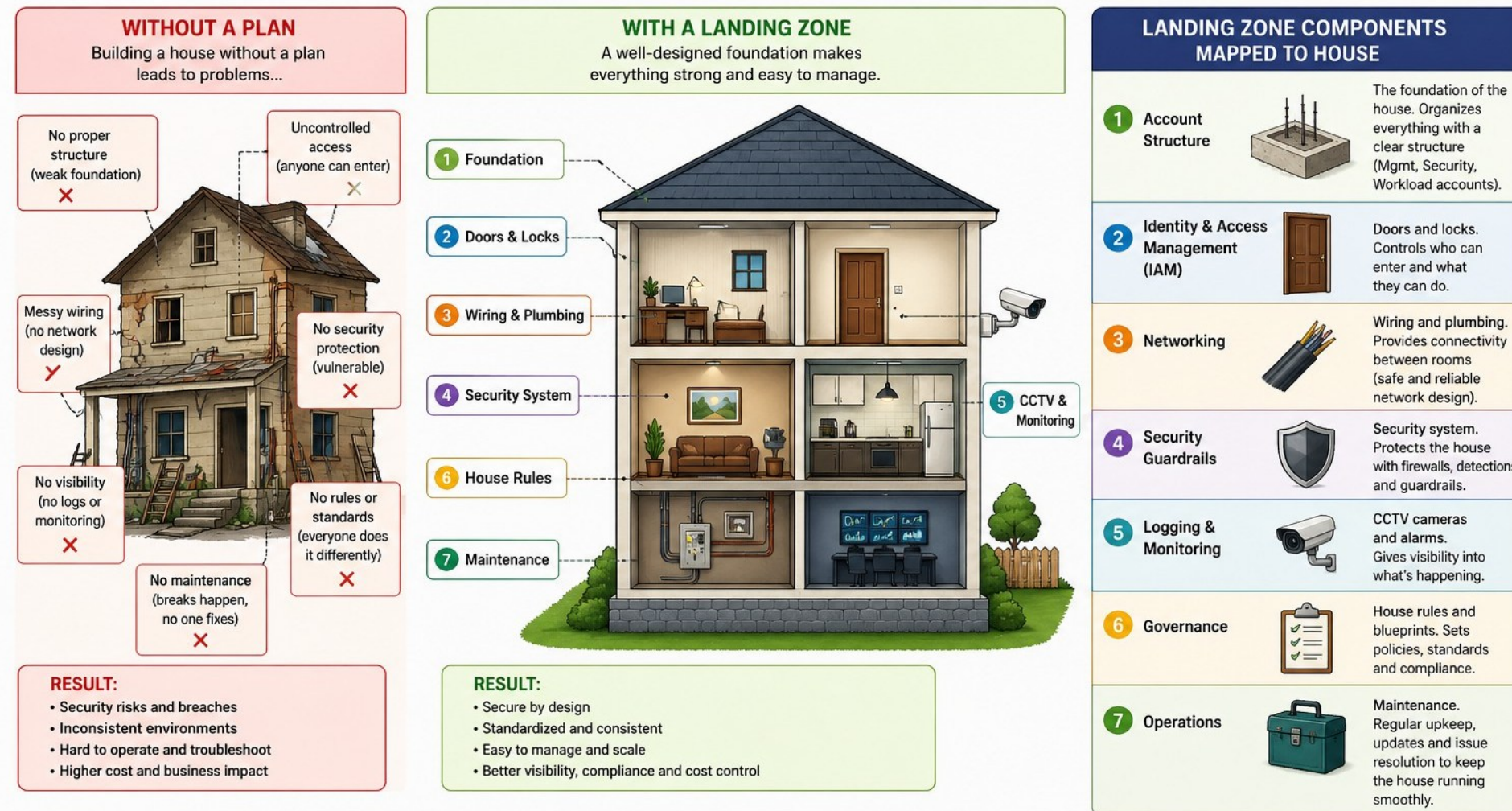


Latihan

17 sesi latihan termasuk certified training, workshop, immersion bagi 385 oarng peserta.

SECURED LANDING ZONE = BUILDING A HOUSE

A landing zone provides a secure, well-architected foundation to build and run workloads in public cloud.



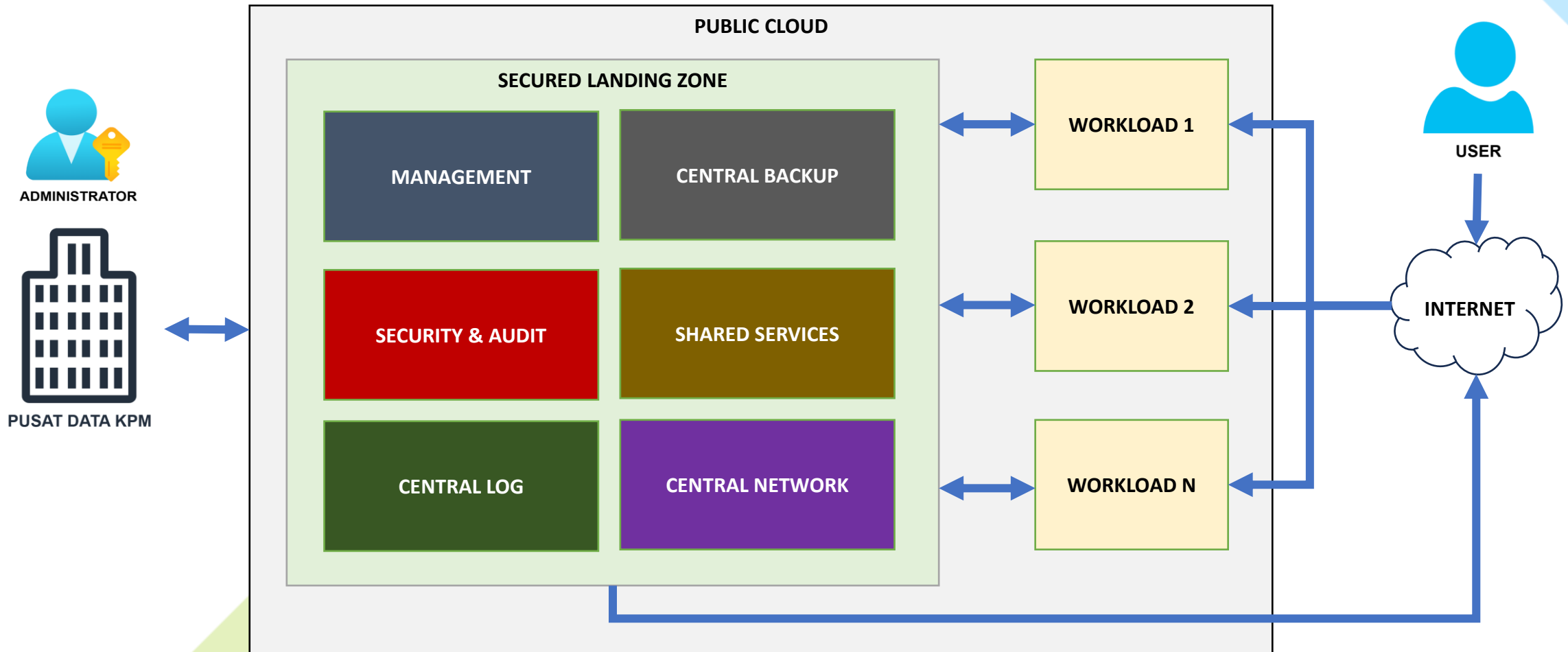
Landing zone = Account structure + identity + network + security + logging + governance + operations

HIGH LEVEL ARCHITECTURE DIAGRAM

- MOE ENTERPRISE CLOUD (MEC) FRAMEWORK



KEMENTERIAN PENDIDIKAN



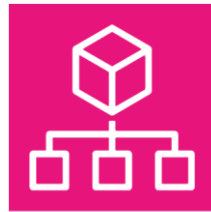
SERVICES IN SECURED LANDING ZONE

- MANAGEMENT ACCOUNT



AWS Control
Tower

- **Landing zone setup**
- Account enrolment
- Baseline guardrails
- Organization CloudTrail
- Enable Deny Region



AWS
Organization

- Creating and managing OUs
- **Grouping workload accounts**
- Applying Service Control Policies (SCP) and Resource Control Policy (RCP)



AWS
CloudFormation

- Deploy **infrastructure as a code (IaC)**.
- For example: Deploying central network resources



AWS Identity
Center

- Single sign-on to AWS accounts
- **Central user and group assignment**
- Integration with an identity provider such as Microsoft Entra ID or Okta where required



AWS
KMS

- KMS provides **encryption keys** for data protection.
- For example: CloudTrail encryption, CloudWatch Logs encryption, EBS default encryption, Backup encryption, S3 and etc.

SERVICES IN SECURED LANDING ZONE

- SECURITY & AUDIT ACCOUNT



KEMENTERIAN PENDIDIKAN



AWS
Config

- **Configuration history**
- Compliance evaluation
- Security Hub controls evidence
- Detecting resource drift and non-compliant configurations



AWS
GuardDuty
(Central)

- It **detects threats** using CloudTrail, VPC DNS, VPC Flow Logs, EKS, S3, runtime, malware, and other signals, depending on enabled protection plans.
- Audit account assigned as delegated admin



AWS
Inspector
(Central)

- It **scans** workloads for **vulnerabilities**
- EC2 vulnerability scanning
- ECR container image scanning
- Lambda vulnerability scanning

Notes:

* Service configured as Administrative (Delegated/Admin) Account.

Central : Centralized across all accounts



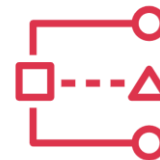
AWS
Security Hub
(Central)

- **Central security dashboard**
- Aggregating findings from GuardDuty, Inspector, IAM Access Analyzer, and other services



AWS Firewall
Manager *

- It centrally **manages security policies** across accounts.
- For example: WAF policies, Security group policies and Network Firewall policies



AWS IAM
Access Analyzer *

- It **identifies resources** that are shared externally or **outside** the intended zone of **trust**.
- For example: Reviewing S3 bucket policies, IAM roles, KMS keys, and other resource policies



AWS S3
(Central for Config)

- It is used for centralized storage for AWS Config.
- It centrally **stores the config** log across accounts.

SERVICES IN SECURED LANDING ZONE

- CENTRAL BACKUP AND LOG ACCOUNT



KEMENTERIAN PENDIDIKAN



AWS
CloudTrail *

- It **records AWS API activity**.
- In Control Tower, the baseline organization trail captures management events across accounts and sends logs to centralized storage.



AWS S3
(Central for Cloudtrail)

- It is used for centralized storage for AWS CloudTrail.
- It centrally **stores the cloudtrail** log across accounts.



AWS Backup
(Central)

- It centrally manages backup policies and vaults.
- Used for:
 - Backup plan management Backup vaults
 - Cross-account backup operations Central backup governance

Notes:

** Service configured as Administrative (Delegated/Admin) Account.*

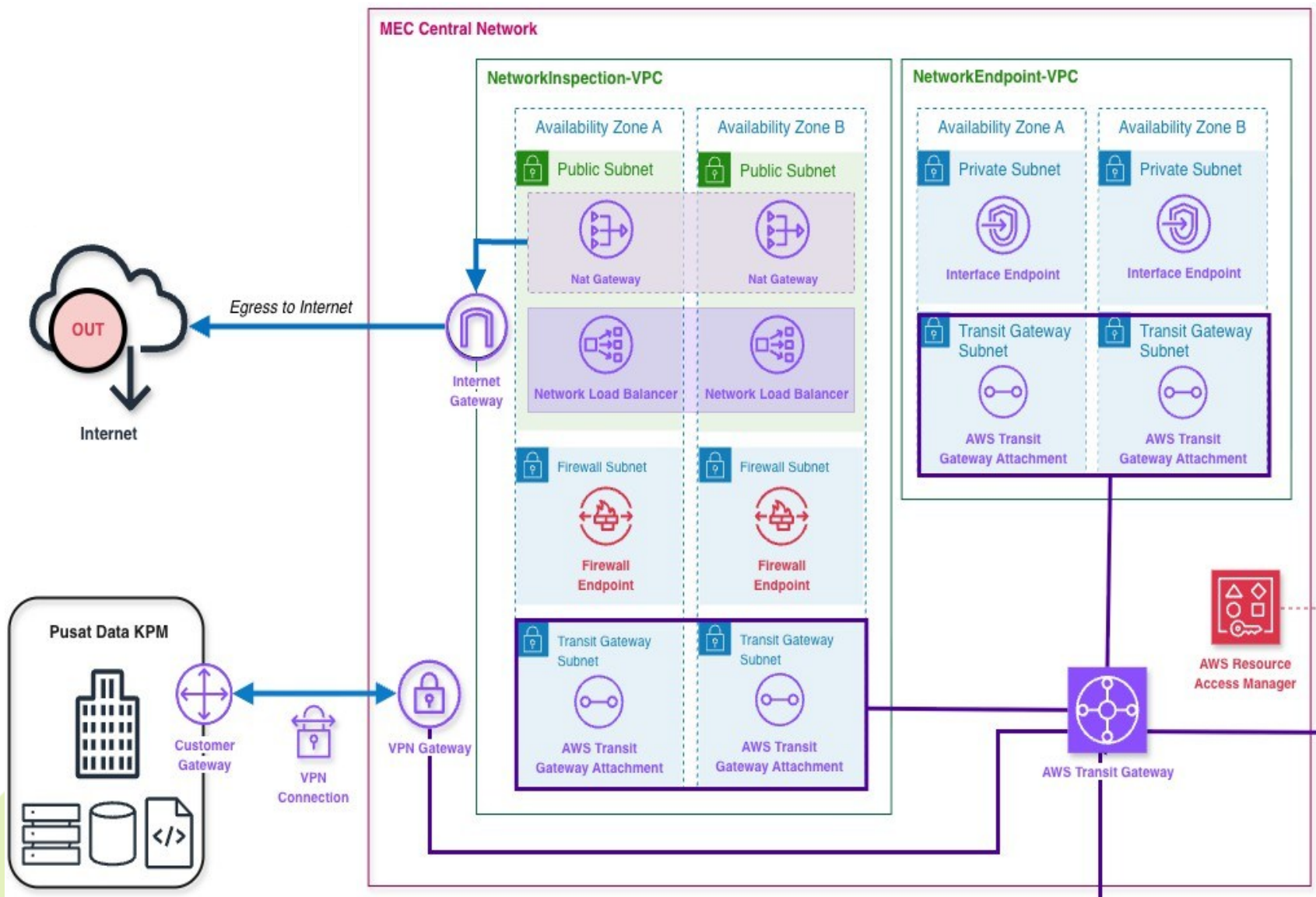
Central : Centralized across all accounts

SERVICES IN SECURED LANDING ZONE

- CENTRAL NETWORK ACCOUNT



KEMENTERIAN PENDIDIKAN



SERVICES IN SECURED LANDING ZONE

- SHARED SERVICES ACCOUNT



KEMENTERIAN PENDIDIKAN



AWS IAM *

- IAM controls permissions inside AWS accounts.
- In SLZ, IAM is used together with IAM Identity Center, IAM roles, and managed policies.
- Shared Service account assigned as delegated admin



AWS System Manager *

- Systems Manager helps manage EC2 instances without direct SSH access.
- **Session Manager access**
- Patch management
- Shared Service account assigned as delegated admin



AWS Identity Center *

- Shared Service account assigned as delegated admin



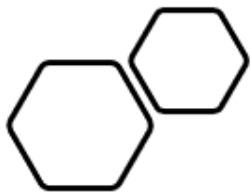
AWS Backup *

- Shared Service account assigned as delegated admin

Notes:

* Service configured as Administrative (Delegated/Admin) Account.

Central : Centralized across all accounts



KEMENTERIAN PENDIDIKAN

Q & A



KEMENTERIAN PENDIDIKAN

**SEKIAN
TERIMA KASIH**