KERAJAAN MALAYSIA

SURAT PEKELILING AM BILANGAN 2 TAHUN 2021

GARIS PANDUAN PENGURUSAN KESELAMATAN MAKLUMAT MELALUI PENGKOMPUTERAN AWAN (CLOUD COMPUTING) DALAM PERKHIDMATAN AWAM

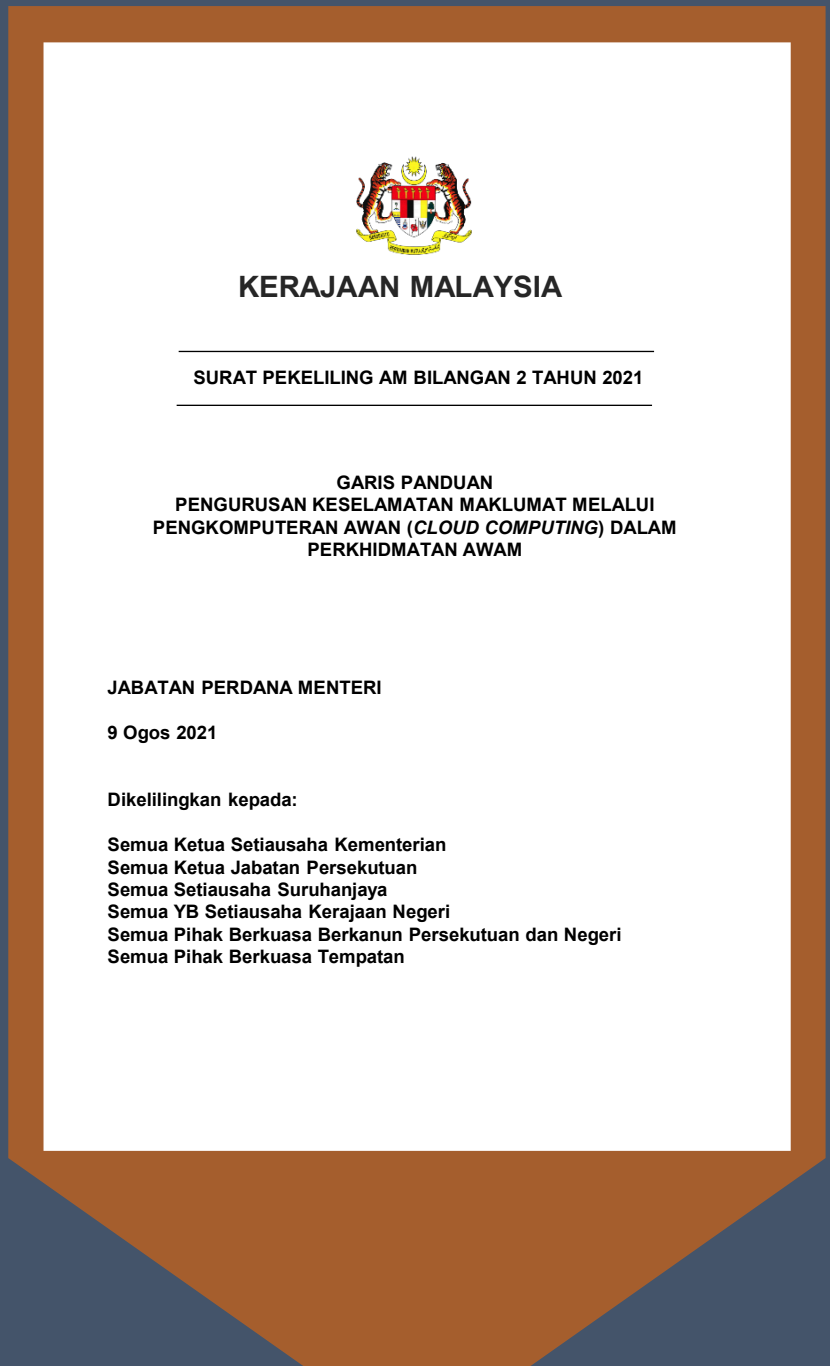
Disediakan oleh:
Bahagian Keselamatan ICT dan Rahsia Rasmi
Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia

KERAJAAN MALAYSIA

TUJUAN TAKLIMAT

Menjelaskan pindaan **Surat Pekeliling Am Bilangan 2 Tahun 2021 Yang Mengandungi Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (Cloud Computing) Dalam Perkhidmatan Awam Versi 2.0**

Garis panduan versi 2.0 ini bertujuan membantu Jabatan menggarap strategi transformasi digital melalui ekosistem pengkomputeran awan yang selamat, diyakini, komprehensif dan kompetitif berasaskan standard dan amalan terbaik keselamatan global.



KERAJAAN MALAYSIA

SURAT PEKELILING AM BILANGAN 2 TAHUN 2021

GARIS PANDUAN
PENGURUSAN KESELAMATAN MAKLUMAT MELALUI PENGKOMPUTERAN AWAN (*CLOUD COMPUTING*) DALAM PERKHIDMATAN AWAM

JABATAN PERDANA MENTERI

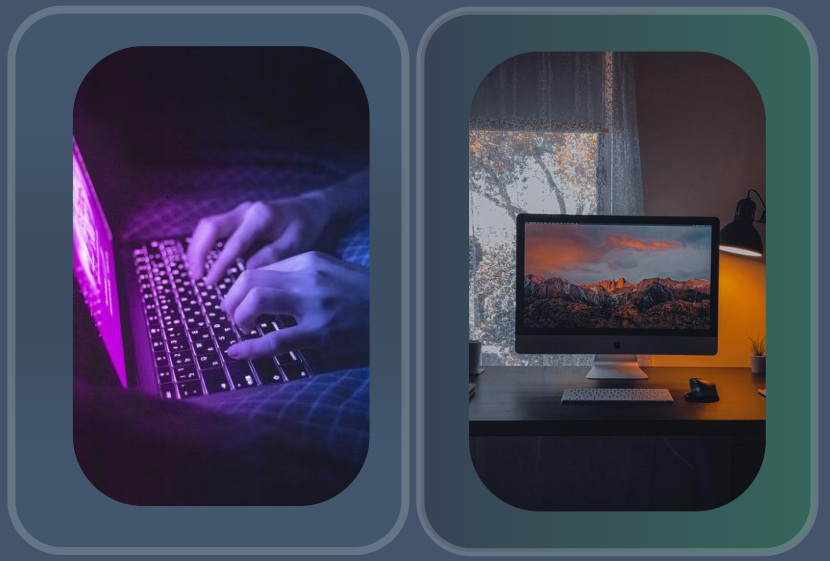
9 Ogos 2021

Dikelilingkan kepada:

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Setiausaha Suruhanjaya
Semua YB Setiausaha Kerajaan Negeri
Semua Pihak Berkuasa Berkanun Persekutuan dan Negeri
Semua Pihak Berkuasa Tempatan

KERAJAAN MALAYSIA

CYBERSECURITY RISK



Cybersecurity risk is an effect of uncertainty on information and technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and **assets**, individuals, other organizations, and the Nation

Sources:
NISTIR 8286 from ISO Guide 73 - Adapted, NIST SP 800-60 Vol. 1 Rev. 1 - Adapted

Personal Cloud Computing Use Cases

Cloud Storage & File Syncing

Google Drive – Offers 15GB of free storage

Icedrive – Gives **10GB** of free storage with secure encryption

Degoo – Provides 100GB of free storage, but with ads.

Dropbox – Gives users 2GB of free storage

Mega – Offers 50GB of free storage with strong encryption

iCloud offers 5GB of free storage

OneDrive – Provides 5GB of free storage from Microsoft

Sync.com – Offers 5GB of free storage with privacy-focused features

Huawei offers 5GB of free storage

Productivity Tools and Photo Backup

Cross-device access for seamless productivity

KERAJAAN MALAYSIA

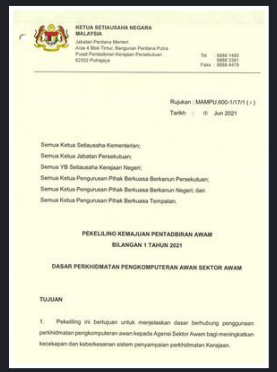
PENGENALAN: PUNCA KUASA SURAT PEKELING AM

Penggunaan pengkomputeran awan (cloud computing) seperti perkongsian maklumat, pemprosesan data dan sebagainya bagi tujuan rahsia rasmi tidak dibenarkan sama sekali kecuali pengkomputeran awan yang dibangunkan dan dibenarkan oleh pihak Kerajaan dan tertakluk kepada arahan-arahan yang dikeluarkan oleh Kerajaan dari semasa ke semasa.

Derived from compliance mandates and legal requirements.

Perenggan 139 Arahan Keselamatan (Semakan Dan Pindaan 2017)

EXISTING POLICY, REGULATION AND PROCEDURES IN PUBLIC SECTOR CLOUD COMPUTING


KETUA SETIAUSAHA NEGARA
MALAYSIA

Rujukan : MAMPU.600-1/17/1 ( )
Tarikh : 16 Jun 2021

Semua Ketua Setiausaha Kementerian;
Semua Ketua Jabatan Persekutuan;
Semua YB Setiausaha Kerajaan Negeri;
Semua Ketua Pengurusan Pihak Berkuasa Berkanun Persekutuan;
Semua Ketua Pengurusan Pihak Berkuasa Berkanun Negeri; dan
Semua Ketua Pengurusan Pihak Berkuasa Tempatan.

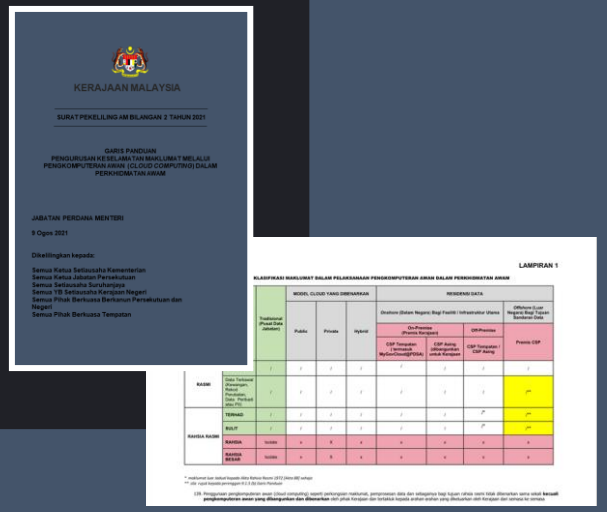
PEKELILING KEMAJUAN PENTADBIRAN AWAM
BILANGAN 1 TAHUN 2021

DASAR PERKHIDMATAN PENGKOMPUTERAN AWAN SEKTOR AWAM

TUJUAN

1. Pekeliling ini bertujuan untuk menjelaskan dasar berhubung penggunaan perkhidmatan pengkomputeran awan kepada Agensi Sektor Awam bagi meningkatkan kecekapan dan keberkesanan sistem penyampaian perkhidmatan Kerajaan.

PKPA Bil. 7/2024
Surat Pekeliling Am ini terpakai kepada semua agensi Sektor Awam bagi semua projek ICT yang dibiayai oleh peruntukan kewangan Persekutuan atau projek ICT yang dilaksanakan melalui kaedah Private Finance Initiative (PFI)/ Public-Private Partnership (PPP).


KERAJAAN MALAYSIA

SURAT PEKELILING AM BILANGAN 2 TAHUN 2021

GARIS PANDUAN
PENGURUSAN KESELAMATAN MAKLUMAT MELALUI PENGKOMPUTERAN AWAN (CLOUD COMPUTING) DALAM PERKHIDMATAN AWAM

JABATAN PERDANA MENTERI

9 Ogos 2021

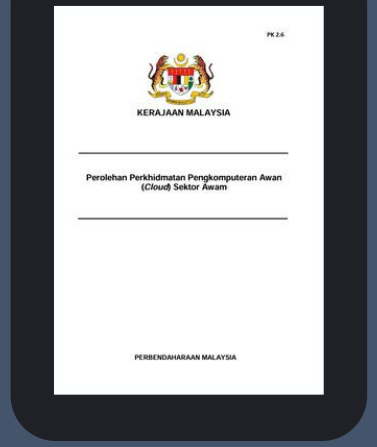
Dikeluarkan kepada:

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Setiausaha Suruhanjaya
Semua YB Setiausaha Kerajaan Negeri
Semua Pihak Berkuasa Berkanun Persekutuan dan Negeri
Semua Pihak Berkuasa Tempatan

LAMPIRAN 1

KLASIFIKASI RISIKO/MAKLUMAT DALAM PELAKSANAAN PENGKOMPUTERAN AWAN DALAM PERKHIDMATAN AWAM

SPA Bil. 1/2021
Pemakaian pekeliling ini terpakai kepada semua agensi Perkhidmatan Awam Persekutuan


PK 2.6

KERAJAAN MALAYSIA

Perolehan Perkhidmatan Pengkomputeran Awan (*Cloud*) Sektor Awam

PERBENDAHARAAN MALAYSIA

PK2.6: Perolehan Perkhidmatan Pengkomputeran Awan Sektor Awam


Kontrak Panel Berpusat / Cloud Framework Agreement (CFA)

5.2 Agensi hendaklah memastikan perkhidmatan *cloud* yang melibatkan penyimpanan dokumen atau maklumat rahsia rasmi diurus berdasarkan peraturan keselamatan yang berkuat kuasa dan tertakluk kepada pematuhan Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (*Cloud Computing*) Dalam Perkhidmatan Awam atau arahan lain yang dikeluarkan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO).


MALAYSIA MADANI

NATIONAL CLOUD COMPUTING POLICY

MADANI : Secure, Sovereign, Inclusive, and Sustainable Cloud Futures

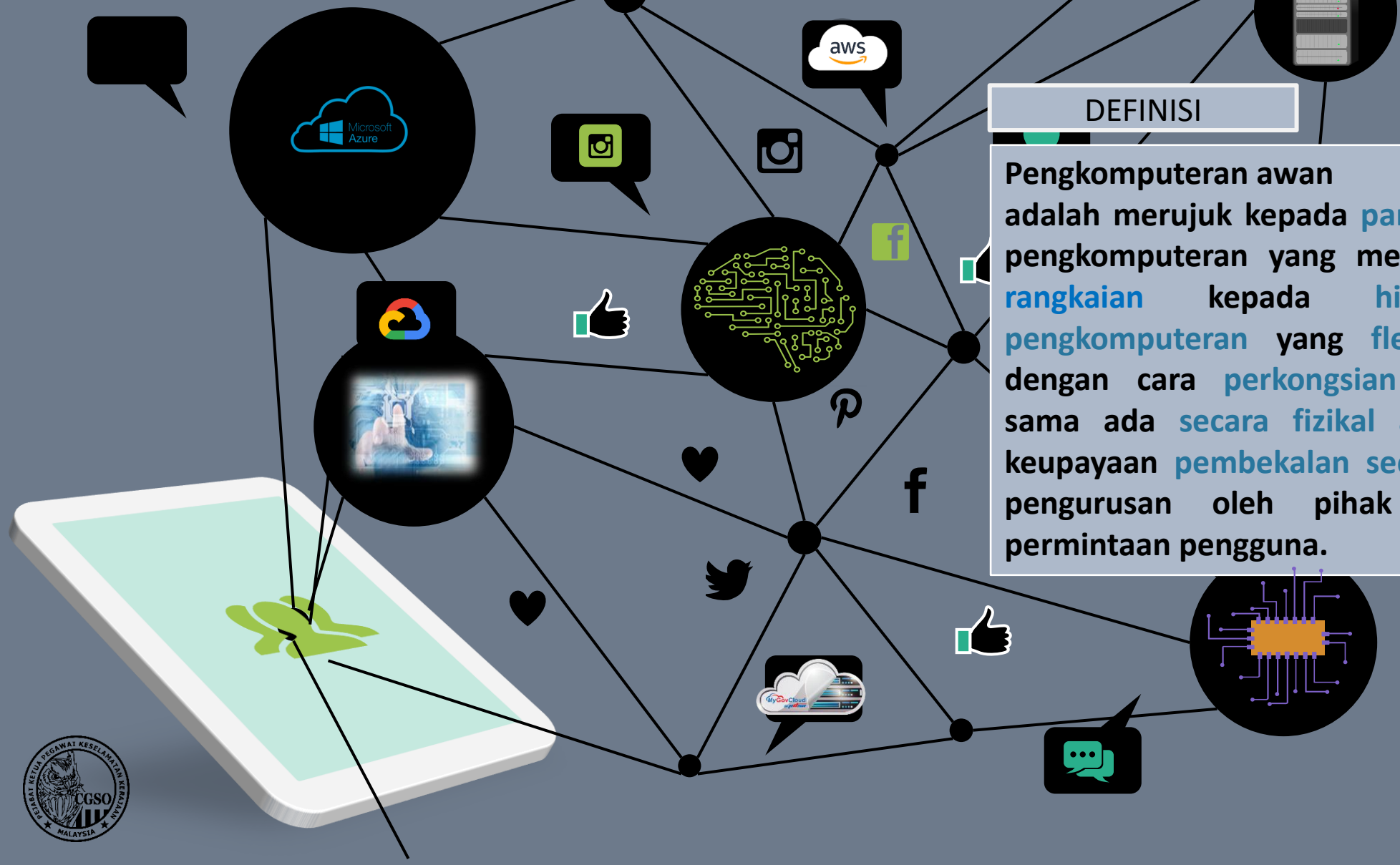
Dasar Pengkomputeran Awan Negara (NCCP)

PERKARA 1 - PENGENALAN

KERAJAAN MALAYSIA

DEFINISI

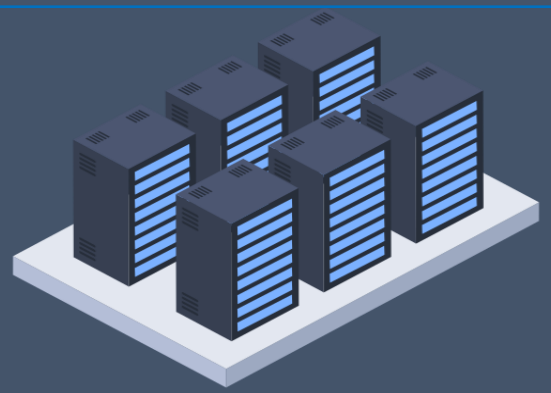
Pengkomputeran awan
adalah merujuk kepada paradigma atau model pengkomputeran yang membolehkan capaian rangkaian kepada himpunan sumber pengkomputeran yang fleksibel dan elastik dengan cara perkongsian sumber bersama, sama ada secara fizikal atau maya dengan keupayaan pembekalan secara layan diri atau pengurusan oleh pihak ketiga mengikut permintaan pengguna.



CONFIGURABLE COMPUTING RESOURCES IN HYPERSCALE DC & DRC

KERAJAAN MALAYSIA

Resource pooling



Global Infrastructure : DC and DRC in multiple locations worldwide

Use Case:
Choose **region** based on latency, compliance, or user base
Deploy across **AZs** for **redundancy and failover**

Measured service

PARTNERED & OPERATED BY

amazon Microsoft TM ONE

On-demand self-service

LARGE-SCALE ICT RESOURCES

Networking

Storage

Computing Power

Rapid elasticity

ACCESSIBLE VIA THE INTERNET

Broad network access

VARIOUS CLIENTS

Bank

Retail

Government

Multi Tenants
(Public Cloud Model)

KERAJAAN MALAYSIA

SALIENT POINT KEPADA PINDAAN


Lampiran kepada Surat Pekeliling Am Bilangan 2 Tahun 2021
versi 2.0

Garis Panduan
Pengurusan Keselamatan Maklumat Melalui
Pengkomputeran Awan (Cloud Computing) Dalam
Perkhidmatan Awam

3 EDITORIAL

* pembetulan kesalahan minor seperti ejaan dan format dokumen

22 SUBSTANTIF

* penjelasan tambahan atau lain-lain perubahan minor dan major ke atas kandungan

KERAJAAN MALAYSIA

Key Challenges in Cloud Adoption

Sovereignty still in gray area

Customer

LEGISLATIVE OBLIGATIONS

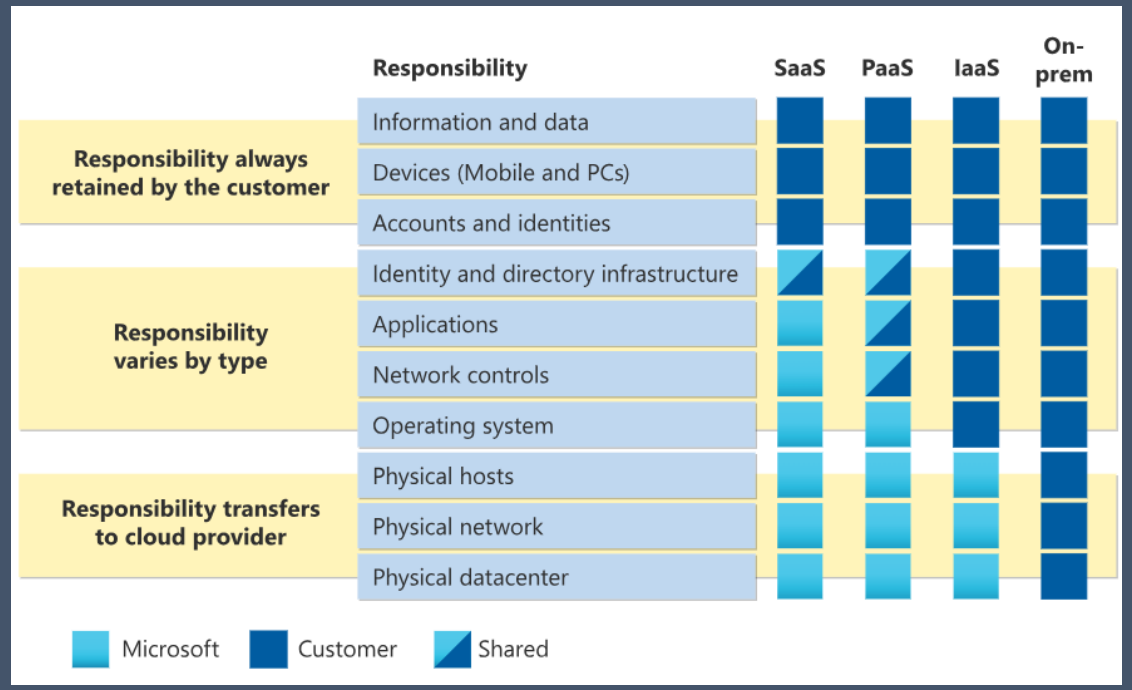
CSP

KERAJAAN MALAYSIA

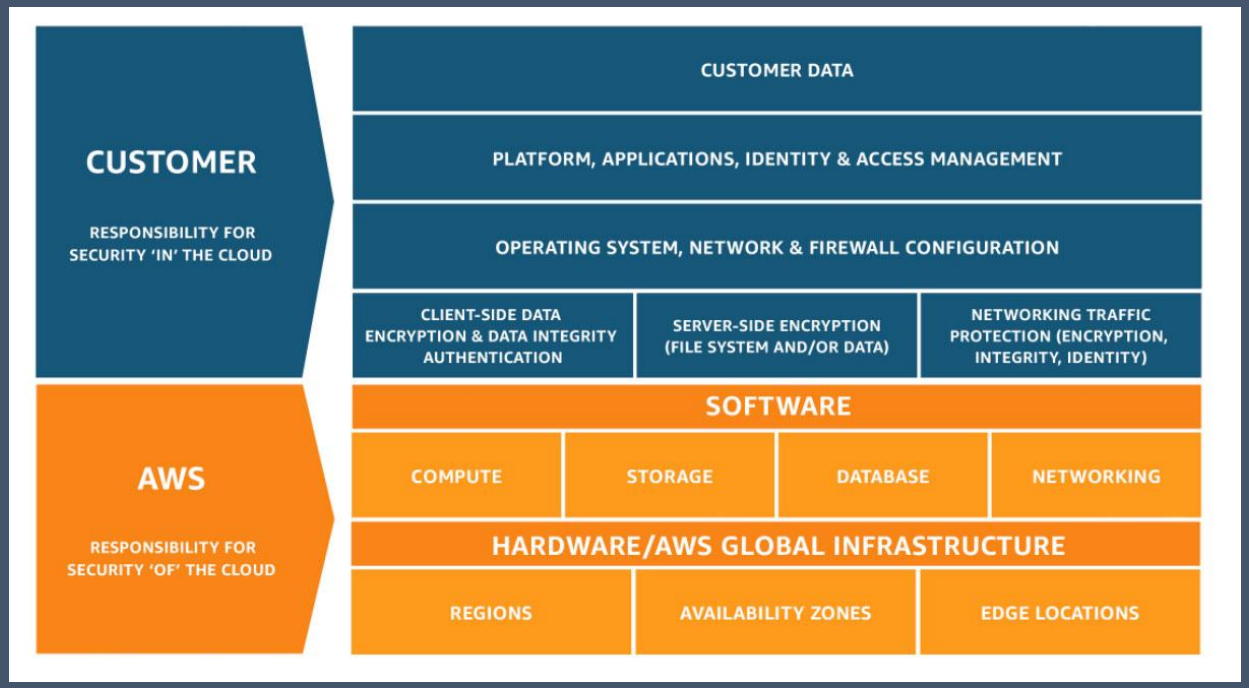
Key Challenges in Cloud Adoption

Security

Shared Responsibility Model



https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility



https://aws.amazon.com/compliance/shared-responsibility-model/

Shared Responsibility Model

KERAJAAN MALAYSIA

Network Engineer

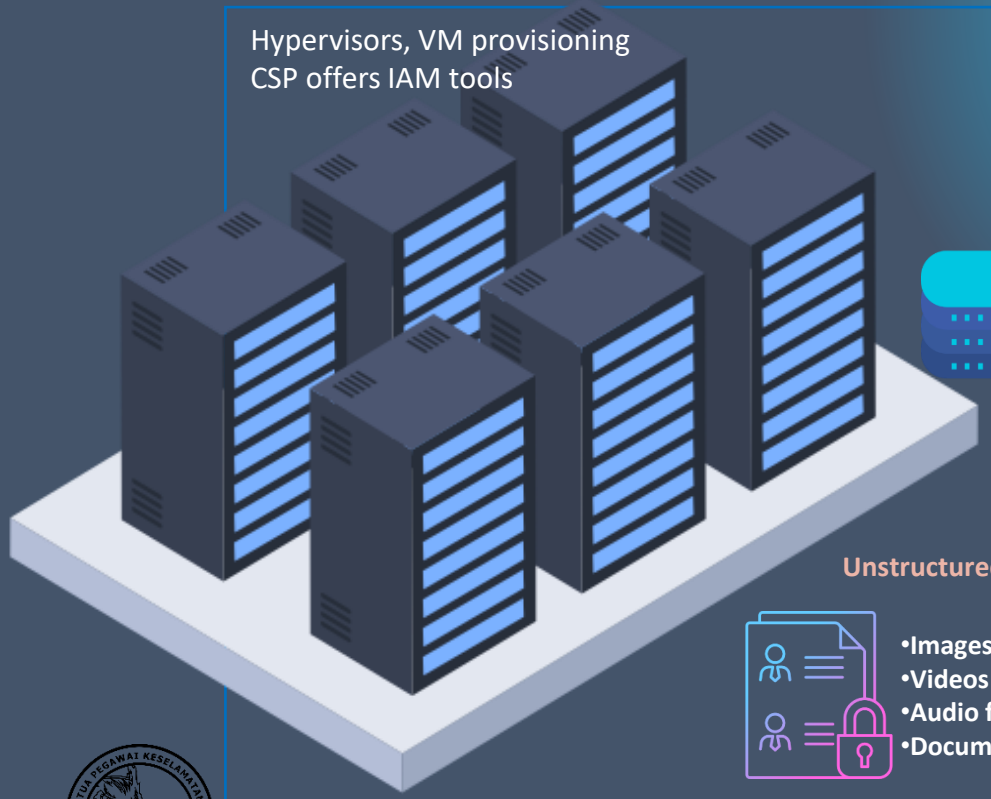
Cloud Engineer

Security Manager

IT / Technology Engineer

CSPs Manages The Data Centers, Physical Server, **Hypervisor**, Power, And Networking.

Hypervisors, VM provisioning
CSP offers IAM tools



Structured Data
PII
Financial Record
Health Record
Geospatial

Unstructured Data

- **Images**: JPEGs, PNGs, and GIFs
- **Videos**: YouTube uploads, surveillance footage, training videos
- **Audio files**: Podcasts, voice memos, call recordings
- **Documents**: PDFs, Word files, presentations, and scanned reports

Config File

TECHNOLOGY STACK

Data Processor/ Data Steward

Identity & Access Management (IAM)
Configure IAM roles, enforce least privilege, use MFA, and monitor access logs.
Application Security
Patch vulnerabilities, validate inputs, and secure APIs and endpoints.
Configuration & Resource Management
Client configures the VM, installs the OS, runtime, middleware, and deploys applications
Endpoint & Device Management

Data Owner

Data Governance & Classification
Compliance & Audit Readiness

by SE Madnick · 2022 · Cited by 3 — This paper details the **growing and evolving threat to consumer data** when stored and processed on corporate computer systems, servers, and networks.

KERAJAAN MALAYSIA

Real-World Examples

Web Hosting: Deploy a website using AWS EC2 or Azure Web Apps.

AI/ML Training: Use GPU-powered instances on Google Cloud to train models.

Data Processing: Run big data jobs on AWS EMR or Azure Databricks.

Disaster Recovery: Spin up backup environments in another region using cloud snapshots.

Gaming Servers: Host multiplayer game backends on scalable compute nodes.

Physical Host, Network and Data Centre

Data Owner

Data Governance & Classification
Compliance & Audit Readiness

- **Images**: JPEGs, PNGs, and GIFs—especially when analyzing content inside the image
- **Videos**: YouTube uploads, surveillance footage, training videos
- **Audio files**: Podcasts, voice memos, call recordings
- **Documents**: PDFs, Word files, presentations, and scanned reports

KERAJAAN MALAYSIA

Key Challenges in Cloud Adoption

Cloud Storage Data Breaches

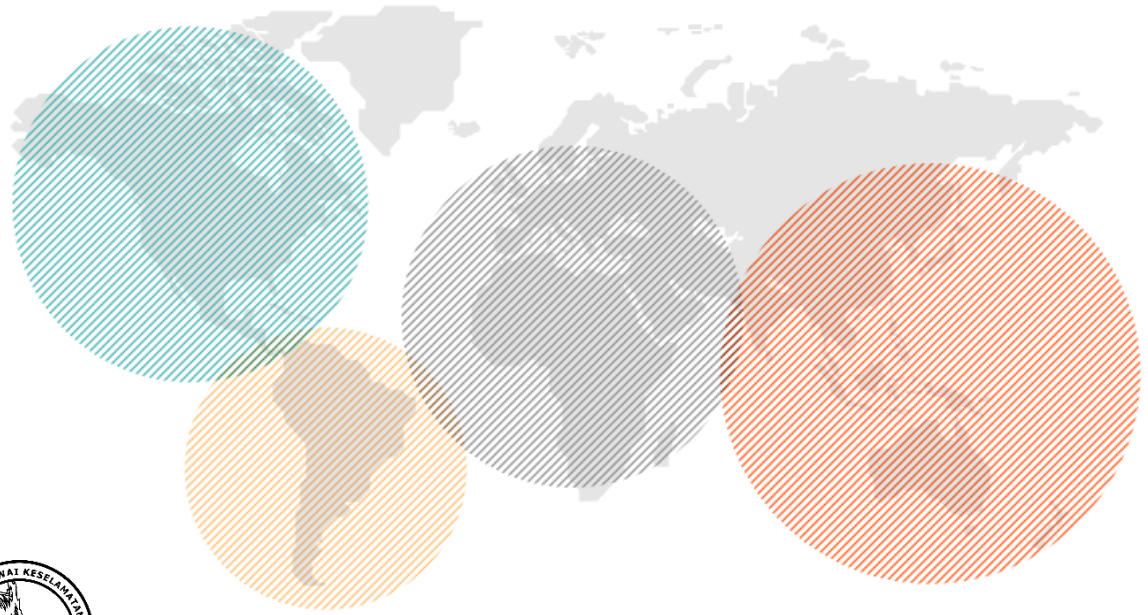
Apple
https://www.apple.com › newsroom › pdfs › The-... PDF

The Rising Threat to Consumer Data in the Cloud

by SE Madnick · 2022 · Cited by 3 — **Bad** actors use different **attack** methods to try to **gain** unauthorized **access** to corporate networks, such as social engineering **attacks**, insider threats, and ...
31 pages

Source: https://www.apple.com/newsroom/pdfs/The-Rising-Threat-to-Consumer-Data-in-the-Cloud.pdf

Examples of Data Breaches by Region



Northern America

Yahoo! (US)
2013-2014
Collectively, 3 billion user accounts[20,21]

Equifax (US)
2017
147 million records[25]

Desjardins (CA)
2017-2019
9.7 million individuals' records[29]

First American Financial (US)
2019
Over 885 million sensitive documents[33]

Capital One (US)
2019
Over 100 million customers[37]

Latin America and the Caribbean

Massive Data Leak in Brazil (BR)
2021
Over 220 million citizens' records[22]

Registro Nacional de las Personas (AR)
2021
Up to 45 million citizens[26]

Government of Costa Rica (CR)
2022
670 gigabytes of sensitive data[30]

Instituto Agrario Dominicano (DR)
2022
Over 1 terabyte of government data allegedly stolen[34]

Europe, Middle East and Africa

Dailymotion (FR)
2016
85 million user accounts[23]

Ticketmaster (EU)
2018
9.4 million customers[27]

Careem (AE)
2018
14.6 million customer records[31]

Pegasus Airlines (TR)
2022
Almost 23 million flight data files[35]

TransUnion (ZA)
2022
54 million customer records[38]

Asia Pacific

Tianya Club (CN)
2011
40 million user records[24]

Cathay Pacific (HK)
2014-2015
9.4 million customer records[28]

Aadhaar (IN)
2018
Up to 1.1 billion citizens' records[32]

SingHealth (SG)
2018
1.5 million patient records[36]

Optus (AU)
2022
9.8 million customer records[39]

KERAJAAN MALAYSIA

Cloud Storage Data Breaches

Dropbox hack leads to leaking of 68m user passwords on the internet

Data stolen in 2012 breach, containing encrypted passwords and details of around two-thirds of cloud firm's customers, has been leaked

The Dropbox data breach has highlighted the problem of password reuse. Photograph: Alamy

Source: https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach

Facebook will not notify more than 530m users exposed in 2019 breach

Company spokesperson said Facebook was not confident it had full visibility on which users would need to be alerted

Facebook has long been under scrutiny over how it handles user privacy. Photograph: Richard Drew/AP

https://www.theguardian.com/technology/2021/apr/08/facebook-2019-breach-users

Cisco WebEx sabotage: How a disgruntled ex-employee caused $2.4 million in damages

September 9, 2024 | Insider Lab

https://insidersecurity.co/cisco-webex-sabotage-how-a-disgruntled-ex-employee-caused-2-4-million-in-damages/

IT Pro
https://www.itpro.com › Security › Data Breaches

Alibaba data breach exposes 1.1 billion pieces of data

16 Jun 2021 — **Alibaba's shopping website Taobao was trawled for 8 months** which resulted in over 1.1 billion pieces of user information being collected by a software ...

Yahoo Finance
https://finance.yahoo.com › news › alibabas-taobao-sho...

Alibaba's Taobao Shopping Site Succumbs To Colossal ...

15 Jun 2021 — A Chinese software developer sifted **Alibaba** Group Holding Ltd's (NYSE: BABA) **Taobao shopping website for eight months** and secretly collected ...

Missing: ~~hacker~~ | Show results with: hacker

Dark Reading
https://www.darkreading.com › cyberattacks-data-breaches

Code Hosting Service Shuts Down After Cyber Attack

20 Jun 2014 — **Code Spaces shuttered its doors** after a hacker accessed the company's Amazon EC2 control panel and erased business data and other information.

Incident

Details of the Incident

In June 2014, Code hosting and project management provider Codespaces.com was subject to a DDoS (Denial of Service Attack). During the attack, the attacker claimed access to their "Amazon EC2 Control panel" leaving behind a number of messages to contact them via Hotmail.

Once access to the EC2 Panel had been restored, Codespaces changed all passwords. However, the threat actor created multiple backdoor logins. When the attacker realized Codespaces was attempting to recover access, the threat actor deleted all EBS snapshots, S3 Buckets, AMIs, and several machines.

Following the damage assessment, it became clear that most Codespaces backups, data, and machine configurations were gone.

https://www.breaches.cloud/incidents/codespaces/

THE ECONOMIC TIMES | News

English Edition ▾ | **Today's ePaper**

Vendor Lock-In

'Microsoft blocks Nayara': Former Army officer issues wake-up call over India's total reliance on foreign operating systems

TheStar 30 YEARS ONLINE

TECHNOLOGY

Monday, 28 Jul 2025

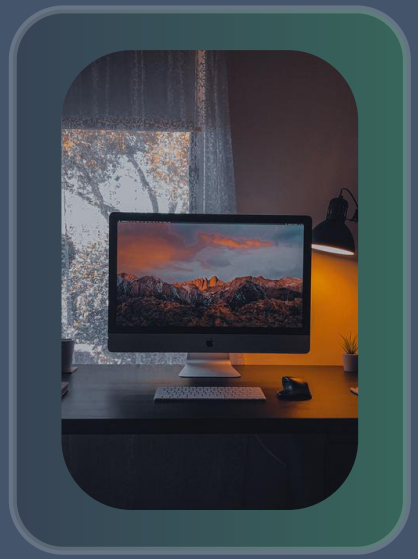
7:24 PM MYT

"Microsoft is currently restricting Nayara Energy's access to its own **data, proprietary tools, and products**—despite these being acquired under fully paid-up licenses," the refiner said in a statement.

https://www.thestar.com.my/tech/tech-news/2025/07/28/russia-backed-indian-refiner-nayara-takes-microsoft-to-court-over-outage

Risiko Kepada Rekod Awam

Ketirisan dan kehilangan maklumat (data loss) Kerajaan



Data loss happens when digital information is unintentionally deleted, corrupted, or becomes inaccessible.

Risiko Kepada Rekod Awam

Bagaimanakah ketirisan atau kehilangan maklumat boleh berlaku?

Cloud Storage Risks – Some free cloud services may delete inactive accounts or experience server failures.

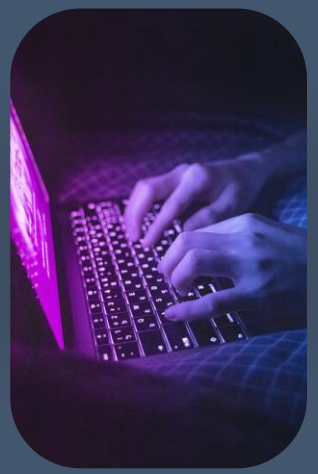
Limited Backup & Recovery Options – Some cloud providers may not offer robust backup solutions, making data recovery difficult after an incident.

Accidental Deletion – Users or system errors can mistakenly erase important files.

Susceptibility to Cyberattacks – Hackers frequently target free cloud storage due to weaker defenses, leading to ransomware, phishing, and malware attacks.

Lack of Encryption – Many free cloud services do not provide end-to-end encryption, making data vulnerable to cyberattacks.

Risiko Kepada Rekod Penting dan Strategik



Kehilangan memori institusi dan memori kebangsaan

Terbitan rasmi perlu dipindahkan ke Arkib Negara Malaysia agar memori institusi (institutional memory) dan memori kebangsaan (national memory) terpelihara. Bahan ini akan menjadi sumber rujukan dan penyelidikan oleh pejabat awam dan orang ramai pada masa akan datang.

Risiko Kepada Rahsia Rasmi

Perkara yang boleh menjejaskan keselamatan dan kedaulatan negara.

KESELAMATAN NEGARA

Apa-apa maklumat yang berkenaan dengan mana-mana agensi atau jabatan yang terlibat dalam operasi atau aktiviti-aktiviti keselamatan negara termasuklah apa-apa perkara yang berhubung dengan sifat kerjanya yang terselindung, pengekalan keamanan dan keharmonian, pembelian, modus operandi, pengagihan bantuan teknik serta juga maklumat yang berhubung dengan kertas-kertas penyiasatan yang serius dan sensitif sifatnya yang, jika tidak dilindungi, akan menyentuh kesentosaan negara.

PERTAHANAN

- Saiz, bentuk, susunan, logistik, perintah tempur, pengagihan, operasi, keadaan bersedia dan latihan Angkatan Tentera Malaysia;
- Senjata, stor atau kelengkapan lain angkatan itu dan pereka ciptaan, pembangunan, pengeluaran dan pengendalian kelengkapan itu serta penyelidikan yang berhubung dengannya;
- Dasar dan strategi pertahanan serta perancangan dan perisikan ketenteraan; dan
- Rancangan-rancangan dan langkah-langkah bagi penyenggaraan bekalan-bekalan dan perkhidmatan-perkhidmatan penting yang diperlukan atau mungkin akan diperlukan semasa peperangan.

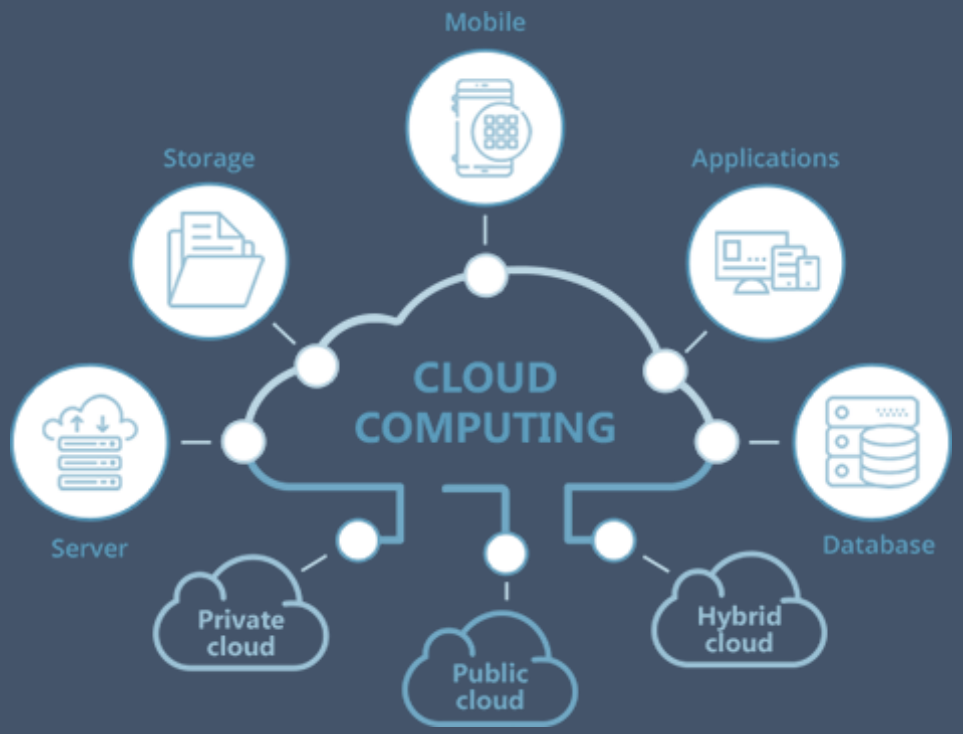
PERHUBUNGAN ANTARABANGSA

Ertinya hubungan antara negara, antara organisasi antarabangsa atau di antara satu atau lebih negara dengan satu atau lebih organisasi sedemikian dan termasuklah apa-apa perkara yang berhubungan dengan sesuatu negara selain daripada Malaysia atau sesuatu organisasi antarabangsa yang berupaya menyentuh hubungan Malaysia dengan sesuatu negara lain atau dengan sesuatu organisasi antarabangsa.

PERKARA 5.2

KERAJAAN MALAYSIA

MODEL PERKHIDMATAN PENGKOMPUTERAN AWAN



Microsoft 365

Teams

salesforce

DDMS 2.0

Perisian Sebagai Perkhidmatan (Software-as-a-Service)

Google app engine

amazon web services

Microsoft Azure

Platform Sebagai Perkhidmatan (Platform-as-a-Service)

MyGovCloud @ pusa

TM ONE

Microsoft Cloud

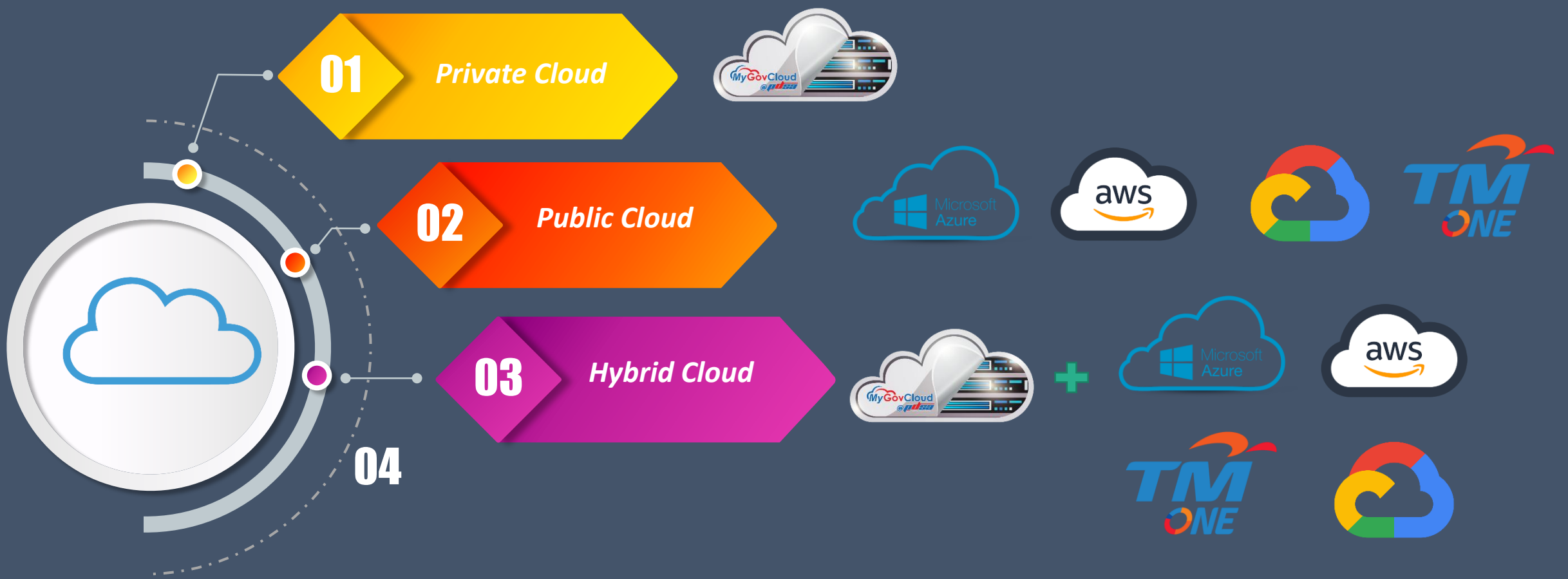
Amazon Elastic Compute Cloud (EC2)

Infrastruktur Sebagai Perkhidmatan (Infrastrucure-as-a-Service)

PERKARA 6

KERAJAAN MALAYSIA

MODEL PELAKSANAAN PENGKOMPUTERAN AWAN



PERKARA 7

KERAJAAN MALAYSIA

RISIKO KESELAMATAN YANG PERLU DIPERTIMBANGKAN

1. Kedaulatan Data (Data Sovereignty)

Mengenalpasti sumber asal (*source of origin*) perkhidmatan pengkomputeran awan

2. Risiko Daripada Perubahan Bidang Kuasa

Hak kontraktual dan **pertindihan bidang kuasa** berhubung dengan tempat penyimpanan dan pemprosesan data secara **logikal atau fizikal**

3. Forensik

Insiden dan pelanggaran keselamatan, ***bit-by-by imaging***

4. Kebergantungan

3rd party dan ***supply chain management risk***

5. Multi-Tenancy

Berkongsi sumber ICT - risiko melalui infrastruktur *virtualization*

6. Ancaman Dari Sumber Dalaman CSP

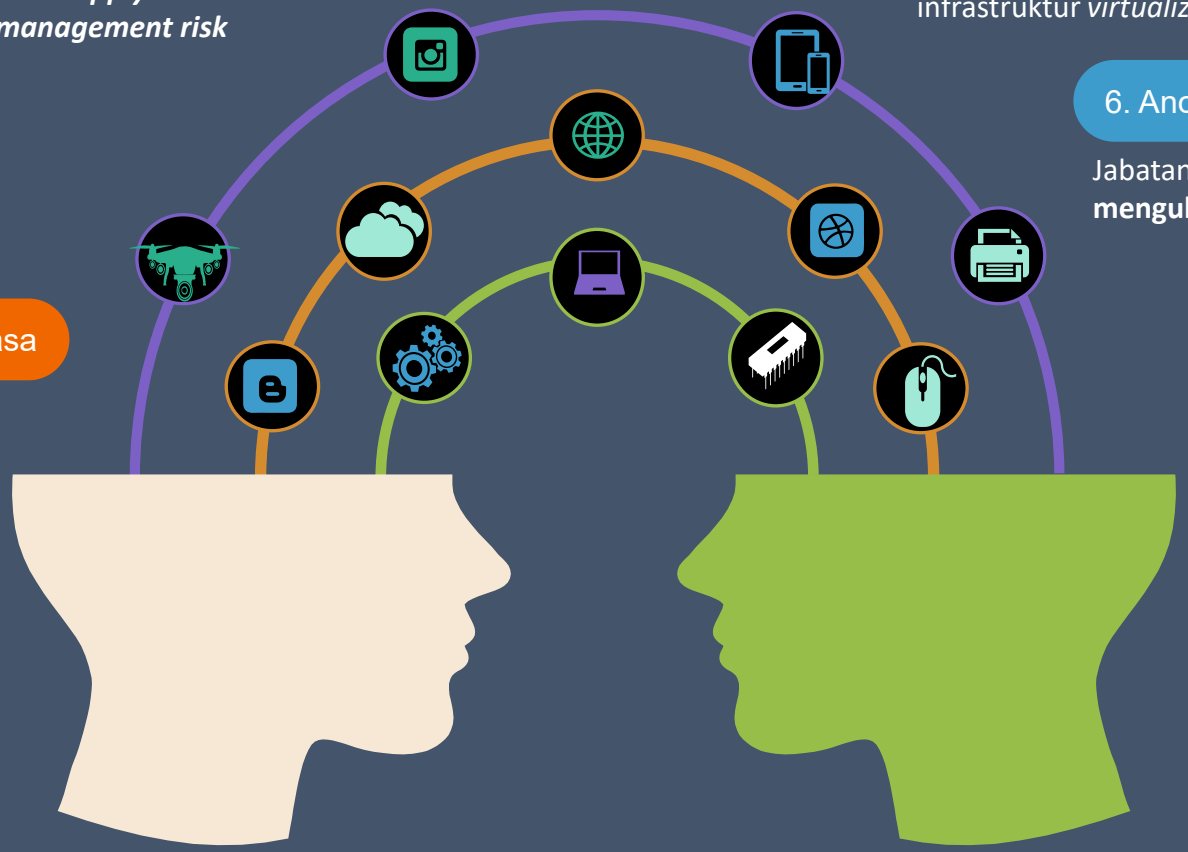
Jabatan tidak mempunyai keupayaan untuk **mengukur tahap keselamatan**

7. Vendor Lock-In

Kesukaran untuk memindahkan perkhidmatan atau data sedia ada kepada CSP atau pihak lain

8. Privasi

Perlanggaran privasi data



PERKARA 9

KERAJAAN MALAYSIA

PEMATUHAN PENGURUSAN MAKLUMAT RAHSIA RASMI

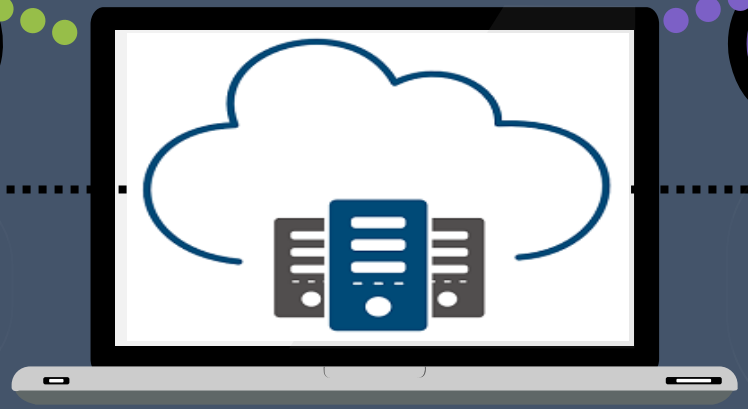
BIDANG KUASA

Semua maklumat rahsia rasmi yang disimpan dan diproses **hendaklah berada di bawah kawalan dan bidang kuasa undang-undang Kerajaan Malaysia**.

KAWALAN PENGGUNA

- Maklumat rahsia rasmi **dihadkan kepada pengguna** *(authorization)* tertentu sahaja.
Akauntabiliti pengguna yang mempunyai akses sumber pengkomputeran awan.

Prasyarat (prerequisite) terhadap sebarang cadangan penggunaan perkhidmatan pengkomputeran awan.



KLASIFIKASI MAKLUMAT

Pengelasan data, maklumat dan rekod rahsia rasmi **hendaklah dilaksanakan terlebih dahulu** dan berpandukan kepada peraturan dan arahan yang berkuat kuasa.

KHIDMAT NASIHAT UNDANG-UNDANG

Khidmat nasihat penasihat udang-undang berhubung dengan kebolehupayaan kuasa perundangan asing diberi kebenaran akses kepada maklumat atau aplikasi Jabatan terutamanya yang diurus oleh CSP asing

PERKARA 10

KERAJAAN MALAYSIA

PENGURUSAN KONTRAK DAN TERMA KESELAMATAN

1 DUE DILIGENCE

Jabatan hendaklah membuat penilaian secara terperinci berdasarkan kepada keperluan, pematuhan kepada dasar sedia ada dan kekangan undang-undang yang berkaitan

2 SLA

SLA hendaklah menjelaskan threshold matrix bersama dengan penalti kewangan sekiranya berlaku gangguan bisnes atau pelanggaran kontrak.

3 HAK MILIK DATA

Data atau maklumat adalah hak milik eksklusif Kerajaan sepenuhnya dan tidak boleh dianggap sebagai aset kepada CSP dan Kerajaan boleh mengambil apa-apa tindakan sebagaimana yang diperlukan.

4 PRIVASI

Memastikan supaya data organisasi tidak disalin, diubahusai, dipadam, diakses tanpa kebenaran Jabatan.

5 AUDIT

Kerajaan hendaklah diberikan hak untuk melaksanakan audit ke atas CSP. Agensi hendaklah membuat semakan keperluan tersebut ada dinyatakan di dalam Terms of Service CSP.

6 PAMPASAN

Ganti rugi *(indemnification)* sekiranya insiden berpunca daripada kesalahan oleh pihak penyedia perkhidmatan

7 LIABILITI

Agensi hendaklah menilai had liabiliti yang mungkin wujud akibat daripada gangguan perkhidmatan yang berlaku di luar kawalan CSP..

8 HAK MENCAPAI ELEMEN

"Pembekal hendaklah memberi hak mencapai elemen sistem yang mengandungi maklumat rasmi dan maklumat rahsia rasmi, pihak Kerajaan boleh mengambil tindakan sebagaimana yang diperlukan".

9 PELUCUTAN PERKHIDMATAN

memastikan *exit plan* disediakan bagi memastikan proses transisi dan migrasi berjalan dengan lancar tanpa kehilangan, kerosakan atau ketirisan data.

PERKARA 12

KAEDAH PERLINDUNGAN DATA DAN MAKLUMAT

KERAJAAN MALAYSIA

1. Enkripsi

- Ciri-ciri keselamatan maklumat
- Dienkrip dalam semua keadaan *(data at rest, data in motion, data in use)*
- Penggunaan Produk Kriptografi Terpercaya (PKT) adalah mandatori di dalam urusan yang melibatkan maklumat rahsia rasmi selaras dengan Dasar Kriptografi Negara

2. Pengasingan

- Lokasi penempatan di dalam fasiliti yang diperakui oleh Kerajaan
- Diasingkan secara logikal (software/virtualization-based architectures) mahupun fizikal (rangkaian, storan, pangkalan data) dalam setiap model pengkomputeran awan

3. Pengurusan Akses dan Identiti

Pengesahan (authentication), kawalan had akses dan pengasingan tugas dan tanggungjawab (segregation of duties) kakitangan yang terlibat dengan perkhidmatan pengkomputeran awan.

4. Perisian dan Aplikasi Keselamatan

Memastikan aplikasi keselamatan yang digunakan adalah efektif, diselenggara secara berkala (kemaskini versi, polisi dan lain-lain), dipercayai dan sah digunakan.

5. Penilaian Tahap Keselamatan

Memastikan supaya produk keselamatan siber yang ingin digunakan mematuhi penilaian keselamatan

6. Sanitasi Data

Melupuskan maklumat secara kekal seperti menulis ganti, penyingkiran, *degaussing*, pemusnahan media secara fizikal atau lain-lain kaedah bagi melindungi ketirisan maklumat

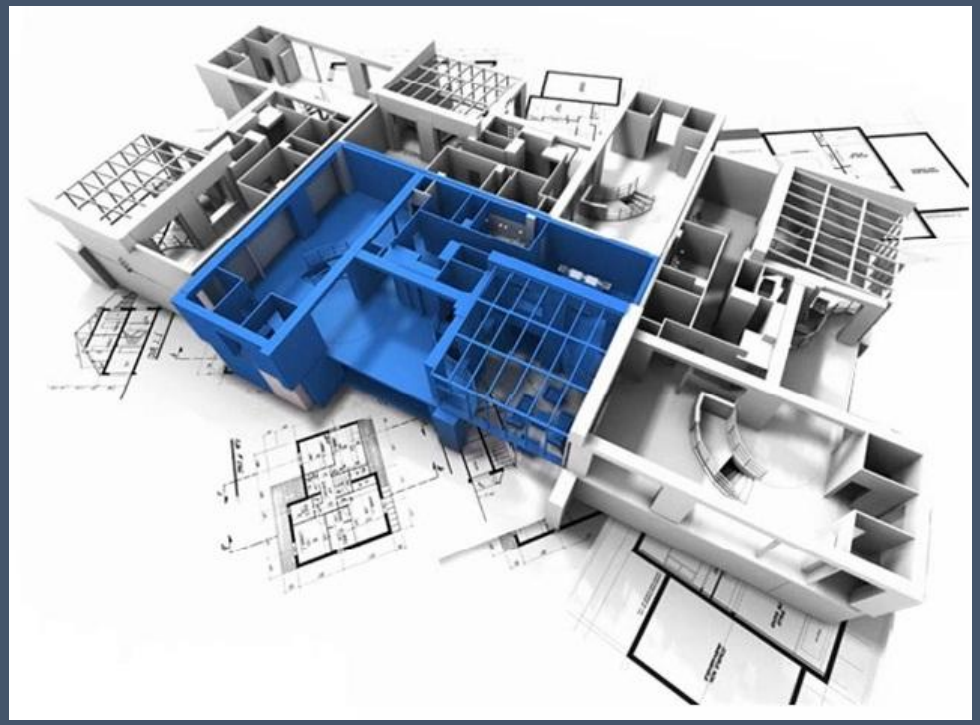
7. Ketirisan Data / Maklumat

Kawalan ketirisan ini boleh dibuat melalui penetapan polisi dan penggunaan penyelesaian teknologi seperti sistem Data Leakage Protection (DLP) dan Data Rights Management (DRM)

PERKARA 13

KERAJAAN MALAYSIA

KAWALAN KESELAMATAN FIZIKAL PUSAT DATA DAN INFRASTRUKTUR ICT



1. Penilaian Keselamatan
2. Pensijilan Keselamatan
3. Kawasan Terperingkat
4. Tapisan Keselamatan
5. Validasi Keselamatan Rahsia Rasmi
6. Sokongan
7. Notifikasi

KERAJAAN MALAYSIA

PENGURUSAN INSIDEN

Pihak Jabatan perlu **memastikan satu mekanisma pemantauan keselamatan terhadap maklumat yang ditempatkan di pengkomputeran awan diwujudkan** sama ada diperingkat jabatan atau pusat bagi menyelaras sebarang insiden ancaman siber yang berkemungkinan berlaku ke atas infrastruktur pengkomputeran awan. Sebarang insiden perlu dibuat penilaian implikasi dan taksiran risiko keselamatan di peringkat jabatan sebelum dilaporkan kepada agensi bertanggungjawab untuk tindakan selanjutnya.

PERKARA 15

KERAJAAN MALAYSIA

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1

CSP mewujudkan atau mempunyai pelan pengurusan kesinambungan perkhidmatan (PKP)

2

Jabatan diberi kebenaran bagi menguji dan membuat penilaian secara on-site di fasiliti CSP

3

Jabatan juga boleh membuat semakan dan pengesahan dokumen PKP sekiranya CSP mempunyai pensijilan berkaitan *Business Continuity Management* (BCM)

4

Satu notifikasi atau makluman rasmi kepada Jabatan hendaklah dibuat apabila PKP diuji.

PERKARA 16

KERAJAAN MALAYSIA

KEBOLEHSEDIAAN DAN SANDARAN DATA

01

Jabatan tidak seharusnya bergantung sepenuhnya terhadap penyedia perkhidmatan apabila berlaku gangguan.

02

Satu pelan pemulihan bencana hendaklah disediakan bagi memudahkan proses migrasi dan **failover** dilakukan dalam tempoh masa yang bersesuaian.

03

Kontrak hendaklah menyatakan dengan jelas obligasi CSP untuk memastikan sistem atau perkhidmatan dapat dibaik pulih (restore) dalam tempoh yang ditetapkan apabila berlaku kegagalan pada sumber pengkomputeran awan.

04

Data validasi juga boleh dilakukan secara automatik bagi memeriksa integriti data pada bila-bila masa

05

CSP mempunyai sumber dan polisi berhubung dengan proses sandaran data yang mudah diuruskan secara atas talian.

SYOR DAN HALATUJU

1

CGSO mengeluarkan Email/Surat Edaran Ketua Pengarah Keselamatan Kerajaan setelah Surat Pekeliling Am Bilangan 2 Tahun 2021 Yang Mengandungi Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (Cloud Computing) Dalam Perkhidmatan Awam Versi 2.0 dikuatkuasakan.

KERAJAAN MALAYSIA

SURAT PEKELILING AM BILANGAN 2 TAHUN 2021

GARIS PANDUAN
PENGURUSAN KESELAMATAN MAKLUMAT MELALUI PENGKOMPUTERAN AWAN (*CLOUD COMPUTING*) DALAM PERKHIDMATAN AWAM

JABATAN PERDANA MENTERI

9 Ogos 2021

Dikelilingkan kepada:

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Setiausaha Suruhanjaya
Semua YB Setiausaha Kerajaan Negeri
Semua Pihak Berkuasa Berkanun Persekutuan dan Negeri
Semua Pihak Berkuasa Tempatan

KERAJAAN MALAYSIA

SYOR DAN HALATUJU

2

CGSO bertanggungjawab menilai dan memastikan pelaksanaan projek ICT Jabatan khususnya projek berimpak tinggi dikemaskini selaras dengan dasar dan polisi baharu Kerajaan.

JTISA, JPICT Kementerian, JPICT Agensi

SYOR DAN HALATUJU

3

CGSO bersedia memberi bantuan dan khidmat nasihat teknikal kepada Jabatan berhubung perubahan versi ini agar pelaksanaannya di peringkat organisasi mencapai objektif dan matlamat seperti yang dihasratkan.

BENGKEL SPESIFIKASI CLOUD FRAMEWORK AGREEMENT (CFA) DAN PEMANTAPAN DASAR CLOUD SEKTOR AWAM

SYOR DAN HALATUJU

4

CGSO merancang dan melaksanakan program jerayawara Surat Pekeliling Am tersebut mengikut zon dan sektor disamping mengadakan program pendidikan dan kesedaran berterusan melalui sesi sindikasi, latihan, bengkel, forum, seminar dan lain-lain kepada pegawai awam.

KERAJAAN MALAYSIA

PERKARA SUBSTANTIF YANG MELIBATKAN PERUBAHAN MAJOR

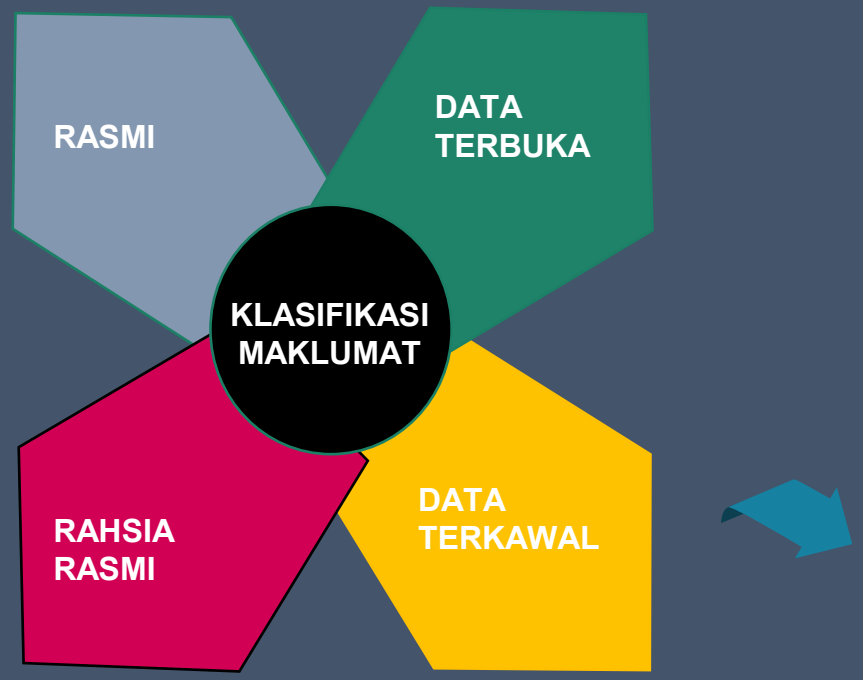
KERAJAAN MALAYSIA

DEFINISI

Data Peribadi	Apa-apa maklumat yang digunakan di dalam transaksi komersial yang berhubungan secara langsung atau tidak langsung dengan seseorang subjek data yang dikenalpasti daripada maklumat tersebut. Data tersebut boleh direkodkan, sama ada secara manual atau elektronik meliputi perkara-perkara objektif dan subjektif tanpa mengira sumber maklumat itu diperolehi meliputi maklumat asas (contohnya nama, alamat dan nombor kad pengenalan) sehinggalah ke maklumat sensitif (contohnya rekod perubatan dan tahap kesihatan) atau apa-apa informasi lain yang ditetapkan menteri di bawah Akta Perlindungan Data Peribadi 2010 [*Akta 709*].
Data Sovereignty	Apa-apa data yang dijana atau diperoleh di dalam negara adalah tertakluk kepada undang-undang dan peraturan di bawah bidang kuasa Kerajaan Malaysia serta tadbir urus yang berkaitan.
Failover	Keupayaan untuk memindahkan sumber ICT secara automatik (tanpa penglibatan manusia) kepada sistem tunggu sedia (standby) apabila berlaku kegagalan atau sesuatu peristiwa di luar kebiasaan (abnormal) pada sistem utama.

KERAJAAN MALAYSIA

Perkara 4.1.3 Data Terkawal / Sensitif



Data Terkawal / Sensitif adalah data yang mempunyai kawalan tertentu di bawah Akta atau Peraturan selain daripada **Akta 88**. Selain itu, data yang mempunyai nilai muka atau sensitif sifatnya yang ditentukan sendiri oleh Jabatan menurut pandangannya.

KERAJAAN MALAYSIA

Perkara 9.1.5 (a) Kaedah Penentuan Residensi Data

Jabatan hendaklah mematuhi dasar berhubung kaedah pemilihan model pelaksanaan dan kawalan residensi data seperti yang diperjelaskan di bawah **LAMPIRAN 1.**

Cloud Adoption Strategy & Policy Versi 2.0

Klasifikasi Maklumat	Peringkat Keselamatan	Tradisional (Pusat Data Jabatan)	MODEL CLOUD YANG DIBENARKAN			RESIDENSI DATA			
			Public	Private	Hybrid	Onshore (Dalam Negara) Bagi Fasiliti / Infrastruktur Utama			Off-Shore (Luar Negara) Bagi Tujuan Sandaran Data
						On-Premise (Premis Kerajaan)		Off-Premise	Premis CSP
						CSP Tempatan (termasuk MyGovCloud@PDSA)	CSP Asing (dibangunkan untuk Kerajaan	CSP Tempatan / CSP Asing	
RASMI	Data Terbuka	/	/	/	/	/	/	/	/
	Data Terkawal (Kewangan, Rekod Perubatan, Data Peribadi atau PII)	/	/	/	/	/	/	/	/**
RAHSIA RASMI	TERHAD	/	/	/	/	/	/	/*	/**
	SULIT	/	/	/	/	/	/	/*	/**
	RAHSIA	Isolate	x	x	x	x	x	x	x
	RAHSIA BESAR	Isolate	x	x	x	x	x	x	x

Langkah 2: Menilai

Tentukan Klasifikasi Data Berdasarkan Kepada Nilai, Impak Dan Sensitiviti.

KERAJAAN MALAYSIA

MAKLUMAT / DATA RASMI

Impak rendah

Kawalan keselamatan rendah

TERBUKA

TERHAD

SULIT

RAHSIA

RAHSIA BESAR

Impak semakin tinggi

Kawalan keselamatan semakin tinggi

Dilindungi oleh Akta Rahsia Rasmi 1972 [Akta 88]

DATA TERKAWAL / SENSITIF

Dilindungi oleh peraturan atau akta seliaan agensi

Impak

PANDUAN PENGELASAN DATA ATAU SISTEM MAKLUMAT ICT

KEBARANGKALIAN IMPAK (POTENTIAL IMPACT)	OBJEKTIF KESELAMATAN		
	KERAHSIAAN Jaminan bahawa maklumat tidak didedahkan kepada entiti yang tidak sah	**INTEGRITI** Jaminan ke atas kesahihan maklumat bahawa ianya tidak dipinda oleh entiti yang tidak sah	**KEBOLEHSEDIAAN** Keadaan yang mana maklumat boleh diperolehi dan digunakan apabila diperlukan oleh entiti yang dibenarkan
RENDAH — LIMITED DAMAGE	Pendedahan **maklumat tanpa kebenaran** boleh mengakibatkan kesan insiden yang RENDAH (**LIMITED**) terhadap urusan kefungsian Jabatan, aset Jabatan atau personel.	Pengubahsuaian atau pelupusan **(destruction) maklumat** tanpa kebenaran mengakibatkan kesan insiden yang RENDAH (LIMITED) terhadap urusan kefungsian Jabatan, aset Jabatan atau personel.	Gangguan akses **terhadap penggunaan maklumat atau sistem maklumat** boleh mengakibatkan kesan insiden yang RENDAH (**LIMITED**) terhadap urusan kefungsian Jabatan, aset Jabatan atau personel.
SEDERHANA — DAMAGE/SERIOUS DAMAGE	Pendedahan **maklumat tanpa kebenaran** boleh mengakibatkan kesan insiden yang **SERIUS** terhadap urusan kefungsian Jabatan, aset Jabatan atau personel.	Pengubahsuaian atau pelupusan **(destruction) maklumat** tanpa kebenaran mengakibatkan kesan insiden yang **SERIUS** terhadap urusan kefungsian Jabatan, aset Jabatan atau personel.	Gangguan akses **terhadap penggunaan maklumat atau sistem maklumat** boleh mengakibatkan kesan insiden yang **SERIUS** terhadap urusan kefungsian Jabatan, aset Jabatan atau personel.
TINGGI — CATASTROPHIC DAMAGE	Pendedahan **maklumat tanpa kebenaran** boleh mengakibatkan kesan insiden yang SANGAT TERUK (**SEVERE OR CATASTROPHIC**), terhadap urusan kefungsian Jabatan, aset Jabatan atau personel.	Pengubahsuaian atau pelupusan **(destruction) maklumat** tanpa kebenaran mengakibatkan kesan insiden yang SANGAT TERUK (**SEVERE OR CATASTROPHIC**), terhadap urusan kefungsian Jabatan, aset Jabatan atau personel.	Gangguan akses **terhadap penggunaan maklumat atau sistem maklumat** boleh mengakibatkan kesan insiden yang SANGAT TERUK (**SEVERE OR CATASTROPHIC**), terhadap urusan kefungsian Jabatan, aset Jabatan atau personel.

KERAJAAN MALAYSIA

Tafsiran Rahsia Rasmi mengikut Seksyen 2 Akta Rahsia Rasmi 1972

1. **Apa-apa suratan yang dinyatakan dalam Jadual Akta Rahsia Rasmi 1972 dan apa-apa maklumat dan bahan berhubungan dengannya**

- Suratan, rekod keputusan dan pertimbangan Jemaah Menteri termasuk suratan, rekod keputusan dan pertimbangan **jawatankuasa-jawatankuasa Jemaah Menteri**
- Suratan, rekod keputusan dan pertimbangan Majlis Mesyuarat Kerajaan Negeri termasuk suratan, rekod keputusan dan pertimbangan **jawatankuasa-jawatankuasa Majlis Kerajaan Negeri**
- Suratan berkenaan dengan **keselamatan negara, pertahanan dan perhubungan antarabangsa**

2. **Apa-apa suratan rasmi, maklumat dan bahan lain yang boleh dikelaskan sebagai 'Rahsia Besar', 'Rahsia', 'Sulit' atau 'Terhad' (mengikut mana yang berkenaan) oleh seorang Menteri, Menteri Besar atau Ketua Menteri atau pegawai awam yang dilantik di bawah seksyen 2B, Akta Rahsia Rasmi 1972**

KERAJAAN MALAYSIA

Maklumat Dalam Jadual Akta Rahsia Rasmi 1972

KESELAMATAN NEGARA

Apa-apa maklumat yang berkenaan dengan mana-mana agensi atau jabatan yang terlibat dalam operasi atau aktiviti-aktiviti keselamatan negara termasuklah apa-apa perkara yang berhubung dengan sifat kerjanya yang terselindung, pengekalan keamanan dan keharmonian, pembelian, modus operandi, pengagihan bantuan teknik serta juga maklumat yang berhubung dengan kertas-kertas penyiasatan yang serius dan sensitif sifatnya yang, jika tidak dilindungi, akan menyentuh kesentosaan negara.

PERTAHANAN

- Saiz, bentuk, susunan, logistik, perintah tempur, pengagihan, operasi, keadaan bersedia dan latihan Angkatan Tentera Malaysia;
- Senjata, stor atau kelengkapan lain angkatan itu dan pereka ciptaan, pembangunan, pengeluaran dan pengendalian kelengkapan itu serta penyelidikan yang berhubung dengannya;
- Dasar dan strategi pertahanan serta perancangan dan perisikan ketenteraan; dan
- Rancangan-rancangan dan langkah-langkah bagi penyenggaraan bekalan-bekalan dan perkhidmatan-perkhidmatan penting yang diperlukan atau mungkin akan diperlukan semasa peperangan.

PERHUBUNGAN ANTARABANGSA

Ertinya hubungan antara negara, antara organisasi antarabangsa atau di antara satu atau lebih negara dengan satu atau lebih organisasi sedemikian dan termasuklah apa-apa perkara yang berhubungan dengan sesuatu negara selain daripada Malaysia atau sesuatu organisasi antarabangsa yang berupaya menyentuh hubungan Malaysia dengan sesuatu negara lain atau dengan sesuatu organisasi antarabangsa.

KERAJAAN MALAYSIA

Perkara 9.1.5 (b)

Peringkat keselamatan bagi data terkawal, Terhad dan Sulit boleh berada di luar negara dengan syarat dan ketetapan seperti berikut;

1. bagi tujuan sandaran data sahaja. Data yang mempunyai maksud rahsia rasmi hendaklah mematuhi keperluan pengurusan mekanisma kawalan rahsia rasmi.

2. Ketua Jabatan hendaklah menilai terlebih dahulu liabiliti atau obligasi undang-undang sama ada di dalam atau di luar negara sebelum membuat sebarang keputusan untuk memindahkan data tersebut ke luar negara.

3. Jabatan hendaklah mendapatkan persetujuan dan kebenaran daripada pihak berkuasa berkaitan yang mengawal selia pelepasan data atau maklumat Kerajaan ke luar negara.

KERAJAAN MALAYSIA

Perkara 9.1.6 Pengurusan dan Kawalan Kriptografi

Jabatan hendaklah memastikan pengurusan dan kawalan kriptografi berada di bawah kawalan dan tanggungjawab sepenuhnya pihak Kerajaan. Bagi menjamin kedaulatan data, **sebarang kekunci kriptografi yang memberi implikasi besar kepada keselamatan** hendaklah menggunakan **perkakasan yang dibenarkan dan disimpan di premis Kerajaan dalam negara**. CSP hendaklah menyediakan infrastruktur sokongan berkaitan bagi memastikan strategi kawalan ini boleh dilaksanakan.

KERAJAAN MALAYSIA

Perkara 9.1.7 Pengecualian Residensi Data

Umumnya, penawaran model public cloud dipercayai lebih menjimatkan berbanding model pelaksanaan yang lain. Model ini membenarkan ***transborder data flow*** dan secara langsung residensi data boleh berada di on-shore atau off-shore. Daripada perspektif teknologi, ada pelbagai mekanisma kawalan bagi melindungi data tetapi data tersebut dikhuatiri mempunyai beberapa risiko tambahan terutamanya melibatkan isu perundangan. Bagi menjamin kedaulatan data dan aset strategik Kerajaan, pemilihan model ini **dikecualikan bagi kategori data atau maklumat yang mempunyai implikasi keselamatan seperti di LAMPIRAN 2**.

KERAJAAN MALAYSIA

LAMPIRAN 2

SENARAI DATA ATAU DOKUMEN YANG TIDAK BOLEH DILEPASKAN

ATAU DI SIMPAN DI LUAR NEGARA

1. Kertas-kertas keputusan kabinet dan jawatankuasa-jawatankuasa kabinet;
2. Kertas-kertas keputusan Majlis Mesyuarat Kerajaan Negeri (MMKN) dan jawatankuasa-jawatankuasa MMKN;
3. Keselamatan Negara;
4. Pertahanan Negara;
5. Perhubungan Antarabangsa;
6. Kertas-kertas siasatan dan perisikan agensi penguatkuasa;
7. Hal-hal kerahsiaan di dalam perundangan;
8. Keistimewaan profesional perundangan;
9. Bahan-bahan Sulit Peperiksaan Awam;
10. Dokumen-dokumen belanjawan negara;
11. Maklumat perdagangan dan pelaburan yang rahsia lagi berharga;
12. Daftar Pemilih;
13. Data-data bancian;
14. Maklumat operasi agensi keselamatan;
15. Data peribadi pembesar negara;
16. Dokumen Geospatial Terperingkat; dan
17. Data pemberi maklumat.

KERAJAAN MALAYSIA

Perkara 10.1.2 Due Diligence

Dalam keadaan tertentu, laporan *Cost Benefit Analysis* (CBA) juga diperlukan bagi membantu pihak Jabatan membuat penilaian risiko dan merancang strategi pemilihan perkhidmatan pengkomputeran awan. Ini kerana terdapat kebarangkalian berlakunya situasi *vendor lock-in* berpunca daripada isu kos. Sebagai contoh, kos bagi *data egress* tidak diketahui atau diperjelaskan di peringkat awal. Perkara ini boleh menyebabkan berlaku pertikaian kewangan dan akhirnya persetujuan di antara pelanggan dan penyedia perkhidmatan gagal diperoleh.

KERAJAAN MALAYSIA

Perkara 12.2.6 (f) Sanitasi Data

***Cryptographic Erase* (CE)** merupakan satu kaedah yang boleh dipertimbangkan bagi melaksanakan sanitasi data di dalam persekitaran pengkomputeran awan. CE memanfaatkan teknologi kriptografi dengan memusnahkan kunci enkripsi (encryption key) dan menyebabkan hanya teks sifer masih kekal di dalam media storan. Kaedah ini berkesan untuk **menghalang *read-access* ke atas data** oleh pihak yang tidak dibenarkan dan menjadikan **proses pemulihan data tidak boleh dilaksanakan (infeasible)**.

KERAJAAN MALAYSIA

Perkara 13.2.3 (a) Pematuhan dan Pensijilan Keselamatan

Pihak CSP adalah tertakluk kepada peraturan yang telah ditetapkan di bawah mana-mana akta berkaitan dan hendaklah melaksanakan apa jua kawalan seperti yang diperuntukkan kepadanya termasuklah memenuhi prosedur pematuhan.

KERAJAAN MALAYSIA

Perkara 16.3 KEBOLEHSEDIAAN DAN SANDARAN DATA

Dalam konteks yang lain, pihak Jabatan hendaklah mempertimbangkan untuk melaksanakan proses sandaran data sama ada di infrastruktur penyedia perkhidmatan yang berbeza atau di premis sendiri atau di mana-mana pusat repositori data yang disahkan atau di bawah milikan pihak Kerajaan.

KERAJAAN MALAYSIA

CLOUD SECURITY AND SOVEREIGN BY DESIGN

CONFIDENTIALITY DESIGN

a) Government maintain exclusive control of the encryption keys (root key) and underlying cryptographic system.
   - Endorsed by Government of Malaysia
   - Crypto Agility

b) Some data required hardware-level isolation.
   - Dedicated servers
   - Operated by legal entity

c) More granular and robust access control.

LEGAL AND INTEGRITY DESIGN

a) Legislative obligations to protect government data.
   - Adhere to local laws / contractual commitments.
   - Rights to audit

b) Retain legal data ownership.

c) Obtain compliance evidence.

d) Zero trust architecture.

e) Data export control.
   - Transborder data flow

AVAILABILITY DESIGN

a) Adhere to data residency requirement stipulates in SPA Bil.2 Tahun 2021.

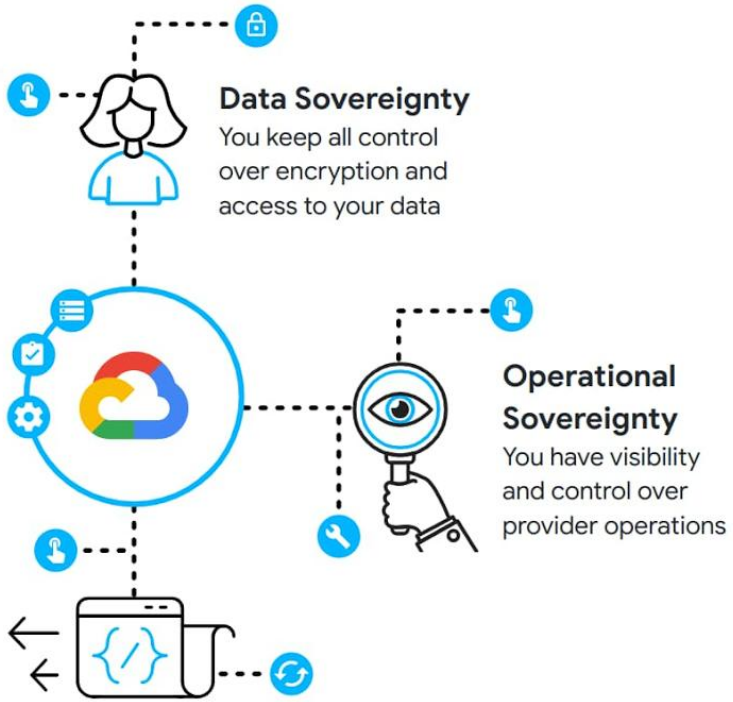
b) Cloud redundancy strategy
   - Data Portability
   - Multi-zone deployments
   - Multi-regional deployments
     - Bilateral agreements.

c) Multi-cloud deployment for mission critical system.

KERAJAAN MALAYSIA

CSP Approach

Three Pillars of Sovereignty in Google Cloud



Sovereign-by-Design

Our approach to digital sovereignty is to continue to make the AWS Cloud sovereign-by-design—as it has been from day one. We will continue to architect and build AWS and deliver features and controls so that you can use AWS services while meeting your regulatory requirements.

- **Control over the location of your data** +
- **Verifiable control over data access** +
- **The ability to encrypt everything everywhere** +
- **Resilience of the cloud** +

KESIMPULAN

Garis panduan ini disediakan sebagai panduan dan rujukan kepada Jabatan mengenai pengurusan perkara rasmi dan rahsia rasmi dan kepentingan melaksanakan langkah-langkah kawalan keselamatan perlindungan dalam persekitaran pengkomputeran awan bagi memastikan keselamatan aset dan maklumat Kerajaan terjamin sepanjang masa.

KERAJAAN MALAYSIA

SEKIAN, TERIMA KASIH

Alamat:

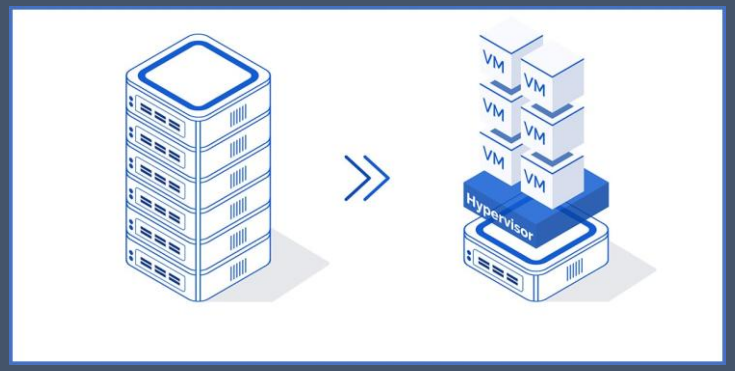
Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia
Jabatan Perdana Menteri,
Aras -1, 1 dan 2, Setia Perdana 7,
Kompleks Setia Perdana,
Pusat Pentadbiran Kerajaan Persekutuan,
62502 Wilayah Persekutuan Putrajaya,
Malaysia.

KERAJAAN MALAYSIA

TECHNOLOGY STACK

Hypervisor

A cloud hypervisor is the virtualization engine that enables multiple virtual machines (VMs) to run on a single physical server in a cloud environment.



https://vikhost.com/wp-content/uploads/2023/10/Hosted-and-Bare-Metal-Hypervisors.jpg

What Does a Cloud Hypervisor Do?

Abstracts hardware: It separates the physical hardware from the operating systems and applications.

Manages VMs: Creates, runs, and isolates multiple virtual machines on a host.

Allocates resources: Dynamically assigns CPU, memory, storage, and network to each VM.

Enables scalability: Supports elastic cloud infrastructure by spinning up/down VMs as needed.

KERAJAAN MALAYSIA

Cloud Adoption Strategy & Policy

Klasifikasi Maklumat	Peringkat Keselamatan	Tradisional (Pusat Data Jabatan)	MODEL CLOUD YANG DIBENARKAN			RESIDENSI DATA			
			Public	*Private*	*Hybrid*	*On-Shore* (Dalam Negara)			*Off-Shore* (Luar Negara)
						On-Premise (Premis Kerajaan)		*Off-Premise*	Premis CSP
						CSP Tempatan (termasuk MyGovCloud@PDSA)	CSP Asing (dibangunkan untuk Kerajaan	CSP Tempatan / CSP Asing	
RASMI	Data Terbuka	/	/	/	/	/	/	/	/
	Data Terkawal (Kewangan, Rekod Perubatan, PII)	/	x	/	/	/	/	/	x
RAHSIA RASMI	**TERHAD**	/	x	/	/	/	/	/*	x
	SULIT	/	x	/	/	/	/	/*	x
	RAHSIA	*Isolate*	x	x	x	x	x	x	x
	RAHSIA BESAR	*Isolate*	x	x	x	x	x	x	x

* *maklumat luar jadual sahaja*