9 OGOS

SPA BIL.2 / 2021

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

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

PEJABAT KETUA PEGAWAI KESELAMATAN KERAJAAN MALAYSIA
JABATAN PERDANA MENTERI

AGENDA

TAKLIMAT KHAS SPA BIL2. TAHUN 2021

01 **Sesi Pengenalan**

- Pengenalan SPA Bil.2 Tahun 2021

02 **Sesi Taklimat Oleh CGSO**

- Latar Belakang dan Punca Kuasa SPA Bil.2 Tahun 2021
- Penjelasan Perkara Utama Kandungan Garis Panduan.

03 **Sesi Soal Jawab**

- Dasar dan Kaedah Pelaksanaan
- Peranan Pegawai Keselamatan Jabatan / (CIO)

04 **Penutup**

- Tamat dan Bersurai

LATAR BELAKANG

ARAHAN KESELAMATAN (SEMAKAN DAN PINDAAN 2017) DAN PELAKSANAAN PENGKOMPUTERAN AWAN DALAM KERAJAAN: KRONOLOGI

2017

Punca Kuasa dan Kajian Analisis Jurang

[**JULAI**] Arahan Keselamatan (Semakan Dan Pindaan 2017) Diluluskan Oleh Jemaah Menteri pada 5 Julai 2017

[**OGOS-OKTOBER**] Penyediaan Draf MJM bagi syor penggunaan *Public Cloud* dalam Perkhidmatan Kerajaan

2018

Inisiatif Kumpulan Kerja

[**OKTOBER**] Edaran maklum balas dan ulasan garis panduan kepada agensi-agensi berkaitan

[**DISEMBER**] Pemurnian garis panduan

2019

Sindikasi Kumpulan Fokus

[**APRIL**] Pemurnian draf garis panduan kali kedua

[**OGOS**] Penglibatan CGSO dalam Jawatankuasa Pengkomputeran Awan (CCC) yang dianggotai oleh 11 Agensi Kerajaan

2020

Penguatkuasaan Dasar/Arahan

[**JANUARI**] Surat Pekeliling Am Bil.1 2020 berkenaan pematuhan dan penguatkuasaan Arahan Keselamatan baharu.

[**OGOS**] Maklum balas dan semakan akhir diperingkat Pengarah-Pengarah Bahagian CGSO

2021

Penyediaan Akhir Garis Panduan

[**FEBRUARI**] Semakan di peringkat Pejabat Penasihat Undang-Undang JPM

[**APRIL & JUN**] Pemurnian draf garis panduan berkenaan komen PUU JPM dan MyDIGITAL Committee on Legislative and Regulatory Framework for Digital Economy and 4IR

LATAR BELAKANG

MyDIGITAL Committee on Legislative and Regulatory Framework for Digital Economy and 4IR

Status/ Issues	Actions	PIC
1 **Implementation of data classification guidelines is large-scale, complex** • Many stakeholders (Federal, State, Local Governments) • Inconsistent understanding of data classification	1 **Set-up programme to implement data classification guidelines** • Track, monitor implementation • Provide training via online roadshow	• MAMPU and CGSO (by end 2021)

Keahliaan Jawatankuasa di bawah kluster Kerajaan yang dipengerusikan oleh Ketua Setiausaha Negara

KPKT

KEMENTERIAN DALAM NEGERI

MALAYSIAN ADMINISTRATIVE MODERNISATION AND MANAGEMENT PLANNING UNIT (MAMPU)

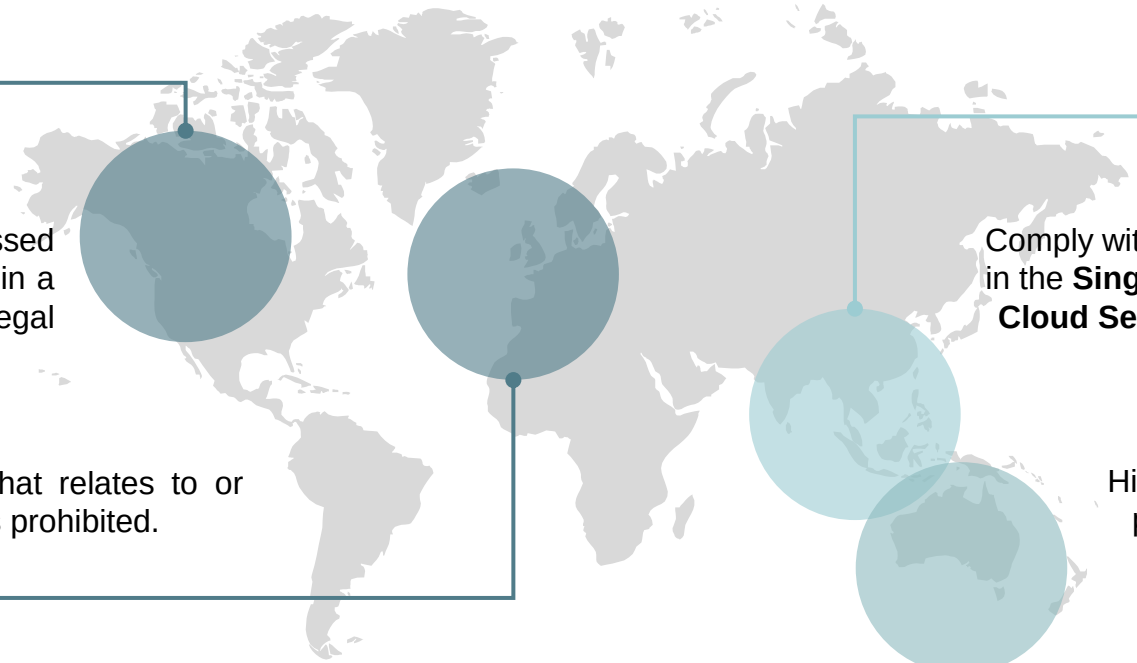
KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

KEMENTERIAN KOMUNIKASI DAN MULTIMEDIA MALAYSIA

JPA

EPU
ECONOMIC PLANNING UNIT
PRIME MINISTER'S DEPARTMENT, MALAYSIA

GLOBAL CLOUD ADOPTION POLICY/STRATEGY



UNITED STATES

All data stored and processed by/for the DoD must reside in a facility under the exclusive legal jurisdiction of the US.

UNITED KINDOM

Off-shoring of information that relates to or supports National Security is prohibited.

SINGAPORE

Comply with the security requirement in the **Singapore-specific Multi-Tier Cloud Security (MTCS) Singapore Standard (SS) 584**

AUSTRALIA

Highly classified information, public clouds are not used**.**

Target : **80%** of Cloud Storage Across Government in 2022

HIGHLIGHTS - KANDUNGAN GARIS PANDUAN

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

Dikeilingkan 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 kepada Pekeliling Am Bilangan _ Tahun 2021

Garis Panduan
...san Keselamatan Maklumat Melalui
...teran Awan (*Cloud Computing*) Dalam
Perkhidmatan Awam

...GAWAI KESELAMATAN MALAYSIA

KLASIFIKASI MAKLUMAT/ DATA
- Rasmi
- Rahsia Rasmi

PENENTUAN MODEL CLOUD DALAM SEKTOR AWAM
- Private Cloud
- Public Cloud
- Hybrid Cloud

RISIKO KESELAMATAN YANG PERLU DIPERTIMBANGKAN
- Kedaulatan Data
- Perubahan Bidang Kuasa
- Forensik/ Data Seizure
- Kebergantungan
- Multi-Tenancy
- Ancaman Sumber Dalaman CSP
- Vendor Lock-In
- Privasi

TADBIR URUS
- Penilaian Risiko

PEMATUHAN PENGURUSAN MAKLUMAT RAHSIA RASMI
- Klasifikasi Maklumat
- Bidang Kuasa
- Kawalan Pengguna
- Khidmat Nasihat Undang-Undang

PENGURUSAN KONTRAK & TERMA KESELAMATAN
- Due Diligence
- SLA
- Data Ownership
- Privasi
- Audit
- Pampasan
- Liabiliti
- Hak Mencapai Elemen
- Exit Process

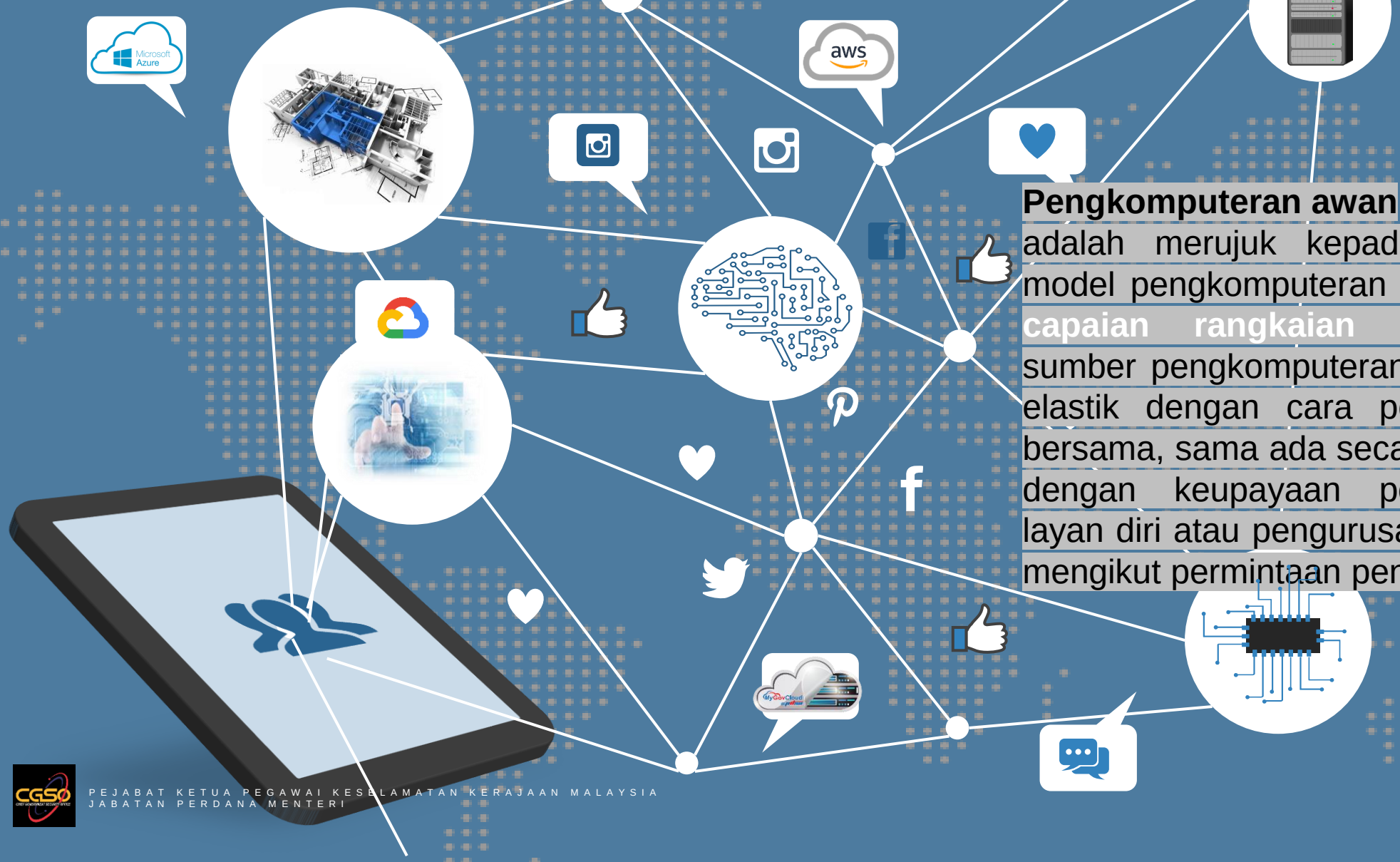
KAEDAH PERLINDUNGAN MAKLUMAT/ DATA
- Enkripsi
- Pengasingan
- Pengurusan Akses dan Identiti
- Perisian Keselamatan
- Penilaian Keselamatan
- Sanitasi Data
- Ketirisan Data / Maklumat

KAWALAN KESELAMATAN FIZIKAL PUSAT DATA/INFRA ICT
- Penilaian Keselamatan
- Pensijilan Keselamatan
- Kawasan Terperingkat
- Tapisan Keselamatan
- Validasi Keselamatan Rahsia Rasmi
- Sokongan
- Notifikasi

PENGURUSAN INSIDEN

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

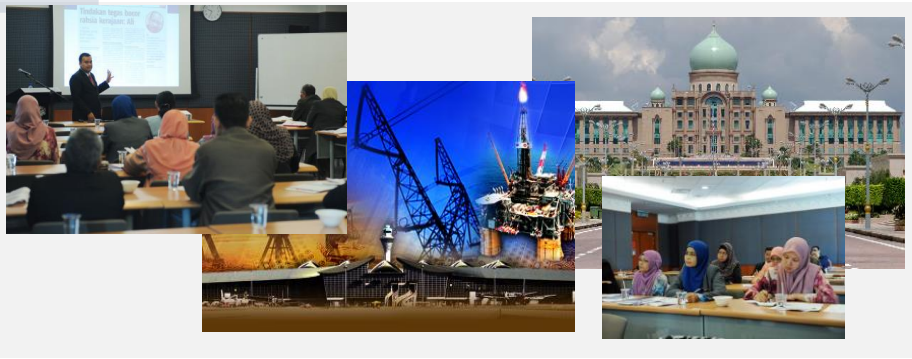
PERKARA 1 - PENGENALAN



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.

DEFINISI

PERKARA 2 - TUJUAN GARIS PANDUAN



01 Sebagai **rujukan kepada agensi sektor awam** mengenai pengurusan keselamatan perlindungan berhubung perkara rasmi dan rahsia rasmi Kerajaan dalam persekitaran pengkomputeran awan;

02 **Membantu sektor awam memahami pengurusan rahsia rasmi dalam pengkomputeran awan** selaras dengan peruntukan undang-undang semasa seperti di bawah Akta Rahsia Rasmi 1972 [Akta 88] dan Arahan Keselamatan (Semakan dan Pindaan 2017); dan

03 **Menerangkan langkah-langkah kawalan mitigasi yang wajar dan efektif** berdasarkan kepada pengolahan risiko yang telah dikenal pasti ke atas aset ICT yang dipindahkan atau digunakan dalam perkhidmatan pengkomputeran awan.

ARAHAN KESELAMATAN (SEMAKAN DAN PINDAAN 2017)

Perenggan 139 menyatakan;

> **"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."**

PERKARA 4 – KLASIFIKASI MAKLUMAT ATAU DATA

RAHSIA RASMI

"apa-apa suratan yang dinyatakan dalam Jadual dan apa-apa maklumat dan bahan yang berhubungan dengannya dan termasuklah apa-apa suratan rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai "Rahsia Besar", "Rahsia", "Sulit" atau "Terhad", mengikut mana-mana yang berkenaan, oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu Negeri atau mana-mana pegawai awam yang dilantik dibawah seksyen 2B. "

MAKLUMAT RASMI

Rasmi adalah berhubungan dengan perkhidmatan awam. Maklumat rasmi yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh mana-mana Jabatan Kerajaan semasa menjalankan urusan rasmi.

.

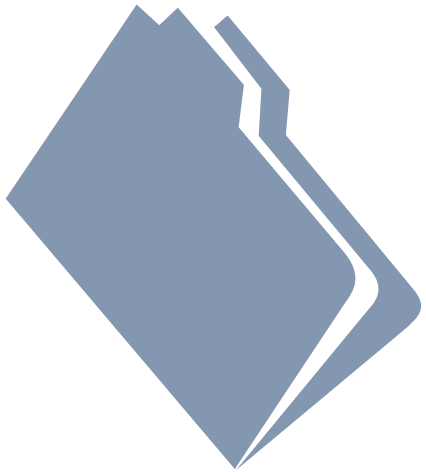
DATA TERBUKA

Data Terbuka adalah maklumat rasmi yang telah dibuat saringan dan pengesahan di peringkat pemula data untuk bebas digunakan, dikongsi serta digunakan semula oleh orang awam, agensi Kerajaan dan organisasi swasta untuk pelbagai tujuan. Jabatan hendaklah mematuhi pekeliling berhubung data terbuka yang sedang berkuat kuasa.

PROSES PENGELASAN MAKLUMAT RAHSIA RASMI

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 jawatankuasajawatankuasa 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**

PERKARA 4 – KLASIFIKASI MAKLUMAT ATAU DATA

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.

PERKARA 4 – KLASIFIKASI MAKLUMAT ATAU DATA

Tafsiran Rahsia Rasmi mengikut Seksyen 2 Akta Rahsia Rasmi 1972

RAHSIA BESAR	RAHSIA	SULIT	TERHAD
Dokumen rasmi, maklumat rasmi dan bahan rasmi			
yang jika didedahkan tanpa kebenaran			
akan 1. menyebabkan kerosakan yang amat besar kepada Malaysia	akan 1. membahayakan keselamatan negara 2. menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia 3. memberi keuntungan besar kepada sesebuah kuasa asing	walaupun tidak membahayakan keselamatan tetapi: 1. memudaratkan kegiatan Kerajaan atau individu 2. menyebabkan keadaan malu, kesusahan kepada pentadbiran 3. memberi keuntungan kepada kuasa asing	selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi perlu juga diberi perlindungan keselamatan

V. PERINGKAT KESELAMATAN DALAM PERSEKITARAN ICT

CONTOH-CONTOH PERINGKAT KESELAMATAN

RAHSIA BESAR

1. Kertas-kertas Jemaah Menteri yang sangat penting mengenai dasar utama Kerajaan berkaitan dengan perkara politik atau ekonomi;
2. Maklumat yang sangat penting mengenai perancangan dan penempatan barisan peperangan Angkatan Tentera jika berlaku peperangan;
3. Surat menyurat dengan kerajaan negara asing mengenai aspek perdagangan dan pertahanan yang sangat penting;
4. Maklumat lengkap berkenaan dengan perubuhan-pertubuhan perisikan Malaysia dan kaedah-kaedahnya.

RAHSIA

1. Arahan-arahan penting untuk perwakilan-perwakilan Malaysia untuk membuat perundangan dngan negara asing;
2. Maklumat-maklumat penting pemasangan-pemasangan tentera;
3. Maklumat-maklumat penting mengenai pertubuhan-pertubuhan subversif dan kegiatan-kegiatannya;
4. Surat menyurat antara jabatan mengenai dasar-dasar penting.

SULIT

1. Lapora-laporan perisikan biasa;
2. Dokumen2 dan panduan2 teknik untuk kegunaan latihan tentera atau polis;
3. Maklumat mengenai perkara-perkara perdangan yang jika terdedah kepada orang yang tidak dibenarkan atau menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran dan Kerajaan; dan
4. Maklumat2 yang mungkin membolehkan pendapatan faedah kewangan daripadanya jika terdedah sebelum masa.

TERHAD

a) Buku2 jabatan bagi maksud arahan;
b) Perintah2 dan arahan biasa jabatan; dan
c) Dokumen2 mengenai beklan barang2 dan alat kelengkapan biasa untuk tentera atau polis.

MELINDUNGI CIRI-CIRI ASAS KESELAMATAN MAKLUMAT

Confidentiality . Integrity . Availability

For the **CORRECT** At the

INFORMATION

INTEGRITY
Ensuring that the information has not been modified

PERSON

CONFIDENTIALITY
Ensuring that only the intended party is able to read the information

MOMENT

AVAILABILITY
Ensuring information is always available as and when needed

TUJUAN PERLINDUNGAN RAHSIA RASMI

SERANGAN ATAU ANCAMAN SIBER

Serangan atau ancaman siber ialah satu percubaan di dalam atau di luar Malaysia terhadap maklumat, sistem komputer dan komunikasi, program komputer dan data yang dirancang atau bertujuan mengendalakan, mengganggu secara serius, merosakkan atau memusnahkan apa-apa sistem komputer atau perkhidmatan komunikasi, perbankan atau kewangan, utiliti, pengangkutan atau infrastruktur penting yang lain termasuklah aktiviti jenayah terancang.

JENAYAH OLEH SINDIKET/GERAKAN TERANCANG

Internet Is Already Misused To Facilitate Terrorists' Activities

Cyber Terrorism

SERANGAN SIBER KE ATAS INFRASTRUKTUR MAKLUMAT KRITIKAL

High Dependency on ICT, Highly Sophisticated

Cyber War

PENIPUAN DALAM TALIAN

Targeting Individuals and Group

Cyber Criminal / Fraud

KANDUNGAN INTERNET

Penyalahgunaan Media Sosial / Laman Web/ Blog

Anti-Government Cyber Propaganda

HACKTIVISM

High-skilled Experts Sponsored By Governments

Political, Economic and Military Cyber Espionage

MAKLUMAT RAHSIA RASMI

Insider & Human Error

Geopolitical / Ideological / Political & Economic Purposes

PERKARA 4 – KLASIFIKASI MAKLUMAT ATAU DATA

Wednesday, 22 February 2017 | MYT 2:49 PM

Police asked to investigate MAHB over Jong-nam CCTV leak

A still image from CCTV footage showing a man purported to be Kim Jong Nam (circled in red) talking to airport staff at KLIA2 on Feb 13, 2017. PHOTO: REUTERS/FUJI TV

News › World news › Flight MH370

Chinese hackers 'stole classified MH370 data' about missing plane after 'infecting Malaysian computers with virus'

BY GARETH ROBERTS
13:57, 20 AUG 2014 | **UPDATED** 14:14, 20 AUG 2014

Government departments were sent e-mails containing a virus disguised as a hoax news report saying the Malaysian Airlines jet had been found.

When the attachment was opened, the virus - known as malware - began extracting sensitive data and sending it to a computer in China.

"Those e-mails contained confidential data from the officials' computers, including the minutes of meetings and classified documents. Some of these were related to the MH370 investigation.

"This was well-crafted malware that anti-virus programs couldn't detect. It was a very sophisticated attack."

Monday, 14 March 2016 | MYT 10:58 AM

Azalina: 31 cases of official secrets leaked in five years

Esscom suspects intelligence leak being exploited in Sabah

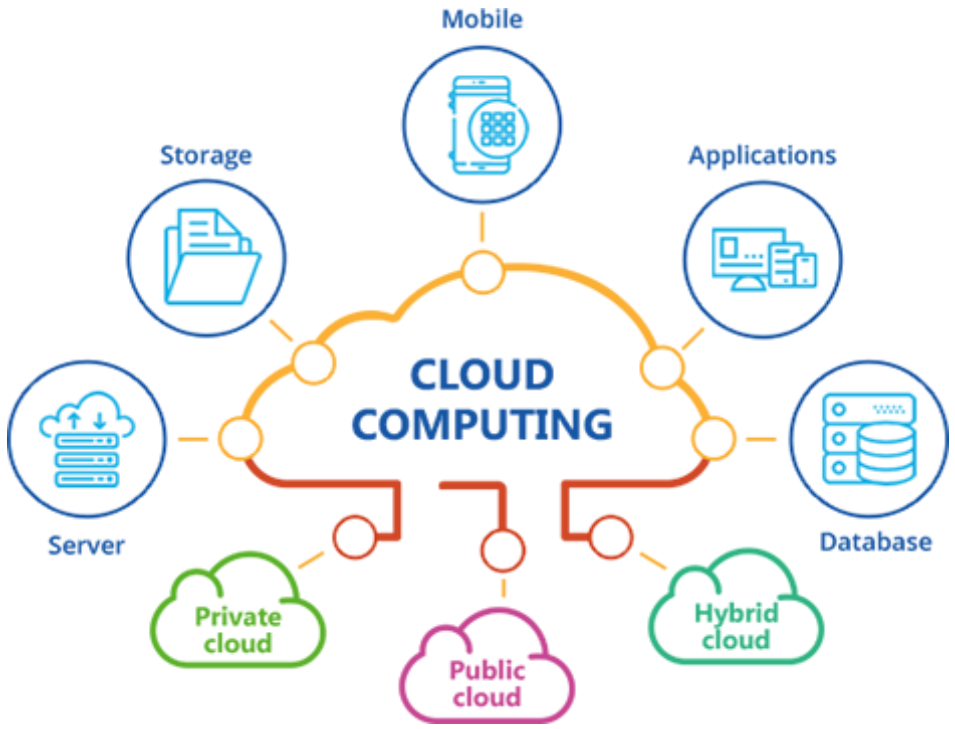
By FAISAL ASYRAF - September 30, 2016 @ 11:52am

KUALA LUMPUR: The Armed Forces will investigate the alarming possibility that classified information transmitted between officers and agencies under the Eastern Sabah Security Command (Esscom) is being intercepted and used by enemies.

Monday, 25 July 2016 | MYT 12:07 PM

UPSR leak: Teacher acquitted of OSA charge

MODEL PERKHIDMATAN PENGKOMPUTERAN AWAN



Microsoft 365 · salesforce · Teams · DDMS 2.0

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

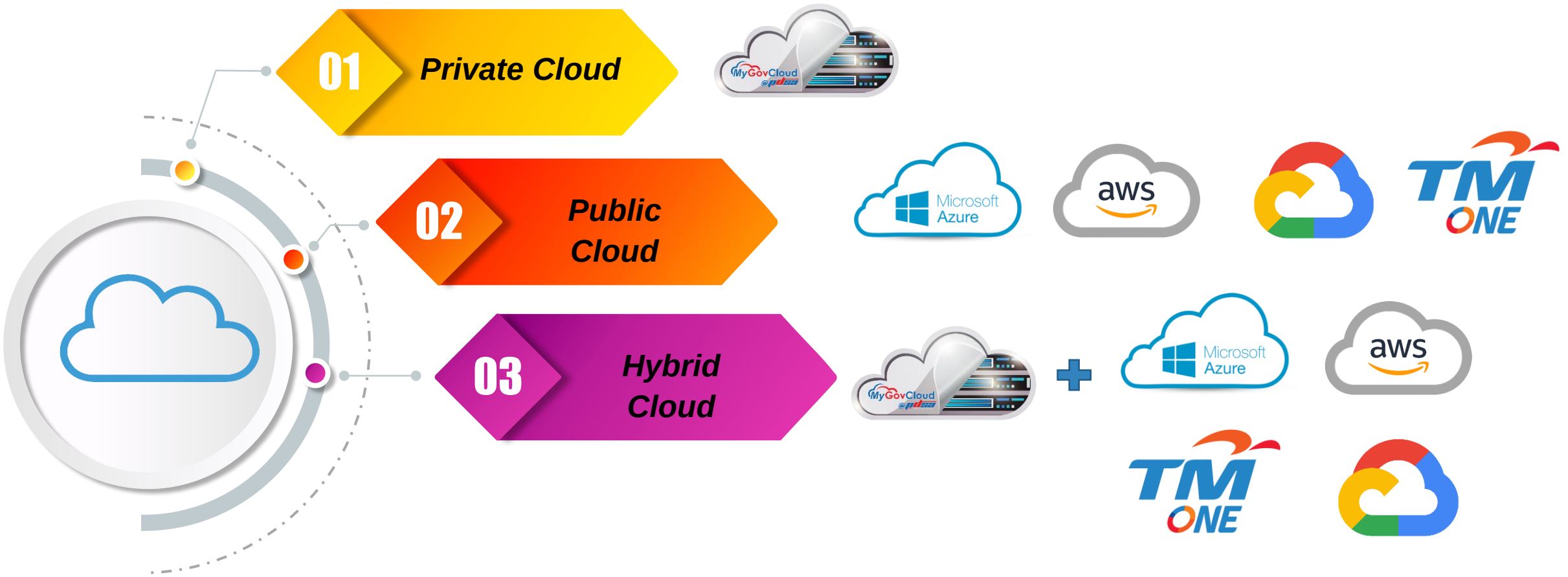
Google app engine · amazon web services · Microsoft Azure

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)

MODEL PELAKSANAAN PENGKOMPUTERAN AWAN



MATRIK KLASIFIKASI MAKLUMAT DALAM PELAKSANAAN PENGKOMPUTERAN AWAN DALAM PERKHIDMATAN AWAM

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.*

139. 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

RISIKO KESELAMATAN YANG PERLU DIPERTIMBANGKAN

4. Kebergantungan

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

3. Forensik

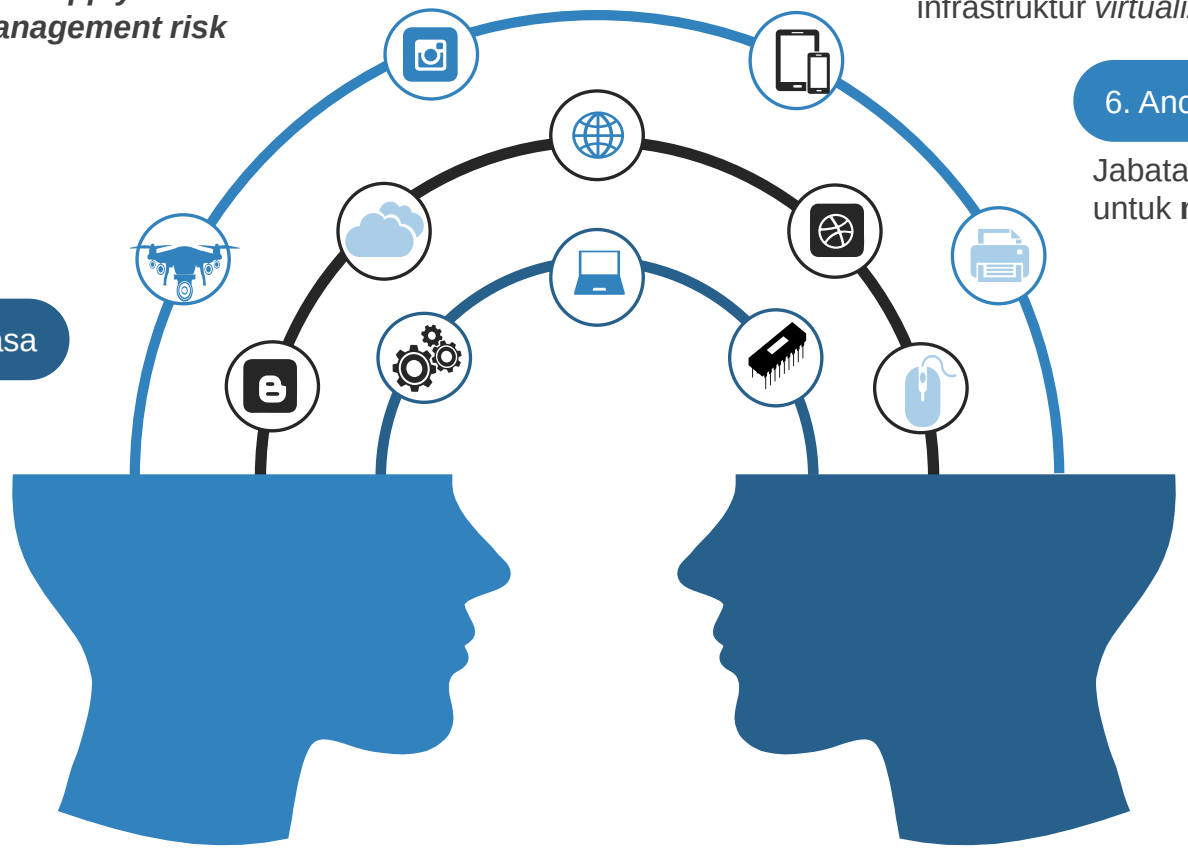
Insiden dan pelanggaran keselamatan, ***bit-by-by imaging***

2. Risiko Daripada Perubahan Bidang Kuasa

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

1. Kedaulatan Data (Data Sovereignty)

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



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

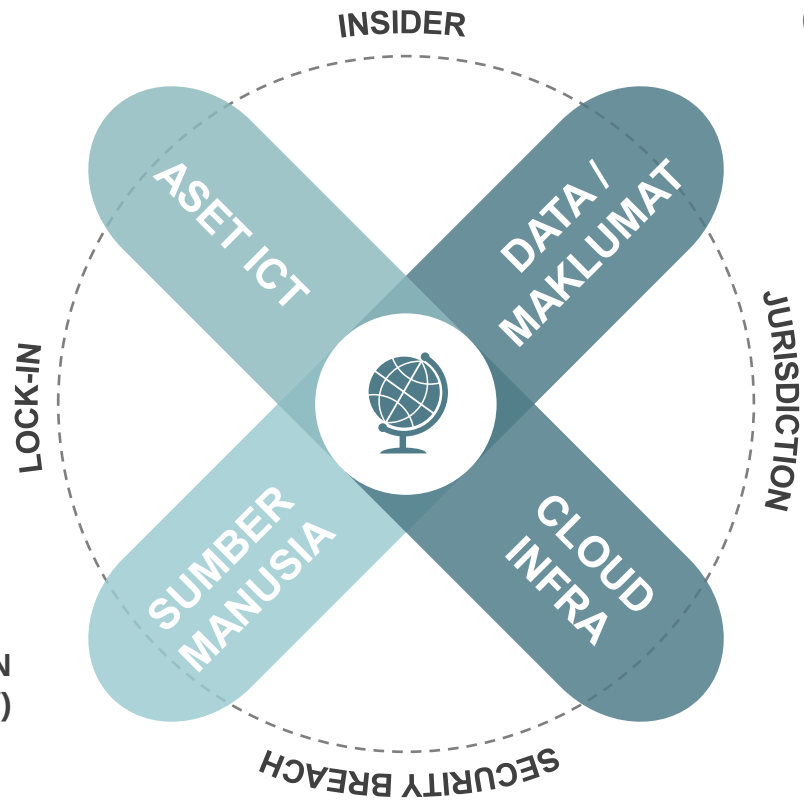
8. Privasi

Perlanggaran privasi data

TADBIR URUS – PENGURUSAN RISIKO

3. MENILAI RISIKO (RISK ASSESMENT)

4. MENENTUKAN PENGOLAHAN RISIKO (RISK TREATMENT)



2. MENGENAL PASTI ANCAMAN (THREAT)

5. MEMANTAU KEBERKESANAN PENGOLAHAN RISIKO

1. MENGENAL PASTI KERENTANAN (VULNERABILITY)

6. MEMANTAU ANCAMAN YANG BERKAITAN DENGAN BAKI RISIKO (RESIDUAL RISK) DAN RISIKO YANG DITERIMA

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

PENGURUSAN KONTRAK DAN TERMA KESELAMATAN

DUE DILIGENCE

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

PRIVASI

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

LIABILITI

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

SLA

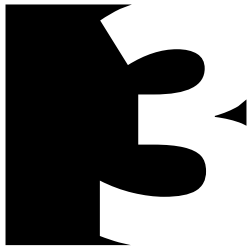
SLA hendaklah menjelaskan threshold matrix bersama dengan penalti kewangan sekiranya berlaku gangguan bisnes atau pelanggaran kontrak.

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.

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".



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.

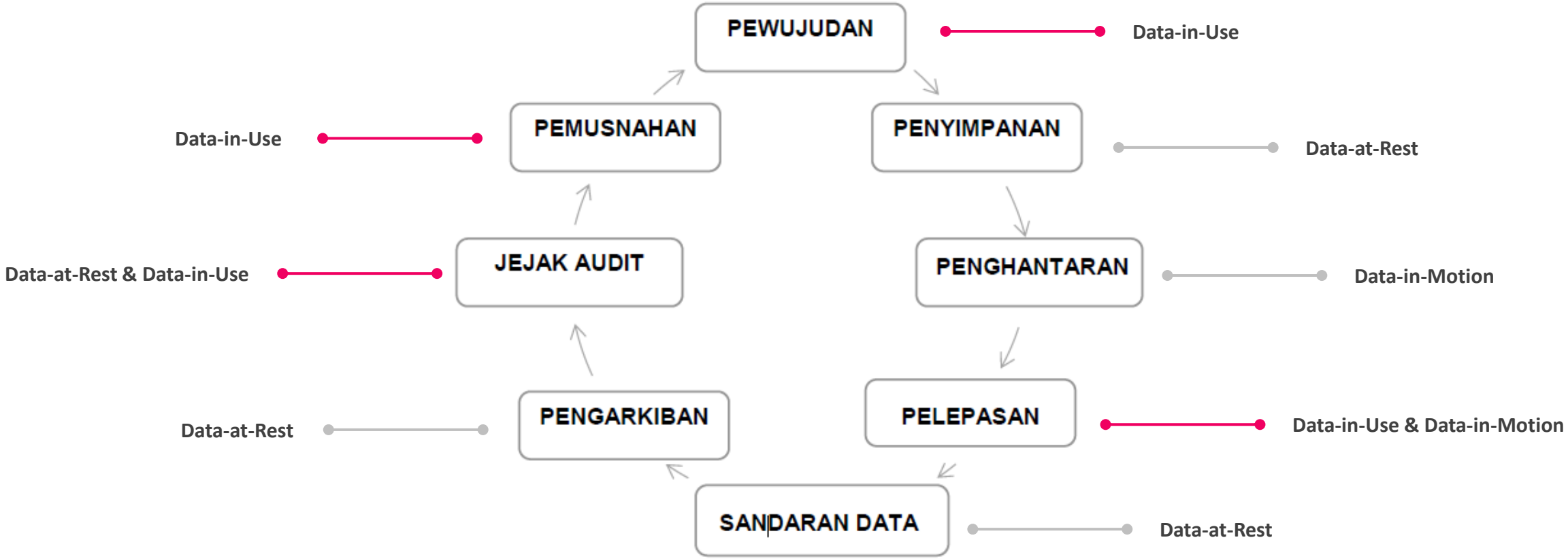
PAMPASAN

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

PELUCUTAN PERKHIDMATAN

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

KEPENTINGAN MELINDUNGI MAKLUMAT DALAM PERSEKITARAN ICT



Rajah 1 : Kitaran Hayat Maklumat

PERKARA 12

KAEDAH PERLINDUNGAN DATA DAN MAKLUMAT

1. Enkripsi

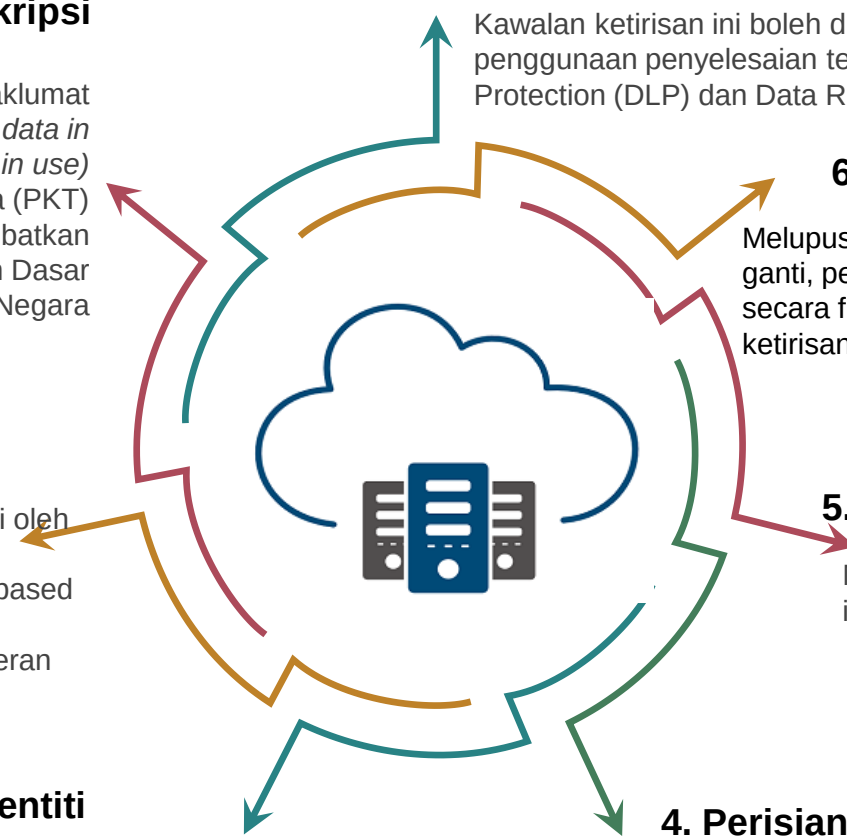
- Ciri-ciri keselamatan maklumat
- Dienkrip dalam semua keadaan *(data at rest, data in motion, data in use)*
- Penggunaan Produk Kriptografi Terpercaya (PKT) adalah mandatori di dalam urusan yang melibatkan maklumat rahsia rasmi selaras dengan Dasar Kriptografi Negara

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

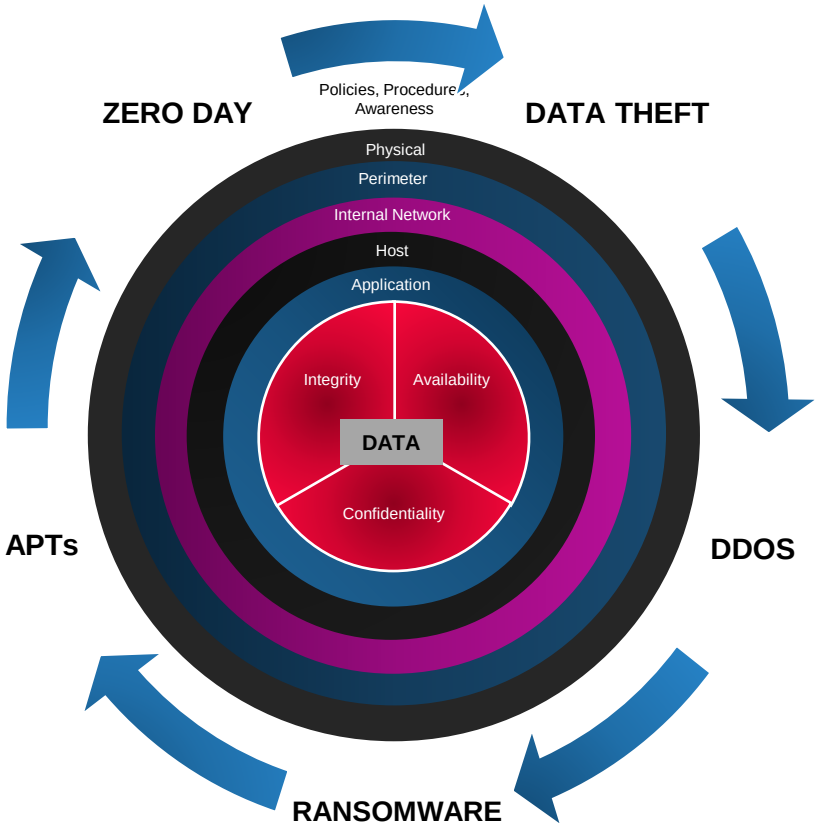
Melupuskan maklumat secara kekal seperti menulis ganti, penyingkiran, *degaussing*, pemusnahan media secara fizikal atau lain-lain kaedah bagi melindungi ketirisan maklumat

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)

PERLINDUNGAN CIRI-CIRI ASAS KESELAMATAN DAN LANGKAH KAWALAN

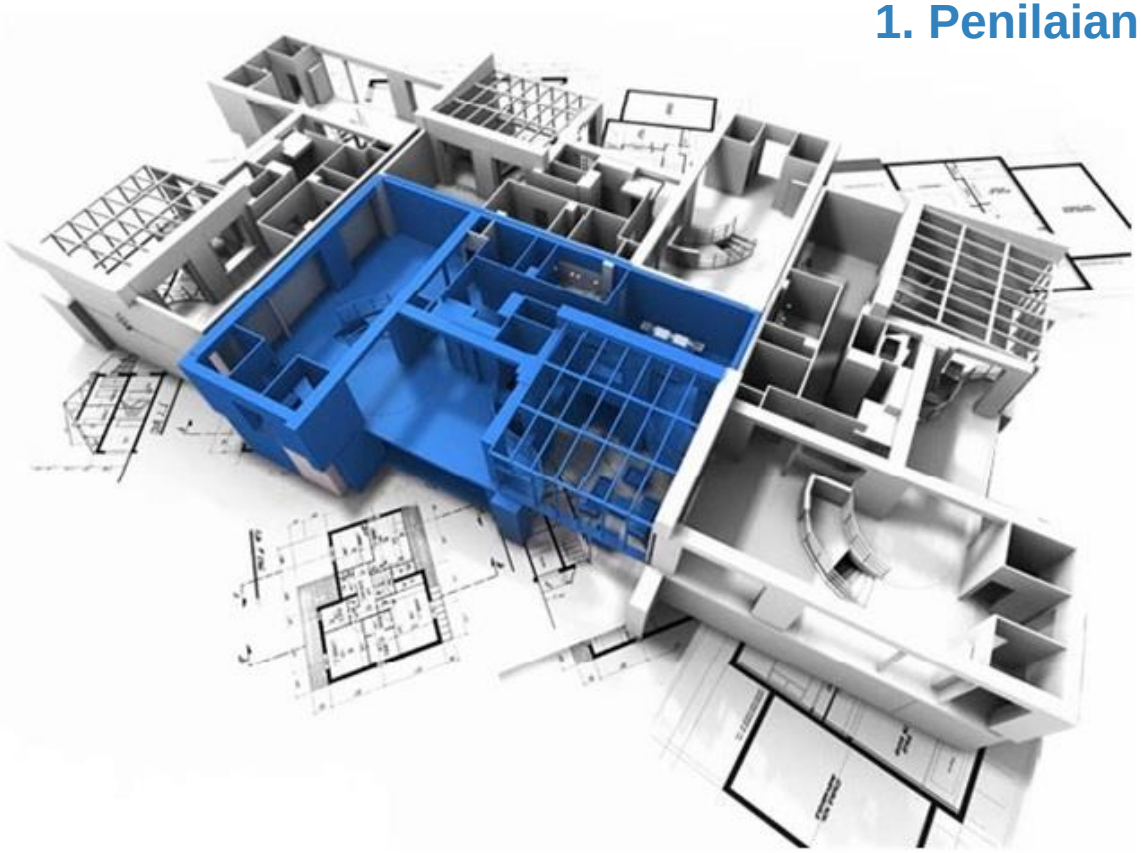
Defense in Depth



Administrative, Physical and Logical Security Control

DATA SECURITY	DATA BASE SECURITY	DATA MASKING DATA ERASURE DATA BAKCUP DATA ENCRYPTION	IRM DLP
APPLICATION SECURITY	SDLC	CODE REVIEW DDOS PROTECTION EMAIL SECURITY	APPLICATION PENETRATION TESTING
HOST SECURITY	OS HARDENING - VULNERABILITY MNGMT (PATCH)	END POINT SECURITY - ANTIVIRUS	HOST FIREWALL
INTERNAL NETWORK SECURITY	NETWORK ADDRESS TRANSLATION	NIPS / IDS	NETWORK SEGMENT & SEGREGATION
PERIMETER SECURITY	WEB GATEWAY - URL FILTERING - MALWARE INSPECTION	- VPN - ACLs - DMZ	FIREWALL - ANTI SPAM GATEWAY
PHYSICAL SECURITY	ENVIRONMENTAL - HVAC - FIRE FIGHTING	DATA CENTRE SECURITY - FENCE , CCTV	GUARD, CAMS
POLICIES, PROCEDURE & AWARENESS SECURITY	USER AWARENESS	DATA CLASSIFICATION	POLICIES

KAWALAN KESELAMATAN FIZIKAL PUSAT DATA DAN INFRASTRUKTUR ICT

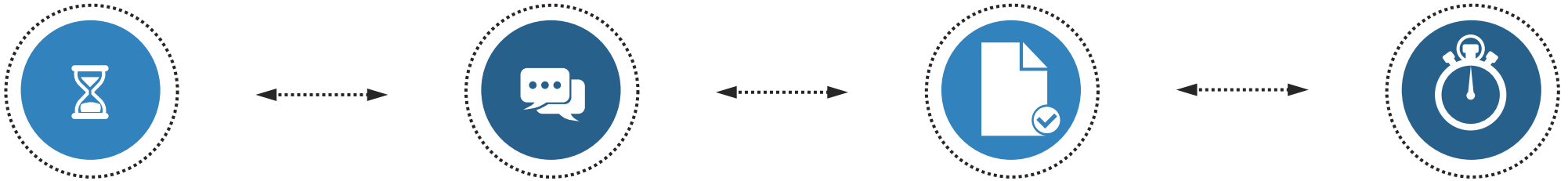


1. Penilaian Keselamatan
2. Pensijilan Keselamatan
3. Kawasan Terperingkat
4. Tapisan Keselamatan
5. Validasi Keselamatan Rahsia Rasmi
6. Sokongan
7. Notifikasi

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.

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.

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.

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.

PENUTUP

Taklimat ini adalah merupakan program pengurusan perubahan (*change management)* untuk semua pegawai CGSO membudayakan (adapt & adopt) dasar baharu keselamatan perlindungan selaras dengan Arahan Keselamatan (Semakan dan Pindaan 2017).

SESI SOAL JAWAB

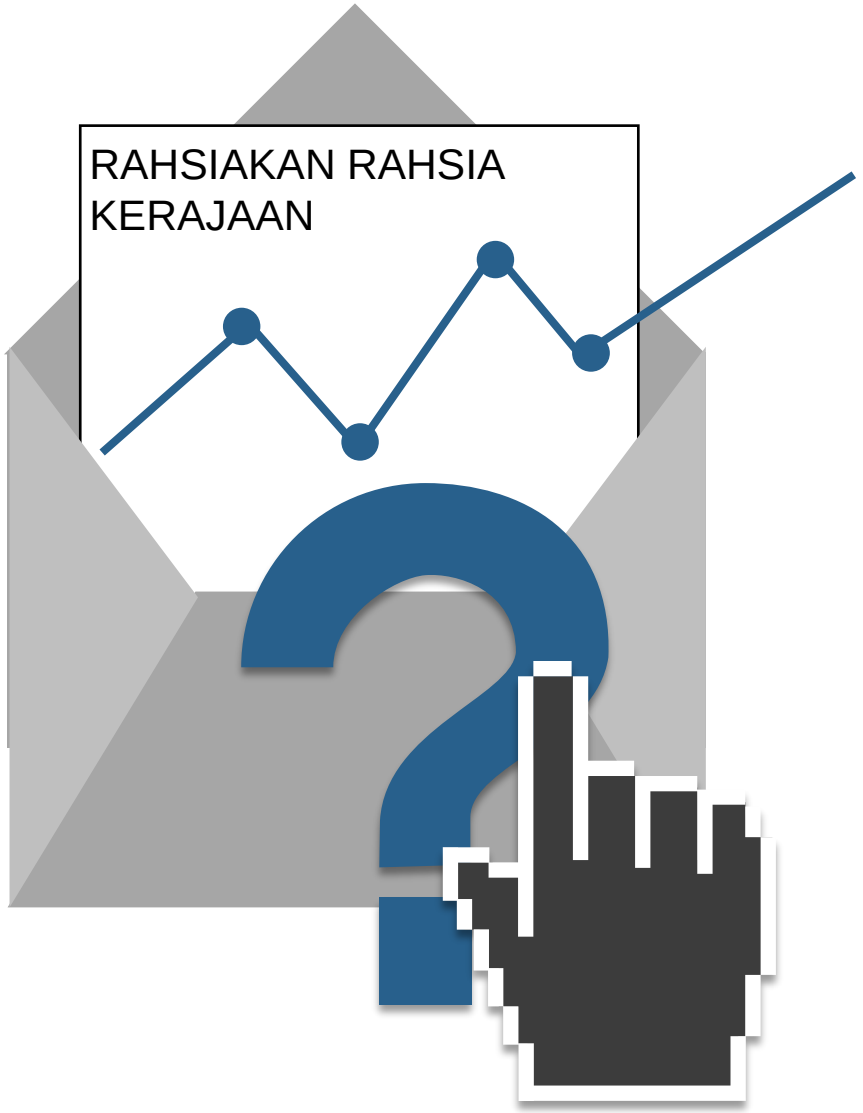
SEKIAN, TERIMA KASIH

1. Email : kictrr@cgso.gov.my

2. Direct Line: 03-88726038 / 03-88726039 | 08-88726039 (Fax)

3. Address:

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.



KRONOLOGI PENYEDIAAN MJM

GLOBAL CLOUD ADOPTION POLICY/STRATEGY

NEGARA	DASAR CLOUD SEMASA	RUJUKAN
GERMANY	In April 2017, the German Parliament passed an act in the Implementation of the NIS-Directive. This act brings several amendments to the Act on the Federal Office for Information Security, including new data security and security breach notification obligations for cloud service providers.	• The Cyber Security Strategy for Germany
JAPAN	Japan's approach to cloud security issues has a strong focus on international standards and promotes the ISO/IEC 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services (issued in 2015). Indeed, **the ISO standard was based on the Japanese national standard for cloud security**. .	• The Government of Japan
US	Impact Level 6 is reserved for the storage and processing of **information classified up to SECRET**. Information that must be processed and stored at Impact Level 6 can only be processed in a DoD private/community or Federal Government community cloud, on-premises or off-premises in any cloud deployment model that restricts the physical location of the information as described in Section 5.2.1, Jurisdiction/Location Requirements. **All data stored and processed by/for the DoD must reside in a facility under the exclusive legal jurisdiction of the US.**	• National Security Agency Cybersecurity Information • Department of Defense
UNITED KINGDOM	53. Organisations that are considering utilising G-cloud service offerings must note the following • **Off-shoring of information that relates to or supports National Security is prohibited.**	• National Cyber Security Centre, UK • UK's G-Cloud Strategy
AUSTRALIA	Security Control: 1529; Revision: 1; Updated: Jul-20; Applicability: S, TS **Only community or private clouds are used for outsourced cloud services**. Security Control: 1529; Revision: 0; Updated: Sep-18; Applicability: S, TS If using outsourced cloud services for **highly classified information, public clouds are not used.**	• Australian Government Information Security Manual
SINGAPORE	The government also requires cloud service providers participating in government bulk procurement exercises for cloud services to comply with the security requirement in the **Singapore-specific Multi-Tier Cloud Security (MTCS) Singapore Standard (SS) 584**	• Infocomm Development Authority of Singapore (IDA)