

KAJIAN KEBIJAKAN PENGUTAMAAN KOMPUTASI AWAN PEMERINTAH (GOVERNMENT CLOUD FIRST POLICY)

ARAH STRATEGIS, STRATEGI, DAN INISIATIF MENUJU NG-CLOUD

TA **2022**

KAJIAN KEBIJAKAN PENGUTAMAAN KOMPUTASI AWAN PEMERINTAH (GOVERNMENT CLOUD FIRST POLICY)

ARAH STRATEGIS, STRATEGI, DAN INISIATIF MENUJU NG-CLOUD

TA 2022



KAJIAN KEBIJAKAN PENGUTAMAAN KOMPUTASI AWAN PEMEINTAH

(GOVERNMENT CLOUD FIRST POLICY)

ARAH STRATEGIS, STRATEGI, DAN INISIATIF NG-CLOUD

Copyright 2022, Dewan TIK Nasional

Editorial Team : Farisya Setiadi
Gede Rizky Gustisa Wisnu
Licsha Rosdiana
Irwansyah Nuzar
Desy Septiyani

Cover Design
& Layout : Ardi Pradana

All rights reserved. No part of this book may be reproduced, scanned, or distributed in any printed or electronic form without permission. Please do not participate in encourage piracy of copyright materials in violation of the author's right. Purchase only authorized editions.

Vi+90 pages, ; 18,5 x 27 cm

ISBN :

DAFTAR ISI

ii	DAFTAR ISI	23	4. Kesiapan Pemerintah Menuju <i>Cloud First Policy</i>
iv	DAFTAR GAMBAR	23	Perjalanan Menuju <i>Cloud First Policy</i> di Suatu Negara
v	DAFTAR TABEL	24	Tantangan dan Hambatan dalam Penyusunan <i>Cloud First Policy</i>
vi	DAFTAR SINGKATAN DAN AKRONIM	24	Implementasi dan Manfaat <i>Cloud First Policy</i>
vii	KATA PENGANTAR	26	Pertimbangan untuk Menyusun <i>Government Cloud First Policy</i>
viii	RINGKASAN EKSEKUTIF	28	5. <i>Benchmarking Government Cloud First Policy</i> di Berbagai Negara
1	1. Konteks dan Motivasi	34	Filipina
3	Tujuan	34	Pakistan
3	Manfaat	43	Arab Saudi
3	Ruang Lingkup	45	Jerman
4	Struktur Kajian	47	Inggris Raya
5.	2. Gambaran Umum <i>Cloud Computing</i>	48	Singapura
6	Karakteristik <i>Cloud Computing</i>	49	Nigeria
7	Model Layanan	50	Analisis <i>Benchmarking</i>
8	Model <i>Deployment</i>	27	6. Regulasi terkait <i>Cloud Computing</i> di Indonesia
10	Manfaat dan Tantangan <i>Cloud Computing</i>	51	7. Kerangka Strategis <i>National Government Cloud</i>
14	3. <i>Cloud Computing</i> untuk Sektor Pemerintahan	54	8. Kesimpulan
14	Isu dan Hambatan <i>Cloud Computing</i> di Sektor Pemerintahan Indonesia	55	Penutup
16	<i>Cloud Computing</i> Membantu Sektor Publik Pemerintahan	56	Referensi
17	Manfaat <i>Cloud Computing</i> untuk Sektor Pemerintahan		
19	Jalan untuk Migrasi <i>Cloud</i> di Sektor Pemerintahan		

DAFTAR GAMBAR

- Gambar 1. Potret Adopsi *Public Cloud* di Indonesia
- Gambar 2. Pengaruh Adopsi *Cloud* Terhadap Jumlah Pekerjaan
- Gambar 3. Karakteristik Utama *Cloud Computing*
- Gambar 4. Model Layanan *Cloud Computing*
- Gambar 5. Model *Deployment Cloud Computing*
- Gambar 6. Manfaat dan Tantangan *Cloud Computing*
- Gambar 7. Isu dan Hambatan *Cloud Computing* di Sektor Pemerintahan
- Gambar 8. Bagaimana *Cloud Computing* Membantu Sektor Publik
- Gambar 9. Manfaat *Cloud Computing* untuk Sektor Pemerintahan
- Gambar 10. Opsi Jalan untuk Migrasi *Cloud* di Sektor Pemerintahan
- Gambar 11. Perjalanan Menuju *Cloud First Policy* di Suatu Negara
- Gambar 12. Tantangan dan Hambatan dalam Penyusunan *Cloud First Policy*
- Gambar 13. Alasan Penerapan *Cloud First Policy* di Suatu Negara
- Gambar 14. Perspektif Pertimbangan Penyusunan *Government Cloud First Policy*
- Gambar 15. Pertimbangan untuk Mendukung Transisi ke Lingkungan *Cloud First*
- Gambar 16. Migrasi *Cloud* pada Kebijakan *Cloud First* Filipina [14]
- Gambar 17. Usulan Struktur Organisasi *Cloud Office* Pakistan [26]
- Gambar 18. Proses Terperinci di Tiap Tahapan Adopsi *Cloud* Arab Saudi [13]
- Gambar 19. Struktur Tata Kelola untuk *Cloud First Policy* di Arab Saudi [13]
- Gambar 20. Regulasi terkait *Cloud Computing* di Indonesia Saat ini
- Gambar 21. Kerangka Strategis *National Government Cloud*
- Gambar 22. *Regulatory Framework* untuk *Government Cloud First Policy*
- Gambar 23. Rekomendasi Struktur Otoritas NG-Cloud
- Gambar 24. Usulan Kerangka Kerja Manajemen Risiko untuk NG-Cloud
- Gambar 25. Usulan Kompetensi untuk NG-Cloud
- Gambar 26. Komponen Menuju Solusi *Cloud Native*
- Gambar 27. Arsitektur *Cloud Native* menggunakan *Microservices*
- Gambar 28. Fase Migrasi Aplikasi ke *Cloud*
- Gambar 29. Framework untuk migrasi *cloud* di Pemerintahan
- Gambar 30. Peta Jalan Implentasi NG-Cloud

DAFTAR TABEL

- Tabel 1. Model Cloud Berdasarkan NIST
- Tabel 2. Perbandingan Teknologi sebagai CapEx dan OpEx
- Tabel 3. Perbandingan Pengadaan TI Tradisional dan Cloud
- Tabel 4. Keuntungan dan Kelemahan dari 4 (empat) Opsi Migrasi Cloud
- Tabel 5. Persyaratan Keamanan Cloud di Filipina
- Tabel 6. Matriks Klasifikasi Data dengan Pemilihan Cloud di Pakistan
- Tabel 7. Analisis Benchmarking Government Cloud First Policy di Enam Negara
- Tabel 8. Matriks Regulasi terkait *Cloud Computing* di Indonesia Saat Ini

DAFTAR SINGKATAN DAN AKRONIM

SPBE	Sistem Pemerintahan Berbasis Elektronik
PSTE	Penyelenggaraan Sistem dan Transaksi Elektronik
PSE	Penyelenggara Sistem Elektronik
UU	Undang-Undang
ITE	Informasi dan Transaksi Elektronik
PP	Peraturan Pemerintah
Perpres	Peraturan Presiden
NIST	<i>National Institute of Standards and Technology</i>
IPPD	Instansi Pusat dan Pemerintah Daerah
PDB	Pendapatan Domestik Bruto
IaaS	<i>Infrastructure as a Service</i>
PaaS	<i>Platform as a service</i>
SaaS	<i>Software as a Service</i>
PCFP	Pakistan Cloud First Policy
CSP	Cloud Service Provider
G2G	<i>Government to Government</i>
G2E	<i>Government to Employee</i>
G2B	<i>Government to Business</i>
G2C	<i>Government to Citizens</i>

KATA PENGANTAR

Puji dan syukur kami haturkan kehadiran Tuhan Yang Maha Esa yang telah mencurahkan berkat rahmat dan karunia-Nya, sehingga kami dapat menyelesaikan kajian Kebijakan Pengutamaan Komputasi Awan Pemerintah (*Government Cloud First Policy*).

Melalui hasil kerja keras kami yang didukung oleh para pemangku kepentingan, kami meyakini *Cloud computing* atau komputasi awan memiliki peran yang sangat sentral dalam mengakomodasi percepatan transformasi digital bagi instansi pemerintah di Indonesia. Komputasi awan ini memungkinkan pemerintah menghasilkan penerapan SPBE yang sistematis, holistik dan berkinerja tinggi. Sehingga besar harapan kami kajian *Government Cloud First Policy* ini dapat menjadi salah satu acuan yang digunakan oleh pemerintah dalam mengoptimalkan teknologi komputasi awan dan pengelolaan sumber daya Teknologi Informasi.

Ucapan terima kasih dan penghargaan yang setinggi-tinginya kami sampaikan kepada seluruh pihak yang telah membantu dan mendukung dalam penyelesaian kajian ini. Kami sangat menyadari kajian Kebijakan Pengutamaan Komputasi Awan Pemerintah (*Government Cloud First Policy*) ini tentu tidak luput dari kekurangan, untuk itu kritik dan masukan yang konstruktif sangat kami harapkan dari seluruh pemangku kepentingan dalam rangka penyempurnaan kajian kami yang akan datang.

RINGKASAN EKSEKUTIF

Melakukan migrasi dari infrastruktur TI tradisional dan penyimpanan data ke layanan *cloud* dapat menghasilkan manfaat besar bagi pemerintah, antara lain dapat menghemat anggaran pemerintah, meningkatkan integritas, kualitas, dan kecepatan dalam memberikan layanan, serta menyediakan akses ke *tools* analitik dan fitur keamanan siber yang tersedia. Manfaat ini telah mendorong pergeseran oleh pemerintah di seluruh dunia dari sistem TI tradisional menuju solusi *cloud*, termasuk layanan *public cloud*.

Selama masa transformasi digital, pemerintah menyesuaikan diri dengan kenormalan baru pasca pandemi virus corona atau Covid-19. Masyarakat yang paham internet dan terhubung secara digital menuntut tingkat layanan yang mudah, cepat, dan handal dari pemerintah mereka. Pemerintah di seluruh Asia dan Pasifik khususnya di Indonesia merespons perubahan dengan memperbarui layanan digital mereka, menambah kemampuan analitik data, dan menerapkan rencana pengembangan ekonomi digital. Di sisi lain, pemerintah Indonesia juga berfokus pada percepatan implementasi sistem pemerintahan berbasis elektronik (SPBE).

Namun, adopsi *cloud computing* masih menghadapi hambatan di sektor pemerintahan Indonesia. Beberapa hambatan yang ditemui antara lain regulasi yang belum terarah, ketimpangan kapabilitas industri *cloud* lokal dan global, persepsi ketakutan hilangnya pekerjaan, pemahaman tentang *cloud* yang kurang, ketakutan akan dipersalahkan dalam adopsi *cloud*, anggaran *cloud* yang tidak sesuai, belum memiliki pengalaman pemanfaatan *cloud*, serta kurangnya publikasi keberhasilan *cloud* di instansi pemerintahan. Terlepas dari hambatan adopsi ini, ada beberapa pertimbangan juga untuk mendukung proses transisi ke lingkungan *cloud first*, yaitu (1) menyusun, melakukan promosi, dan sosialisasi *cloud first policy* (2) melakukan akreditasi, kepatuhan, dan keamanan *cloud* (3) menyusun klasifikasi data (4) membangun kontrol dan privasi data (5) mendesain pengadaan dan kontrak *cloud*.

Laporan kajian Government Cloud First Policy ini merumuskan sebuah Kerangka Strategis National Government Cloud (NG-Cloud) yang diharapkan menjadi acuan untuk mengakselerasi adopsi dan tata kelola *cloud* pemerintahan. Kerangka strategis ini berisi arah strategis, dimensi, strategis, serta inisiatif-inisiatif. Arah strategis NG-Cloud diselaraskan dengan Visi SPBE yang telah ditetapkan pemerintah Indonesia. Dari arah strategis, terdapat tiga dimensi, antara lain NG-Cloud Governance, NG-Cloud Ecosystem, dan NG-Cloud Deployment. Pada masing-masing dimensi memiliki strategi yang berbeda-beda. Salah satu contohnya pada dimensi NG-Cloud Governance yang memiliki strategi "mendorong penyusunan Government Cloud First Policy". Setelah itu, beberapa inisiatif diusulkan sesuai dengan strategi di masing-masing domain Kerangka Strategis NG-Cloud. Dewan TIK Nasional juga merekomendasikan peta jalan implementasi *cloud* untuk pemerintah Indonesia berdasarkan Kerangka Kerja NG-Cloud dengan jangka waktu lima tahun. Peta jalan ini dibagi tiga fase yaitu jangka pendek, jangka menengah, dan jangka panjang. Dengan demikian, rekomendasi kerangka strategis NG-Cloud diusulkan oleh Dewan TIK Nasional sebagai upaya strategis dalam proses transisi Pemerintah Indonesia menuju ekosistem *cloud* yang selaras dan terintegrasi dengan baik secara Nasional.

01 KONTEKS DAN MOTIVASI

KEY FACTS

Beberapa realita yang ada dari penggunaan *public cloud* oleh Pemerintah:

- » *Cloud computing* bersifat hemat biaya karena meniadakan atau mengurangi kebutuhan untuk pengadaan peralatan yang mahal. Penghematan dapat mencapai 10-20 persen dari anggaran operasional TI tahunan.
- » Solusi on-premise tidak secara inheren lebih aman, karena sebagian besar keamanan tingkat lanjut dapat diterapkan secara *real-time* saat menggunakan infrastruktur *cloud*.
- » Layanan *cloud* lebih baik dalam mendorong inovasi karena mudah digunakan, dapat ditingkatkan dengan cepat, dan menyediakan layanan baru saat tersedia, secara signifikan mengurangi waktu yang diperlukan untuk beralih dari ide ke sebuah solusi.
- » Penggunaan *cloud computing* dapat mengurangi konsumsi energi dan emisi karbon hingga 30%, karena skala ekonomi.

Sumber: Digital Development Partnership. 2022. Government Migration to Cloud Ecosystems. Washington: International Development Association of The World Bank.

Komputasi awan atau yang selanjutnya disebut *cloud computing* merupakan salah satu topik yang sangat mendominasi di sektor TI saat ini. Umumnya, *cloud computing* memungkinkan perusahaan untuk menyediakan layanan TI seperti *computing power* dan *data storage* sesuai dengan permintaan. Hanya sumber daya yang telah digunakan oleh organisasi yang dikenakan biaya oleh perusahaan penyedia layanan *cloud* [1] atau dikenal dengan *pay on your demand*. Pemanfaatan *cloud computing* memiliki banyak keunggulan, antara lain penghematan biaya, skalabilitas, dan ketersediaan yang tinggi, sehingga membuat *cloud computing* menarik untuk digunakan di berbagai sektor. Khususnya pada sektor publik di Pemerintahan, menurut Khan et al. pada penelitian [1] dengan memanfaatkan *cloud computing*, pemerintah dapat lebih berfokus pada bisnis intinya yaitu melayani masyarakat ketimbang mengelola sumber daya dan tugas pemeliharaan TI.

Memberikan layanan secara efisien dan mencapai penghematan biaya adalah dua pendorong utama adopsi *cloud* di sektor pemerintahan. Gartner memperkirakan pertumbuhan dalam penggunaan layanan *public cloud* oleh pemerintah, dengan perkiraan pengeluaran untuk tumbuh rata-rata 17,1% per tahun hingga 2021 [2]. Pengeluaran *end-user* atau pengguna akhir di seluruh dunia untuk layanan *public cloud* diperkirakan akan tumbuh 20,4% pada tahun 2022 menjadi total \$494,7 miliar, naik dari \$410,9 miliar pada tahun 2021, menurut perkiraan terbaru dari Gartner. Pada tahun 2023, pengeluaran pengguna akhir diperkirakan akan mencapai hampir \$600 miliar [3].

Penggunaan *cloud* oleh instansi pemerintah saat ini begitu bervariasi tergantung pada operasional di tingkat nasional, negara bagian atau provinsi, atau juga lokal. Secara umum di beberapa negara, pemerintah daerah menghabiskan 20,6% anggaran TI mereka untuk *cloud*, dan pemerintah nasional menghabiskan 22%. [2]. Selain itu, beberapa kategori TI dari organisasi yang dapat bertransisi ke penggunaan *cloud* antara lain perangkat lunak aplikasi, perangkat lunak infrastruktur, layanan proses bisnis, dan sistem infrastruktur. Menurut penelitian Gartner [4], pada tahun 2025, 51% pengeluaran TI dalam empat kategori ini akan beralih dari solusi tradisional ke *public cloud*, dibandingkan dengan 41% pada tahun 2022.

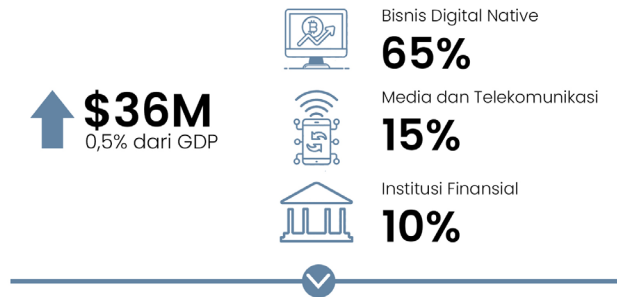
Pandemi Covid-19 menunjukkan pentingnya digitalisasi di layanan pemerintah, karena negara-negara yang telah berinvestasi dalam teknologi ini lebih mampu beradaptasi dengan krisis dan menunjukkan ketahanan yang lebih besar dibandingkan negara-negara yang rendah dalam adopsi pemanfaatan teknologi. Hal ini mencakup kemampuan aparat sipil negara untuk beralih ke pekerjaan jarak jauh, pemberian layanan secara daring, penggunaan data untuk mengelola pekerjaan yang ditargetkan, serta operasional yang berkelanjutan. Virtualisasi proses-proses ini yang dapat difasilitasi oleh teknologi dan layanan *cloud computing* menunjukkan langkah penting lainnya dalam jalur pengembangan digital bagi pemerintah [5].

Melihat kondisi industri *cloud computing* di Indonesia saat ini, pasar *public cloud* di Indonesia sedang bertumbuh dan mewakili salah satu pasar dengan pertumbuhan tercepat di Kawasan Asia Pasifik [6]. Menurut laporan dari Boston Consulting Group (BCG) di tahun 2019 [6] di mana sebelum terjadinya pandemi Covid-19, BCG memperkirakan dampak kumulatif dari ekonomi Indonesia pada adopsi *public cloud* di tahun 2019-2023 sebesar 36 miliar USD (lihat Gambar 1). Pertumbuhan ini setara dengan 0,5% dari PDB tahunan Indonesia. Bisnis berbasis digital menjadi kekuatan utama dalam pertumbuhan adopsi *cloud* ini, yang kemudian disusul oleh industri pelayanan finansial serta industri retail dan barang konsumsi.

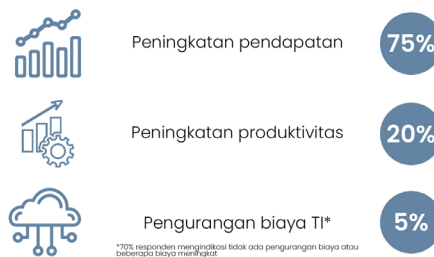
Berkaitan dengan peluang pekerjaan di masa mendatang, menurut laporan BCG [6] adopsi *public cloud* di Indonesia dapat menciptakan 70.000 pekerjaan langsung atau *direct jobs* selama lima tahun ke depan. Sekitar 47.000 pekerjaan berada dalam peran non-digital seperti pemasaran, penjualan, keuangan, dll. Sejumlah 23.000 lainnya akan menjadi pekerjaan digital yang 3.000 di antaranya bekerja pada layanan *cloud* dan industri TI dan 20.000 sisanya pekerjaan digital dalam vertikal industri. efek lainnya dalam adopsi *public cloud* di Indonesia akan memengaruhi 275.000 pekerjaan tidak langsung atau *indirect jobs*, sehingga total pekerjaan potensial yang berpengaruh signifikan dari penggunaan *public cloud* menjadi 345.000 atau setara dengan 0,3% dari total jumlah pekerjaan di Indonesia saat ini (lihat Gambar 2).

Gambar 1. Potret Adopsi *Public Cloud* di Indonesia

Nilai tambah dampak dari PDB (\$M) selama 2019-2023



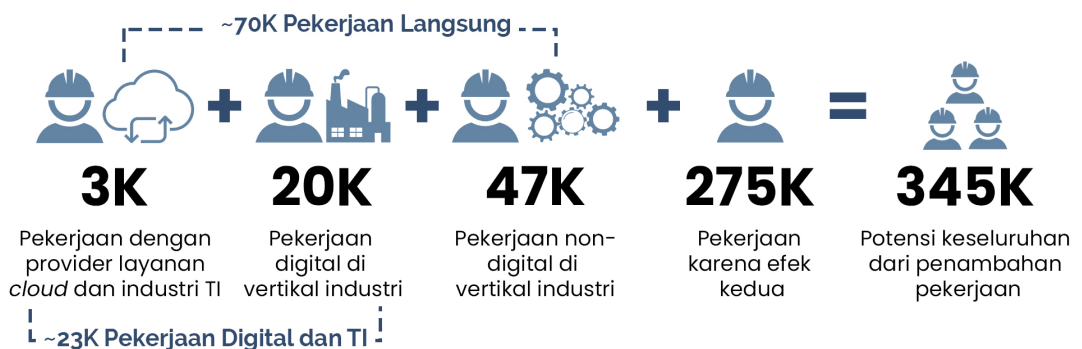
Nilai ekonomi melalui tiga layer



Sumber: [6] – telah diolah kembali

Dalam rangka mendukung percepatan transformasi digital bagi instansi pemerintah di Indonesia, pemanfaatan teknologi *cloud computing* memiliki peran yang sangat sentral. Melalui teknologi *cloud computing* ini, memungkinkan pemerintahan untuk menyederhanakan dan mengoptimalkan pengelolaan sumber daya TI dan memfasilitasi adopsi teknologi yang baru ke depannya. Di masa mendatang, kebutuhan teknologi *cloud computing* akan meningkat seiring dengan terjadinya pertumbuhan secara eksponensial terhadap *volume* data yang diproses serta meluasnya layanan digital. Hal ini membuat pemerintah membutuhkan infrastruktur *cloud computing* yang dapat diperluas serta dieskalasi dengan cepat dan fleksibel [7]

Gambar 2. Pengaruh Adopsi *Cloud* Terhadap Jumlah Pekerja



Sumber: [6] – telah diolah kembali

Adopsi *cloud computing* di sektor pemerintahan di Indonesia tidak terlepas dari keterkaitannya dengan Pusat Data Nasional (PDN). PDN sebagai salah satu infrastruktur Sistem Pemerintahan Berbasis Elektronik (SPBE) berdasarkan Perpres No. 95 Tahun 2018 tentang SPBE. Kemudian berdasarkan laporan yang telah disusun oleh Wantiknas [8], adanya pembangunan 4 (empat) Pusat Data Nasional terintegrasi yang juga selaras dengan arahan Presiden mengenai 5 (lima) langkah percepatan transformasi digital. PDN ini dibangun di kawasan Jabodetabek, Batam, Ibu Kota Nusantara (IKN), dan Labuan Bajo [9]. Tantangan kedepannya yaitu bagaimana pemanfaatan *cloud computing* di sektor pemerintahan di Indonesia dapat terintegrasi dengan ekosistem PDN yang telah dibangun.

Adopsi suatu kebijakan atau *policy* yang berkaitan dengan pemanfaatan *cloud computing* dibutuhkan oleh Pemerintah Indonesia. Dengan kata lain, perlu disusunnya *Government Cloud First Policy* sebagai landasan hukum dalam pemanfaatan teknologi *cloud computing* di instansi pemerintah di Indonesia. Beberapa negara yang telah memiliki kebijakan atau strategi *cloud* antara lain Amerika Serikat [10], Inggris Raya [11], Australia [12], Arab Saudi [13], dan Filipina [14]. Selain itu, kebijakan ini untuk memastikan adanya ketentuan hukum yang sesuai untuk pengadaan *cloud* sebagai bagian dari persyaratan pengadaan negara. Di sisi lain, kebijakan ini tentunya akan mengarah pada pengurangan biaya modal untuk layanan infrastruktur TI, peningkatan respons layanan digital terhadap kebutuhan masyarakat, peningkatan transparansi, dan peningkatan penyampaian publik [15]. Ditambah lagi, adopsi *cloud computing* ini memungkinkan pemerintahan untuk mengoptimalkan pengelolaan sumber daya TI dan memfasilitasi adopsi tren teknologi baru di masa depan sehingga dengan menguasai teknologi canggih mampu memperkuat fondasi agar Indonesia bertransformasi dari negara berkembang menjadi negara maju.

Maka dari itu, Dewan Teknologi Informasi dan Komunikasi (WANTIKNAS) menyusun kajian rekomendasi tentang *Government Cloud First Policy* sebagai referensi untuk menyusun *Cloud First Policy* bagi pemerintahan di Indonesia serta mempromosikan penggunaan *cloud* yang utama atau "*Cloud First*". Melalui kajian ini diharapkan Pemerintah Indonesia dapat melakukan *leapfrog* atau melompat lebih jauh dalam merumuskan strategi *cloud computing*.

Manfaat

Manfaat yang diharapkan dalam penyusunan Kajian *Government Cloud First Policy* ini adalah sebagai berikut.

1. Manfaat bagi Instansi Pusat Pemerintah yaitu dapat menggunakan hasil kajian ini sebagai bahan pertimbangan dalam penyusunan *Government Cloud First Policy* di Indonesia dalam rangka menghadapi transformasi digital di Pemerintahan.
2. Manfaat bagi praktisi yaitu sebagai referensi untuk melakukan riset lebih lanjut mengenai penyusunan kebijakan *Cloud Computing* di Instansi Pusat Pemerintah untuk mendukung transformasi digital di Indonesia.

Ruang Lingkup

Kajian *Government Cloud First Policy* ini lebih berfokus pada isu yang diangkat menjadi topik utama. Beberapa batasan penelitian yang diberikan oleh penulis sebagai berikut:

1. Pembahasan pelayanan publik dalam kajian ini merupakan pelayanan publik yang diselenggarakan oleh Instansi Pusat dan Pemerintah Daerah.
2. Hasil akhir dari kajian ini adalah kajian literatur dan analisis rekomendasi dari

pembandingan *best practices* dan *lesson learned* penerapan *Government Cloud Policy* di beberapa negara dalam mendukung pemanfaatan *Cloud Computing* di instansi pemerintah.

Struktur Kajian

Kajian *Government Cloud First Policy* ini disusun berdasarkan struktur yang telah ditentukan sebagai berikut:

- BAGIAN 1** menjelaskan mengenai konteks dan motivasi dari penyusunan kajian rekomendasi ini yang di dalamnya mencakup tujuan, manfaat, ruang lingkup, dan struktur kajian.
- BAGIAN 2** menjelaskan bagaimana gambaran umum dari cloud computing yang meliputi karakteristik *cloud computing*, model layanan, model *deployment*, serta manfaat dan tantangan dari *cloud computing*.
- BAGIAN 3** menyajikan penjelasan mengenai *cloud computing* untuk sektor pemerintahan yang berisi berbagai isu dan hambatan, manfaat, serta bagaimana jalan untuk migrasi dan adopsi *cloud* di sektor pemerintahan.
- BAGIAN 4** menjelaskan bagaimana kesiapan yang diperlukan pemerintah untuk menuju *cloud first policy* yang meliputi pengetahuan terkait perjalanan *cloud first policy* di suatu negara, tantangan dan hambatan dalam penyusunan kebijakan *cloud first*, implementasi dan manfaat *cloud first policy*, serta pertimbangan untuk menyusun *Government Cloud First Policy*.
- BAGIAN 5** menyajikan hasil benchmarking dari *Government Cloud First Policy* yang ada di beberapa negara.
- BAGIAN 6** menyajikan penjelasan mengenai arah regulasi yang berkaitan dengan *cloud computing* di Indonesia.
- BAGIAN 7** menyajikan suatu *framework National Government Cloud* sebagai bahan pertimbangan pemerintah yang berisi arah strategis, strategi, dan inisiatif untuk transisi menuju cloud di pemerintahan.
- BAGIAN 8** menjelaskan kesimpulan dari kajian *Government Cloud First Policy*.

Pemerintah Indonesia perlu mengupayakan untuk menyusun *Government Cloud First Policy* sebagai fondasi kebijakan pemanfaatann komputasi awan di lingkungan pemerintahan. Melalui kebijakan ini, diharapkan mampu mendorong akselerasi inisiatif-inisiatif Pemerintah di sektor TIK seperti Transformasi Digital Nasional, SPBE, Satu Data Indonesia, hingga Pusat Data Nasional.

02 GAMBARAN UMUM CLOUD COMPUTING

KEY FACTS

Pemanfaatan *cloud* dapat berdampak positif bagi suatu organisasi. Organisasi dapat melakukan hal-hal berikut:

- » Mengurangi biaya *overhead* TI sebesar 30 hingga 40 persen.
- » Membantu meningkatkan dan menurunkan proses TI sesuai kebutuhan, sehingga mengoptimalkan penggunaan aset TI.
- » Meningkatkan fleksibilitas TI secara keseluruhan dalam memenuhi kebutuhan bisnis, seperti rilis fitur bisnis yang lebih sering (penyedia *cloud* menawarkan solusi yang jauh lebih canggih daripada komputasi dan penyimpanan dasar, seperti big data dan layanan *machine learning*).
- » Meningkatkan kualitas layanan dengan solusi terdepan semisal, secara otomatis mengalokasikan lebih banyak penyimpanan ke *database* (organisasi mampu mengurangi insiden TI hingga 70 persen dengan menggunakan *cloud computing*).

Sumber: Digital McKinsey, 2018. Creating Value with The Cloud, McKinsey & Company

Cloud Computing merupakan model yang memungkinkan akses jaringan di mana-mana dan sesuai dengan permintaan ke kumpulan sumber daya *computing* yang dapat dikonfigurasi (misalnya seperti jaringan, server, penyimpanan, aplikasi, dan layanan) serta dapat dengan cepat disediakan dan dirilis dengan upaya manajemen atau interaksi penyedia layanan *cloud* yang minimal. Selain itu, Amazon Web Services [16] menyatakan bahwa *cloud computing* merupakan pengiriman IT *resources* sesuai permintaan melalui jaringan publik atau pribadi tanpa biaya di muka, tanpa kontrak jangka panjang, dan harga bayar sesuai pemakaian. Risiko yang ada dalam penggunaan layanan *cloud* pada dasarnya sama dengan alih daya tradisional layanan TIK. Risiko dan kerentanan tersebut dikaitkan dengan pilihan penyedia, lokasi, saluran komunikasi, serta arsitektur. Model *cloud* terdiri dari 5 (lima) karakteristik, 3 (tiga) model layanan, dan 4 (empat) model *deployment* (lihat Tabel 1).

Tabel 1. Model *Cloud* Berdasarkan NIST

Lima Karakteristik	Tiga Model Layanan	Empat Model Deployment
On-demand self-service	Software as a Service (SaaS)	Public cloud
Broad network access	Aplikasi desktop, CRM, akunting	Community cloud
Resource pooling	Platform as a Service (PaaS) Database, platform pengembangan, sistem operasi	Private cloud
Rapid elasticity		Hybrid cloud Kombinasi <i>public cloud</i> dengan <i>private cloud/community cloud</i>
Measured service	Infrastructure as a Service (IaaS) Storage, processing, virtualisasi	

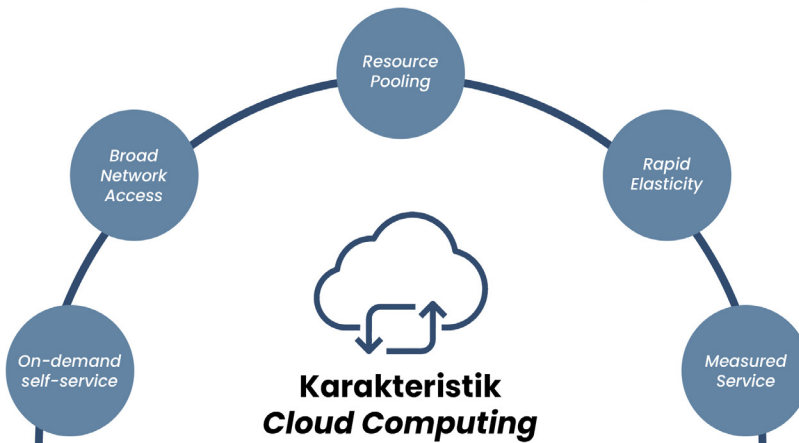
Sumber: [17] - telah diolah kembali

Berdasarkan pemetaan model *cloud* pada Tabel 1, berikut dijelaskan dari masing-masing model *cloud* tersebut.

Karakteristik *Cloud Computing*

Cloud computing memanfaatkan beberapa elemen termasuk skala, virtualisasi, ketahanan, efisiensi biaya, orientasi layanan, dan *agility*. Elemen-elemen ini digabungkan di bawah definisi NIST [17] menjadi 5 (lima) karakteristik utama (lihat Gambar 3):

Gambar 3. Karakteristik Utama *Cloud Computing*



Sumber: [17] - telah diolah kembali

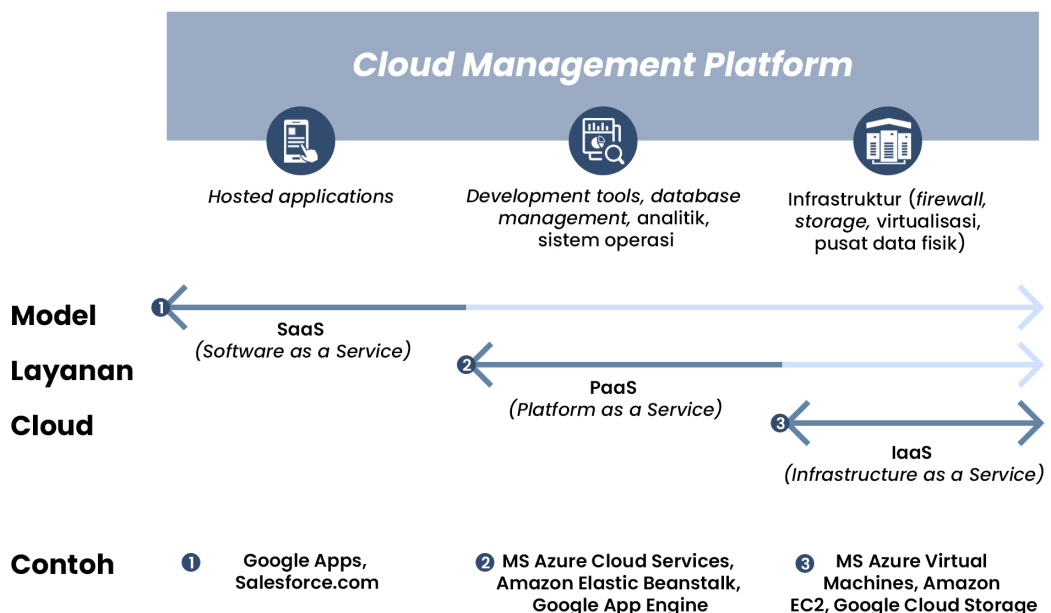
- 1. On-demand self-service:** Penyediaan kapabilitas *computing* yang dilakukan sepihak, seperti waktu server dan penyimpanan jaringan, disediakan oleh pengguna akhir atau *end user*, tanpa memerlukan interaksi manusia dengan setiap penyedia layanan.
- 2. Broad network access:** Ketersediaan kapabilitas melalui jaringan dengan aksesibilitas melalui mekanisme standar yang mendorong penggunaan oleh konsumen melalui berbagai *platform* (misalnya telepon, laptop, dan PC).

3. **Resource pooling:** Pengumpulan sumber daya komputasi untuk melayani banyak konsumen menggunakan model multi-penyewa, dengan sumber daya fisik dan virtual berbeda yang ditetapkan serta ditetapkan kembali berdasarkan permintaan. Terdapat tingkat lokasi yang independen, konsumen mungkin dapat menentukan lokasi pada tingkat abstraksi yang lebih tinggi (misalnya negara, negara bagian, atau pusat data) tetapi bukan lokasi yang tepat dari sumber daya yang disediakan. Contoh sumber daya termasuk penyimpanan, pemrosesan, memori, *bandwidth* jaringan, dan mesin virtual.
4. **Rapid elasticity:** Penyediaan kapabilitas yang cepat dan elastis untuk meningkatkan dan menurunkan sumber daya dengan cepat. Hal ini dilakukan dalam beberapa kasus secara otomatis. Bagi konsumen, kemampuan yang tersedia untuk penyediaan seringkali dan hampir tidak terbatas serta dapat dibeli dalam jumlah berapa pun dan kapan saja.
5. **Measured service:** Sumber daya yang dikontrol dan dioptimalkan secara otomatis digunakan dengan memanfaatkan kapabilitas pengukuran pada beberapa tingkat abstraksi, sesuai dengan jenis layanan (misalnya, penyimpanan, pemrosesan, *bandwidth*, dan akun pengguna aktif). Penggunaan sumber daya dapat dipantau, dikendalikan, dan dilaporkan sehingga memberikan transparansi bagi penyedia dan konsumen dari layanan yang digunakan.

Model Layananan

Pada intinya, *cloud computing* menawarkan 3 (tiga) model layanan berbeda yaitu menyediakan aplikasi, *platform*, dan infrastruktur sebagai layanan. Model layanan ini menyediakan beberapa dukungan TI yang dibutuhkan untuk menyebarkan solusi TI (lihat Gambar 4).

Gambar 4. Model Layanan Cloud Computing



Sumber: [13] - telah diolah kembali

Berdasarkan Gambar 4, model layanan yang berbeda tersedia di *cloud*, tergantung dari kebutuhan suatu organisasi. Layanan aplikasi yang berjalan di infrastruktur *cloud* penyedia dikenal sebagai **Software as a Service (SaaS)**. Menggunakan aplikasi yang dihosting dapat diartikan penyewa tidak perlu membeli, melakukan instalasi, memperbarui, dan memelihara aplikasi secara lokal. Sebagai gantinya, pengguna dapat menjalankan aplikasi melalui peramban web lainnya. Contoh dari SaaS adalah aplikasi *desktop* seperti pengolah kata dan *spreadsheet*, sistem akuntansi serta CRM.

Platform as a Service (PaaS) menawarkan semua yang diperlukan organisasi untuk mendukung pembuatan dan penerapan layanan digital, seperti bahasa pemrograman, pustaka, dan *tools* yang didukung oleh penyedia. Sebuah *platform* dapat berupa basis data atau seluruh pengembangan serta pengujian.

Infrastructure as a Service (IaaS) menyediakan seluruh sumber daya data yang dibutuhkan organisasi di pusat data atau ruang server sendiri, seperti penyimpanan, jaringan, dan sumber daya *computing* mendasar lainnya. Meskipun organisasi membeli SaaS dan PaaS secara bertahap menjadi tersebar luas, membeli kapasitas penyimpanan dan pemrosesan masih lebih umum dilakukan.

Model Deployment

Cloud computing juga memiliki 3 (tiga) model *deployment* utama, dengan sebagian besar negara mengadopsi komposisi ketiganya (lihat Gambar 5). Masing-masing model *deployment* ini dapat menawarkan model layanan yang berbeda-beda. Perbedaan utama terletak pada tingkat kontrol dan kepemilikan yang diasumsikan penyedia layanan *cloud* dengan kepemilikan pengguna.

Gambar 5. Model Deployment Cloud Computing

	<i>Private Cloud</i>	<i>Community Cloud</i> (cth. Milik Pemerintah)	<i>Public Cloud</i>
Pengguna	Digunakan oleh satu organisasi (cth. satu Kementerian)	Digunakan oleh komunitas konsumen (cth. beberapa Kementerian Pemerintah)	Digunakan oleh publik umum
Model Operasional	Dimiliki dan dioperasikan oleh organisasi itu sendiri, pihak ketiga, atau kombinasi keduanya	Dimiliki dan dioperasikan oleh satu atau lebih organisasi dari komunitas atau pihak ketiga	Dimiliki dan dioperasikan oleh bisnis (lokal/internasional), Pemerintah, organisasi akademik
Lokasi	<i>On</i> atau <i>Off Premises</i>	<i>On</i> atau <i>Off Premises</i>	<i>On Premises</i> dari penyedia <i>cloud</i>
SLA/Uptime	Tidak ada garansi, redundansi data dikelola sendiri	Digaransi oleh provider, redundansi data dikelola oleh provider	Digaransi oleh provider, redundansi data dikelola oleh provider
Timeline	<i>Longer timelines</i> , dikarenakan deployment dan testing	<i>Faster timelines</i> , model <i>plug and play</i>	<i>Faster timelines</i> , model <i>plug and play</i>
Contoh	<i>Private cloud</i> US Ministry of Defense	KSA National Information Center, Singapore G-Cloud	AWS, Google Cloud, Singtel

Hybrid Cloud – Kombinasi dari tiga model di atas

Sumber: [13] - telah diolah kembali

Berdasarkan Gambar 5, berikut dijelaskan masing-masing model deployment dari cloud computing menurut NIST [17]:

1. **Private Cloud:** Infrastruktur *cloud* disediakan untuk penggunaan eksklusif oleh satu organisasi yang terdiri dari beberapa pengguna. Infrastrukturnya mungkin dimiliki, dikelola, dan dioperasikan oleh organisasi, pihak ketiga, atau kombinasi dari semuanya. Lokasi fisiknya mungkin ada di dalam atau di luar premis. Tidak ada jaminan pada SLA/Waktu Aktif dan redundansi data dikelola oleh entitas itu sendiri. Pengembangan solusi pada *Private Cloud* biasanya menghabiskan lebih banyak waktu karena semua penerapan dan pengujian perlu dilakukan secara internal. Contoh dari *Private Cloud* untuk sektor Pemerintah adalah *Cloud* milik instansi pusat dan pemerintah daerah (IPPD), yang biasanya melayani unit kerja atau kumpulan unit kerja.
2. **Community Cloud:** Infrastruktur *cloud* ini disediakan untuk penggunaan eksklusif oleh komunitas konsumen tertentu dari organisasi yang memiliki minat yang sama/sejajar (misalnya misi, persyaratan keamanan siber, kebijakan, dan pertimbangan kepatuhan). Infrastruktur ini mungkin dimiliki, dikelola, dan dioperasikan oleh satu atau lebih organisasi dalam komunitas, pihak ketiga, atau kombinasi dari seluruhnya. Lokasi fisiknya mungkin berada di dalam atau di luar premis. SLA/Waktu Aktif dijamin oleh penyedia layanan dan redundansi data juga dikelola oleh penyedia. Model ini menawarkan model “*plug and play*” yang memungkinkan jadwal yang lebih cepat untuk penerapan solusi baru.
3. **Public Cloud:** Infrastruktur *cloud* ini disediakan untuk penggunaan terbuka oleh berbagai entitas. Infrastruktur ini mungkin dimiliki, dikelola, dan dioperasikan oleh unit bisnis, akademik, atau instansi pemerintah, atau kombinasi dari semuanya. *Public Cloud* biasanya dilayani oleh pemain global (seperti AWS, Google Cloud, Microsoft Azure) serta oleh pemain lokal (misalnya pemain telekomunikasi dan TIK lokal). SLA/Waktu Aktif dijamin oleh penyedia layanan dan redundansi data juga dikelola oleh penyedia. Model ini juga menawarkan model “*plug and play*” yang memungkinkan jadwal lebih cepat untuk penerapan solusi baru.
4. **Hybrid Cloud:** Infrastruktur *cloud* ini adalah komposisi dari dua atau lebih infrastruktur *cloud* yang berbeda (*private, community, atau public*) yang tetap menjadi entitas unik, tetapi terikat bersama oleh teknologi standar atau kepemilikan yang memungkinkan portabilitas data dan aplikasi. Pendekatan *multi-cloud*, model serupa, adalah komposisi dari dua atau lebih infrastruktur *cloud* yang berbeda tetapi tanpa konektivitas atau orkestrasi di antara keduanya. Pendekatan semacam itu telah didukung secara global.

Dari laporan McKinsey [18], banyak sektor publik pemerintahan yang memilih menggunakan *private* atau *community cloud* yang dikelola oleh unit *shared-service* (contoh pada US Federal Government General Service Administration). Memang dalam banyak kasus, *private cloud* lebih aman dan mudah dikelola daripada sistem TI saat ini dari sektor publik karena organisasi dapat membangun keamanan dan tata kelola ke dalam semua arsitektur dari awalnya. *Public cloud* mungkin menjadi cocok untuk sektor publik jika organisasi sudah matang pada kapabilitasnya dalam menangani isu keamanan dan tata kelolanya.

Manfaat dan Tantangan *Cloud Computing*

Penghematan biaya merupakan salah satu manfaat paling umum yang terkait dengan pemanfaatan *cloud computing*. Hal ini juga menjadi motivasi banyak negara ketika pemerintah telah menetapkan strategi TIK di mana *cloud computing* memainkan peran kunci. *Cloud computing* memiliki beberapa manfaat dan tantangan ketika suatu organisasi mengadopsinya (lihat Gambar 6). Dalam sebuah studi yang dilakukan oleh Asosiasi Otoritas Lokal dan Regional Norwegia pada laporan strategi *cloud computing* Norwegia [19], organisasi menganggap pendorong utama untuk mengadopsi *cloud computing* yaitu faktor keuangan, keinginan

Gambar 6. Manfaat dan Tantangan *Cloud Computing*



Sumber: [19] [5] - telah diolah kembali

untuk fokus pada pengembangan layanan, skalabilitas dan fleksibilitas, serta kemudahan akses layanan. Berikut dijelaskan beberapa manfaat dan tantangan dari penerapan *cloud computing*.

1. Efektivitas Biaya

Banyak organisasi secara otomatis memikirkan pengurangan biaya ketika *cloud computing* disebutkan. Ada beberapa alasan untuk ini yaitu bahwa layanan *cloud* tidak memerlukan infrastruktur lokal sehingga dapat mempengaruhi biaya investasi dan pengoperasian TIK. *Cloud computing* juga dapat mengurangi biaya untuk pembaruan, administrasi lisensi perangkat lunak, dll. Selain itu, model penetapan harga untuk layanan *cloud*, yang mencakup pengukuran dan pembayaran untuk penggunaan, juga membuat biaya untuk setiap layanan menjadi transparan.

2. Skalabilitas

Layanan *cloud* menawarkan kapasitas yang lebih praktis dan tidak terbatas untuk pemrosesan dan penyimpanan data. Sumber daya di *cloud* dialokasikan ke organisasi pelanggan hanya jika diperlukan. Hal ini berarti bahwa perusahaan tidak perlu khawatir akan kehabisan kapasitas jika semisal layanan publik yang disediakan digunakan lebih dari yang diperkirakan. Ini juga dapat menjadi keuntungan bagi perusahaan dengan layanan yang rentan terhadap kelebihan beban selama periode puncak yang seringkali tidak dapat diramalkan.

Elemen yang membuat layanan *cloud* hemat biaya dan skalabel juga dapat menciptakan tantangan bagi organisasi yang mengelola data pribadi, informasi rahasia, atau pun informasi di area di mana terdapat pembatasan melalui peraturan yang berlaku di suatu negara. Untuk menawarkan layanan yang terjangkau, penyedia menggunakan kapasitas gratis apa pun yang mereka miliki di sistem mereka. Akibatnya, organisasi tidak akan pernah mengetahui pusat data mana atau di negara mana informasi mereka disimpan di waktu tertentu

3. Keamanan

Cloud computing dapat meningkatkan keamanan TIK ketika penyedia layanan memiliki keahlian dan sumber daya yang lebih baik daripada pelanggan. Hal ini menjadi tidak berlaku untuk keamanan fisik dari tempat di mana perangkat keras berada. Pusat data yang besar umumnya memiliki tahapan keamanan yang komprehensif, dan pembatasan ketat tentang siapa yang boleh memasuki lokasi. Penyedia layanan mengganti perangkat keras dan meningkatkan perangkat lunak secara teratur. Selain itu, terdapat juga skema sertifikasi untuk pusat data yang menunjukkan tingkat keamanan mana yang dipenuhi oleh pusat data.

4. Efisiensi Energi

Penyedia layanan di *public cloud* dapat mengalokasikan sumber daya perangkat keras mereka ke sejumlah besar pelanggan. Hal ini membuat konsumsi energi lebih efisien daripada jika semua pelanggan memiliki pusat data mereka sendiri dengan perangkat keras, sistem pendingin, dll. Tren saat ini adalah bagi penyedia layanan *cloud* dan pusat data untuk mengkonsolidasikan pusat data mereka menjadi energi yang besar dan semakin meningkat. Pusat data ini sering terletak di area dengan akses stabil ke energi murah

5. Fleksibilitas

Dalam banyak kasus, *cloud computing* memudahkan organisasi untuk mengaktifkan layanan untuk digunakan dari lokasi yang berbeda dan dari jenis klien yang berbeda (PC, tablet, ponsel). Perusahaan publik dan swasta semakin mengizinkan karyawan mereka untuk menggunakan PC, tablet, dll. Kebijakan ini sering disebut sebagai *Bring Your Own Device* atau BYOD. BYOD menimbulkan tantangan baru dalam hal keamanan dan ketersediaan. Layanan *cloud* dapat mempermudah pengguna untuk menyimpan pekerjaan mereka di area penyimpanan perusahaan mereka di *cloud* daripada secara lokal di peralatan pribadi mereka. Sebagian besar perusahaan memiliki karyawan yang telah menggunakan layanan *cloud* konsumen yang tidak sah untuk memberi mereka fleksibilitas dalam hari kerja mereka. Ini menimbulkan risiko bagi perusahaan, karena perjanjian lisensi pengguna akhir di pasar konsumen sering memberi penyedia layanan otoritas luas untuk apa yang mungkin mereka lakukan dengan data pelanggan mereka.

6. Proteksi Data

Layanan *cloud* dapat memberikan perlindungan tingkat tinggi untuk data sensitif dengan mencegah identifikasi tidak sah atas data yang disimpan di *cloud*. Untuk melindungi dan mengamankan data di lingkungan *cloud*, organisasi harus mengetahui data apa yang mereka miliki dan di mana data tersebut berada. Selain itu, perlunya untuk mengetahui jenis atau kelas data apa yang terpapar, bagaimana data tersebut terpapar, potensi risikonya, aplikasi mana yang diakses, oleh siapa, dan untuk tujuan apa.

7. Kinerja dan Keandalan

Indikator utama keandalan dari layanan *cloud* adalah *uptime persentase* waktu server beroperasi. Sistem lokal atau *on-premise* dapat memiliki *uptime* hampir 100 persen. Akan tetapi menjalankan aplikasi 24/7 dalam sistem lokal kurang efisien dibandingkan solusi *cloud* publik yang memiliki opsi pengoptimalan yang lebih baik, dapat disesuaikan dengan permintaan aktual, dan memberikan tindakan penggantian yang ekstensif jika terjadi bencana atau gangguan sistem. Pemanfaatan yang ditingkatkan dari penyedia layanan *cloud* publik yang hyperscale memiliki manfaat tambahan juga menghasilkan penghematan keseluruhan dalam konsumsi energi.

8. Inovasi

Layanan *cloud* dapat mengurangi cakupan investasi yang diperlukan untuk memulai perusahaan baru. Karena tidak diperlukan investasi besar dalam perangkat keras dan infrastruktur atau lisensi perangkat lunak, modal awal akan lebih sedikit.

Untuk sektor publik, *platform* semacam itu dapat mempermudah pengujian dan adopsi layanan publik baru. Ini sangat penting bagi instansi pemerintah, karena mereka biasanya memiliki sedikit sumber daya untuk dialokasikan pada tugas-tugas seperti ini. Dengan cara ini *cloud computing* dapat berkontribusi baik untuk pengembangan layanan di sektor publik maupun pemerintahan.

03

CLOUD COMPUTING UNTUK SEKTOR PEMERINTAHAN

KEY FACTS

Pemerintah tidak dapat mengimbangi inovasi sektor swasta hanya dengan memperbarui infrastrukturnya setiap beberapa tahun. Bergerak menuju *cloud computing* menawarkan penghematan yang jelas bagi pemerintah. Penghematan biaya lainnya berasal dari:

- » Membayar hanya untuk sumber daya yang digunakan.
- » Mengambil keuntungan dari skala ekonomi: berada di lingkungan bersama yang dapat berbagi biaya pusat data, meningkatkan efisiensi operasional, dan mengurangi konsumsi daya secara keseluruhan.
- » Meningkatkan transparansi: lingkungan *cloud* memungkinkan pemantauan penggunaan yang tepat, sehingga memudahkan untuk mengoptimalkan sumber daya.
- » Daya saing teknologi: mengakses teknologi terbaru menawarkan lebih banyak kemampuan untuk investasi inti, memungkinkan pemerintah untuk berbuat lebih banyak dengan biaya lebih sedikit.

Sumber: ITAC. 2020. Governments Embracing Cloud "An Opportunity for Modernization, Innovation and Transformation".

Saat ini, masyarakat mengharapkan pemerintah untuk memberikan layanan, menyebarkan informasi, dan melibatkan mereka melalui sarana digital. Transformasi sektor publik cenderung memanfaatkan teknologi untuk secara mendasar mengubah cara pemerintah beroperasi dan memberikan layanan. Ketika sektor swasta bertransformasi lebih cepat, ekspektasi masyarakat terhadap tingkat layanan mereka mendorong lembaga publik untuk memberikan layanan yang lebih cepat, lebih berkualitas, dan lebih baik. Dalam beberapa tahun terakhir, banyak pemerintah telah memulai perjalanan transformasi digital, dengan melakukan digitalisasi banyak layanan yang digunakan masyarakat dan perusahaan, serta adopsi teknologi dasar seperti sistem identifikasi digital, sistem manajemen basis data nasional, dan *platform* pembayaran digital.

Isu dan Hambatan *Cloud Computing* di Sektor Pemerintahan Indonesia

Berdasarkan hasil *focus group discussion* yang dilakukan oleh Dewan TIK Nasional dengan *stakeholder* di bidang *cloud computing* [20] [21] [22], berikut beberapa isu yang menjadi tantangan dalam pemanfaatan *cloud computing* di sektor pemerintahan di Indonesia (lihat Gambar 7).

Gambar 7. Isu dan Hambatan *Cloud Computing* di Sektor Pemerintahan



Sumber: [20] [21] [22] - telah diolah kembali

- 1. Regulasi yang belum terarah.** Peraturan atau regulasi yang mengatur pemanfaatan dan tata kelola *cloud computing* di sektor pemerintahan masih belum didefinisikan secara jelas. Sebagai negara dengan pemerintahan yang terdesentralisasi dengan adanya otonomi daerah, pemerintah Indonesia bergantung pada adanya mandat dan/ atau ketentuan eksplisit dalam suatu peraturan sebagai landasan bagi setiap kebijakan/ program/proyek oleh instansi pemerintah mana pun. Tanpa landasan hukum yang tegas sebagai kepastian regulasi, instansi pusat atau daerah dapat ditemukan bersalah ketika mereka menyebarkan data dan beban kerja mereka di *cloud*, terutama ketika ada kebijakan yang mengatur pengadaan TI khususnya *cloud* yang dapat dianggap temuan dan bertentangan oleh regulator.
- 2. Ketimpangan kapabilitas industri cloud lokal dan global.** Pada isu yang spesifik terkait bisnis ini, industri *cloud* lokal belum mampu bersaing dengan perusahaan *cloud* global pada pengadaan *cloud* di sektor pemerintahan. Hal ini akibat dari masih minimnya kapabilitas infrastruktur, sistem, dan SDM TI untuk mendukung *cloud* pada industri *cloud* lokal. Ditambah dengan pengalaman perusahaan *cloud* lokal yang belum mumpuni ketimbang perusahaan global. Maka dari itu, tantangan yang diperlukan kedepannya adalah bagaimana pemerintah mampu mengatur lingkup pengadaan *cloud* agar industri *cloud* tetap tumbuh dan berkembang secara ekonomi sekaligus juga menjadi tempat terbaik bagi investasi CSP global.
- 3. Persepsi ketakutan hilangnya pekerjaan.** Bagi SDM bidang TI yang berada di K/L/D, migrasi dari sistem TI tradisional ke pemanfaatan *cloud computing* bisa mengancam hilangnya pekerjaan mereka. Padahal sebaliknya dengan diutamakannya *cloud computing*, mampu membuka pekerjaan dan kompetensi jenis baru dalam mendukung pemanfaatan *cloud*.
- 4. Pemahaman tentang cloud yang kurang.** Hal ini berhubungan dengan literasi yang diperoleh oleh SDM di sektor pemerintahan yang masih rendah terhadap *cloud computing*. Seperti contohnya masih merasa ketakutan akan hilangnya data bila menggunakan *cloud* walaupun keandalan dan keamanan *cloud* yang sudah teruji dan tersertifikasi digunakan di beberapa organisasi. Maka dari itu, literasi *cloud* masih rendah, sehingga belum dapat membedakan definisi pemanfaatan infrastruktur TI tradisional dengan *cloud computing* serta belum dapat melihat dampak positif yang bisa diperoleh jika menggunakan *cloud*.
- 5. Ketakutan akan dipersalahkan.** Isu ini masih berkaitan dengan belum matangnya kebijakan terkait pemanfaatan *cloud* untuk sektor pemerintahan yang ada. Pada instansi pemerintah khususnya di daerah masih takut untuk mengadopsi *cloud* walaupun telah mendapat dukungan dari pimpinan daerahnya. Ini akibat dari belum adanya payung peraturan terkait pemanfaatan *cloud* yang didefinisikan dan bisa diturunkan ke masing-masing pemerintah daerah.
- 6. Anggaran yang tidak sesuai.** Di beberapa instansi pemerintahan, anggaran untuk pengadaan *cloud* masih dimasukkan ke dalam biaya tetap. Padahal biaya dan harga dari penggunaan *cloud* cenderung dinamis sesuai pemakaian dan kondisi bisnis (Lihat Tabel 2). Dalam istilah bisnisnya yaitu bayar sesuai dengan yang dipakai atau *pay as you go*. Selain itu, ditemukan juga bahwa saat ini Lembaga sektor publik di Indonesia yang telah mengadopsi *cloud* akhirnya membayar lebih banyak anggaran TI mereka karena masih mempertahankan infrastruktur TI tradisional mereka. Maka dari itu, pengadaan terhadap penggunaan *cloud* perlu ditinjau kembali oleh sektor pemerintahan di Indonesia agar anggaran yang dikeluarkan bisa sesuai dan efektif.

Tabel 2. Perbandingan Teknologi sebagai *CapEx* dan *OpEx* [23]

Teknologi sebagai <i>CapEx</i>	Teknologi sebagai <i>OpEx</i>
Investasi besar di depan	Berlangganan regular dengan bermacam-macam tipe pembayaran
Melakukan estimasi kebutuhan kapasitas di masa mendatang	Bayar hanya untuk penggunaan kapasitas
Perangkat keras/lunak yang statis dengan <i>refresh cycle</i> membutuhkan sumber daya tenaga kerja	Kelincahan dan pembaruan yang rutin (biasanya otomatis), akses ke inovasi,
Berpotensial untuk proses yang panjang untuk mengestimasi anggaran dan menerima <i>approval</i>	Mengakselerasi proses penganggaran karena persyaratan pengeluaran jangka pendek yang lebih rendah
<i>Update</i> ketika dimungkinkan, membutuhkan investasi tambahan	Akses terkini pada <i>update</i> dan teknologi terbaru
Tim TI <i>in-house</i> bertanggung jawab pada manajemen operasional (termasuk <i>backup, update, repair</i>)	Otomatisasi tingkat tinggi dan penegakan kepatuhan keamanan

Sumber: [23] - telah diolah kembali

- Belum memiliki pengalaman pemanfaatan cloud.** Pada isu ini, masih berkaitan dengan kapabilitas SDM yang rendah di instansi pemerintahan untuk menyusun strategi pemanfaatan *cloud*, tata kelola *cloud*, hingga anggaran yang dibutuhkan untuk *cloud*.
- Kurangnya publikasi keberhasilan cloud di instansi pemerintahan.** Dalam isu terakhir ini, beberapa instansi pemerintah pusat maupun daerah di Indonesia sebenarnya telah berhasil mengadopsi *cloud* dengan baik walaupun belum memiliki kebijakan *cloud* yang mengikat. Akan tetapi, keberhasilan itu masih jarang untuk dipublikasikan karena instansi pemerintah masih memiliki ambiguitas terhadap regulasi yang berkaitan dengan *cloud* saat ini.

Cloud Computing Membantu Sektor Publik Pemerintahan

Secara global, beberapa Pemerintah telah mengadopsi teknologi *cloud computing*. Hal ini dilakukan terutama untuk mendapatkan keuntungan dari keunggulan *cloud computing*, terutama dalam hal peningkatan efisiensi, peningkatan *agility*, keandalan layanan, keamanan siber yang lebih kuat, dan peningkatan inovasi (lihat Gambar 8). Berikut beberapa penjelasannya.

Gambar 8. Bagaimana Cloud Computing Membantu Sektor Publik



Sumber: [13] - telah diolah kembali

- 1. Peningkatan efisiensi:** Pada intinya, *cloud computing* adalah tentang pengumpulan dan berbagi sumber daya di berbagai aplikasi dan entitas, yang mengarah pada peningkatan pemanfaatan aset. Peningkatan pemanfaatan ini berarti bahwa lebih banyak nilai yang diperoleh dari aset, mengoptimalkan kondisi saat ini dan mengurangi kebutuhan untuk perluasan kapasitas di masa mendatang sehingga dapat diterjemahkan menjadi efektivitas biaya. Hal ini juga sejalan dengan pemerintah yang akan lebih fokus pada pelayanan publik.
- 2. Kelincahan dan keandalan yang ditingkatkan:** Dengan memanfaatkan skalabilitas *cloud computing*, entitas biasanya dapat meningkatkan responsivitas layanan, terutama pada kasus permintaan yang berfluktuasi. Tidak seperti TI tradisional yang biasanya dibangun di atas kapasitas tetap terhadap permintaan yang diperkirakan, solusi *cloud* menawarkan fleksibilitas kepada pengguna untuk meningkatkan dan menurunkan skala penggunaan tergantung pada permintaan. Selain itu, dapat meningkatkan pengalaman pengguna secara keseluruhan dengan investasi tambahan minimal yang diperlukan sambil meminimalkan gangguan layanan dan pemadaman yang mungkin terjadi.
- 3. Keamanan siber yang lebih kuat:** Selain mencapai lingkungan yang lebih efisien, inovatif, dan gesit, *cloud computing* membantu meningkatkan keamanan siber secara keseluruhan. Melalui protokol keamanan siber terbaik di kelasnya dalam komunikasi jaringan, layanan *cloud* biasanya menawarkan keamanan siber tingkat tinggi yang sulit dicapai oleh sektor pemerintah itu sendiri. Faktanya, Penyedia layanan *cloud* terkemuka telah terbukti berinvestasi secara signifikan ke dalam aktivitas riset dan pengembangan terkait keamanan siber.
- 4. Peningkatan inovasi:** *Cloud computing* pada dasarnya merupakan pendorong inovasi untuk seluruh ekosistem digital. Inovasi ini mencakup ruang lingkup utama solusi cloud (infrastruktur, platform, perangkat lunak) dan merupakan pendorong untuk mengubah cara institusi pemerintah menyebarkan layanan digitalnya. Pada akhirnya pemerintah mampu meningkatkan kepercayaan dan kepuasan publik.

Secara keseluruhan, dampak *cloud computing* mampu melampaui sektor TI pemerintah, sehingga ini akan mempercepat transformasi digital di pemerintahan dengan mendorong adopsi teknologi terdepan seperti kecerdasan buatan, teknologi revolusi industri ke-4, dll. Hal ini tentu akan membantu meningkatkan kepuasan masyarakat melalui inovasi layanan yang diberikan oleh sektor pemerintah, karena layanan *cloud* akan membantu pemerintah beralih dari layanan TI tradisional yang membutuhkan lebih banyak dokumen dan waktu tunggu yang lebih lama, ke layanan digital yang lebih cepat dan otomatis.

Manfaat *Cloud Computing* untuk Sektor Pemerintahan

Pemerintah di masa mendatang perlu merespons perubahan dengan memperbarui layanan digital mereka, meningkatkan kemampuan analitik data mereka, dan menerapkan rencana pengembangan ekonomi digital. Banyak dari perubahan ini dimungkinkan oleh teknologi *cloud computing*, sehingga muncul beberapa manfaat yang dapat diperoleh dari adopsi *cloud computing* di sektor Pemerintahan (lihat Gambar 9).

Gambar 9. Manfaat *Cloud Computing* untuk Sektor Pemerintahan



Sumber: [24] - telah diolah kembali

Cloud computing mampu mengurangi biaya pembelian, pengaturan, dan menjalankan serta memelihara layanan teknologi. Pengadaannya yang unik membuat pengadaan *cloud* berbeda dengan pengadaan TI tradisional (lihat Tabel 3). *Cloud computing* menawarkan peluang kepada pemerintah untuk merampingkan operasi teknologi dan meningkatkan efisiensi, terutama yang berkaitan dalam waktu yang dibutuhkan untuk memproses layanan digital yang dihadapi masyarakat.

Cloud computing juga memungkinkan pemerintah untuk merespons dengan lincah persyaratan masyarakat, dan memungkinkan layanan publik yang jauh lebih cepat, jika diperlukan semisal dalam kasus di mana layanan digital mungkin menghadapi periode permintaan puncak, seperti mengajukan pengembalian pajak daring tepat sebelum tenggat waktu. Menggunakan *cloud computing* memungkinkan pemerintah untuk menangani lonjakan permintaan tanpa gangguan layanan, karena dukungan teknologi yang disediakan dapat ditingkatkan sesuai kebutuhan.

Demikian pula, *cloud computing* mampu meningkatkan ketahanan pemerintah dan menawarkan kelangsungan bisnis dan layanan pemulihan bencana di mana mungkin ada fasilitas pusat data yang mengalami pemadaman listrik yang disebabkan oleh bencana alam, atau jika peristiwa buruk lainnya. *Cloud computing* meningkatkan ketahanan pemerintah terhadap ancaman keamanan siber, karena dengan memindahkan layanannya ke *cloud* menawarkan kemampuan dan perlindungan keamanan siber dengan jaminan *availability* dan privasi yang lebih kuat.

Tabel 3. Perbandingan Pengadaan TI Tradisional dan Cloud

Faktor Pembeda	Pengadaan TI Tradisional	Pengadaan Cloud
Persyaratan	Persyaratan yang sangat preskriptif, mencari solusi <i>end-to-end</i>	Persyaratan berbasis kinerja, inovasi cepat
Biaya/harga	Kapasitas diketahui, harga tetap, dan kontrak jangka waktu tetap	Sesuai permintaan, berbasis konsumsi, dan <i>pay-as-you-go</i>
Syarat & Ketentuan Kontrak	Syarat dan ketentuan berfokus pada perangkat keras/lunak	Syarat dan ketentuan provider layanan <i>cloud</i> , standar SLA
Tata Kelola	Proses persetujuan yang berat dan kontrol tersentralisasi	<i>Self-service</i> , kontrol terdistribusi dengan tata kelola
Keamanan dan Audit	Jaminan keamanan dan audit	Tanggung jawab Bersama dan sertifikasi pihak ketiga

Sumber: [25] – telah diolah kembali

Cloud computing juga memungkinkan pemerintah untuk mencapai kemampuan teknologi dan analitis yang lebih baik. Dengan kata lain, organisasi mungkin kesulitan mengakses, semisal kecerdasan buatan dan *machine learning*, yang menawarkan kekuatan superkomputer untuk pemrosesan data skala besar dan kemampuan analitik.

Terakhir yaitu migrasi ke *cloud computing* membantu memfasilitasi jalur pengembangan sumber daya manusia di sektor publik dan juga membantu infrastruktur TI pemerintah yang tahan terhadap tantangan masa depan, karena migrasi ke *cloud* mengharuskan semua profesional teknologi untuk selalu mengikuti perkembangan peralatan dan perangkat lunak terbaru, bukan hanya fokus pada pemeliharaan platform teknologi yang menua.

Jalan untuk Migrasi Cloud di Sektor Pemerintahan

Setelah sebuah pemerintahan memutuskan untuk memulai migrasi data dari infrastruktur TI tradisional ke beberapa bentuk layanan *cloud*, ada berbagai jalur dan opsi yang dijelaskan pada bagian ini [5]. Berbagai pertimbangan mendorong seluruh pemerintah dan lembaga untuk mempertimbangkan untuk bermigrasi ke *cloud*. Pendekatan pemerintah secara keseluruhan berfokus pada investasi TI yang lebih besar dan mendasar dengan jangka waktu yang lama untuk pengembalian investasi, seperti membangun koneksi *throughput bandwidth* tinggi atau menyiapkan skema data induk umum di seluruh instansi pemerintah. Pemerintah yang memilih untuk bermigrasi ke layanan *cloud* memiliki 4 (empat) opsi dasar untuk dipilih (lihat Gambar 10).

Gambar 10. Opsi Jalan untuk Migrasi Cloud di Sektor Pemerintahan



Sumber: [5] – telah diolah kembali

1. Migrasi ke *private cloud* (dengan data yang disimpan secara *on-premise*)

Private cloud sering digunakan oleh instansi pemerintah, lembaga keuangan, dan organisasi menengah hingga besar lainnya dengan operasional bisnis penting yang mampu meningkatkan kontrol di lingkungan mereka. Untuk beberapa organisasi, *private cloud* mungkin satu-satunya pilihan realistis untuk memastikan kepatuhan terhadap peraturan. Banyak pelanggan *private cloud* menghosting data di pusat data mereka sendiri atau dengan layanan cloud pihak ketiga. Dalam kedua kasus tersebut, layanan dan infrastruktur disimpan di dalam jaringan pribadi, dan perangkat keras serta perangkat lunak tersedia untuk pelanggan itu sendiri. *Private cloud* mampu memaksimalkan investasi jangka panjang dengan mempertahankan semua yang ada di internal organisasi, namun dengan mengorbankan struktur modal dan biaya yang tinggi.

2. Migrasi ke pusat data *co-location* (dengan data disimpan secara eksternal)

Pada opsi kedua memungkinkan implementasi yang lebih cepat, karena dapat menghapus kebutuhan untuk membangun pusat data baru sambil memberikan beberapa manfaat dari *public cloud*, seperti mengurangi kebutuhan akan staf teknis internal. Pada dasarnya, ini adalah opsi untuk menempatkan peralatan server data bersama dengan menyewa pusat data *co-location*, yang juga dikenal sebagai pusat data pihak ketiga. Pada saat yang sama, opsi ini masih memiliki kelemahan seperti biaya tinggi dan kemampuan terbatas untuk mengatasi lonjakan permintaan.

3. Migrasi ke *hybrid cloud* (dengan data yang disimpan *on-premise* atau di *private cloud* bersama dengan data yang disimpan atau diproses oleh penyedia jasa *public cloud*)

Opsi ketiga yaitu menggabungkan solusi *public cloud* dan *private cloud*, sehingga memungkinkan data dan aplikasi mengalir di antara dua lokasi. Dalam *hybrid cloud* mengacu pada interkoneksi penyimpanan *on-premise* atau *private cloud* dengan *public cloud*. Banyak organisasi dan pemerintah memilih opsi *hybrid* untuk memungkinkan mereka mengatasi tantangan tertentu, seperti kepatuhan terhadap regulasi, kecepatan dan kualitas Internet yang rendah, atau keamanan yang lebih baik, sambil di saat bersamaan memberikan fleksibilitas yang lebih besar terhadap layanan digital.

4. Migrasi ke *public cloud* (dengan data yang disimpan secara eksternal)

Opsi keempat merupakan opsi *cloud computing* yang paling luas biasanya disediakan oleh perusahaan pihak ketiga, yang mungkin atau mungkin bukan penyedia *hyperscale cloud*. Untuk memperoleh manfaat penuh dari struktur biaya rendah dan peningkatan kapasitas yang cepat yang ditawarkan oleh *public cloud*, migrasi harus didahului dengan penilaian pada proyek percontohan atau pilot *project* sebelumnya. Dalam bermigrasi ke *public cloud*, pemerintah dapat menggunakan dua atau lebih layanan *cloud* dari dua atau lebih penyedia layanan *cloud*. Pemerintah dapat memilih opsi ini untuk menghindari penguncian vendor, memiliki lebih banyak layanan untuk dipilih, atau memastikan akses ke inovasi teknologi terbaru. Terdapat ringkasan keuntungan dan kelemahan dari keempat opsi migrasi cloud ini (lihat Tabel 4).

Tabel 4. Keuntungan dan Kelemahan dari 4 (empat) Opsi Migrasi Cloud

Opsi	Keuntungan	Kelemahan
Migrasi ke <i>private cloud</i>	<ul style="list-style-type: none"> Perangkat keras, penyimpanan data, dan koneksi dapat disesuaikan secara tepat untuk task yang diinginkan untuk memastikan keamanan dengan investasi yang besar. Kepatuhan terhadap regulasi mungkin sulit untuk data yang diklasifikasikan sebagai kategori sangat rahasia. 	<ul style="list-style-type: none"> Fleksibilitas untuk memenuhi permintaan yang fluktuatif terbatas. Kurangnya sistem cadangan yang ekstensif untuk menyediakan pemulihan bencana dapat menyebabkan kurangnya keandalan Kemampuan keamanan terbatas; solusi cloud pribadi akan berjuang untuk tetap setara dengan fitur keamanan berbasis cloud
Migrasi ke pusat data <i>co-location</i>	<ul style="list-style-type: none"> Private cloud eksternal sering kali menawarkan lebih banyak skalabilitas daripada infrastruktur lokal. Biaya pelatihan karyawan, operasi, dan pemeliharaan lebih rendah 	<ul style="list-style-type: none"> Visibilitas dan kontrol mungkin berkurang, karena kurangnya alat untuk memantau deployment secara efektif
Migrasi ke <i>hybrid cloud</i>	<ul style="list-style-type: none"> Organisasi dapat memelihara infrastruktur private untuk aset sensitif atau beban kerja yang memerlukan latensi rendah. Sumber daya tambahan di public cloud dapat diakses saat dibutuhkan. Transisi ke cloud tidak perlu berlebihan, karena migrasi dapat dilakukan secara bertahap, dengan beban kerja bertahap seiring waktu. 	<ul style="list-style-type: none"> Interoperabilitas dapat menjadi tantangan, karena sulit untuk mengelola beberapa sistem yang berbeda secara bersamaan. Infrastruktur tambahan meningkatkan kompleksitas. Biaya harus dikeluarkan untuk pelatihan karyawan, operasi, dan pemeliharaan.
Migrasi ke <i>public cloud</i>	<ul style="list-style-type: none"> Biaya modal adalah nol, karena tidak perlu membeli perangkat keras atau perangkat lunak. Solusi baru yang dapat segera diuji. Penyedia layanan menyediakan semua pemeliharaan. Skalabilitas hampir tidak terbatas serta sumber daya sesuai permintaan selalu tersedia untuk memenuhi kebutuhan yang cepat berubah. Keandalannya tinggi, karena jaringan server yang luas memastikan terhadap kegagalan. Fitur lanjutan, seperti keamanan yang mendukung kecerdasan buatan. 	<ul style="list-style-type: none"> Pengguna kehilangan kendali dan visibilitas sehubungan dengan bagaimana dan di mana data disimpan dan dikelola. Persyaratan kepatuhan perlindungan data dari setiap industri harus dipastikan. Di negara-negara dengan kompleksitas regulasi yang tinggi, persyaratan residensi data mungkin mengharuskan jenis data tertentu disimpan on-premise, sementara beban kerja lainnya dapat disimpan di public cloud. Keamanan bersama berarti bahwa ancaman terhadap keamanan juga dibagi. Pengguna mungkin terkunci ke vendor. Masalah ini dapat dikurangi melalui solusi multicloud. Namun, solusi multicloud akan

Sumber: [5] - telah diolah kembali

Cloud computing atau komputasi awan akan menjadi teknologi yang wajib diterapkan oleh Pemerintah Indonesia seiring dengan banyaknya digitalisasi layanan pemerintah. Maka dari itu, hambatan utama yang muncul adalah mengenai regulasi yang belum terarah, sehingga perlunya payung hukum yang jelas dalam pemanfaatan teknologi *cloud computing* di pemerintahan.

04

MENUJU CLOUD FIRST POLICY: PERJALANAN, ISU, DAN TANTANGAN

KEY FACTS

Pada bulan Maret 2017, Pemerintah Inggris Raya menerbitkan Strategi Digital 2017, termasuk tujuan yang akan membantu menciptakan lingkungan yang mendukung untuk *Cloud*:

- » Membangun infrastruktur dan konektivitas digital kelas dunia.
- » Meningkatkan keterampilan dan inklusi digital.
- » Menciptakan lingkungan terbaik untuk bisnis digital dan tingkatkan digitalisasi sektor lain.
- » Memperkuat keamanan siber.
- » Mempromosikan Pemerintah Digital.
- » Membuka kekuatan data dalam ekonomi dan digunakan untuk publik.

Sumber: UK Government. 2017. UK Digital Strategy. <https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy>

Cloud merupakan kebijakan yang dimaksudkan untuk mendefinisikan dan mendorong migrasi sektor publik dari solusi TI tradisional ke model berbasis *cloud*. Mengingat manfaat yang dapat diberikan *cloud computing*, *cloud first policy* ditargetkan untuk mengakselerasi adopsi *cloud* di pemerintahan. Untuk meningkatkan adopsi *cloud*, instansi pemerintahan wajib:

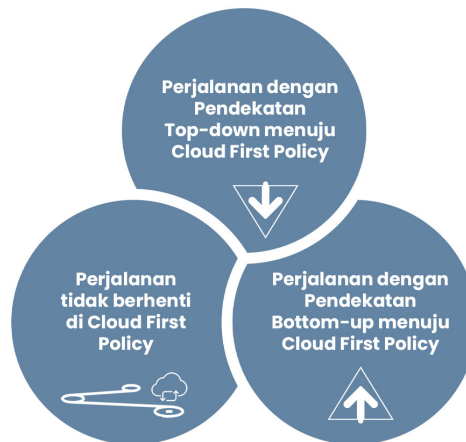
1. Menyertakan *cloud* sebagai bagian dari rencana strategis TIK dan anggaran,
2. Memanfaatkan *cloud* untuk semua proyek dan beban kerja TI, dan
3. Mempertimbangkan *cloud* yang utama (*cloud first*) ketika melakukan migrasi dan pengembangan aplikasi atau infrastruktur TI saat ini.

Sementara itu, *Cloud First Policy* ditujukan untuk mempercepat adopsi cloud dalam pemerintahan dan mengarahkan lembaga pemerintah untuk menggunakan layanan *public cloud* untuk modernisasi TI [21]. Melalui kebijakan *Cloud First* dapat menjadi pondasi yang penting, sehingga pemerintah dapat memastikan bahwa pemanfaatan *cloud computing* merupakan pertimbangan utama saat mempromosikan teknologi digital yang muncul melalui strategi nasional [24].

Perjalanan Menuju *Cloud First Policy* di Suatu Negara

Dari hasil *focus group discussion* yang diselenggarakan Dewan Teknologi Informasi dan Komunikasi (Wantiknas) dengan pihak eksternal stakeholder terkait [21], berikut beberapa perjalanan yang bisa dilakukan oleh suatu Negara untuk menghasilkan *Cloud First Policy* (lihat Gambar 11).

Gambar 11. Perjalanan Menuju *Cloud First Policy* di Suatu Negara



Sumber: [21] - telah diolah kembali

1. Perjalanan dengan Pendekatan *Top-down* menuju *Cloud First Policy*

Pemerintah biasanya akan memulai perjalanan setelah menyadari peran potensial dari adopsi *cloud* besar-besaran untuk mengatasi permasalahan nasional. Hal ini dapat mencakup misalnya, meningkatkan produktivitas negara melalui pertumbuhan ekonomi digital, atau meningkatkan keamanan nasional melalui infrastruktur digital yang lebih baik. Realisasi ini kemudian akan diformalkan dalam dokumen strategi atau dokumen lain yang serupa dengan imperatif nasional, misalnya, peta jalan yang menguraikan bahwa ekonomi digital mencakup transformasi tidak hanya bisnis, tetapi juga pemerintah dan menetapkan kebijakan untuk migrasi data/beban kerja pemerintah ke *cloud*.

2. Perjalanan dengan Pendekatan *Bottom-up* menuju *Cloud First Policy*

Di sisi lain, terdapat kasus di mana ada adopsi *cloud* yang tersebar di berbagai lembaga, yang perlu didukung oleh peraturan nasional untuk meningkatkan adopsi lebih lanjut oleh lembaga lain dan/atau untuk memfasilitasi di luar adopsi *ad-hoc*. Jika *Cloud First Policy* kemudian dikeluarkan tanpa strategi Nasional menyeluruh yang mengamanatkannya, Indonesia mungkin cocok dengan jenis perjalanan ini.

3. Perjalanan tidak berhenti di *Cloud First Policy*

Pendekatan *Cloud First* dapat dilihat sebagai langkah pertama dalam strategi jangka panjang untuk beralih ke pendekatan *Cloud-Native* yang sesungguhnya. *Cloud-Native* adalah kondisi akhir *cloud* yang optimal, di mana pelanggan pemerintah berinovasi menggunakan penawaran *public cloud* terbaru (seperti *microservices* dan *IoT*), dan menjalankan prinsip '*born in the cloud*' yang dioptimalkan sebagai kebalikan dari solusi '*lift and shift*'.

Tantangan dan Hambatan dalam Penyusunan *Cloud First Policy*

Seiring dengan transisi pemerintah menuju *Cloud First Policy*, kebijakan ini mampu mengidentifikasi beberapa potensi ketimpangan kebijakan dalam adopsi *cloud* di pemerintahan. Untuk mengoptimalkan perjalanan *cloud*, para pemimpin di pemerintahan perlu melakukan beberapa hal (lihat Gambar 12).

Gambar 12. Tantangan dan Hambatan dalam Penyusunan *Cloud First Policy*



Sumber: [21] - telah diolah kembali

Implementasi dan Manfaat *Cloud First Policy*

Kebijakan *cloud first* adalah kebijakan yang mencakup instansi Pemerintah dan bertujuan untuk mempercepat penyebaran layanan *cloud computing* instansi pemerintahan ini saat membuat keputusan investasi TI baru. Tujuan ini dicapai dengan mengamanatkan pemerintah untuk mempertimbangkan opsi *cloud* setiap kali keputusan investasi TI baru dibuat, sejalan dengan pedoman kebijakan, proses, dan tata kelola sebagaimana didefinisikan dalam *Cloud First Policy*. Tujuan dari kebijakan tersebut adalah untuk meningkatkan efisiensi, efektivitas serta meminimalkan total biaya kepemilikan aset instansi pemerintah, sekaligus meningkatkan keamanan informasi siber dengan mengadopsi model *cloud* yang tepat untuk setiap tujuan (d disesuaikan dengan undang-undang, kebijakan, dan peraturan klasifikasi data pemerintah serta peraturan terkait lainnya). Ini juga memungkinkan interoperabilitas dan karenanya meningkatkan komunikasi antara pemerintahan yang berpartisipasi.

Beberapa pemerintah dari negara-negara maju telah memilih *Cloud First Policy* dengan variasi tujuan yang berbeda seperti yang disebutkan di atas. Berdasarkan [13], alasan mengapa negara-negara ini menerapkan *Cloud First Policy* dapat diringkas diringkas sebagai berikut (lihat Gambar 13).

Gambar 13. Alasan Penerapan *Cloud First Policy* di Suatu Negara



Sumber: [13] - telah diolah kembali

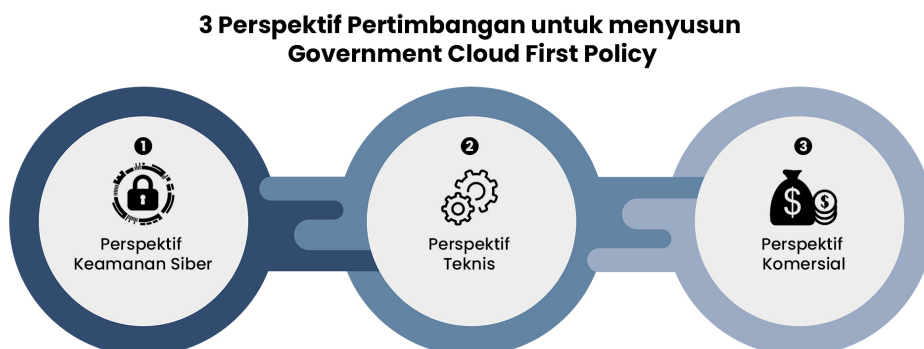
Sementara itu, berdasarkan hasil *focus group discussion* yang diselenggarakan Dewan Teknologi Informasi dan Komunikasi (Wantiknas) dengan *stakeholder* terkait [21] [22], berikut beberapa manfaat yang diperoleh suatu Negara dari adanya *Cloud First Policy*:

1. Kebijakan ini mampu mendorong pemilihan *cloud first* sebagai bagian dari infrastruktur TI agar kinerja layanan menjadi lebih baik di seluruh sektor pemerintahan.
2. Kebijakan ini membuat instansi pemerintah tidak perlu melakukan investasi besar di awal untuk perangkat keras dan menghabiskan banyak waktu untuk pekerjaan berat dalam mengelola perangkat keras tersebut. Dengan begitu, instansi pemerintah dapat menyediakan jenis dan ukuran sumber daya *computing* yang tepat yang mereka butuhkan untuk menggerakkan ide-ide inovatif mereka ataupun mengoperasikan departemen TI mereka.
3. Dari laporan *Centre for Strategic and International Studies* (CSIS) yang akan datang menyebutkan bahwa adopsi *cloud* oleh pemerintah akan menghasilkan ekonomi yang lebih efisien dan pertumbuhan Pendapatan Domestik Bruto (PDB) yang lebih tinggi hingga 0,37%.
4. Melalui kebijakan ini, pemerintah dapat lebih lanjut membuat kontrak dengan penyedia layanan *cloud* di level *whole of Government*, sehingga akan ada penghematan pada anggaran pemerintah mengingat penetapan harga *volume* besar *cloud* yang berbeda dan bisa lebih murah.

Pertimbangan untuk Menyusun *Government Cloud First Policy*

Potensi investasi pemerintah dalam *cloud computing* untuk sektor publik harus dievaluasi berdasarkan setiap kasusnya [13]. Setiap kasus harus dinilai dari perspektif keamanan siber untuk memastikannya memenuhi persyaratan keamanan siber nasional, perspektif teknis untuk memastikan kelayakan teknis dan operasionalnya serta perspektif komersial untuk memastikannya mewakili solusi paling hemat biaya yang tersedia. Berikut uraian dari 3 (tiga) perspektif tersebut (lihat Gambar 14).

Gambar 14. Perspektif Pertimbangan Penyusunan *Government Cloud First Policy*



Sumber: [13] - telah diolah kembali

1. Perspektif Keamanan Siber

Pada saat mempertimbangkan migrasi ke layanan *cloud*, keamanan siber adalah aspek kunci untuk evaluasi dan diatur oleh peraturan dan undang-undang yang dikeluarkan oleh instansi pemerintah terkait. Oleh karena itu, kebijakan tersebut perlu memperhitungkan keamanan dan perlindungan data serta membangun otoritas pengambilan keputusan untuk kebijakan tersebut. Semua peraturan keamanan siber yang dikeluarkan oleh Lembaga Keamanan Siber Nasional harus ditinjau saat merancang atau mengimplementasikan solusi *cloud* apa pun untuk memastikan kepatuhannya terhadap kontrol dan persyaratan keamanan.

2. Perspektif Teknis

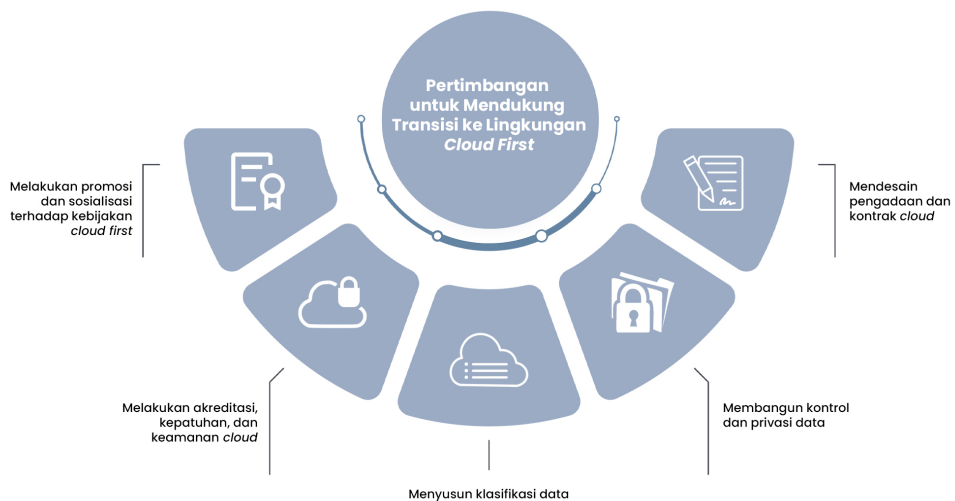
Aspek berikutnya yang harus dipertimbangkan saat bermigrasi ke *cloud* adalah kelayakan teknisnya. Misalnya, solusi yang sangat sensitif terhadap latensi mungkin lebih baik dihosting secara lokal *on-premise*, terutama jika solusi layanan *cloud* tidak menghadirkan fitur teknis yang sama.

3. Perspektif Komersial

Cloud computing memiliki potensi yang signifikan dalam hal manfaat ekonomi bagi organisasi yang bermigrasi. Namun, aspek ekonomi perlu dinilai berdasarkan kasus yang ada. Misalnya, aplikasi yang dikustomisasi dan spesifik untuk pengguna akhir terkadang lebih mahal untuk dimigrasikan ke *cloud* dibandingkan dengan aplikasi yang sedari awal sudah disesuaikan ke *cloud*.

Singkatnya, setiap kasus harus dikelola secara terpisah dan harus dievaluasi secara ketat berdasarkan 3 (tiga) dimensi yang telah diuraikan. Selain itu, dari pengalaman beberapa negara yang telah mengadopsi *cloud first policy* untuk melakukan modernisasi infrastruktur TI mereka, [25] telah mengidentifikasi beberapa pertimbangan untuk mendukung transisi ke lingkungan *cloud first* (lihat Gambar 15).

Gambar 15. Pertimbangan untuk Mendukung Transisi ke Lingkungan *Cloud First*



Sumber: [25] - telah diolah kembali

05

GOVERNMENT CLOUD FIRST POLICY DI BERBAGAI NEGARA

KEY FACTS

Dengan realisasi manfaat yang ditawarkan oleh layanan *cloud*, baik pemerintah maupun perusahaan sedang mempertimbangkan strategi *Cloud-First* sebagai alternatif. Kebijakan *Cloud-First* dapat dirumuskan untuk mendorong efisiensi operasional, menghemat anggaran TI, memperoleh manfaat dari skalabilitas, dan memastikan pencadangan dan pemulihan data. Di saat yang bersamaan, adopsi layanan *cloud* membawa keamanan siber dan persyaratan kepatuhan privasi data, yang harus ditangani untuk implementasi kebijakan *Cloud-First* yang efisien.

Sumber: KSA Government. 2020. On Overview on the Global Governmental Efforts on Fostering the Use of Cloud Computing. Communications & Information Technology Commission.

Pada bab ini membahas terkait perbandingan penerapan *Government Cloud First Policy* di beberapa negara dalam rangka mendukung pemanfaatan *Cloud Computing* di Institusi Pemerintahnya. Tujuan dari dilakukannya benchmarking ini yaitu untuk membandingkan kebijakan terkait *cloud computing* yang ada di beberapa negara, sehingga dapat diperoleh pengetahuan dan referensi untuk menyusun suatu *Government Cloud First Policy* di Indonesia. Dengan adanya benchmarking dalam kajian ini, diharapkan mampu memperoleh insight terkait hal-hal apa saja yang perlu masuk di dalam *Government Cloud First Policy* apabila

kebijakan ini disusun oleh Pemerintah Indonesia dan tentunya dengan tetap memperhatikan konteks lokal dalam Negeri. Beberapa Negara yang dipilih untuk dijadikan benchmarking dalam kajian ini, antara lain Filipina, Pakistan, Arab Saudi, Inggris Raya, Singapura, dan Nigeria. Berikut dijelaskan rangkuman hasil benchmarking *Government Cloud First Policy* di berbagai negara.

Filipina

Pemerintah Filipina telah mengeluarkan kebijakan *Cloud First* di tahun 2017 melalui *Department of Information and Communications Technology* (DICT). Kemudian tiga tahun berselang, kebijakan ini dilakukan amandemen *Department Circular No.10* tahun 2020 tentang *Government Cloud First Policy*. Dalam pembuatannya, pemerintah Filipina mengadopsi *Cloud First Playbook* yang dikeluarkan oleh [25] dengan modifikasi yang disesuaikan dengan kondisi lingkungan pemerintahannya. Berikut beberapa aspek yang diatur dalam *Cloud First Policy* dari Filipina.

a. Peran dari DICT GovCloud

DICT berperan untuk terus mendukung upaya lembaga untuk mengadopsi solusi *cloud* sesuai dengan kebutuhan mereka. Untuk memperluas dan memenuhi persyaratan layanan *cloud* di sektor publik, DICT akan mengembangkan daftar penyedia layanan *cloud* terakreditasi. Bersama dengan sumber daya lokal dari DICT dengan rangkaian penyedia layanan *cloud* terakreditasi akan disebut sebagai versi baru dari GovCloud.

b. Manfaat dalam Menjaga Pra-Akreditasi Vendor GovCloud

Di dalam kebijakannya, DICT mengatur mengenai pra-akreditasi terhadap vendor dari GovCloud yang memiliki manfaat antara lain:

- 1. Menghemat waktu.** Dengan memanfaatkan daftar pra-akreditasi, Instansi Pemerintah Filipina dapat merampingkan proses tender *cloud computing* yang hanya melibatkan penyedia yang telah masuk pra-akreditasi, dibandingkan dengan meminta lembaga melakukan penilaian individu terhadap penyedia layanan *cloud* untuk setiap tender atau mengembangkan pusat data mereka sendiri atau fasilitas *cloud on-premise*.
- 2. Memastikan kualitas.** Daftar vendor *cloud* yang telah diakreditasi sebelumnya akan diperiksa sebelumnya untuk memastikan layanan mereka memenuhi kontrol keamanan wajib untuk penggunaan *cloud* pemerintah.
- 3. Memastikan kepatuhan.** Pengoperasian GovCloud baru diatur oleh hukum Republik Filipina. Semua kontrak, perjanjian, dan perjanjian tingkat layanan yang berkaitan dengan hal yang sama terikat oleh hukum Filipina dan setiap klaim atau masalah yang diajukan akan diselesaikan di pengadilan Filipina atau badan peradilan Filipina.

c. Klasifikasi Data

Mengklasifikasikan data ke dalam kategori terpisah memungkinkan Pemerintah Filipina untuk melindungi informasi pemerintah dengan lebih baik dan membuat keputusan berdasarkan informasi yang lebih baik terkait dengan akses, penyimpanan, dan transmisi data Pemerintah. Pada bagian klasifikasi data, secara garis besar dibagi menjadi tiga tingkatan yaitu:

1. **Tier 1: Data Tidak Sensitif atau Tidak Terklasifikasi** dapat disimpan di *public cloud* terakreditasi atau GovCloud;
2. **Tier 2: Data yang Dibatasi atau Sensitif** dapat disimpan di *public cloud* terakreditasi atau GovCloud, dengan persyaratan enkripsi; dan
3. **Tier 3: Data Rahasia atau di atas Data Sensitif** mungkin memerlukan penerapan *private cloud (on-premise)* dengan persyaratan enkripsi khusus.

Instansi pemerintah direkomendasikan untuk memilih model *cloud deployment* yang sesuai dengan kebutuhan spesifik lembaga dan jenis data yang ditanganinya menurut Klasifikasi Data Sektor Publik. Berdasarkan pada klasifikasi data tiap instansi, akan ada persyaratan untuk menerapkan kontrol tertentu. Instansi mungkin menemukan bahwa kontrol ini ditangani oleh penyedia *public cloud* atau bahwa mereka hanya dapat dilayani oleh *private cloud* yang dikirimkan *on-premise*.

d. Keamanan Cloud

Manfaat memigrasikan beban kerja dan data pemerintah ke GovCloud atau ke *public* adalah kemampuan untuk meningkatkan keamanan data secara keseluruhan. Penyedia layanan *cloud* terakreditasi di GovCloud akan memenuhi standar keamanan internasional, akan disertifikasi dengan tepat dan akan mematuhi semua hukum dan standar industri Filipina yang relevan. Dalam menentukan pendekatan manajemen risiko instansi secara keseluruhan, lembaga dapat merujuk ke Rencana Keamanan Siber Nasional 2022 untuk panduan. Kontrol keamanan yang ditetapkan dapat mencakup salah satu atau beberapa hal berikut:

1. Keamanan Personil
2. Keamanan fisik dan lingkungan
3. Manajemen kelangsungan bisnis dan respons insiden
4. Manajemen inventaris dan konfigurasi
5. Enkripsi data
6. Kontrol akses, pemantauan, dan pencatatan
7. Keamanan dan pemantauan jaringan
8. Keamanan dan integritas sistem

e. Kerangka Kerja Keamanan

Mengelola keamanan layanan *cloud* yang dikontrak adalah tanggung jawab yang dibagi antara unit kontrak dan penyedia layanan *cloud*. Unit kontrak yang bertanggung jawab untuk memilih dan menerapkan kontrol keamanan untuk setiap beban kerja yang beroperasi di *cloud*, sedangkan penyedia layanan *cloud* bertanggung jawab untuk memastikan bahwa layanan yang digunakan oleh unit kontrak sangat aman dan tangguh sehingga tersedia untuk digunakan sesuai permintaan. Keamanan data GovCloud dan *public cloud* bergantung pada:

1. Memenuhi persyaratan keamanan untuk setiap tingkat klasifikasi data; dan
2. Mempekerjakan alat dan prosedur standar untuk audit

Selain itu, penyedia layanan *cloud* Pemerintah harus menyediakan audit keamanan pada akses data, termasuk log dan jejak audit untuk memastikan persyaratan keamanan dan privasi yang ditentukan terpenuhi. Instansi pemerintah harus mengandalkan audit *logical* dan pemantauan keamanan berkelanjutan untuk memastikan layanan *cloud*

memenuhi kerahasiaan dan integritas data yang telah disepakati, tidak ada pelanggaran data, dan data serta beban kerja terus tersedia.

f. Kedaulatan Data

Manfaat *cloud* paling baik diwujudkan ketika tidak ada batasan residensi data yang ditempatkan pada data. Pembatasan residensi data melemahkan skala ekonomi serta manfaat keamanan yang dapat diperoleh dari infrastruktur *cloud* bersama. Namun demikian, di mana lembaga memiliki kekhawatiran dengan akses ekstrateritorial ke data atau di mana Data Rahasia *Tier 3*, maka standar dan kontrol keamanan yang sesuai harus digunakan atau lembaga harus bekerja sama dengan DICT untuk mempertimbangkan *private deployment*, solusi *cloud on-premise*.

g. Kebijakan Migrasi

Memigrasikan data dan beban kerja ke *cloud* meningkatkan ketersediaan dan fungsionalitas layanan serta meningkatkan interoperabilitas dengan rentang data dan beban kerja pemerintah lainnya yang lebih luas. Migrasi ke *cloud* juga memungkinkan otomatisasi proses tertentu yang lebih besar, meningkatkan ketersediaan dan kelincahan sumber daya komputasi untuk proses yang memiliki tuntutan pemrosesan variabel. Pada kebijakan *Cloud First* yang dikeluarkan oleh Pemerintah Filipina, terdapat proses migrasi *cloud* (lihat Gambar 16).

Gambar 16. Migrasi *Cloud* pada Kebijakan *Cloud First* Filipina [14]



Berdasarkan Gambar 16, proses migrasi dilakukan dalam 3 tahapan yaitu:

- 1. Take Stock.** Pada tahapan ini dilakukan identifikasi bagaimana sumber daya TI diselaraskan dengan tujuan organisasi dan bagaimana biaya dioptimalkan. Selain itu dilakukan juga penentuan klasifikasi data hingga pertimbangan pemetaan keamanan.
- 2. Plan.** Pada tahap ini dilakukan penetapan tanggung jawab dalam pengelolaan *cloud*, identifikasi kesenjangan kompetensi *cloud*, menentukan pembagian dan izin data, pemilihan *cloud* yang sesuai, dan membuat *roadmap* migrasi *cloud*.
- 3. Migrate and Manage.** Pada tahapan ini perlu melacak, mendokumentasikan, dan menganalisis secara berulang terhadap proses migrasi yang dilakukan. Selain itu, memantau kinerja dan penggunaan layanan terhadap tujuan dan membandingkan biaya dengan rencana migrasi yang telah dibuat.

h. Data Ownership, Retrieval, dan Interoperability

Pada bagian ini, terdapat 5 (lima) aspek yang diatur yaitu:

- 1. Data Ownership.** Institusi pemerintah di Filipina akan mempertahankan kontrol dan kepemilikan penuh atas data mereka, dengan identitas penyedia layanan *cloud* dan kontrol akses yang tersedia untuk membatasi akses ke infrastruktur

dan data. Penyedia layanan *cloud* harus memberi pelanggan pilihan tentang bagaimana mereka menyimpan, mengelola, dan melindungi data mereka, dan tidak memerlukan kontrak atau eksklusivitas jangka panjang.

2. **Ownership.** Kontrak layanan dan *Service Level Agreement* (SLA) lain yang terkait dengan penyediaan layanan *cloud* untuk instansi Pemerintah harus dengan jelas menyatakan bahwa setiap data yang dimigrasikan ke *cloud* tetap menjadi milik entitas Pemerintah yang mengadakan kontrak, terlepas dari siapa yang memiliki, mengelola, atau mengoperasikan *cloud*.
3. **Access.** Akses, *retrieval*, modifikasi, dan penghapusan data tetap menjadi hak instansi Pemerintah yang mengadakan kontrak dan akan tercermin dalam kontrak layanan yang relevan.
4. **Interoperability.** Komponen sistem *cloud* dapat berasal dari sumber yang berbeda termasuk implementasi *public* dan *private cloud*. Komponen-komponen ini harus diganti dengan komponen baru atau berbeda dari penyedia yang berbeda dan terus bekerja, untuk memfasilitasi pertukaran data antar sistem.
5. **Open Data.** Entitas pemerintah harus mendukung prinsip data terbuka dan jika memungkinkan secara teknis dan ekonomis, menyediakan data yang tidak dibatasi untuk Instansi Pemerintah lainnya dan publik melalui *cloud*. Sesuai dengan prinsip dan kebijakan ini, instansi Pemerintah juga harus mengelola aset data mereka untuk mempromosikan keterbukaan dan penggunaan untuk kepentingan publik.

i. Proses Akreditasi untuk Provider Layanan Cloud

Proses akreditasi untuk penyedia layanan *cloud* yang akan terdaftar di GovCloud Filipina akan diatur oleh DICT, termasuk persyaratan jaminan keamanan dasar yang diperlukan sebelum terdaftar di GovCloud. Hal Ini untuk memastikan tingkat keandalan layanan dasar dari penyedia layanan *cloud* GovCloud dan untuk memastikan bahwa mereka memiliki platform yang aman dan terkontrol dengan menyediakan serangkaian fitur keamanan yang diperlukan yang dapat digunakan oleh instansi pemerintah. Instansi harus memastikan bahwa mereka hanya mempertimbangkan vendor yang memiliki akreditasi GovCloud atau vendor yang dapat memenuhi proses akreditasi sebagaimana ditentukan oleh mereka. Untuk memberikan tingkat jaminan yang lebih tinggi kepada lembaga yang ingin menerapkan di GovCloud, DICT menyediakan daftar sertifikasi dasar yang diperlukan untuk diakreditasi di GovCloud (lihat Tabel 5).

Tabel 5. Persyaratan Keamanan *Cloud* di Filipina

Persyaratan	Sertifikasi Dasar dan/atau Kebutuhan Protokol	Deskripsi
Persyaratan jaminan keamanan	<ul style="list-style-type: none"> • ISO/IEC 27001 - Information Security Management • Payment Card Industry (PCI) Data Security Standard (DSS) • Optional: Service Organization Control (SOC) 1 and 2 • Optional: ISO/IEC 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors 	<p>Ini adalah Persyaratan Jaminan Keamanan dasar dan opsional untuk Penyedia Layanan Cloud yang akan diakreditasi di GovCloud.</p> <p>Persyaratan Jaminan Keamanan ini memastikan bahwa Penyedia Layanan Cloud memiliki sertifikasi keamanan yang diperlukan untuk menampung beban kerja pemerintah.</p>

Sumber: [14] - telah diolah kembali

Pakistan

Pemerintah Pakistan mengeluarkan *Cloud First Policy* di tahun 2022 melalui *Ministry of Information Technology & Telecommunication* [26]. Berikut beberapa aspek yang diatur dalam *Cloud First Policy* dari Pakistan.

a. Gambaran Umum

Kebijakan ini membayangkan transformasi digital Pakistan dengan mengoptimalkan pengeluaran TIK, pemanfaatan teknologi berbasis *cloud* terbaru secara efisien, penyampaian layanan warga yang cepat, tata kelola yang lebih baik, peningkatan kolaborasi di antara organ-organ pemerintah, dan peningkatan transparansi & akuntabilitas.

PCFP berlaku untuk semua PSE di bawah pemerintah federal yang bermaksud melakukan investasi TIK baru. PCFP juga akan menjadi panduan yang berguna bagi sektor-sektor yang diatur dan organisasi sektor swasta saat mereka terus melakukan transformasi digital. PCFP dikeluarkan untuk mendukung transformasi digital lanskap TIK di Pakistan, meningkatkan efisiensi, menyediakan layanan berkualitas, dan mendorong investasi di bidang TIK

b. Kondisi *Cloud Computing* Saat Ini

Infrastruktur terdistribusi yang tersedia dalam lingkup kecil sulit untuk dikelola. Memperkirakan dan merencanakan ekspansi masa depan dalam infrastruktur yang terfragmentasi adalah pekerjaan yang menantang. Terdapat kebutuhan mendesak untuk memiliki infrastruktur terkonsolidasi untuk Lembaga Sektor Publik di Pakistan. Saat ini, pemanfaatan layanan *cloud* di sektor publik masih rendah dan sebagian besar pusat data hanya melayani kebutuhan satu organisasi saja. *Cloud* menawarkan keamanan dan optimalisasi sumber daya yang lebih baik, baik dalam hal personel atau komputasi, penyimpanan, atau pemanfaatan jaringan, yang tidak dapat dicapai dalam infrastruktur TIK yang terfragmentasi.

Dengan penerapan solusi *cloud*, peran pusat data tertentu diganti dengan domain kompetensi untuk otomatisasi proses, pengoptimalan sumber daya, arsitektur, dan manajemen biaya. Salah satu tujuan dari kebijakan ini adalah pengembangan SDM terampil yang mendukung *cloud* untuk mendorong adopsi dan implementasi *cloud* di seluruh Pakistan. Lembaga Sektor Publik akan difasilitasi untuk meningkatkan kompetensi SDM TI mereka yang ada dan mengubah mereka menjadi SDM yang mendukung *cloud*. Inisiatif khusus untuk pelatihan dan peningkatan kompetensi SDM akan diprioritaskan untuk percepatan adopsi *cloud*.

c. Model *Deployment Cloud* yang Diterapkan

Berikut beberapa model *deployment cloud* yang diatur pada kebijakan *cloud first* di Pakistan antara lain:

1. *Public Cloud*

Infrastruktur *cloud* disediakan untuk penggunaan terbuka oleh masyarakat umum. Kemudian, model *cloud* ini mungkin dimiliki, dikelola, dan dioperasikan oleh bisnis, akademik, atau Lembaga Sektor Publik, atau kombinasi dari semuanya. Dapat ditemukan dimana saja serta sumber daya infrastruktur *cloud* yang dapat digunakan bersama oleh sejumlah organisasi.

2. **Government Cloud**

Infrastruktur *cloud* disediakan untuk digunakan oleh Lembaga Sektor Publik saja. Ini mungkin dimiliki, dikelola, dan dioperasikan oleh bisnis, akademik, atau Lembaga Sektor Publik, atau kombinasi dari semuanya. Model ini hanya bisa berlokasi di Pakistan serta sumber daya infrastruktur *cloud* hanya dapat digunakan bersama oleh Lembaga Sektor Publik.

3. **Private Cloud**

Infrastruktur *cloud* disediakan untuk penggunaan eksklusif oleh satu organisasi/ Lembaga Sektor Publik. Dikelola dan dioperasikan oleh organisasi, pihak ketiga, atau kombinasi dari mereka. Itu hanya dapat berlokasi di Pakistan baik *on-premise* atau *off-premise* organisasi yang memilikinya.

4. **Hybrid Cloud**

Hybrid *cloud* adalah solusi yang menggabungkan satu atau lebih model *deployment cloud*. Memungkinkan data dan aplikasi untuk dibagikan di antara model. Sebuah organisasi dapat menyimpan data sensitifnya di satu jenis *cloud* sedangkan data publik di model yang lain, sehingga menjaga kebutuhan keamanannya serta memanfaatkan sumber daya komputasi yang kuat dari *public cloud*.

d. **Cakupan Hasil Kebijakan**

Pada bagian ini dijelaskan mengenai beberapa cakupan lainnya yang diatur dalam *cloud first policy* di Pakistan.

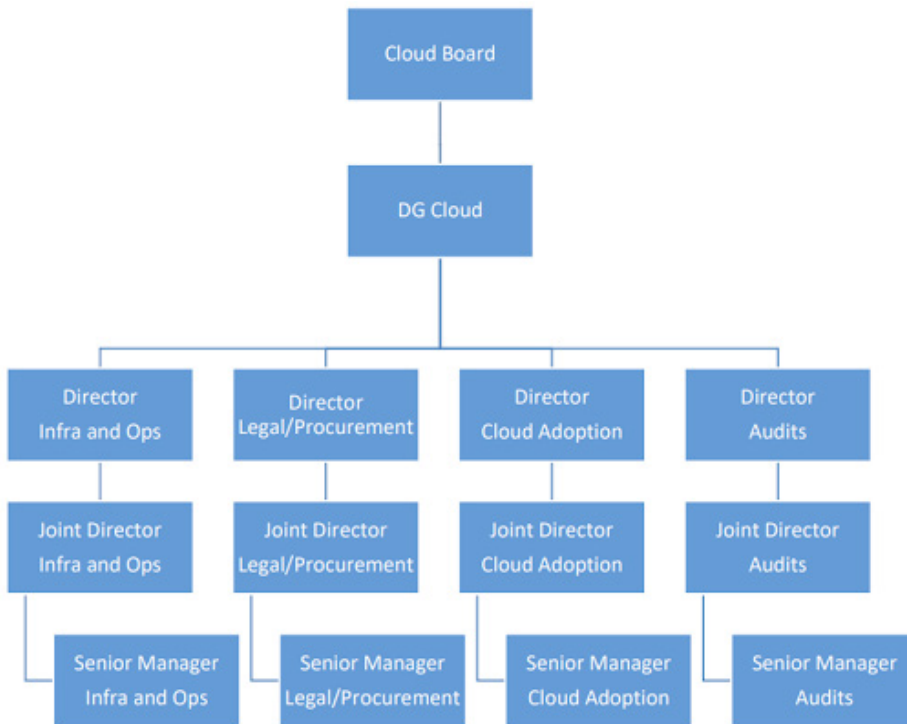
1. **Kedaulatan Data dan Alur Data**

Kebijakan ini mengakui kemampuan dan skala ekonomi yang diperoleh saat tidak ada persyaratan residensi data. Penyedia layanan *cloud* adalah penyedia skala besar dan memiliki pusat data di seluruh dunia. Klien biasanya memiliki opsi untuk membatasi data mereka ke wilayah geografis tertentu. Tanpa persyaratan residensi data, data milik Pemerintah Pakistan dapat disimpan di luar perbatasan Pakistan dan ada kemungkinan Pemerintah Pakistan kehilangan akses ke datanya atau data tersebut tunduk pada hukum negara lain. Namun, setiap kali ada kasus penggunaan yang sah yang memerlukan aliran data lintas batas, maka pemangku kepentingan yang relevan dapat berkonsultasi dengan *Cloud Office* untuk memastikan standar keamanan dan kontrol yang sesuai diterapkan untuk aliran data tersebut.

2. **Struktur Organisasi Kantor Cloud**

Struktur tata kelola yang diamanatkan dan ditentukan memastikan kelancaran implementasi dan operasi layanan *cloud* yang optimal melalui unit khusus. Untuk percepatan implementasi kebijakan ini, *Ministry of Information Technology and Telecommunications* (MoITT) Pakistan akan mendirikan kantor khusus untuk memfasilitasi dan mengawasi hal-hal yang terkait dengan adopsi *cloud* (lihat Gambar 17). Kantor ini akan bertindak sebagai pemimpin untuk adopsi *cloud* di Pakistan dan akan menentukan kriteria untuk akreditasi/registrasi layanan penyedia *cloud* sesuai dengan standar domestik dan internasional dan mendukung provinsi dalam upaya adopsi *cloud* mereka untuk membawa keseragaman dalam adopsi *cloud* di seluruh Pakistan.

Gambar 17. Usulan Struktur Organisasi *Cloud Office* Pakistan [26]



Seperti yang ditunjukkan pada Gambar 17, Dewan *Cloud* akan dipimpin oleh Sekretaris MoITT Pemerintah Pakistan, sementara Kepala Sekretaris dari semua provinsi atau perwakilan mereka dan dua pakar industri akan menjadi anggota dewan. Sekretaris utama atau perwakilan mereka akan menjadi bagian dari *Cloud Board* sebagai anggota setelah pemerintah provinsi masing-masing mengadopsi kebijakan *cloud first* sejalan dengan kebijakan ini.

3. Akreditasi Provider Layanan *Cloud* untuk Data Pemerintah

Penyedia layanan *cloud* akan memenuhi standar domestik dan internasional yang ditetapkan untuk akreditasi penyedia layanan *cloud* untuk memenuhi persyaratan akreditasi Kantor *Cloud*. Kantor *Cloud* akan merumuskan kriteria akreditasi dan tolok ukur untuk semua penyedia layanan *cloud* yang memilih untuk memberikan layanan kepada Lembaga Sektor Publik. Kriteria akan didasarkan pada tolok ukur internasional seperti keamanan, keandalan, biaya, interoperabilitas, ketersediaan, dan parameter lain yang ditetapkan. Proses agar penyedia layanan *cloud* dicantumkan dalam daftar terakreditasi akan diatur oleh Kantor *Cloud*. Kantor *Cloud* akan mempertahankan daftar terakreditasi penyedia layanan *cloud* untuk Lembaga Sektor Publik. Hal ini akan mempermudah pengadaan layanan *cloud* untuk Lembaga Sektor Publik. Mereka diwajibkan untuk menyediakan layanan dari daftar penyedia layanan *cloud* yang terakreditasi saja. Kantor *Cloud* akan memiliki wewenang untuk mencabut akreditasi penyedia layanan *cloud* jika terjadi ketidakpatuhan.

4. Audit ICT

Audit adalah sarana untuk memastikan bahwa penyedia layanan cloud memberikan tingkat perlindungan yang memadai untuk perlakuan aset informasi sesuai dengan standar yang ditetapkan oleh *Cloud Office*. Kebijakan ini mengamankan bahwa penyedia layanan *cloud* memberikan laporan audit yang memuaskan atau menanggapi permintaan audit yang dibuat oleh *Cloud Office*. Otoritas terkait dan pihak ketiga bersertifikat lainnya akan dapat memantau dan melakukan audit untuk memvalidasi kontrol yang disepakati secara kontrak. Selain itu, penyedia layanan *cloud* juga harus menggunakan mekanisme audit internal untuk memastikan bahwa persyaratan yang ditentukan dipatuhi. Audit dapat dilakukan secara berkala atau sesuai kebutuhan. *Cloud Office* dapat menunjuk badan audit mana pun untuk melaksanakan audit berdasarkan kriteria yang ditetapkan oleh *Cloud Office*.

5. Klasifikasi Data

Klasifikasi data adalah proses pengorganisasian data ke dalam kategori-kategori sehingga data tersebut dapat dimanfaatkan sesuai dengan sensitifitas dan kekritisannya. Lembaga Sektor Publik akan memiliki berbagai jenis informasi dan informasi tersebut akan dikaitkan dengan berbagai tingkat sensitivitas. Kerangka klasifikasi data menyediakan *tools* untuk mengklasifikasikan dan mengkategorikan data berdasarkan sensitivitas masing-masing dan karenanya memungkinkan Lembaga Sektor Publik untuk menentukan kontrol terhadap setiap kategori klasifikasi (lihat Tabel 6).

Tabel 6. Matriks Klasifikasi Data dengan Pemilihan *Cloud* di Pakistan

Klasifikasi Data Sektor Publik	Tipe <i>Cloud</i>	Keamanan
Data Terbuka	<i>Public Cloud</i> dengan Penyedia Layanan <i>Cloud</i> yang teregistrasi	<i>Baseline</i>
Publik	<i>Public Cloud</i> dengan Penyedia Layanan <i>Cloud</i> yang teregistrasi	<i>Baseline</i>
<i>Restricted</i>	<i>Government Cloud</i> dengan Penyedia Layanan <i>Cloud</i> yang teregistrasi	<i>Intermediate</i>
<i>Sensitif/Confidential</i>	<i>Government Cloud</i> dengan Penyedia Layanan <i>Cloud</i> yang teregistrasi	<i>Enhanced</i>
<i>Secret</i>	<i>Private (Cloud</i> digunakan dalam satu organisasi) atau <i>Government Cloud</i> dengan Penyedia Layanan <i>Cloud</i> yang teregistrasi	<i>Highest</i>

Sumber: [26] - telah diolah kembali

6. Kerangka Kerja Keamanan

Keamanan Informasi adalah serangkaian praktik untuk menjaga keamanan data dari akses, perubahan, pengungkapan, gangguan, atau penghancuran yang tidak sah, baik data diam, bergerak, atau dalam pemrosesan. Hal ini dimaksudkan untuk menjamin kerahasiaan, integritas, dan keamanan data.

Klasifikasi data sering dirancang bersama dengan persyaratan keamanan informasi yang sesuai untuk mengelola setiap tingkat informasi. Model *cloud* yang menampung data rahasia harus memenuhi persyaratan keamanan untuk model tersebut. Kebijakan ini mengamankan Kantor Cloud untuk menentukan garis dasar keamanan, berdasarkan standar domestik dan internasional, untuk model *cloud* berbeda yang ditetapkan untuk menghosting kelas data yang berbeda untuk Lembaga Sektor Publik. Penyedia layanan *cloud* dan Lembaga Sektor Publik harus menjaga integritas sepenuhnya untuk melindungi data dan memenuhi persyaratan keamanan yang ditetapkan oleh Kantor *Cloud* Pakistan dan/atau otoritas terkait lainnya. Kegagalan untuk memenuhi salah satu kewajiban atau kewajiban merupakan pelanggaran. Setiap pelanggaran data harus diungkapkan kepada Kantor *Cloud* dan otoritas terkait lainnya segera setelah pelanggaran tersebut ditemukan. Kantor *Cloud* dan/atau otoritas terkait lainnya, sebagaimana ditentukan dalam peraturan yang berlaku, dapat mencari laporan insiden dan menentukan tindakan respon yang sesuai.

Selain memenuhi standar keamanan dasar, audit dan mekanisme pemantauan keamanan harus ada untuk memastikan layanan *cloud* memenuhi integritas data, persyaratan kerahasiaan, dan tidak ada pelanggaran data, serta data dan beban kerja terus tersedia.

e. Pengadaan

Pengadaan pemerintah merupakan aspek yang sangat relevan dengan perkembangan *cloud computing*. Lembaga Sektor Publik harus mempertimbangkan layanan *cloud* untuk semua keputusan pengadaan TIK baru mereka. Setiap keputusan pengadaan TIK baru untuk memilih layanan kecuali *cloud* harus mendapat persetujuan dari Kantor *Cloud*. Selain itu, Lembaga Sektor Publik juga akan meminta persetujuan dari Kantor *Cloud* untuk meng-*host* data di *private cloud* dan harus menunjukkan perlunya hosting di *private cloud*. Demikian pula, organisasi yang ingin membangun *Private Cloud* sendiri harus mendapat persetujuan dari Kantor *Cloud*. Aspek-aspek berikut akan dipertimbangkan saat pengadaan layanan *cloud*:

1. *Value for money* untuk memenuhi tujuan layanan yang diberikan;
2. Transisi dari anggaran modal ke belanja operasional;
3. Dampak jangka pendek, menengah, dan panjang pada keuangan, tata kelola, teknologi, relevansi, kesesuaian;
4. Kesesuaian *Service Level Agreements* (SLA) dengan kebutuhan Lembaga Sektor Publik; dan
5. Informasi tentang pedoman keamanan data dan kepatuhan terhadap undang-undang nasional dan standar internasional tentang privasi data dan keamanan siber

Secara umum, layanan *cloud* disediakan berdasarkan “*pay as you use*”. Organisasi yang membutuhkan layanan TIK tidak harus membeli peralatan untuk mendapatkan layanan. Ini adalah pergeseran dari cara tradisional pengadaan TIK di sektor publik di Pakistan yang didasarkan pada pembelian peralatan dan menimbulkan pengeluaran modal. Untuk mencapai tujuan kebijakan ini, perspektif baru untuk pembelian dan pengoperasian TIK akan dipertimbangkan. Pendekatan “*Pay as you use*” dan “*Self Service*” memungkinkan penskalaan layanan dan berguna karena data dan kebutuhan komputasi agensi berfluktuasi.

Setelah kebijakan ini disetujui, MoITT bersama Badan Pengatur Pengadaan Barang/ Jasa (PPRA), Kementerian Keuangan, dan otoritas terkait lainnya akan menyusun mekanisme untuk beralih dari Belanja Modal (*Capex*) ke Belanja Operasional (*Opex*), yang lebih relevan untuk penyediaan layanan *cloud*. Selanjutnya, akan diberikan panduan kepada Lembaga Sektor Publik mengenai aspek-aspek pengadaan layanan *cloud* tersebut di atas.

1. Pengadaan Terpusat

Manfaat sebenarnya dari *cloud computing* dapat diwujudkan dengan entitas terpusat yang memberikan fasilitas kepada Lembaga Sektor Publik untuk kebutuhan pengadaan *cloud* mereka. Ini memberikan kenyamanan, efisiensi, pengurangan biaya, dan proses pemesanan yang disederhanakan. Permintaan agregat untuk teknologi *cloud* umum oleh Lembaga Sektor Publik menghasilkan penawaran terbaik dari Penyedia Layanan *Cloud*. Ini juga menyelaraskan Lembaga Sektor Publik yang berbeda di atas persyaratan dan ketentuan umum daripada yang berbeda untuk setiap organisasi. Kantor Akuisisi Cloud (CAO) akan menjadi kantor terpusat untuk pengadaan TIK di semua Lembaga Sektor Publik. CAO akan memiliki visibilitas permintaan agregat Lembaga Sektor Publik yang akan menghasilkan penawaran biaya dan layanan yang lebih baik oleh penyedia layanan *cloud*.

2. Kontrak dengan Penyedia Layanan *Cloud*

Kantor Cloud terkait akan mengeluarkan pedoman untuk pelaksanaan kontrak *cloud computing* antara Lembaga Sektor Publik dan Penyedia Layanan *Cloud*. Pedoman ini akan mencakup bidang-bidang berikut:

» Mengatur SLA

SLA adalah usaha yang mengikat penyedia layanan *cloud* pada tingkat layanan. Antara lain, mereka menetapkan hukuman untuk provider jika kontrak tidak dipenuhi. Mereka sangat berkaitan dengan klausul tentang keamanan (pemindaian kerentanan, *patching* dan manajemen perubahan, pemeriksaan kontrol kualitas, persyaratan sertifikasi, dll) dan perlindungan data (periode retensi, pelaksanaan hak subjek data, ketersediaan pemrosesan, dll.)

Lembaga Sektor Publik harus memantau secara ketat kepatuhan penyedia layanan *cloud* dengan ketentuan SLA utama antara lain pada aspek-aspek berikut:

- Ketersediaan dan ketepatan waktu layanan;
- Kerahasiaan dan integritas data;
- Kontrol perubahan;
- Kepatuhan standar keamanan, termasuk kerentanan dan manajemen penetrasi;
- Kesiambungan bisnis termasuk pemulihan bencana dan rencana kontinjensi; dan
- Dukungan *Help Desk*

- » **Persyaratan Interoperabilitas**
Lembaga Sektor Publik akan membutuhkan interoperabilitas komponen infrastruktur *cloud* untuk bekerja sama untuk mencapai hasil yang diinginkan berdasarkan standar internasional. Komponen dapat berasal dari sumber yang berbeda termasuk implementasi *public cloud* dan *private cloud*. Komponen harus dapat diganti dengan komponen baru atau berbeda dari penyedia layanan *cloud* yang berbeda dan terus bekerja, untuk memfasilitasi pertukaran data antar sistem.
- » **Migrasi antara Penyedia Layanan Cloud**
Lembaga Sektor Publik dapat memutuskan untuk mengubah/bermigrasi antara penyedia layanan *cloud* karena berbagai alasan. Migrasi awal mereka ke *cloud* harus memfasilitasi migrasi antar *platform* di masa mendatang. Ini dapat diaktifkan dengan mendefinisikan standar teknologi dalam proses pengadaan mereka. Jika Lembaga Sektor Publik membangun infrastruktur mereka menggunakan komponen standar dan tersedia secara luas, ini akan memfasilitasi migrasi data mereka ke *cloud* dan antar penyedia layanan *cloud*.
- » **Kepemilikan Data**
Lembaga Sektor Publik akan memiliki kepemilikan penuh atas data mereka. Mereka akan memutuskan bagaimana dan di mana data mereka disimpan dan dikelola. Data yang disimpan di *cloud* tetap menjadi milik Lembaga Sektor Publik terlepas dari siapa yang memiliki, mengelola, atau mengoperasikan *cloud*. Lembaga Sektor Publik berhak mengakses, mengambil, memodifikasi, atau menghapus data terlepas dari lokasi fisik *cloud*. Selain itu berhak juga untuk menyetujui, menolak atau mencabut akses ke data oleh pihak ketiga.

Arab Saudi

Pemerintah Pakistan mengeluarkan *Cloud First Policy* di tahun 2022 melalui *Ministry of Information Technology & Telecommunication* [26]. Berikut beberapa aspek yang diatur dalam *Cloud First Policy* dari Pakistan.

Pemerintah Arab Saudi mengeluarkan *Cloud First Policy* di tahun 2020 melalui *Ministry of Communications and Information Technology*. Hal ini sejalan dengan inisiatif yang dibuat oleh Pemerintah Arab Saudi untuk menuju Digital Saudi, sehingga menjadi negara terdepan pada sektor ICT di wilayah Timur Tengah dan Afrika Utara. Berikut beberapa aspek yang diatur dalam *Cloud First Policy* dari Arab Saudi.

a. Cakupan *Cloud First Policy* Arab Saudi

Kebijakan ini berlaku untuk semua entitas Pemerintah kecuali Otoritas Moneter Arab Saudi dan entitas lain yang terutama bertanggung jawab atas keamanan dan pertahanan nasional, seperti:

- Kementerian Pertahanan (MoD).
- Keamanan Kepresidenan Negara (PSS).
- Kementerian Dalam Negeri (Kemendagri).
- Otoritas Keamanan Siber Nasional (NCA)

Juga kebijakan ini sangat disarankan untuk entitas terdaftar komersial yang dimiliki sepenuhnya atau sebagian oleh Pemerintah KSA serta sektor swasta. Selain itu, perlunya membuat kebijakan *Cloud First* internal yang serupa untuk organisasi masing-masing.

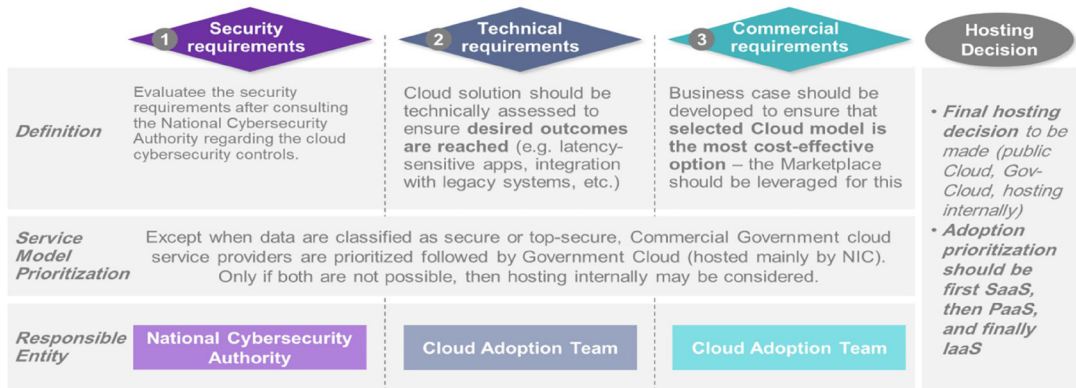
b. Panduan Kebijakan

Saat melakukan investasi TI baru, entitas yang tercakup dalam kebijakan ini diharuskan untuk mempertimbangkan opsi *cloud computing* dan harus mengadopsi pendekatan multi-segi seperti yang dijelaskan pada tahap-tahap berikut ini:

- 1. Tahap Permulaan:** Semua investasi TI baru yang akan dilakukan oleh salah satu entitas yang termasuk dalam cakupan *cloud first policy* harus melalui proses. Investasi TI baru mencakup pengadaan perangkat keras dan perangkat lunak baru, pembaruan perangkat keras dan pembaruan lisensi perangkat lunak yang ada. Patut dicatat bahwa entitas yang termasuk dalam cakupan kebijakan ini harus mematuhi undang-undang, peraturan, dan kontrol yang terkait dengan klasifikasi data dan peraturan lain terkait lokasi hosting data mereka dengan cara apa pun.
- 2. Tahap 1:** Jika data diklasifikasikan dalam level 1 (*top secure*) atau level 2 (*secure*), penyedia layanan cloud pemerintah (NIC) harus diandalkan hanya jika persyaratan teknis dan keamanan siber terpenuhi. Jika penyedia layanan cloud pemerintah tidak memenuhi persyaratan teknis dan keamanan siber, entitas kemudian dapat meminta persetujuan dari tim adopsi cloud computing untuk menghosting perangkat lunak/aplikasi secara internal (*private cloud*).
- 3. Tahap 2:** Jika data tidak diklasifikasikan dalam level 1 (*top secure*) atau level 2 (*secure*), entitas harus menggunakan model penerapan Penyedia Layanan Cloud Pemerintah Komersial hanya jika persyaratan keamanan, teknis, dan komersial terpenuhi untuk tujuan memaksimalkan nilai dan manfaat dari biaya optimal serta beragam penawaran. Berkenaan dengan klasifikasi data, data yang diklasifikasikan di level 3 (*restricted*) harus mendapatkan persetujuan dari Badan Pengelola Data Nasional, dan untuk data yang diklasifikasikan di level 4 (*open*), dapat langsung digunakan melalui penyedia layanan cloud pemerintah komersial dengan ketentuan memenuhi persyaratan keamanan, komersial dan teknis.
- 4. Tahap 3:** Hanya jika persyaratan keamanan, teknis, dan komersial tidak dapat dipenuhi oleh Penyedia Layanan Cloud Pemerintah Komersial, entitas harus menilai solusi dari penyedia layanan cloud pemerintah (NIC) dan harus mengadopsi model ini ketika persyaratan terpenuhi. Misalnya, ketika Kantor Manajemen Data Nasional tidak setuju untuk mengandalkan Penyedia Layanan Cloud Pemerintah Komersial untuk data yang diklasifikasikan sebagai (*restricted*), cloud pemerintah harus diadopsi.

Selain itu, dengan tujuan mencapai TI yang lebih efisien dan lebih termanfaatkan di sektor Pemerintah Arab Saudi, entitas yang tercakup dalam cakupan kebijakan ini tidak lagi diizinkan untuk membeli atau membangun infrastruktur pusat data baru (misalnya pusat data, server, atau lainnya, penyimpanan media, peralatan jaringan, sumber daya yang tidak pernah terputus). Proses pasti yang harus diikuti mencakup keamanan siber, dimensi komersial dan teknis di setiap tahapannya (lihat Gambar 18).

Gambar 18. Proses Terperinci di Tiap Tahapan Adopsi Cloud Arab Saudi [13]



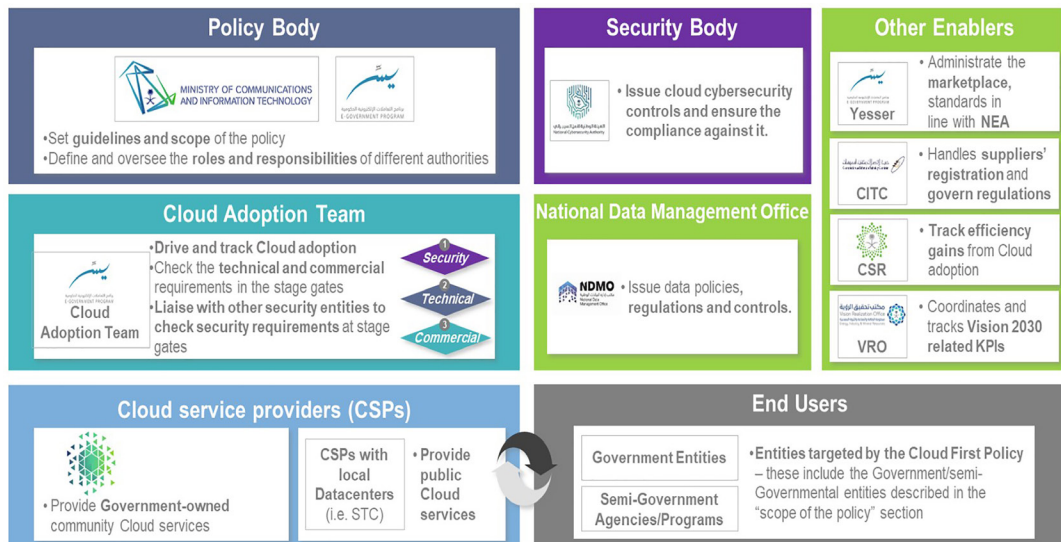
Berdasarkan Gambar 18, berikut penjelasan beberapa persyaratan yang muncul dalam tahapan adopsi cloud di Arab Saudi.

- 1. Persyaratan Keamanan Siber:** menilai apakah persyaratan keamanan *cyber*, yang didasarkan pada undang-undang klasifikasi data yang mengatur di KSA, persyaratan otentikasi, dan tindakan serta peraturan keamanan *cyber* spesifik lainnya, dipenuhi oleh model *Cloud* yang sedang dipertimbangkan (*Commercial Government Cloud* atau *Government Cloud*) saat berhubungan dengan Badan Keamanan yang ditugaskan (lihat bagian Tata Kelola).
- 2. Persyaratan Komersial:** menilai aspek komersial dari kasus adopsi *Cloud* untuk memastikan bahwa itu menghasilkan kasus bisnis yang positif, yaitu bahwa model komputasi *Cloud* yang dipilih (*Cloud* Pemerintah Komersial atau *Cloud* komunitas milik Pemerintah) menawarkan opsi yang paling hemat biaya untuk setiap kasus tertentu. Ini harus dilakukan dalam koordinasi dengan tim adopsi komputasi *Cloud* (lihat bagian Tata Kelola).
- 3. Persyaratan Teknis:** menilai aspek teknis dari kasus migrasi *Cloud*, untuk memastikan bahwa solusi *Cloud* akan mencapai hasil yang diinginkan (misalnya untuk kasus aplikasi yang sensitif terhadap latensi, integrasi dengan sistem lama, dll.). Ini harus dilakukan dalam koordinasi dengan tim adopsi komputasi *Cloud* (lihat bagian Tata Kelola).

c. Struktur Tata Kelola

Struktur tata kelola yang terdefinisi dengan baik harus ada untuk memastikan pelaksanaan yang lancar dan hasil yang optimal. Dalam kasus Kerajaan Arab Saudi, peran dan tanggung jawab untuk berhasil mengimplementasikan *cloud first policy* (lihat Gambar 19).

Gambar 19. Struktur Tata Kelola untuk *Cloud First Policy* di Arab Saudi [13]



Berdasarkan Gambar 19, berikut penjelasan singkat dari tiap domain di dalam struktur tata kelola *Cloud First Policy* di Arab Saudi:

1. Policy Body

Dalam *policy body* terdapat *Ministry of Communications and Information Technology* (MCIT) Arab Saudi yang berperan untuk menentukan tujuan dan cakupan *Cloud First Policy* serta menentukan peran dan tanggung jawab berbagai entitas yang terlibat dalam konteks *cloud first policy*.

2. Cloud Adoption Team

Pada bagian ini, peran dari tim adopsi *cloud* di Arab Saudi untuk mendorong *cloud* di seluruh entitas pemerintah yang berbeda melalui percontohan dan entitas pendukung selama proses migrasi dengan keahlian teknis dan komersial. Selain itu memiliki tugas untuk menangani akreditasi penyedia layanan *cloud* di sektor pemerintahan.

3. National Data Management Office

Dalam domain ini, tugas utama dari Kantor Data Arab Saudi yaitu untuk menetapkan kebijakan klasifikasi data, menjalankan penerapannya, dan memastikan kepatuhannya.

4. Security Body

Pada bagian ini, menjadi tugas dari Otoritas Keamanan Siber Nasional (NCA) Arab Saudi untuk menerbitkan kontrol keamanan siber *cloud* dan peraturan terkait lainnya serta memverifikasi kepatuhannya.

5. Enablers

Dalam domain ini, dilakukan kobalorasi dengan 4 (empat) *stakeholders* antara lain Yesser, Center of Spending Rationalization (CSR), Vision Realization Office (VRO), dan Komisi Komunikasi dan Teknologi Informasi (CITC).

6. Cloud Service Providers

Di domain ini, terdapat Pusat Informasi Nasional (NIC) yang bertugas menyediakan layanan *Government Cloud* kepada entitas pemerintah. Selain itu. *Stakeholder* lainnya adalah penyedia layanan *cloud* yang bertugas menyediakan layanan *public cloud* bagi entitas pemerintah di Arab Saudi.

7. End Users

Domain terakhir ini merupakan entitas pemerintah sebagaimana telah didefinisikan pada cakupan kebijakan. Entitas ini adalah pembeli layanan cloud.

Jerman

Jerman telah mengeluarkan strategi komputasi awan pemerintah atau *Government Cloud Strategy* dalam upaya membentuk kerangka kerja arsitektur di tahun 2021 dan diperbaharui kembali di tahun 2022 [27]. Strategi yang disusun ini menggunakan pendekatan federal dan telah disetujui oleh IT Planning Council Jerman. Di sisi lain, strategi ini merupakan bagian dari IT Planning Council untuk memperkuat kedaulatan digital dari implementasi TI administrasi publik.

Government Cloud Strategy dari Jerman ini dimaksudkan untuk memperkenalkan standar umum dan antarmuka untuk solusi cloud administrasi publik dalam rangka untuk membangun infrastruktur cloud federal yang dapat dioperasikan secara menyeluruh. Melalui keputusannya, IT Planning Council Jerman menugaskan Kelompok Kerja *Cloud Computing* dan *Digital Sovereignty* untuk mengembangkan arsitektur cloud pemerintah Jerman. Kemudian Kelompok Kerja *Cloud Computing* dan *Digital Sovereignty* menugaskan Sub Kelompok Kerja *Technology* dan *Operations* untuk mendesain teknis dan operasionalisasi cloud pemerintah.

a. Tujuan dan Struktur dari Konsep *Government Cloud*

Tujuan dari strategi *Government Cloud* Jerman ini adalah menentukan standar umum untuk infrastruktur komputasi awan administrasi publik di Jerman serta lokasinya. Spesifikasi *Government Cloud* Jerman dibangun berdasarkan konsep sebagai dasar implementasi komputasi awan pemerintah Jerman. Fokus dari kerangka kerja arsitektur cloud ini adalah sebagai fondasi untuk standar operasional layanan cloud saat ini dan masa mendatang serta solusi perangkat lunak untuk membangun atau merampingkan peluang yang dibutuhkan oleh pemerintah Jerman.

b. Struktur Dasar *Government Cloud* Jerman

Bagian ini menguraikan struktur dasar *Government Cloud* Jerman. Mulai dari prinsip, elemen dan peran, serta skenario di dalam *Government Cloud* Jerman.

1. Prinsip

Pemerintah Federal, negara bagian federal, dan kota madya menetapkan beberapa persyaratan umum untuk *Government Cloud* Jerman dan standarnya dalam strategi *Government Cloud* pemerintah Jerman.

- **Operasi TI terdistribusi:** Operasi terdistribusi *Government Cloud* Jerman akan dimungkinkan diletakkan di pusat data yang dioperasikan oleh Pemerintah Federal, negara bagian federal, dan kota madya.
- **Ketersediaan umum layanan cloud:** Diperkirakan bahwa layanan cloud yang ditawarkan dalam *Government Cloud* Jerman akan tersedia untuk digunakan oleh semua entitas administrasi publik di Pemerintah Federal, negara bagian federal dan tingkat kotamadya.
- **Penggunaan perangkat lunak OS (OSS):** OSS akan diprioritaskan saat membangun *Government Cloud* Jerman.

- **Manajemen pusat layanan:** Diperkirakan bahwa pengguna *Government Cloud* Jerman akan dapat mencari, menugaskan, mengadaptasi, dan membatalkan layanan melalui satu portal layanan *cloud* pusat, yang dapat diakses dari jaringan yang berbeda (mis. Internet, jaringan administratif).
- **Pengembangan lebih lanjut secara bersama:** Dalam rangka bekerja sama dalam proyek pengembangan publik dan mendorong pengembangan lebih lanjut pada komponen perangkat lunak utama.

2. Elemen dan Peran *Government Cloud*

Peran-peran berikut ditentukan dengan maksud untuk mendefinisikan kompetensi atau tanggung jawab yang jelas dalam konsep *Government Cloud* Jerman.

- **Pelanggan layanan *cloud*** – pelanggan layanan *cloud* mendapatkan layanan dari *Government Cloud* Jerman melalui broker layanan *cloud* atau langsung dari penyedia layanan *cloud*. pelanggan ini mungkin otoritas, entitas dalam administrasi publik atau penyedia layanan TI dalam administrasi publik.
- **Broker layanan *cloud*** – broker layanan *cloud* mendapatkan layanan *cloud* dari penyedia layanan *cloud* dalam *Government Cloud* Jerman dan bertanggung jawab untuk mengoperasikan dan menyediakan layanan *cloud* ini kepada pelanggan layanan *cloud* sesuai dengan kewajiban kontrak. Elemen ini dapat bertindak sebagai penghubung antara penyedia layanan *cloud* dan pelanggan layanan *cloud*.
- **Penyedia layanan *cloud*** – penyedia layanan *cloud* menawarkan layanan dalam *Government Cloud* Jerman dan bertanggung jawab untuk menyediakan layanan tersebut.
- **Pengguna portal layanan *cloud*** – portal layanan *cloud* adalah titik masuk utama bagi pegawai pelanggan layanan *cloud*, yang dapat mencari, meminta, mengonfigurasi, dan mengelola berbagai layanan *cloud* pemerintah di sana.
- **Badan koordinasi** – badan koordinasi mengoordinasikan pengembangan lebih lanjut dari *Government Cloud* Jerman. Badan ini bertanggung jawab untuk portal layanan *cloud*, pengembangan dan integrasinya dengan lokasi *cloud*, serta untuk katalog layanan (daftar semua layanan yang ditawarkan dalam *Government Cloud* Jerman). Badan koordinasi mewajibkan penyedia layanan TI yang berpartisipasi dalam *Government Cloud* Jerman untuk menegakkan standar *Government Cloud* Jerman.
- **Vendor perangkat lunak** – vendor perangkat lunak adalah entitas atau komunitas yang terhubung secara fleksibel yang menyediakan perangkat lunak kepada operator perangkat lunak sesuai dengan standar *Government Cloud* Jerman.

3. Skenario dalam *Government Cloud* Jerman

Skenario ini akan digunakan sebagai dasar untuk menjelaskan berbagai macam peran yang dilakukan oleh penyedia layanan TI administrasi publik dalam *Government Cloud* Jerman

Skenario 1: Pengadaan melalui broker layanan cloud

Pelanggan layanan *cloud* (otoritas/entitas dalam administrasi publik) menugaskan broker layanan *cloud*-nya (penyedia layanan TI untuk administrasi publik) untuk menyediakan perangkat lunak atau layanan *cloud*. Broker layanan *cloud* memesan layanan *cloud* yang diperlukan di portal layanan *cloud* dari penyedia layanan *cloud*. Broker layanan *cloud* menyediakan layanan kepada pelanggan layanan *cloud*-nya.

Skenario 2: Pengadaan langsung dalam Government Cloud Jerman

Pelanggan layanan *cloud* (otoritas/entitas administrasi publik) membatalkan layanan *cloud* yang tersedia di portal layanan *cloud* untuk penyediaan dari penyedia layanan *cloud* secara langsung (bergantung pada jenis layanan yang dimaksud, operator perangkat lunak, operator *platform*, atau integrator *cloud*). Penyedia layanan *cloud* menyediakan layanan *cloud* dan pelanggan layanan *cloud* dapat membatalkan layanan yang disediakan dari penyedia layanan *cloud*.

Skenario 3: Penyediaan layanan cloud dalam Government Cloud Jerman

Penyedia layanan *cloud* (bergantung pada jenis layanan yang dimaksud, operator perangkat lunak, operator *platform*, atau integrator *cloud*) menyediakan layanan *cloud*-nya sendiri melalui portal layanan *cloud* berdasarkan model layanan *IaaS*, *PaaS*, atau *SaaS*. Layanan ini dapat dipesan dan kemudian digunakan kembali.

c. Standardisasi dalam Government Cloud Jerman

Government Cloud Jerman memperkenalkan dan menyusun standar untuk semua operator perangkat lunak yang berpartisipasi, operator *platform* dan standar *cloud* mereka serta integrator *cloud* di tingkat Pemerintah Federal, negara bagian federal, dan kota madya. Terdapat 6 (enam) area untuk standardisasi untuk strategi *Government Cloud* Jerman yaitu:

1. Pengembangan *platform*.
2. Penyediaan dan pengelolaan aplikasi.
3. Repositori kode.
4. Layanan infrastruktur dan *technology stack*.
5. Standar operasi dan model operasi.
6. Integrasi dengan penyedia *cloud* eksternal

Inggris Raya

Pemerintah Inggris Raya telah menerapkan kebijakan *Cloud First*, yang berarti bahwa semua organisasi sektor publik harus mempertimbangkan dan mengevaluasi solusi *cloud* untuk layanan digital sebelum opsi lainnya. Tujuan utamanya adalah untuk memodernisasi layanan publik. Kebijakan tersebut bersifat wajib bagi pemerintah pusat sekaligus sangat direkomendasikan kepada seluruh sektor publik. Selain itu, *cloud first policy* memprioritaskan solusi *public cloud* daripada opsi *community*, *private*, atau *hybrid*. Alasannya adalah solusi *public cloud* sebagai opsi standar akan membawa lebih banyak manfaat, baik bagi entitas pemerintah maupun pengguna akhir atau *end-user*. Salah satu contohnya yaitu di Kementerian Kehakiman telah menerapkan *cloud first policy*. Tujuannya adalah untuk memindahkan semua sistemnya ke *public cloud*, dengan alasan bahwa *cloud* akan dapat mengurangi biaya hosting secara keseluruhan hingga 60% dalam jangka panjang. Meskipun telah meninggalkan Uni

Eropa, Inggris terus mengikuti kerangka kerja GDPR (*General Data Protection Regulation*) sehubungan dengan pengelolaan data *on-premise*.

Terlepas dari *cloud first policy* yang menyeluruh, Departemen Publik di Inggris bebas memilih alternatif solusi *cloud* atau solusi *public cloud*, tetapi alternatif tersebut harus menawarkan tingkat keamanan yang tepat, fleksibilitas yang memadai, dan harga yang lebih baik. istilah “*value for money*” didefinisikan sebagai “mengamankan gabungan kualitas dan efektivitas terbaik untuk pengeluaran paling sedikit selama periode penggunaan barang atau jasa yang dibeli.” Diakui bahwa solusi *cloud* yang cocok untuk semua tidak ada, karena Kementerian yang berbeda menghadapi tantangan yang berbeda. Oleh karena itu, Kementerian diizinkan untuk menggunakan solusi selain *public cloud*.

Singapura

Singapura meluncurkan kebijakan *Commercial Cloud First* pada tahun 2018. Target utama kebijakan tersebut adalah untuk migrasi sistem TIK pemerintah ke opsi *commercial cloud* yaitu *public cloud* pada tahun 2023. Tujuannya adalah untuk memiliki setidaknya 70 persen sistem pemerintah yang kurang sensitif (misalnya, sumber daya manusia dan keuangan) yang didukung oleh *commercial cloud* pada saat itu. Argumen utama untuk transisi ke *cloud* adalah untuk meningkatkan ketersediaan dan kualitas layanan publik, biaya hosting yang lebih rendah, memotong *downtime system*, menopang pertumbuhan ekonomi, dan meningkatkan akses ke ekosistem solusi dan layanan global. Pemerintah juga telah menciptakan *private cloud* seluruh pemerintah, yang dikenal sebagai G-cloud untuk pengganti solusi *public cloud* yang dianggap tidak dapat memenuhi persyaratan keamanan dan tata kelola. Namun, G-cloud dirancang agar kompatibel dengan solusi *public cloud*, sehingga membuka peluang untuk solusi *hybrid cloud*.

Pemerintah Singapura mengakui bahwa solusi satu *cloud* yang cocok untuk semua tidak ada. Oleh karena itu, jika kebutuhan masing-masing Kementerian atau lembaga tidak dapat sepenuhnya dipenuhi oleh penyedia *public cloud* atau G-cloud, mereka berwenang untuk merancang solusi yang disesuaikan berdasarkan pendekatan *hybrid*.

Nigeria

Pemerintah Nigeria meluncurkan *Cloud First Policy* pada tahun 2019 melalui Badan Pengembangan Teknologi Informasi Nasional atau disebut NITDA. Dalam kebijakan ini berfokus untuk mempertahankan pembangunan negara dan meningkatkan kualitas layanan sektor publik, semua lembaga publik federal, serta lembaga publik di tingkat negara bagian dan lokal, harus memprioritaskan solusi berbasis *cloud* bila memungkinkan. Kebijakan tersebut juga berlaku bagi perusahaan yang dimiliki sepenuhnya atau sebagian oleh pemerintah. Dua target utama *cloud first policy* adalah (1) untuk meningkatkan adopsi *cloud computing* di antara lembaga publik federal (serta perusahaan kecil dan menengah yang menyediakan layanan digital kepada pemerintah) sebesar 30 persen pada tahun 2024; dan (2) untuk meningkatkan investasi keseluruhan dalam infrastruktur *cloud computing* sebesar 35 persen, juga pada tahun 2024. Selain itu, ditekankan bahwa penyedia layanan *cloud* lokal di Nigeria akan menerima dukungan lebih lanjut untuk meningkatkan daya saing mereka yang pada dasarnya memungkinkan mereka untuk beroperasi dan bersaing di industri *cloud*.

Cloud first policy menyatakan bahwa semua lembaga publik diharapkan untuk memprioritaskan layanan *cloud* untuk memaksimalkan manfaatnya. Dalam praktiknya, saat melakukan pengadaan layanan *cloud*, mereka harus mempertimbangkan banyak faktor seperti nilai uang,

kebutuhan khusus mereka untuk penyimpanan data, risiko vendor *lock-in* dan berdampak pada keuangan dalam jangka pendek, menengah, dan panjang. Opsi *public*, *private*, dan *hybrid cloud* tidak diberikan prioritas oleh pemerintah Nigeria, sehingga opsi yang dipilih harus bergantung pada sensitivitas data masing-masing entitas publik.

Analisis Benchmarking

Benchmarking yang dilakukan dalam kajian ini memilih 6 (enam) negara yang telah memiliki *Government Cloud First Policy* antara lain, Filipina, Pakistan, Arab Saudi, Inggris Raya, Singapura, dan Nigeria. Terdapat perbandingan dari domain apa saja yang ada di dalam *Government Cloud First Policy* di keenam Negara tersebut (lihat Tabel 7).

Tabel 7. Analisis Benchmarking Government Cloud First Policy di Enam Negara

Negara/ Domain	Filipina	Pakistan	Arab Saudi	Inggris Raya	Singapura	Nigeria
Definisi Cloud Computing	✓	✓	✓	✓	✓	✓
Model Layanan Cloud	✓	✓	✓	✓	✓	✓
Model Deployment Cloud	✓	✓	✓	✓	✓	✓
Keamanan Cloud	✓	✓	✓	✓	✓	✓
Klasifikasi Data	✓	✓	✓	✓	✓	✓
Kontrol dan Privasi Data	✓	✓	-	✓	✓	✓
Kedaulatan Data	✓	✓	-	-	✓	✓
Residensi Data	✓	-	-	✓	✓	-
Migrasi Cloud	✓	✓	✓	✓	✓	✓
Data Ownership, Retrieval, dan Interoperability	✓	✓	-	✓	✓	✓
Akreditasi Provider Layanan Cloud	✓	✓	-	✓	✓	✓
Pengadaan Cloud	✓	✓	✓	✓	✓	✓
Audit Cloud	✓	✓	✓	✓	✓	✓
Organisasi/Lembaga Pengelola Cloud	-	✓	✓	✓	✓	✓

diolah oleh WANTIKNAS

06

REGULASI TERKAIT CLOUD COMPUTING DI INDONESIA

KEY FACTS

Beberapa prioritas utama pembuat kebijakan layanan *public cloud* adalah sebagai berikut:

- » Menerapkan peraturan privasi data untuk memberikan tingkat kepercayaan kepada pengguna tentang data pribadi mereka di *cloud*.
- » Untuk membuat organisasi akuntabel dan menerapkan mekanisme dan tindakan khusus untuk menangani data pengguna secara bertanggung jawab.
- » Untuk meluncurkan kebijakan atau strategi '*Cloud-First*' demi menciptakan peluang bersama bagi organisasi dan penyedia layanan *cloud*. Hal ini akan menarik investasi dari penyedia layanan *cloud* lokal dan global.
- » Menciptakan lingkungan yang kondusif untuk pengembangan *Government Cloud* (G-Cloud).

Sumber: KSA Government, 2020. On Overview on the Global Governmental Efforts on Fostering the Use of Cloud Computing. Communications & Information Technology Commission.

Masifnya perkembangan teknologi informasi salah satunya adalah *cloud computing*. Saat ini di Indonesia penggunaan *cloud* sudah menjadi kebutuhan utama baik di sektor swasta maupun pemerintahan. Khususnya di sektor pemerintahan, ada banyak manfaat dan peluang yang bisa diperoleh ketika beralih ke *cloud computing*. Maka dari itu, regulasi menjadi salah satu hal penting dalam memanfaatkan peluang dan manfaat *cloud computing* bagi IPPD. Banyak pemerintah di berbagai negara telah memperkenalkan kebijakan *cloud computing* dengan nama *cloud first policy*. Melihat kondisi di Indonesia saat ini, beberapa IPPD telah berhasil mengadopsi teknologi *cloud computing*, tetapi dalam pelaksanaannya masih belum diatur dalam acuan regulasi secara nasional.

Kebijakan *cloud-first* atau dengan kata lain kebijakan yang mengutamakan cloud mewajibkan Kementerian/Lembaga hingga Pemerintah Daerah untuk memprioritaskan penggunaan dan pengadaan sistem *cloud* secara default di mana opsi *cloud computing* bersifat aman, andal, serta hemat biaya. Sampai saat ini, terdapat beberapa regulasi di Indonesia yang berkaitan dengan *cloud computing*. Berikut beberapa regulasi yang berkaitan dengan adopsi *cloud computing* di Pemerintahan Indonesia saat ini (lihat Gambar 20).

Berikut merupakan beberapa dasar hukum yang berkaitan dengan adopsi *cloud computing* di Pemerintahan Indonesia untuk saat ini:

1. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tahun tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;

Key Takeaways:

Dalam UU ini, terdapat aturan mengenai penyelenggaraan sistem elektronik yang selanjutnya dilaksanakan oleh Penyelenggara Sistem Elektronik atau PSE. Pada dasarnya penyedia/penyelenggara layanan *cloud* merupakan bagian dari PSE, sehingga semua konsekuensi hukum PSE sebagaimana diatur dalam UU No. 19/2016 tentang ITE berlaku juga bagi penyedia/penyelenggara layanan *cloud*.

2. Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;

Key Takeaways:

Dalam PP ini, terdapat aturan mengenai penyelenggaraan sistem elektronik yang selanjutnya dilaksanakan oleh Penyelenggara Sistem Elektronik atau PSE. Pada dasarnya penyedia/penyelenggara layanan *cloud* dalam PP ini masuk kategori sebagai PSE lingkup publik ataupun PSE lingkup privat, sehingga semua konsekuensi hukum PSE sebagaimana diatur dalam PP No. 71/2019 tentang PSTE berlaku juga bagi penyedia/penyelenggara layanan *cloud*. Dalam rangka pengawasan dan perlindungan hukum, Pemerintah Indonesia mengatur syarat dan ketentuan terhadap PSE lingkup publik dan privat sebagai penyedia/penyelenggara layanan *cloud computing*, antara lain kewajiban pendaftaran (pasal 6), perangkat keras (pasal 7), perangkat lunak (pasal 8-9), tenaga ahli (pasal 10), tata kelola (pasal 11-21), pengamanan (pasal 22-33), uji kelaikan (pasal 34), dan pengawasan (pasal 35).

3. Peraturan Pemerintah Republik Indonesia Nomor 5 Tahun 2021 tentang Penyelenggaraan Perizinan Berusaha Berbasis Risiko;

Key Takeaways:

Penyedia/penyelenggara layanan *cloud computing* yang termasuk dalam kategori PSE lingkup privat wajib melakukan perizinan sebelum melakukan kegiatan secara masif dan/atau digunakan oleh orang banyak. Melalui PP No. 5/2021 ini, penyedia/penyelenggara layanan *cloud computing* masuk ke dalam sektor Pos, Telekomunikasi, dan Sistem Transaksi Elektronik dengan bidang usaha risiko menengah tinggi.

4. Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;

Key Takeaways:

Melalui Perpres No. 95/2018 tentang SPBE, terdapat arah kebijakan dan strategi SPBE yang salah satu lingkungannya adalah Teknologi Informasi dan Komunikasi atau TIK. Di dalam lingkup TIK, teknologi *cloud computing* dapat digunakan untuk mencapai optimalisasi penggunaan aplikasi umum SPBE, sehingga mampu melakukan bagi pakai aplikasi umum SPBE.

Selain itu, peran teknologi *cloud computing* muncul pada peta rencana strategis SPBE yang berisi berbagai inisiatif yang digunakan sebagai pedoman untuk melakukan pembangunan, pengembangan, dan penerapan SPBE nasional. Salah satunya yaitu inisiatif strategis pada area TIK yang berkaitan dengan Pusat Data Nasional atau PDN. Dikatakan bahwa PDN diarahkan menggunakan teknologi *cloud computing* sehingga bagi pakai data, aplikasi, dan infrastruktur dapat dilakukan.

5. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat;

Key Takeaways:

Dalam Permen Kominfo No. 5/2020 tentang PSE Lingkup Privat ini, menjadi dasar hukum yang spesifik bagi penyedia/penyelenggara layanan *cloud* sebagai PSE lingkup privat yang menyediakan, menyelenggarakan, mengelola, dan/atau mengoperasikan layanan *cloud computing* sebagaimana diatur pada Pasal 1 angka (10). Selain itu, melalui Pasal 12 telah diatur juga mengenai kewajiban yang harus dilakukan oleh penyedia/penyelenggara layanan *cloud*.

6. Undang-Undang Republik Indonesia No. 27 Tahun 2022 tentang Perlindungan Data Pribadi

Key Takeaways:

Pada undang-undang ini, mengatur perlindungan data pribadi dalam sistem elektronik yang diselenggarakan oleh penyelenggara sistem elektronik. Dalam kondisi saat ini, penyedia/penyelenggara layanan *cloud* di Indonesia termasuk sebagai penyelenggara sistem elektronik. Melalui undang-undang ini disebutkan bahwa perlindungan data dalam sistem elektronik dilakukan terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan data pribadi. Dengan adanya undang-undang ini, tentu menjadi hal yang krusial yang perlu diperhatikan oleh penyedia/penyelenggara layanan *cloud* di Indonesia. Selanjutnya terkait dengan perlindungan data pribadi akan diperkuat melalui beberapa peraturan turunan dari Undang-Undang Perlindungan Data Pribadi.

7. Peraturan Presiden No. 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital

Key Takeaways:

Penggunaan *cloud* tidak terlepas dari fungsinya yaitu untuk penyimpanan dan pemrosesan data. Data yang disimpan tentunya akan diproses dan kemudian menghasilkan suatu informasi yang bermanfaat bagi penggunanya. Melalui peraturan ini, mengatur perlindungan infrastruktur informasi vital yang meliputi beberapa sektor, antara lain administrasi pemerintahan, energi dan sumber daya mineral, transportasi, keuangan, kesehatan, teknologi informasi dan komunikasi, pangan, pertahanan, dan sektor lain yang ditetapkan oleh Presiden. Keterhubungan dari adopsi *cloud computing* dengan adanya peraturan ini dapat disimpulkan bahwa perlunya perlindungan data-data yang ada pada sektor-sektor tersebut. Pada akhirnya, penyedia/penyelenggara layanan *cloud* perlu patuh terhadap Peraturan Presiden ini.

8. Surat Edaran Menteri Komunikasi dan Informatika Republik Indonesia Nomor 3 Tahun 2021 tentang Pedoman Penggunaan Layanan Komputasi Awan Pihak Ketiga Bagi Kementerian/Lembaga Tahun Anggaran 2021

Key Takeaways:

Kementerian Komunikasi dan Informatika mengeluarkan Surat Edaran yang bertujuan sebagai pedoman bagi Kementerian/Lembaga dalam menggunakan layanan *cloud computing* pihak ketiga serta untuk meningkatkan keamanan dalam proses pengelolaan, pemrosesan, dan/atau penyimpanan data elektronik yang digunakan oleh Kementerian/Lembaga dalam penggunaan layanan *cloud computing* pihak ketiga. Dalam surat edaran ini diatur mengenai definisi, panduan umum, mitigasi risiko terhadap data elektronik, dan kontrol keamanan pada layanan *cloud computing* yang digunakan oleh Kementerian/Lembaga.

Matriks Regulasi Cloud Computing

Tabel 8. Matriks Regulasi terkait Cloud Computing di Indonesia Saat Ini

	UU No. 19/2016 tentang Informasi dan Transaksi Elektronik	PP No. 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik	PP No. 5/2021 tentang Penyelenggaraan Perizinan Berusaha Berbasis Risiko	Perpres No. 95/2018 tentang Sistem Pemerintahan Berbasis Elektronik	Permen Kominfo No. 5/2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat	SE Menteri Kominfo No. 3/2021 tentang Pedoman Penggunaan Layanan Komputasi Awan Pihak Ketiga Bagi Kementerian/Lembaga TA. 2021	Undang-Undang Republik Indonesia No. 27 Tahun 2022 tentang Perlindungan Data Pribadi	Peraturan Presiden No. 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital
Definisi <i>cloud computing</i>					V			
Penggunaan <i>cloud computing</i> di sektor pemerintahan				V				
Pengamanan <i>cloud</i>		V						V

Berkaca dari beberapa Negara seperti Filipina, Pakistan, Arab Saudi, Inggris Raya, Singapura, dan Nigeria telah memiliki kebijakan dalam pemanfaatan *cloud computing* di negaranya. Beberapa menyebutnya dengan nama *Cloud First Policy*. Penerapan kebijakan ini tentunya memiliki tantangan yang berbeda-beda di tiap Negaranya, sehingga Pemerintah Indonesia perlu mempertimbangkan konteks di dalam negeri ketika akan menyusun *Government Cloud First Policy*.

07

KERANGKA STRATEGIS NATIONAL GOVERNMENT CLOUD

KEY FACTS

Tujuan utama dari adanya sebuah kebijakan *cloud* atau *cloud policy* adalah untuk:

- » Meningkatkan kesadaran akan potensi manfaat dari penggunaan solusi *cloud computing* oleh Pemerintah untuk memberikan layanan publik yang lebih gesit, terukur, dan responsif.
- » Memberikan arahan strategis dan kejelasan untuk adopsi yang lebih luas dari layanan *cloud computing* yang sesuai di seluruh sektor publik, dengan pertimbangan yang tepat untuk klasifikasi data, manajemen keamanan informasi, dan proses terstruktur.
- » Menetapkan berbagai mekanisme di mana sumber daya *cloud computing* dapat diakses secara aman dan bertanggung jawab oleh sektor publik.
- » Mendorong penggunaan layanan dan aplikasi berbasis *cloud* yang aman dan sesuai untuk tujuan.

Sumber: Trinidad and Tobago Government, 2020. *Cloud Computing Consideration Policy*, Ministry of Public Administration.

Di antara proses transformasi digital sektor pemerintahan di beberapa negara, peran penting dimainkan oleh teknologi *cloud computing*, yang memungkinkan untuk menyederhanakan dan mengoptimalkan pengelolaan sumber daya TI dan memfasilitasi adopsi teknologi digital baru. Kebutuhan akan teknologi *cloud* di masa mendatang akan meningkat mengingat pertumbuhan eksponensial terhadap *volume* data yang diproses serta banyaknya layanan digital yang membutuhkan infrastruktur komputasi yang dapat diperluas dan diskalakan dengan cepat dan fleksibel. Hal-hal tersebut menjadi sulit dicapai oleh pemerintah apabila masih menggunakan pusat data tradisional. Maka dari itu, untuk mengakomodir pemanfaatan dan pengelolaan *cloud* pemerintahan di Indonesia, Dewan TIK Nasional mengusulkan untuk dibuatnya regulasi **Government Cloud First Policy** sebagai payung hukum penerapan teknologi *cloud* bagi Pemerintah Indonesia.

Gambar 21. Kerangka Strategis National Government Cloud

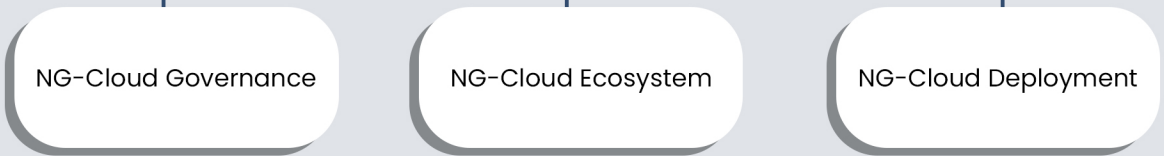
VISI SPBE

Terwujudnya sistem pemerintahan berbasis elektronik yang terpadu dan menyeluruh untuk mencapai birokrasi dan pelayanan publik yang berkinerja tinggi

ARAH STRATEGIS

Terwujudnya akselerasi adopsi komputasi awan pada sistem pemerintahan berbasis elektronik yang terpadu dan menyeluruh untuk mencapai birokrasi dan pelayanan publik yang berkinerja tinggi

DIMENSI



STRATEGI

- | | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> > Mendorong Penyusunan <i>Government Cloud First Policy</i> > Melakukan Pengembangan Kebijakan dan Standar dalam mendukung adopsi <i>cloud</i> > Membentuk Struktur Model Tata Kelola <i>Cloud</i> | <ul style="list-style-type: none"> > Menciptakan Lingkungan Terpercaya (Trusted Environment) dalam Adopsi <i>Cloud</i> > Mendorong Pengembangan Kapasitas SDM <i>Cloud (Capacity Building)</i> | <ul style="list-style-type: none"> > Melakukan Pengembangan Arsitektur NG-Cloud > Konsolidasi NG-Cloud dan PDN > Melaksanakan Pengembangan Program Percepatan NG-Cloud |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Inisiatif

Di samping itu, dalam upaya mendorong Pemerintah Indonesia untuk memindahkan operasional TI-nya ke lingkungan *cloud* sebagai bagian dari program Transformasi Digital, Dewan TIK Nasional melalui kajian ini memberikan rekomendasi berupa **Kerangka Strategis *National Government Cloud*** yang setelahnya akan disebut dengan **NG-Cloud**. Tujuan utama dari penerapan NG-Cloud yaitu untuk memastikan pengeluaran TI Pemerintah Indonesia didorong oleh layanan *cloud* serta pengadaan TI yang bersifat *seamless* oleh semua IPPD yang memanfaatkan infrastruktur *cloud*. Dengan implementasi NG-Cloud oleh Pemerintah Indonesia diharapkan mampu mengakselerasi adopsi dan tata kelola *cloud* pemerintahan dalam rangka mendukung penerapan Sistem Pemerintahan Berbasis Elektronik di IPPD. Rekomendasi Kerangka Strategis *National Government Cloud* untuk Pemerintah Indonesia diilustrasikan pada Gambar 21.

Melalui Kerangka Strategis ini, Dewan TIK Nasional mengusulkan arah strategis yang mengacu pada Visi SPBE di dalam Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik yaitu :

“Terwujudnya akselerasi adopsi komputasi awan pada sistem pemerintahan berbasis elektronik yang terpadu dan menyeluruh untuk mencapai birokrasi dan pelayanan publik yang berkinerja tinggi”

Sementara itu, Dewan TIK Nasional merekomendasikan NG-Cloud sebagai *Hybrid Cloud* yang menggabungkan layanan di lingkungan *public cloud* dengan Pusat Data Nasional (PDN) berdasarkan inisiatif dari beberapa IPPD dan diimplementasikan oleh “NG-Cloud Board”. Kerangka Strategis NG-Cloud memiliki potensi besar untuk meningkatkan efisiensi dan kinerja pemerintah. Hal ini memungkinkan terciptanya *value* dengan meningkatkan efisiensi operasional TI dan merespon lebih cepat terhadap kebutuhan layanan. Beberapa dimensi yang diturunkan dari arah strategis di dalam Kerangka Strategis NG-Cloud yaitu:

- Membentuk struktur tata kelola yang bertanggung jawab untuk menyusun dan menetapkan regulasi dan standar (**NG-Cloud Governance**).
- Membangun ekosistem untuk mengembangkan lingkungan *cloud* yang terpercaya dan memastikan ketersediaan sumber daya (**NG-Cloud Ecosystem**).
- Memulai transformasi aplikasi pemerintah ke lingkungan *cloud* dengan menerapkan *pilot project* yang *scalable* (**NG-Cloud Deployment**).

NG-Cloud Governance

Dimensi dari Framework NG-Cloud yaitu NG-Cloud Governance atau dapat disebut dengan istilah Tata Kelola NG-Cloud. Menerapkan NG-Cloud Governance merupakan tantangan tersendiri bagi Pemerintah. Pemanfaatan *cloud* ke depannya menjadi semakin penting bagi IPPD, sehingga prosesnya akan menjadi lebih rumit. Beberapa tantangan yang muncul, antara lain penataan regulasi terkait *cloud*, meningkatnya aplikasi di *cloud*, dan jumlah SDM yang terlibat dalam penggunaan dan pengelolaan aplikasi yang semakin bertambah.

Beberapa tantangan di atas diperkirakan akan muncul saat mengadopsi, mengoperasikan, dan mengelola *cloud* di Pemerintahan. Tantangan tersebut biasanya berasal dari tidak adanya

kebijakan dan standar cloud serta badan pengatur dan pengelola cloud yang terpusat. Tujuan dari dimensi NG-Cloud Governance adalah untuk memberikan kejelasan, panduan, dan dorongan yang diperlukan untuk adopsi *cloud computing* yang lebih luas di Pemerintahan. Mulai dari kebijakan hingga otoritas pengelola *cloud*. NG-Cloud Governance memiliki 3 (tiga) strategi yang tercantum di bawah ini:

1. Mendorong Penyusunan *Government Cloud First Policy*.
2. Melakukan Pengembangan Kebijakan dan Standar dalam Mendukung Adopsi *Cloud*.
3. Membentuk Struktur Model Tata Kelola *Cloud*.

Strategi 1. Mendorong Penyusunan *Government Cloud First Policy*

Inisiatif:

1. Menyusun dan menetapkan *Government Cloud First Policy* dalam upaya untuk meningkatkan layanan publik, optimasi sumber daya SPBE, mengakselerasi ekonomi digital, memberdayakan SDM lokal, melestarikan lingkungan.

Deskripsi:

Inisiatif ini perlu dilaksanakan untuk memastikan bahwa pemerintah dapat melihat komputasi awan sebagai pilihan utama dalam pengadaan dan implementasi TI sebagai upaya mendukung sistem pemerintahan berbasis elektronik. Dengan kata lain, ketika mempertimbangkan pengadaan produk/layanan TI baru, pemerintah mempertimbangkan dan menilai solusi komputasi awan sebagai prioritas.

Penetapan kebijakan *Government Cloud First Policy* dapat menandakan penerimaan pemerintah terhadap komputasi awan. Kemudian, perlu terciptanya komitmen seluruh pemerintah untuk komputasi awan sebagai pilihan *default* untuk TI pemerintah. Kebijakan ini juga bisa mengirimkan pesan yang jelas untuk pemerintah yang bisa menjadi kenormalan baru, dengan kemampuan komputasi, efisiensi, dan inovasi yang tidak dapat dilakukan oleh pusat data tradisional. Dalam penyelenggaraan pemerintahan, kebijakan ini memastikan pengambilan kebijakan nasional yang lebih tepat dan memberikan kesempatan kepada IPPD untuk memperoleh pemerataan teknologi. Dewan TIK Nasional merekomendasikan beberapa hal-hal yang perlu diatur dalam *Government Cloud First Policy*. Kerangka kerja peraturan (*regulatory framework*) diilustrasikan pada Gambar 22.

Kebijakan ini nantinya berlaku untuk semua IPPD yang ingin menghosting data, aplikasi, atau layanan mereka di lingkungan cloud terpusat melalui koordinasi dengan NG-Cloud. Dengan kata lain, **memastikan kebijakan *Government Cloud First* bersifat Nasional sebagai pendekatan *Whole-of-Government*** untuk dapat mengoordinasikan penerapan *cloud* di pemerintahan pusat maupun pemerintahan daerah. **Terakhir yaitu memastikan kebijakan *Government Cloud First* ini dapat mewadahi *cloud service provider* lokal dan global** agar kompetisi akan terjadi pada tingkat yang setara (*level playing field*), sehingga industri *public cloud* dalam negeri mampu tetap tumbuh, berkembang, dan berdaya saing. Hal ini sejalan dengan Instruksi Presiden Republik Indonesia Nomor 2 Tahun 2022 tentang Percepatan Peningkatan Penggunaan Produk Dalam Negeri dan Produk Usaha Mikro, Usaha Kecil, dan Koperasi dalam Rangka Menyukseskan Gerakan Nasional Banggan Buatan Indonesia pada Pelaksanaan

Pengadaan Barang/Jasa Pemerintah. Walaupun demikian, kebutuhan infrastruktur *cloud* pemerintah ke depannya akan sesuai syarat dan ketentuan yang ditetapkan dan tetap memberikan tempat terbaik bagi investasi perusahaan global di dalam negeri.

Outcome:

- *Penerbitan Government Cloud First Policy*
- *Penerbitan Kebijakan untuk Transformasi dan Migrasi Legacy System*
- *Pelaksanaan Workshop Policy Awareness*

Strategi 2. Melakukan Pengembangan Kebijakan dan Standar dalam Mendukung Adopsi *Cloud*

Inisiatif:

1. Merancang kebijakan *procurement* (pengadaan) *cloud* untuk dapat mengoordinasikan dan mengintegrasikan pengadaan *cloud* di pemerintahan pusat maupun pemerintahan daerah.

Deskripsi:

Pengadaan pemerintah merupakan aspek yang sangat relevan dengan perkembangan penerapan komputasi awan. IPPD perlu mempertimbangkan pemanfaatan *cloud* untuk semua keputusan pengadaan TI baru mereka. Melalui kebijakan pengadaan *cloud* yang ditetapkan secara nasional, diharapkan dapat memberikan arahan kepada IPPD untuk kebutuhan pengadaan *cloud computing* mereka. Ini memberikan aturan hukum yang jelas, kenyamanan, efisiensi, pengurangan biaya dan proses pengadaan *cloud* yang disederhanakan.

NG-Cloud akan menjadi Unit/Lembaga terpusat untuk mengintegrasikan dan mengoordinasikan pengadaan *cloud* di semua IPPD. NG-Cloud akan memiliki visibilitas terhadap permintaan penggunaan *public cloud* IPPD yang kemudian akan dikoordinasikan untuk menghasilkan penawaran biaya dan layanan yang lebih baik oleh CSP.

Outcome:

- *Penerbitan Kebijakan Pengadaan Cloud*

2. Merancang kebijakan dan standar keamanan *cloud* untuk menjamin penyelenggaraan layanan digital pemerintah yang aman, tangguh, dan terpercaya.

Deskripsi:

Pada pusat data tradisional, pemerintah bertanggung jawab sendiri atas keamanan di seluruh lingkungan operasi. Pada lingkungan *cloud*, khususnya untuk pemanfaatan *public cloud*, solusi keamanan yang diterapkan dapat dibagi antara pemerintah dan CSP. Masing-masing pihak mempertahankan kendali penuh atas aset, proses, dan fungsi yang mereka miliki. Tanggung jawab masing-masing pihak bervariasi tergantung pada layanan yang digunakan dan bagaimana layanan tersebut diintegrasikan ke dalam

lingkungan secara menyeluruh. Selain itu, perlu diatur dalam kebijakan ini terkait hal-hal yang menjadi tanggung jawab bersama (*shared responsibilities*) untuk keamanan *cloud* antara pemerintah dan CSP sebagai penyedia *public cloud*.

Perlunya kebijakan dan standar keamanan *cloud* ini adalah untuk memastikan bahwa penyediaan layanan *cloud* untuk IPPD sesuai dengan persyaratan bisnis dan keamanan. Penyediaan layanan *cloud* tersebut dapat diperoleh dari Pusat Data Nasional sebagai *private cloud* maupun *public cloud* dari CSP. Standar keamanan *cloud* yang diperlukan oleh pemerintah juga dapat mengacu pada standar keamanan *cloud* yang telah digunakan dan diakui secara global (semisal ISO 27001, 27017, 27018, 27701). Ketika kebijakan dan standar keamanan *cloud* diterapkan dengan baik, hal itu dapat memperkuat ketahanan pemerintah dalam upaya adopsi *cloud* yang mendukung sistem pemerintahan berbasis elektronik.

Outcome:

- Penerbitan Kebijakan Keamanan Cloud
- Penetapan Standar Keamanan Cloud

3. Menyusun *guideline* (pedoman) adopsi teknologi *cloud computing* di pemerintahan sebagai petunjuk ketentuan dasar dari kebijakan *Government Cloud First Policy* untuk dapat memberikan arah yang jelas bagi IPPD dalam memanfaatkan *cloud*.

Deskripsi:

Bagi IPPD yang ingin mengadopsi *cloud* atau dalam proses mengadopsi *cloud* di masa mendatang, perjalanan menuju adopsi *cloud* akan memiliki pencapaian tertentu. Pencapaian ini mengarah dari satu ke yang lain dan kondisi akhirnya yaitu solusi *cloud*. Pencapaian ini tentu akan berbeda satu dengan yang lainnya tergantung bagaimana IPPD nantinya menetapkan strategi *cloud* mereka. Maka dari itu, perlu disiapkan *guideline* untuk membantu IPPD dalam memahami dan menavigasi melalui *framework* dan standar dalam perjalanannya menuju adopsi *cloud*. *Guideline* ini mencakup cara mewujudkan *best practice* adopsi dan penggunaan *cloud* serta memaksimalkan kapabilitas teknis, keamanan, dan SDM.

Outcome:

- Penerbitan *Guideline* Adopsi Cloud untuk Sektor Pemerintahan

Strategi 3. Membentuk Struktur Otoritas Tata Kelola *Cloud*

Inisiatif:

1. Membentuk Unit/Lembaga yang mengoordinasikan tata kelola dan transisi *cloud* di tingkat Nasional sebagai upaya kolaborasi antara pemerintah pusat dan pemerintah daerah dalam menerapkan *cloud*, melakukan akreditasi penyedia layanan *cloud*, dan menentukan klasifikasi data.

Deskripsi:

Unit/lembaga tata kelola *cloud* di tingkat Nasional perlu dibentuk dalam rangka menyelaraskan pemanfaatan *cloud* di seluruh IPPD. Unit/Lembaga ini akan mengambil

tanggung jawab untuk menetapkan peraturan, standar, dan prinsip yang diperlukan untuk melakukan penerapan, pengembangan, dan pengelolaan NG-Cloud. Hal-hal yang menjadi tugas dari unit/Lembaga ini tentunya harus sejalan dan patuh terhadap *Government Cloud First Policy* yang akan diilustrasikan pada Gambar 23, yang menunjukkan rekomendasi struktur otoritas NG-Cloud bagi Pemerintah Indonesia.

Dalam upaya mendukung SPBE, Otoritas NG-Cloud melakukan koordinasi dengan stakeholder yang masuk di dalam Tim Koordinasi SPBE. Sementara itu, Dewan TIK Nasional juga perlu berperan dalam koordinasi dengan Otoritas NG-Cloud dalam rangka merumuskan kebijakan umum dan arahan strategis pembangunan TIK Nasional. Otoritas NG-Cloud memiliki fokus untuk melakukan tata kelola pemanfaatan komputasi awan di pemerintahan secara Nasional yang terdiri dari unit-unit berikut:

- **NG-Cloud Board + Ketua**

NG-Cloud Board di sini bertanggung jawab atas proses pengambilan seluruh keputusan otoritas NG-Cloud. Di dalam NG-Cloud Board terdapat representatif dari berbagai sektor yang ada di pemerintahan Indonesia. NG-Cloud Board akan bekerja dengan seorang Direktur. Direktur tersebut memegang tanggung jawab untuk mengelola tiga divisi, yaitu divisi teknis, divisi pengembangan, dan divisi operasional.

- **Tim Penasihat**

Tim Penasihat di sini bertujuan untuk memberikan pendapat ahli dan melakukan analisis terkait pemanfaatan teknologi komputasi awan untuk mendukung proses pengambilan keputusan Board dan CEO dari NG-Cloud. Anggotanya merupakan praktisi di bidang komputasi awan. Tugas dari Tim Penasihat yaitu untuk memberikan rekomendasi dan dukungan mengenai seluruh prosedur dan keputusan tata kelola komputasi awan pemerintah, serta untuk menyoroti isu dan masalah yang dapat menyebabkan ancaman.

- **Divisi Teknis**

Divisi ini memiliki tugas dan tanggung jawab untuk:

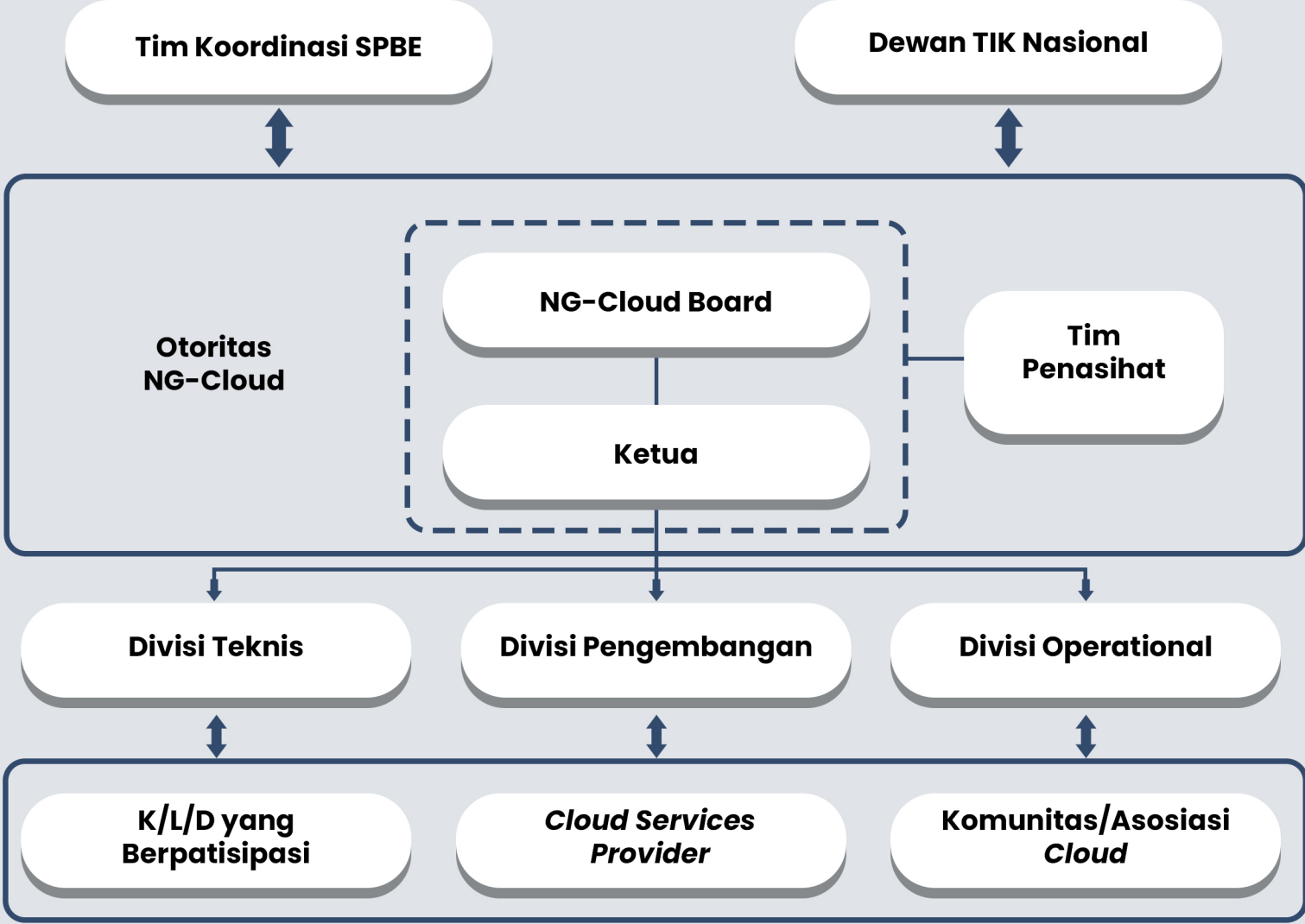
1. Menetapkan peraturan, standar, dan prinsip dari NG-Cloud yang harus diikuti oleh CSP dan IPPD,
2. Merancang dan mengelola kerangka kerja arsitektur NG-Cloud yang berdasarkan pada semua solusi *cloud* yang diusulkan,
3. Memastikan bahwa semua solusi *cloud* sesuai dengan kerangka kerja dan standar,
4. Memastikan keamanan dari layanan *cloud* yang digunakan oleh IPPD sesuai dengan kebijakan dan standar keamanan yang telah ditetapkan, dan
5. Menetapkan kebijakan terkait proses pertukaran data dan klasifikasi data.

- **Divisi Pengembangan**

Divisi ini memiliki tugas dan tanggung jawab untuk:

1. Merancang desain dan pengembangan layanan *cloud* pemerintah,
2. Melaksanakan manajemen proyek dan perubahan pada implementasi NG-Cloud di seluruh IPPD
3. Menyusun solusi pengadaan *cloud* pemerintah yang mencakup prosedur dan artefak negosiasi kontrak dengan CSP (RFP, SLA, dll.),
4. Menangani akreditasi dan sertifikasi CSP yang akan menawarkan layanannya ke Pemerintah,

Gambar 23. Rekomendasi Struktur Otoritas NG-Cloud



Sumber: Wantiknas

5. Merancang prosedur dukungan dan pemeliharaan cloud pemerintah,
6. Menjaga hubungan prosedural antara CSP sebagai penyedia layanan dan IPPD yang berpartisipasi, dan
7. Melacak kemajuan adopsi *cloud* dan membuat dasbor kemajuan nasional dalam pemanfaatan teknologi komputasi awan.

- **Divisi Operasional**

Divisi ini memiliki tugas dan tanggung jawab untuk:

1. Menyusun prosedur dan implementasi penerapan solusi *cloud* pemerintah,
2. Mengelola proses *scaling up/down cloud* secara Nasional sesuai dengan kebutuhan,
3. Melaksanakan dukungan utama untuk IPPD yang mengadopsi *cloud* melalui NG-Cloud, dan
4. Melakukan manajemen operasional seperti, mengelola ketersediaan sistem, pemantauan dan penyetelan kinerja *cloud*, keamanan *cloud*, dll.

Outcome:

- *Pembentukan Otoritas Tata Kelola NG-Cloud*

NG-Cloud Ecosystem

Cloud Ecosystem atau Ekosistem Cloud di pemerintahan merupakan penggambaran lingkungan keseluruhan yang terdiri dari unsur internal dan eskternal yang bekerja sama untuk meluncurkan layanan NG-Cloud. Teknologi komputasi awan tidak seperti beberapa teknologi lainnya, tetapi sebuah teknologi transformasional yang membutuhkan ekosistem untuk dikembangkan sesuai dengan kebutuhan organisasi. Khususnya bagi pemerintah Indonesia dimana ekosistem NG-Cloud sangat dibutuhkan untuk mendukung sistem pemerintahan berbasis elektronik demi terwujudnya akselerasi transformasi digital pemerintah. Maka dari itu, ekosistem yang baik sangat penting untuk keberhasilan implementasi strategi NG-Cloud di pemerintahan. NG-Cloud Ecosystem memiliki 2 (dua) strategi yang tercantum di bawah ini:

1. Menciptakan Lingkungan Terpercaya (*Trusted Environment*) dalam Adopsi *Cloud*.
2. Mendorong Pengembangan Kapasitas SDM *Cloud* (*Capacity Building*)

Strategi 1. Menciptakan Lingkungan Terpercaya (*Trusted Environment*) dalam Adopsi *Cloud*

Inisiatif:

1. **Mengelola risiko dari pemanfaatan *cloud* di Pemerintahan dalam upaya memastikan sistem dan data yang dimigrasi ke *cloud* tidak menimbulkan risiko yang baru dan tidak teridentifikasi bagi IPPD.**

Deskripsi:

Pada umumnya, pemerintah dapat mengatasi risiko ketika mereka memiliki kontrol yang besar atas proses dan peralatan yang terlibat. Tingkat kontrol yang tinggi memungkinkan pemerintah untuk mempertimbangkan alternatif, menetapkan prioritas, dan bertindak tegas demi kepentingan terbaik mereka ketika menghadapi suatu insiden. Demi terwujudnya keberhasilan adopsi *cloud* untuk mendukung sistem pemerintahan

berbasis elektronik, pemerintah perlu memahami dengan jelas karakteristik cloud secara spesifik, komponen arsitektur untuk setiap jenis layanan dan model deployment cloud, serta peran NG-Cloud dalam membangun sebuah ekosistem cloud yang aman.

Dewan TIK Nasional mengusulkan sebuah Kerangka Kerja Manajemen Risiko *Cloud* berdasarkan standar internasional seperti yang mengacu pada NIST [28] dan diharapkan mampu diterapkan ke ekosistem NG-Cloud. Kerangka kerja ini dapat digunakan untuk mengatasi risiko keamanan yang terkait dengan adopsi *cloud* di pemerintahan dengan memasukkan hasilnya ke dalam syarat dan ketentuan kontrak dengan CSP. Kerangka Kerja Manajemen Risiko yang diterapkan pada ekosistem NG-Cloud sebagai bagian dari pengelolaan risiko *cloud* diilustrasikan pada Gambar 24. Terdapat juga beberapa langkah yang perlu dilakukan pemerintah di dalam kerangka kerja ini.

Outcome:

- *Penetapan Metodologi untuk Cloud Risk Assessment*
- *Penetapan Rencana Penanganan Risiko atau Risk Treatment*
- *Pelaksanaan Kontrol Risiko dari Adopsi Cloud*

2. Membentuk dan menyelaraskan klasifikasi data dengan solusi enkripsi terdepan untuk menjaga kerahasiaan, kemudahan akses, dan integritas data di sektor pemerintahan.

Deskripsi:

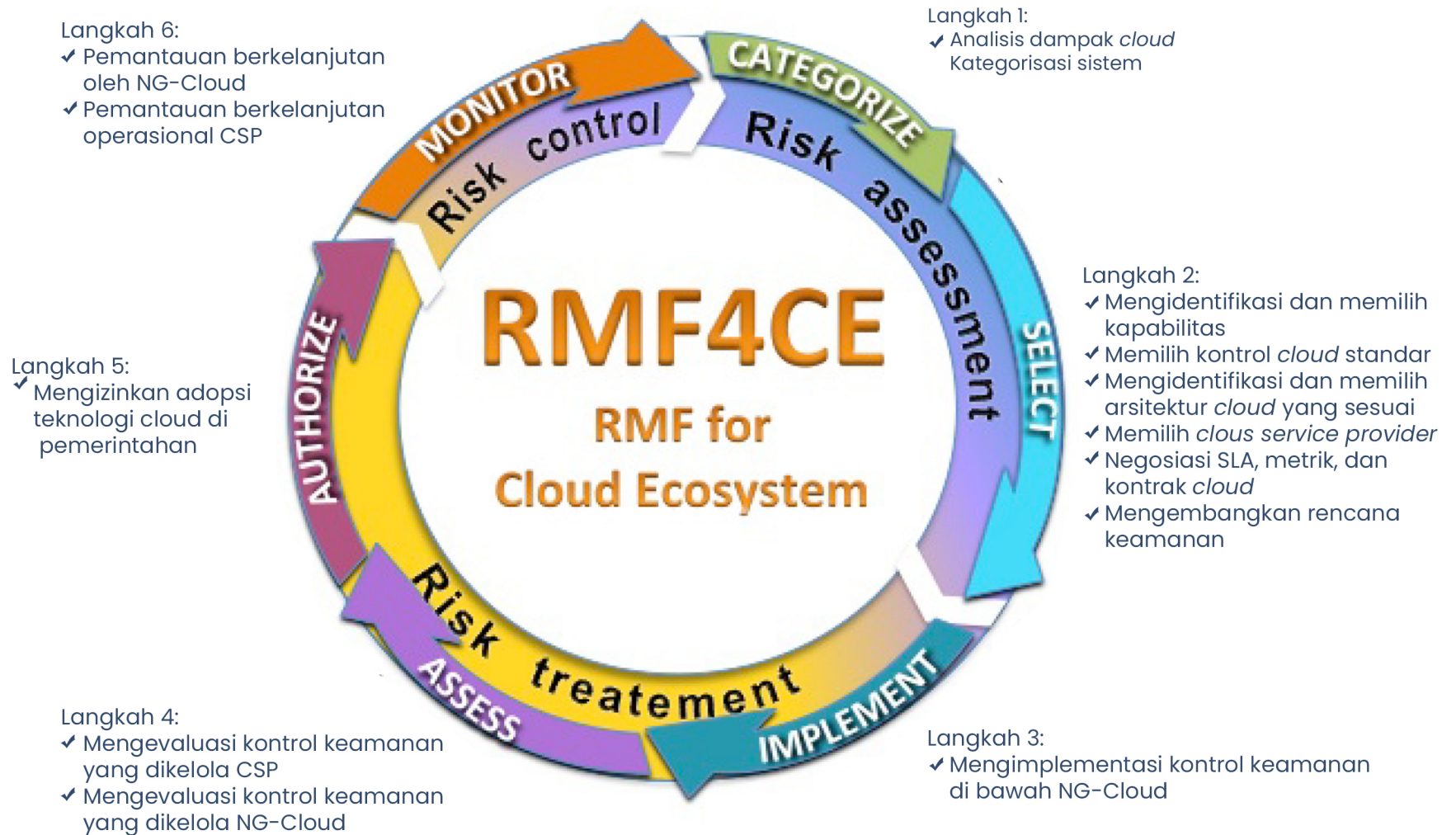
Kerangka klasifikasi data sangat penting bagi pemerintahan saat mereka melakukan migrasi ke *cloud*. Hal ini memungkinkan pemerintah untuk memahami lebih baik bagaimana data harus diklasifikasikan dan perlindungan privasi, serta keamanan yang perlu diterapkan untuk memastikan bahwa data tersebut aman. Proses klasifikasi data menghasilkan berbagai kategori data berdasarkan penilaian risiko yang diterapkan. Penilaian risiko tersebut juga harus mempertimbangkan data rahasia mana yang tidak dapat disimpan di *public cloud* karena peraturan yang ada di dalam negeri.

Kerangka klasifikasi data yang jelas sangat penting untuk memastikan bahwa manfaat penting dari komputasi awan dicapai dengan biaya yang efektif. Hal ini memungkinkan pemerintah untuk lebih memahami jenis data apa yang dapat disimpan pada setiap jenis model *cloud*. Untuk tingkat sensitivitas untuk kerangka klasifikasi data akan dikendalikan oleh perlindungan privasi dan keamanan tertentu. Berdasarkan hasil FGD eksternal yang dilakukan oleh Dewan TIK Nasional, berikut diusulkan kerangka klasifikasi data [29] dalam upaya mendukung ekosistem NG-Cloud:

1. Data Strategis (*Secret*)

- Jenis data ini dipertimbangkan sebagai data pemerintah yang sangat sensitif. Biasanya berupa Data Resmi Pemerintah yang diklasifikasikan sebagai "Sangat Rahasia" atau "Rahasia" dan memerlukan perlindungan privasi dan keamanan tambahan.
- Jenis data ini harus disimpan dan diproses di *cloud* bila diperlukan, tetapi memerlukan solusi yang dianggap sesuai untuk informasi keamanan nasional, termasuk opsi *private cloud* (seperti menggunakan PDN).
- Contoh dari data rahasia yaitu informasi penegakan hukum dan informasi intelijen pemerintah.

Gambar 24. Usulan Kerangka Kerja Manajemen Risiko untuk NG-Cloud



Sumber: NIST [28] – telah diolah kembali

2. Data Risiko Tinggi (*Official*)

- *Examples of high risk data include biometrics data and medical records.*
- Data berisiko tinggi (Data Pemerintah dan Warga Negara): Jenis data ini terkait dengan orang perorangan, dan mencakup Informasi Identifikasi Pribadi.
- Di Indonesia Informasi Identifikasi Pribadi meliputi nama, alamat, nomor rekening, alamat email, nomor paspor, nomor telepon, nomor identitas, serta data kesehatan fisik atau kondisi subjek data.
- Data ini diklasifikasikan sebagai data sensitif karena hilangnya kerahasiaan, integritas, atau ketersediaan data dapat berdampak buruk pada subjek data atau entitas terkait.
- Data ini harus dipindahkan ke solusi *cloud* yang memenuhi kebijakan dan persyaratan hukum untuk sensitivitas data, termasuk enkripsi data saat disimpan dan disebar, autentikasi pengguna yang kuat, dan pelatihan keamanan informasi untuk individu yang memiliki akses ke sistem tempat data berada.
- Contoh data risiko tinggi meliputi data biometrik dan rekam medis.

3. Data Risiko Sedang ke Rendah (*Unclassified*)

- Risiko Sedang (Proses Bisnis Rutin Pemerintah Rutin): Informasi ini dapat disimpan dengan aman di *public cloud*. Diusulkan agar kebijakan internal IPPD diterapkan untuk memastikan keamanan data, seperti meninjau data yang ada untuk melihat apakah akan dikategorikan seperti ini. Setidaknya ini harus mencakup pelatihan kesadaran keamanan informasi untuk pegawai, serta enkripsi data saat disimpan dan disebar. Contoh data risiko sedang yaitu email pemerintah, intranet pemerintah, dan otomatisasi kantor.
- Risiko berisiko rendah ini bersifat terbuka, tersedia, dan dapat diakses oleh publik. Kategori tersebut mencakup data yang dianggap tidak sensitif atau rahasia. Ini adalah jenis data terbesar yang dipegang oleh pemerintah dan harus tersedia untuk bermigrasi ke *public cloud*. Contoh data dengan risiko rendah termasuk situs web pemerintah, laporan tahunan, informasi anggaran, dan data terbuka lainnya.

Outcome:

- *Penerapan Klasifikasi Data pada Adopsi Cloud*

3. Merancang dan menetapkan *framework* keamanan *cloud* dalam upaya mendorong langkah-langkah keamanan untuk pemanfaatan *cloud* di sektor pemerintahan.

Deskripsi:

Framework keamanan *cloud* dapat membantu pemerintah memulai atau meningkatkan program keamanan siber mereka dalam rangka pemanfaatan teknologi komputasi awan. Hal ini mendorong komunikasi di antara *stakeholder* internal dan eksternal tentang keamanan siber, dan untuk perintahan secara nasional. Penetapan *framework* ini juga menjadi salah satu upaya yang perlu dilakukan NG-Cloud untuk menetapkan langkah-langkah keamanan dari adopsi *cloud* (*private cloud* berupa PDN atau *public cloud* dari CSP) yang nantinya dilaksanakan oleh IPPD.

Dewan TIK Nasional mengusulkan untuk merancang dan menetapkan *framework* keamanan *cloud* yang dapat mengacu pada standar internasional seperti ISO dan NIST, sehingga nantinya dapat digunakan oleh NG-Cloud. Ke depannya diharapkan melalui *framework* keamanan *cloud* ini terdapat fungsi-fungsi keamanan yang bila dapat dikelola dengan baik akan memberikan pandangan komprehensif tentang siklus hidup mengelola keamanan siber untuk adopsi *cloud* di instansi pemerintah dari waktu ke waktu.

Outcome:

- *Penetapan Framework Keamanan Cloud*

4. Melaksanakan Akreditasi *Cloud Service Provider* yang memenuhi kualifikasi untuk menjamin keamanan dan keandalan yang ditawarkan CSP serta mempermudah pengadaan *cloud* bagi pemerintah.

Deskripsi:

Dewan TIK Nasional mengusulkan pemerintah melalui NG-Cloud untuk menggunakan sistem akreditasi *cloud* yang diakui secara nasional dan internasional untuk mengevaluasi CSP. Proses akreditasi ini perlu mencakup persyaratan keamanan dasar untuk memastikan tingkat keandalan layanan *cloud* dari CSP dan untuk memastikan bahwa CSP memiliki *platform* yang aman dan terkendali. Selain itu, CSP yang memenuhi syarat juga perlu diminta untuk mematuhi standar keamanan yang ditetapkan nantinya serta memerlukan audit rutin yang sesuai dengan sensitivitas informasi yang diproses oleh CSP.

Outcome:

- *Penetapan Cloud Service Provider yang terakreditasi*
- *Penetapan perjanjian dengan Cloud Service Provider yang terakreditasi*

Strategi 2. Mendorong Pengembangan Kapasitas SDM *Cloud* (*Capacity Building*)

Inisiatif:

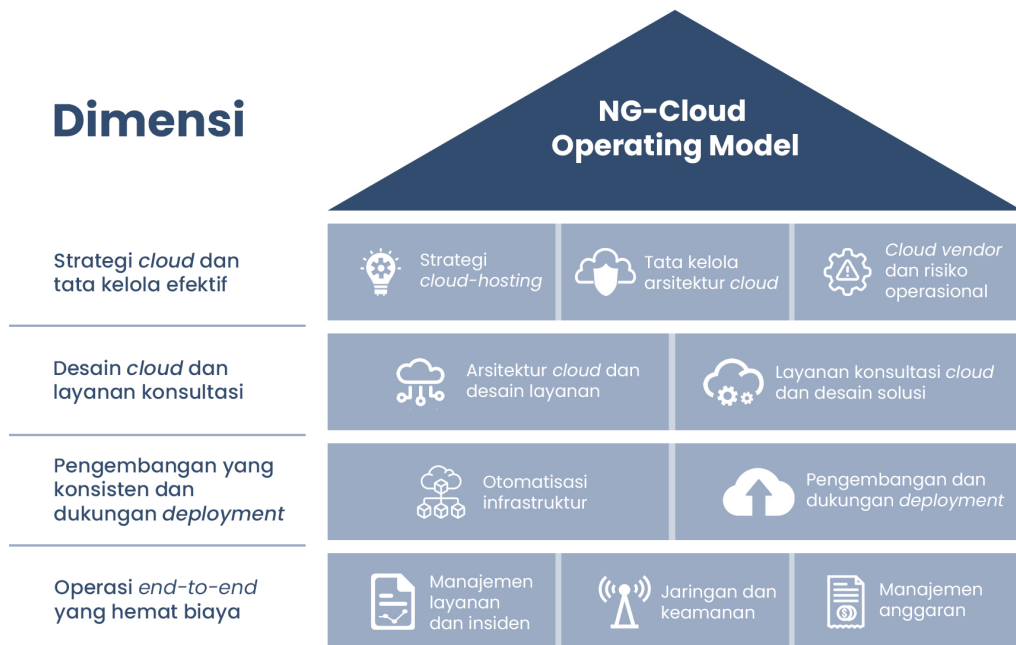
1. Mengembangkan kompetensi SDM TI pemerintah dalam rangka penyelenggaraan NG-Cloud melalui pelatihan/sertifikasi nasional/internasional sehingga mampu mendukung penyelenggaraan layanan digital pemerintah dengan teknologi *cloud*

Deskripsi:

Salah satu keberhasilan adopsi *cloud* di pemerintahan akan bergantung pada ketersediaan dan pengembangan SDM TI. Adopsi *cloud* memerlukan SDM dengan pelatihan dan pengalaman yang diperlukan dalam teknologi *cloud*, dan memiliki keahlian yang berbeda untuk memastikan migrasi yang berhasil di *cloud*. Khususnya untuk PDN yang nantinya akan diusulkan masuk ke dalam ekosistem NG-Cloud, Dewan TIK Nasional merekomendasikan pemerintah untuk dapat menyediakan dan mengembangkan kompetensi SDM di bidang *cloud*. Beberapa bidang keterampilan

yang diperlukan antara lain arsitek sistem *cloud*, pakar keamanan dan privasi data, analis data, perancang/pengembang aplikasi *cloud*, dan administrator untuk mengelola beban kerja *cloud*. Di samping itu, ke depannya NG-Cloud juga perlu berfokus pada keterampilan baru yang diperlukan untuk mendukung operasi *cloud* di PDN.

Gambar 25. Usulan Kompetensi untuk NG-Cloud



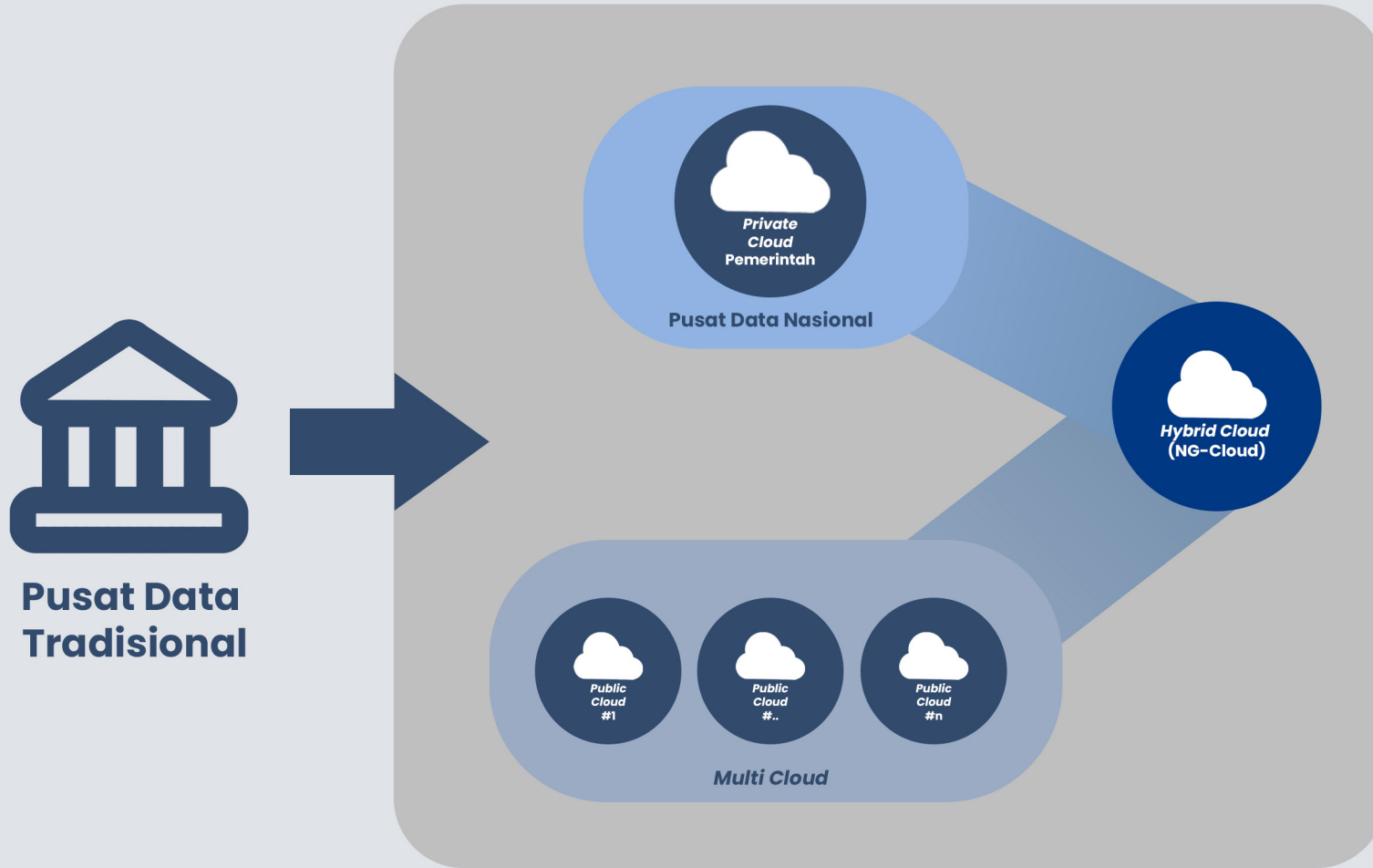
Sumber: [31] – telah diolah kembali

Pengelolaan *cloud* secara Nasional yang berhasil melalui NG-Cloud akan bergantung pada kemampuan dan pengembangan kompetensi SDM. NG-Cloud perlu bekerja pada perumusan dan implementasi kebijakan yang diperlukan untuk melatih individu SDM dalam pengelolaan komputasi awan. Kebutuhan kompetensi SDM dalam pengelolaan komputasi awan dapat mengacu pada Peta Okupasi yang telah dirancang oleh Kementerian Kominfo [30] dalam kerangka Kerangka Kualifikasi Nasional Indonesia (KKNI) bidang TIK. Selain itu, kami juga mengusulkan kerangka kompetensi untuk NG-Cloud yang diadaptasi dari [31] dalam rangka tersedianya keahlian di bidang *cloud* yang komprehensif (lihat Gambar 25).

Pelatihan/sertifikasi yang nantinya diturunkan berdasarkan kebijakan yang berlaku dapat dielaborasi dengan jenis-jenis kompetensi di bidang *cloud* pada Peta Okupasi [30]. Hal ini perlu dilakukan untuk memastikan SDM TI di dalam otoritas NG-Cloud dapat mengembangkan keterampilan dan kompetensi yang ditingkatkan di bidang-bidang berikut antara lain:

1. **Pengembangan Cloud Pemerintah**, untuk lebih memahami layanan dan peluang adopsi *cloud* IPPD di unit/departemen mereka dan di seluruh pemerintahan secara Nasional. Contoh okupasinya yaitu pengembang *cloud computing* dan arsitek *cloud computing*.

Gambar 26. Usulan Model Layanan *Cloud* di Pemerintahan



Sumber: Wantiknas

2. **Kapasitas Analitis**, untuk mengevaluasi berbagai pilihan dalam pemberian layanan *cloud* berdasarkan berbagai kriteria. Contoh okupasinya yaitu *cloud computer analyst*.
3. **Operasional Cloud**, misalnya mengevaluasi, menegosiasikan, memantau dan menegakkan kontrak serta *Service Level Agreement (SLA)* untuk memastikan bahwa pemerintah menerima *value* dan manfaat penuh dari adopsi *cloud* berdasarkan kontrak atau perjanjian. Contoh okupasinya yaitu insinyur *cloud computing*.
4. **Teknis Cloud**, untuk melihat peluang teknologi baru yang disesuaikan dengan area yang sedang berkembang seperti arsitektur dan penerapan solusi ke *cloud* di pemerintahan. Beberapa contoh okupasinya yaitu ahli *cloud computing*, *cloud applications manager*, dan keamanan *cloud computing*.

Outcome:

- *Penyelenggaraan program pelatihan cloud untuk SDM TI pengelola cloud pemerintah pada Pusat Data Nasional (PDN)*
- *Penyelenggaraan peningkatan kompetensi SDM TI di internal Otoritas NG-Cloud*

NG-Cloud Deployment

Fokus dari dimensi ini yaitu untuk membangun serangkaian inisiatif penting untuk merancang dan menerapkan NG-Cloud guna mendukung sistem pemerintahan berbasis elektronik di seluruh IPPD. Pemerintah perlu mengidentifikasi dan memberikan persyaratan untuk layanan umum sebagai penawaran SaaS/PaaS melalui NG-Cloud. Dewan TIK Nasional merekomendasikan NG-Cloud untuk mencakup teknologi *cloud* multivendor. Hal ini terdiri dari dua model *deployment* dasar:

Private Cloud Pemerintah

Cloud ini dimiliki oleh pemerintah melalui Pusat Data Nasional (PDN), menyediakan infrastruktur *cloud* untuk pemerintah dan pada dasarnya memiliki jaminan layanan tinggi, sedang, dan rendah yang mencakup keamanan dan ketersediaan *cloud*.

Public Cloud

Melakukan pemanfaatan *public cloud* yang tersedia secara komersial untuk mendapatkan manfaat dari biaya sumber daya komputasi yang lebih rendah. Model ini hanya dapat digunakan untuk layanan *cloud* jaminan rendah.

Saat Pemerintah nantinya melakukan transisi dari sistem infrastruktur TI lama untuk penyimpanan dan pemrosesan data, NG-Cloud nantinya akan merekomendasikan pemerintah untuk dapat memilih untuk menggunakan *private cloud*/PDN, *public cloud*, model *multi-cloud*, atau solusi *hybrid cloud* yang menggabungkan dan menghubungkan dua jenis layanan *cloud* yang berbeda (lihat Gambar 25). Walaupun demikian, NG-Cloud Board tetap perlu mempertimbangkan beberapa persyaratan dan aturan yang ada sebelum IPPD menentukan model layanan *cloud* yang akan dipilih. NG-Cloud Deployment memiliki 3 (tiga) strategi yang tercantum di bawah ini:

1. Melakukan Pengembangan Arsitektur NG-Cloud.
2. Konsolidasi NG-Cloud dan PDN.
3. Melaksanakan Pengembangan Program Percepatan NG-Cloud

Strategi 1. Melakukan Pengembangan Arsitektur NG-Cloud

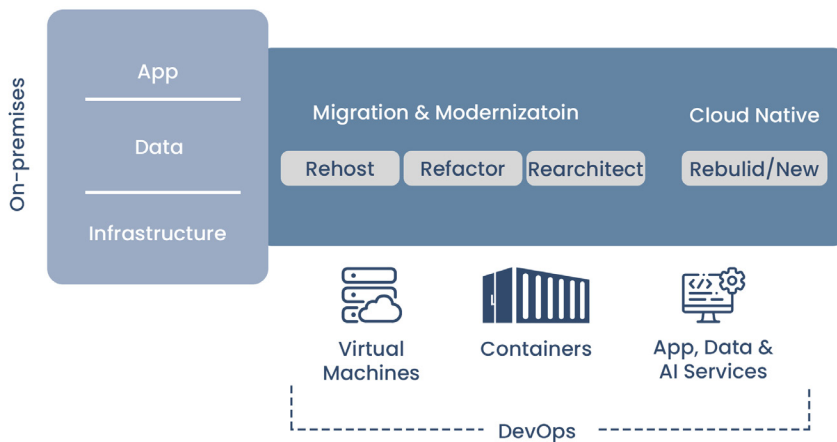
Inisiatif:

1. Memfokuskan aktivitas dan pengembangan arsitektur NG-Cloud dengan solusi *Cloud Native Architecture* agar terciptanya optimasi transisi *legacy system* dan inovasi sistem baru yang bersifat “*Ready to Cloud*”

Deskripsi:

NG-Cloud yang akan dibangun ke depannya perlu disesuaikan dengan rekomendasi tata kelola *cloud* secara nasional, yaitu bagaimana NG-Cloud memiliki kemampuan untuk ekspansi di masa mendatang. Perluasan adopsi dapat dilakukan dengan menambahkan sumber daya fisik tambahan atau melalui integrasi dengan layanan *cloud* lainnya. NG-Cloud memerlukan gabungan fasilitas yang memungkinkan pemantauan manajemen atas layanan dan penggunaannya. Selain itu, Dewan TIK Nasional mengusulkan bagaimana ke depannya seluruh sistem yang ada dapat mengarah ke solusi *cloud native* yang tentunya dapat dikoordinasi oleh NG-Cloud. Hal ini berlaku pada aplikasi yang akan dilakukan transisi/migrasi dan sistem baru yang bersifat *cloud native* (lihat Gambar 27).

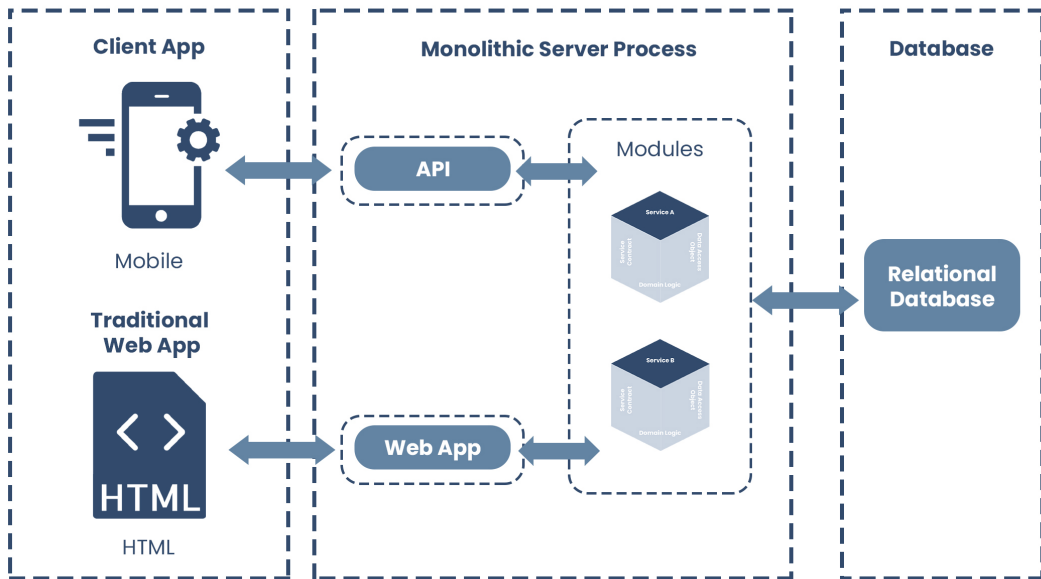
Gambar 27. Komponen Menuju Solusi *Cloud Native*



Sumber: [32] – telah diolah kembali

Aplikasi *cloud native* dirancang, dikembangkan, dan dikelola dengan cara yang konsisten pada lingkungan *cloud* tempat aplikasi tersebut akan dijalankan. Berbeda dari aplikasi tradisional, *cloud native* dikembangkan menggunakan praktik DevOps, desain arsitektur *microservices* yang memanfaatkan *platform* PaaS dan integrasi API di seluruh ekosistem yang lebih luas [32], sehingga diharapkan arsitektur ini diterapkan ke dalam ekosistem NG-Cloud. Selain itu, diperlukan juga dukungan infrastruktur untuk mendukung aplikasi *cloud native* dalam rangka penerapan arsitektur *cloud native* oleh NG-Cloud. Infrastruktur yang diperlukan harus memiliki kemampuan redundansi dan *failover* untuk mencegah gangguan layanan dan ketersediaan aplikasi, serta menunjang otomatisasi tingkat tinggi.

Gambar 28. Arsitektur *Cloud Native* menggunakan *Microservices*



Sumber: Wantiknas – diolah kembali dari [33]

Berkaitan dengan aplikasi yang digunakan di pemerintahan, terdapat aplikasi umum dan khusus dengan fungsi sebagai administrasi pemerintahan (G2G, G2E) dan pelayanan publik (G2B, G2C). Perlunya aplikasi-aplikasi ini dikembangkan dengan konsep *cloud native* untuk mendorong standarisasi layanan pemerintah yang bersifat nasional. Solusi *cloud native architecture* secara umum menggunakan desain *microservices* yang diilustrasikan pada Gambar 28.

Dengan penerapan *cloud native architecture*, Pemerintah diharapkan mampu meningkatkan kecepatan, kelincahan, dan inovasi dalam memberikan layanannya sambil juga mendapatkan akses ke kemampuan lebih luas yang sangat diperlukan. Dengan peningkatan kecepatan layanan yang diberikan melalui sistem pemerintahan berbasis elektronik juga diimbangi dengan solusi yang lebih inovatif. Tata kelola TI menjadi lebih agile, merespons kebutuhan layanan digital lebih cepat melalui pendekatan agile dan DevOps.

Outcome:

- *Penetapan Model NG-Cloud Arsitektur*
- *Penetapan Solusi Cloud Native untuk NG-Cloud Arsitektur*

2. Merancang dan menetapkan NG-Cloud *procurement framework* (kerangka kerja pengadaan) yang mengacu pada *best practices* atau *lesson learned* negara lain sehingga menciptakan integrasi layanan dan efisiensi biaya *cloud*.

Deskripsi:

Pengadaan pemerintah merupakan aspek yang sangat krusial untuk penerapan dan pengembangan komputasi awan. Praktik pembelian TI secara tradisional dan persyaratan kontrak dapat menghambat sifat komputasi awan yang skalabel, hemat biaya, dan inovatif. Pengadaan *cloud* di IPPD memberikan peluang untuk mengevaluasi kembali strategi pengadaan yang ada termasuk kerangka kerja pengadaan NG-Cloud untuk menciptakan proses pengadaan yang fleksibel yang memungkinkan IPPD untuk mengambil manfaat penuh dari *cloud*. Dewan TIK Nasional mendorong untuk menetapkan NG-Cloud *procurement framework* sebagai acuan IPPD yang akan melaksanakan pengadaan *cloud* dan agar dapat selaras secara Nasional. Beberapa hal yang perlu menjadi fokus NG-Cloud dalam pengadaan *cloud* di pemerintahan, antara lain

1. Pengembangan berkelanjutan untuk kontrak *cloud* NG-Cloud
Membangun kontrak yang telah dinegosiasikan untuk menyederhanakan pengadaan *cloud*. Katalog layanan *cloud* dengan panduan pembelian harus dibuat untuk menginformasikan IPPD tentang layanan yang tersedia.
2. Pengembangan unit pengadaan *cloud* di dalam NG-Cloud
Hal ini berhubungan dengan tugas dari NG-Cloud untuk menyediakan layanan *cloud*, konsultasi *cloud*, dan layanan implementasi *cloud*. Ini akan memungkinkan NG-Cloud untuk bermitra dengan CSP yang terdaftar dan terakreditasi untuk bekerja dengan tiap IPPD.

Selain itu, berdasarkan [15] Pemerintah yang nantinya diwakili oleh NG-Cloud perlu mempertimbangkan faktor-faktor berikut saat menetapkan *framework* pengadaan layanan *cloud*:

1. *Value for money* untuk memenuhi tujuan layanan yang dimaksudkan;
2. Transisi dari anggaran modal (*Capex*) ke belanja operasional (*Opex*);
3. Dampak jangka pendek, menengah dan panjang pada keuangan;
4. Kesesuaian *service level agreements* dalam kaitannya dengan kebutuhan khusus IPPD;
5. Paket *cloud* dan langganan;
6. Menghindari adanya “*vendor lock-in*,” dan
7. Persaingan pasar.

Dengan adanya NG-Cloud *procurement framework* tidak terlepas dari diperlukannya *Service Level Agreements* (SLA) untuk memastikan persyaratan yang disepakati untuk penyediaan layanan komputasi awan yang dapat diandalkan. Perlunya NG-Cloud dan CSP untuk menyetujui SLA (semisal kinerja dan ketersediaan) layanan *cloud* apa yang ditawarkan. Penerapan syarat dan ketentuan di dalam SLA untuk adopsi *cloud* pemerintahan harus sesuai dengan standar internasional yang akan membantu memperkuat kepercayaan Pemerintah terhadap layanan *cloud*.

Gambar 29. Fase Migrasi Aplikasi ke *Cloud*



Sumber: [34] - telah diolah kembali Wantiknas

Pada akhirnya Dewan TIK Nasional mengusulkan adanya inisiatif yang diperlukan bagi NG-Cloud untuk dapat memberikan panduan dan kerangka kerja bagi IPPD terkait dengan cara pengadaan *cloud*.

Outcome:

- *Penetapan NG-Cloud Framework Procurement*

3. Menyusun rencana migrasi cloud di sektor pemerintahan sebagai bagian dari pengembangan aplikasi SPBE dengan penerapan teknologi *cloud computing* sesuai dengan arah kebijakan SPBE Nasional.

Deskripsi:

Ruang lingkup dan cakupan yang luas dari transformasi digital di pemerintahan dengan penerapan *cloud* akan membutuhkan perubahan yang berarti dalam cara IPPD memandang TI. IPPD yang sebelumnya menganggap TI sebagai investasi dalam aplikasi, server, dan jaringan secara di tempat atau *on-premise* tetapi ke depannya perlu memandang TI dalam hal layanan yang diberikan. Selain itu pentingnya sumber daya komputasi yang *scalable* yang bertujuan membuat sumber daya komputasi dapat diakses sesuai dengan permintaan dan dengan biaya yang sesuai dengan kualitas layanan berdasarkan ketentuan dalam SLA layanan *cloud*. Hal ini tentunya akan berdampak bagaimana pemerintah akan melakukan migrasi aplikasi SPBE dengan penerapan teknologi komputasi awan. Dewan TIK Nasional mengusulkan bahwa migrasi aplikasi-aplikasi tersebut bisa dimulai berdasarkan prioritas. Secara umum, komponen penting untuk migrasi aplikasi ke *cloud* ditunjukkan pada Gambar 29.

Selain perlunya membangun aplikasi *cloud native* untuk mengganti sistem lama demi mendukung penerapan *cloud native architecture* di masa mendatang, pemerintah juga perlu menyusun rencana migrasi *cloud* terhadap sistem lama yang ingin dilakukan transisi ke sistem dengan teknologi *cloud*.

Pada waktunya, NG-Cloud perlu memberikan menetapkan metodologi dan strategi migrasi kepada IPPD mengenai tahapan dan persiapan migrasi sistem ke *cloud*. Dewan TIK Nasional mengusulkan *framework* untuk merencanakan migrasi *cloud* agar dapat memberikan perspektif strategis bagi IPPD (lihat Gambar 30).

NG-Cloud perlu mempertimbangkan portofolio TI yang ada di beberapa sektor yang dikelola oleh IPPD secara menyeluruh dan membuat *roadmap* untuk penyebaran dan migrasi *cloud*. *Roadmap* migrasi *cloud* ini harus memprioritaskan layanan yang memiliki nilai harapan tinggi dan kesiapan tinggi untuk memaksimalkan manfaat yang diterima dan meminimalkan risiko. *Roadmap* migrasi *cloud* selanjutnya akan menentukan dengan tepat layanan mana yang akan menggunakan *cloud* sebagai fase inisiasi dari *roadmap*.

Gambar 30. *Framework* untuk migrasi cloud di Pemerintahan



Sumber: [15] [35] – telah diolah kembali oleh Wantiknas

Outcome:

- *Penetapan metodologi untuk migrasi ke cloud*
- *Daftar target layanan dan aplikasi yang diprioritaskan ke cloud*

Strategi 2. Konsolidasi NG-Cloud dan PDN

Inisiatif:

1. **Mendayagunakan ekosistem Pusat Data Nasional (PDN) yang berkolaborasi dengan *cloud service provider* lokal dan global agar terwujudnya integrasi dan *sharing resources* Sistem Pemerintahan Berbasis Elektronik**

Deskripsi:

Pusat Data Nasional merupakan salah satu infrastruktur strategis pemerintah di bidang TIK dapat menjadi aset vital bagi terselenggaranya layanan sistem pemerintahan berbasis elektronik. Karena Pusat Data Nasional (PDN) adalah bagian dari infrastruktur SPBE, maka ekosistemnya perlu dimanfaatkan dengan baik. PDN yang dibangun nantinya akan berbasis *cloud* [36]. Dengan begitu, Dewan TIK Nasional mengusulkan untuk menggabungkan ekosistem PDN sebagai *private cloud* milik pemerintah dengan pemanfaatan *public cloud* dari CSP yang pada akhirnya bermuara dan dikoordinasikan oleh NG-Cloud.

Outcome:

- *Infrastruktur PDN yang mampu untuk adopsi *cloud computing* yang terkonsolidasi*
- *Integrasi *cloud* dengan inisiatif infrastruktur NG-Cloud*

Strategi 3. Melaksanakan Pengembangan Program Percepatan NG-Cloud

Inisiatif:

1. **Membentuk *pilot project* pembangunan dan penerapan NG-Cloud untuk memahami dan membuktikan *value* dari adopsi *cloud computing* agar dapat lebih menyempurnakan solusi NG-Cloud sebelum diluncurkan.**

Deskripsi:

Inisiatif ini berguna dalam membentuk fondasi untuk membangun dan menyebarkan NG-Cloud. Dewan TIK Nasional mengusulkan otoritas NG-Cloud untuk bertanggung jawab dalam membentuk *pilot project* pembangunan dan penerapan NG-Cloud dengan menargetkan pelaksanaan pada sektor yang akan dipilih. Hal ini dapat memperoleh pengalaman yang nyata dalam adopsi *cloud* serta sebagai percontohan sehingga diharapkan terciptanya adopsi *cloud* di semua sektor. Beberapa hal-hal yang perlu diperhatikan dalam membentuk *pilot project* ini antara lain:

1. Kesiapan Pemerintah di sektor TIK (khususnya tata kelola *cloud*) untuk menyebarkan solusi dan menyediakan dukungan *pilot project* adopsi *cloud* pada sektor yang dipilih;

2. Penilaian kebutuhan dari sektor yang dipilih untuk layanan yang ditransisikan ke *cloud*;
3. Identifikasi persyaratan pengembangan kapasitas komputasi awan pada sektor yang dipilih;
4. Penilaian segmen pasar *cloud* yang mencakup permintaan sektor pemerintah dan penawaran *cloud* dari CSP secara keseluruhan; dan
5. Penyempurnaan parameter layanan *cloud* yang meliputi syarat dan ketentuan, harga, serta ketersediaan.

Tujuan dari dibentuknya *pilot project* ini adalah untuk menguji, memahami, dan membuktikan implikasi transisi di pemerintahan ke solusi berbasis *cloud* dalam rangka penyempurnaan solusi NG-Cloud yang diusulkan. Pertimbangan lainnya dalam membentuk *pilot project* ini adalah kemudahan transisi dari sektor yang dipilih ke lingkungan komputasi awan. Hal ini berguna untuk menguji coba migrasi *cloud* pada layanan yang lebih mudah dimigrasikan, sehingga keberhasilan yang cepat mendorong pemerintah untuk melaksanakan migrasi *cloud* yang lebih besar di sektor lainnya.

Outcome:

- *NG-Cloud yang beroperasi dalam koordinasi dengan beberapa IPPD*
- *Penyediaan layanan cloud melalui lebih dari satu cloud (hybrid cloud) terintegrasi di bawah satu manajemen NG-Cloud*

1. Melaksanakan sosialisasi dan publikasi pemanfaatan *cloud* di sektor pemerintahan untuk meningkatkan partisipasi dan pengetahuan mengenai adopsi teknologi *cloud* di instansi pusat maupun daerah.

Deskripsi:

Membangun kesadaran atau *awareness* dari manfaat teknologi yang bisa diperoleh di sektor pemerintahan sangatlah penting. Khususnya untuk membangun *awareness* dari manfaat adopsi *cloud* bagi *stakeholder* di pemerintahan yang dimulai dari level tertinggi hingga bawah. Dewan TIK Nasional mengusulkan bahwa otoritas NG-Cloud juga perlu berperan aktif untuk melakukan sosialisasi ke seluruh IPPD untuk meningkatkan pengetahuan dan *awareness* dari manfaat adopsi *cloud* bisa diselaraskan secara Nasional. Secara spesifik, sosialisasi ini dapat diintegrasikan dengan bagaimana adopsi *cloud* ke depannya dapat mendukung sistem pemerintahan berbasis elektronik yang telah menjadi amanah Peraturan Presiden Nomor 95 Tahun 2018 tentang SPBE.

Berhubungan dengan inisiatif *pilot project* sebelumnya, kegiatan publikasi juga perlu dilakukan oleh NG-Cloud sebagai bagian dari menyosialisasikan pemanfaatan *cloud* di pemerintahan. Publikasi ini untuk memperlihatkan keberhasilan adopsi *cloud* yang diinisiasi di sektor yang dipilih, sehingga ke depannya dapat meningkatkan partisipasi dan kepercayaan di sektor-sektor lainnya dalam memanfaatkan *cloud*.

Outcome:

- *Pelaksanaan Workshop Cloud Awareness*
- *Pelaksanaan Kegiatan Publikasi keberhasilan Adopsi Cloud*
- *Pelaksanaan Cloud Awarding Program*

Peta Jalan Implementasi

Peta jalan implementasi ini disusun berdasarkan Kerangka Kerja *National Government Cloud* (NG-Cloud) dengan jangka waktu lima tahun, Peta jalan di bawah ini mewakili inisiatif dan hasil yang diharapkan pada tiap strategi di tiap dimensi (lihat Gambar 31). Dewan TIK Nasional mengusulkan bahwa kegiatan di dalam peta jalan ini dapat dilaksanakan dengan pendekatan paralel.

Gambar 31. Peta Jalan Implementasi NG-Cloud

	Jangka Pendek (0-2) Tahun	Jangka Menengah (2-3) Tahun	Jangka Panjang (3-5) Tahun
<p>Dimensi 1. NG-Cloud Governance</p> <p>Strategi 1 Menyusun <i>Government Cloud First Policy</i></p> <p>Strategi 2 Mengembangkan Kebijakan dan Standar</p> <p>Strategi 3 Membentuk Struktur Model Tata Kelola Cloud</p>	<ul style="list-style-type: none"> ✓ Menyusun dan menetapkan <i>Government Cloud First Policy</i> ✓ Merancang kebijakan <i>procurement</i> (pengadaan) cloud ✓ Merancang kebijakan dan standar keamanan cloud ✓ Membentuk tim <i>ad-hoc</i> dengan fungsi koordinasi tata kelola dan transisi cloud di tingkat Nasional 	<ul style="list-style-type: none"> ✓ Menyusun <i>guideline</i> (pedoman) adopsi teknologi <i>cloud computing</i> di pemerintahan ✓ Membentuk unit/lembaga yang mengoordinasikan tata kelola dan transisi cloud di tingkat Nasional 	
<p>Dimensi 2. NG-Cloud Ecosystem</p> <p>Strategi 1 Menciptakan Lingkungan Terpercaya (<i>Trusted Environment</i>)</p> <p>Strategi 2 Mengembangkan Kapasitas SDM Cloud</p>	<ul style="list-style-type: none"> ✓ Membentuk dan menyelaraskan klasifikasi data dengan solusi enkripsi terdapat ✓ Merancang dan menetapkan <i>framework</i> keamanan cloud ✓ Mengembangkan kompetensi SDM TI pemerintah dalam rangka penyelenggaraan NG-Cloud 	<ul style="list-style-type: none"> ✓ Mengelola risiko dari pemanfaatan cloud di pemerintahan ✓ Melaksanakan akreditasi <i>cloud service provider</i> yang memenuhi kualifikasi untuk penyelenggaraan <i>public cloud</i> 	<ul style="list-style-type: none"> ✓ Menyediakan CSP yang terakreditasi dan terintegrasi oleh NG-Cloud
<p>Dimensi 3. NG-Cloud Deployment</p> <p>Strategi 1 Mengembangkan Arsitektur NG-Cloud</p> <p>Strategi 2 Konsolidasi NG-Cloud dan PDN</p> <p>Strategi 3 Mengembangkan Program Percepatan NG-Cloud</p>		<ul style="list-style-type: none"> ✓ Melakukan aktivitas dan pengembangan arsitektur NG-Cloud dengan solusi <i>Cloud Native Architecture</i> ✓ Merancang dan menetapkan NG-Cloud <i>procurement framework</i> (kerangka kerja pengadaan) ✓ Menyusun rencana migrasi cloud di pemerintahan ✓ Mendayagunakan ekosistem PDN yang berkolaborasi dengan CSP lokal dan global ✓ Membentuk <i>pilot project</i> pembangunan dan penerapan NG-Cloud ✓ Melaksanakan kegiatan sosialisasi dan <i>awareness</i> pemanfaatan cloud di pemerintahan 	<ul style="list-style-type: none"> ✓ Mendorong CSP terakreditasi untuk menawarkan layanan cloud ke sistem pengadaan ✓ Melaksanakan migrasi cloud secara bertahap di tiap sektor ✓ Menyelesaikan konsolidasi PDN dan <i>public cloud</i> dari CSP ✓ Melaksanakan kegiatan publikasi keberhasilan adopsi cloud yang diwakili sektor tertentu

Sumber: Wantiknas

KESIMPULAN

Melihat dari apa yang telah dilakukan Pemerintah di berbagai negara, *cloud computing* mampu mendorong transformasi digital di sektor pelayanan publik. Perubahan teknologi yang cepat telah menciptakan peluang bagi pemerintah untuk mengambil keuntungan dari manfaat *cloud computing* untuk mengurangi biaya pengembangan teknologi lama, mengembangkan proses bisnis yang *agile* dan baru untuk pemerintahan digital, memungkinkan peningkatan kompetensi sumber daya manusia, meningkatkan pelayanan publik, serta kemampuan *recovery* yang cepat di waktu krisis.

Akan tetapi, adopsi *cloud computing* di sektor publik pemerintahan masih memiliki beberapa tantangan, antara lain kebutuhan untuk lebih memahami tata kelola dan karakteristik *cloud computing* bagi penyusunan *cloud first policy* pemerintah dan diperlukan pelaksanaan pelatihan untuk menerapkan perlindungan data dan keamanan *cloud* pemerintah. Selain itu, penyesuaian kebijakan *cloud first* di seluruh pemerintah juga perlu dilakukan, antara lain seperti mekanisme pengadaan *cloud* untuk memungkinkan pemilihan *cloud computing* yang lebih mudah, dan reformasi manajemen sumber daya manusia untuk memastikan bahwa SDM TI yang dipekerjakan siap untuk mendukung penggunaan dan pengelolaan teknologi *cloud* di pemerintahan. Khususnya bagi Pemerintah Indonesia, diperlukan adopsi *cloud* secara menyeluruh yang mendukung kebijakan Transformasi Digital Nasional dan Sistem Pemerintahan Berbasis Elektronik.

Kebijakan *cloud first* yang telah disusun di beberapa negara yang memungkinkan mendukung penggunaan *cloud computing* di sektor publik maupun sektor pemerintahan. Kebijakannya disusun oleh otoritas pusat, sehingga mampu mengatasi kemungkinan fragmentasi pendekatan kebijakan. Hal ini dilakukan untuk mencapai konsistensi yang lebih besar dari persyaratan akuntabilitas dan penerapan standar teknis internasional yang mengatur keamanan informasi, serta memungkinkan interoperabilitas untuk berbagi informasi lintas lembaga atau unit. Selain itu, Dewan TIK Nasional juga mengusulkan suatu Kerangka Strategis National Government Cloud (NG-Cloud) sebagai upaya strategis dalam proses transisi Pemerintah Indonesia menuju ekosistem *cloud* yang selaras dan terintegrasi dengan baik.

PENUTUP

Laporan akhir ini disusun guna memberikan pengetahuan atau *knowledge* terkait pemanfaatan *cloud computing* serta gambaran perbandingan *Government Cloud First Policy* dalam bentuk **Kajian Kebijakan Pengutamaan Komputasi Awan Pemerintah (Government Cloud First Policy)**. Kajian ini disusun dari proses riset dan diskusi dengan pihak eksternal. Kemudian rekomendasi hasil kajian ini dibuat berdasarkan analisis data primer (yang diperoleh dari hasil diskusi dengan eksternal) dan analisis data sekunder (referensi *paper*, jurnal, *report*, dan peraturan pemerintah terkait pemanfaatan *cloud computing*).

Selanjutnya Dewan Teknologi Informasi dan Komunikasi Nasional (Wantiknas) perlu melakukan kegiatan koordinasi dengan pihak-pihak terkait guna mendapatkan *insight* lebih baik yang berkaitan dengan *Government Cloud First Policy* serta bagaimana Pemerintah Indonesia dapat dengan segera menyusun kebijakan *cloud first* ini. Pada akhirnya, melalui kebijakan *Government Cloud First Policy* nantinya diharapkan mampu mendorong adopsi *cloud computing* di layanan publik maupun pemerintahan dalam rangka percepatan Transformasi Digital dan SPBE di instansi pemerintahan di Indonesia.

■ ■ ■

REFERENSI

- [1] B. Zwattendorfer, K. Stranacher, A. Tauber and P. Reichstadter, "Cloud Computing in E-Government across Europe A Comparison," *Technology-Enabled Innovation for Democracy, Government and Governance*, pp. 181-195, 2013.
- [2] R. v. d. Meulen, "Understanding Cloud Adoption in Government," 11 April 2018. [Online]. Available: <https://www.gartner.com/smarterwithgartner/understanding-cloud-adoption-in-government>.
- [3] M. Rimol, "Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly \$500 Billion in 2022," 19 April 2022. [Online]. Available: <https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022>.
- [4] S. Moore, "Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025," 9 Februari 2022. [Online]. Available: <https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending>.
- [5] Digital Development Partnership, "Government Migration to Cloud Ecosystems," *International Development Association of The World Bank*, Washington, 2022.
- [6] A. Gupta, K. kushansh, P. Santhanam, T. Osako, T. Nguyen and V. Rastogi, "Ascent to the Cloud: How Six Key APAC Economies Can Lift-off," *Boston Consulting Group*, Singapura, 2019.
- [7] Department for Digital Transformation and National Cybersecurity Agency, *Italian Cloud Strategy*, *Ministro per l'innovazione tecnologica e la transizione digitale*, 2021.
- [8] Wantiknas, "Langkah Strategis Pusat Data Nasional," *Dewan TIK Nasional*, Jakarta, 2020.
- [9] F. Rahmawati, "Kominfo Bangun 4 Pusat Data Nasional di Indonesia," 27 Juni 2022. [Online]. Available: <https://aptika.kominfo.go.id/2022/06/kominfo-bangun-4-pusat-data-nasional-di-indonesia/>.
- [10] US Government, "Federal Cloud Computing Strategy," *Executive Office of The President of the United States*, 2019.
- [11] UK Government, "Government Cloud First Policy," *Central Digital and Data Office*, 2013.
- [12] Australian Government, "Secure Cloud Strategy," *Digital Transformation Agency*, 2021.
- [13] MCIT, *KSA Cloud First Policy*, *Ministry of Communications and Information Technology of KSA*, 2020.
- [14] DICT, *The Philippine Government Cloud First Policy*, *Quezon City: Department of Information and Communications Technology*, 2017.

- [15] National Information Technology Development Agency, Nigeria Cloud Computing Policy, Nigeria Government, 2019.
- [16] AWS, "Overview of Amazon Web Services," Amazon Web Services, 2022.
- [17] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST Special Publication 800-145, pp. 1-3, 2011.
- [18] K. Nichols and K. Sprague, "How Governments Can Get Ahead in the Cloud," McKinsey, Atlanta, 2012.
- [19] MLGM, Cloud Computing Strategy for Norway, Norwegian Ministry of Local Government and Modernisation, 2016.
- [20] A. Budiyanto, Interviewee, Rapat FGD tentang Cloud First Policy dengan Asosisasi Cloud Computing Indonesia. [Interview]. 22 Juni 2022.
- [21] AWS Cloud Indonesia, Interviewee, Rapat FGD terkait Cloud First Policy dengan AWS Cloud Indonesia. [Interview]. 23 Juni 2022.
- [22] Google Cloud Indonesia, Interviewee, Rapat FGD terkait Cloud First Policy dengan Google Cloud Indonesia. [Interview]. 18 Agustus 2022.
- [23] ITAC, "Governments Embracing Cloud "An Opportunity for Modernization, Innovation, and Transformation"," Information Technology Association of Canada, 2019.
- [24] T. Abell, A. Husar and L. M. Ann, "Cloud Computing as a Key Enabler for Digital Government Across Asia and the Pacific," Asian Development Bank, Manila, 2021.
- [25] AWS Institute, "Cloud First Playbook for Asia Pacific (APAC)," Amazon Web Services, 2019.
- [26] MITT, Pakistan Cloud First Policy, Ministry of Information Technology & Telecommunciation of Pakistan, 2022.
- [27] Germany Government, "Germany's Government Cloud Strategy: Target Architecture Framework," FITKO (Federal IT Cooperation), Frankfurt, 2022.
- [28] M. Iorga and A. Karmel, "Managing Risk in the Coud," in Cloud Computing Security: Foundations and Challenges, Boca Raton, FL, CRC Press, 2017.
- [29] Google Cloud Indonesia, "Best Practices for a Data Classification Framework," Jakarta, 2022.
- [30] Kemkominfo, Daftar Unit Kompetensi Okupasi: Dalam Rangka Kualifikasi Nasional Indonesia Bidang Teknologi Informasi dan Komunikasi (TIK), Jakarta: Pusat Pengembangan Profesi dan Sertifikasi Kemkominfo, 2018.
- [31] S. Dutta, G. Grewal and H. Hrishikesh, "Six Simple Steps Pave the Way to the Cloud," Boston Consulting Group, New Jersey, 2019.

- [32] Avanade, "The CIO Guide to Cloud Native Applications: Unlock the Value of the Cloud," Avanade Inc, 2019.
- [33] S. R. Goniwada, Cloud Native Architecture and Design: A Handbook for Modern Day Architecture and Design with Enterprise-Grade Examples, California: Apress Media, 2022.
- [34] S. Mohammad, J. Taylor and E. Widun, Oakland County Michigan Cloud Strategy, Michigan, 2017.
- [35] Trinidad and Tobago Government, Cloud Computing Consideration Policy, Ministry of Public Administration of Trinidad and Tobago, 2020.
- [36] H. T. Husna, "Menkominfo: Pusat Data Nasional Berbasis Cloud akan Beroperasi di 2024," Aptika Kominfo, 12 Juli 2022. [Online]. Available: <https://aptika.kominfo.go.id/2022/07/menkominfo-pusat-data-nasional-berbasis-cloud-akan-beroperasi-di-2024/>. [Accessed 12 Oktober 2022].