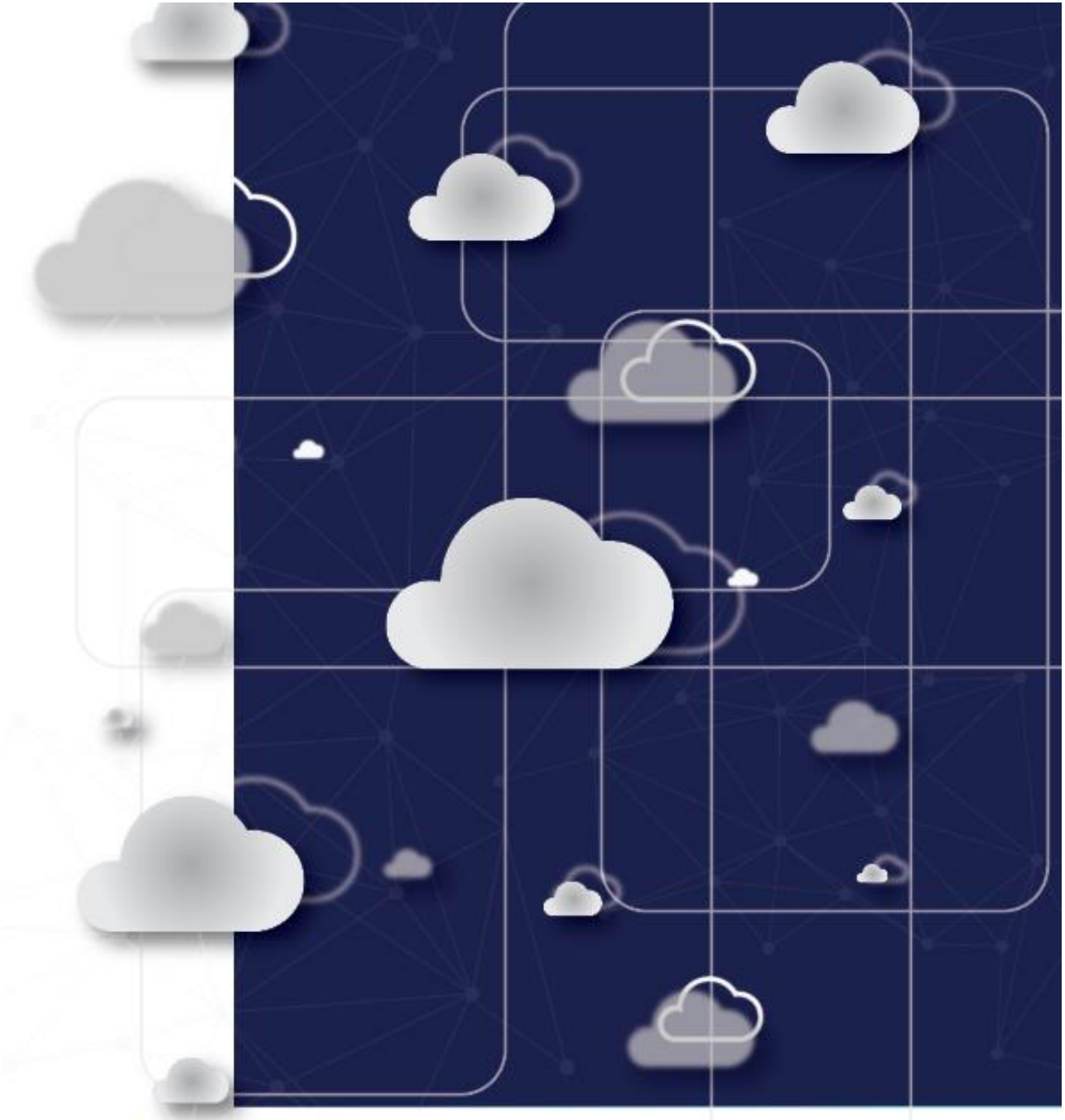


# Tinjauan Strategis

## Keamanan Siber Indonesia

*Teknologi Cloud dan Tata Kelola Data*

POLITEKNIK SIBER DAN SANDI NEGARA - UNIVERSITAS INDONESIA
Bersinergi mewujudkan Keamanan Siber Indonesia

**PENULIS:**
Dr. Amiruddin, S.Kom., M.T.I.
Ir. Setiadi Yazid, M.Sc., Ph.D.
Bayu Anggorojati, S.T., M.Sc., Ph.D.
Hermawan Setiawan , S.Si., M.TI.
Rahmat Purwoko, S.T., M.T.
Herman Kabetta, M.T.
R. Budiarto Hadiprakoso, M.M.S.I.
I Komang Setia Buana, M. T.



**EDITOR:**
Dimas Febriyan Priambodo, M.Cs.
Septia Ulfa Sunaringtyas,S.Tr.MP.,M.T.

**LAYOUT DAN DESAIN:**
Dimas Dwiki Ismoyo, S.Tr.TP.



Diterbitkan oleh Politeknik Siber dan Sandi Negara Press
Jl. H.USA Ciseeng, Bogor, Jawa Barat, 16120, Telp. (0251) 8541742,
email:perpustakaan@poltekssn.ac.id

**Tinjauan Strategis Keamanan Siber Indonesia:** Komputasi Awan dan Tata Kelola Data ini merupakan hasil kerjasama penelitian antara Politeknik Siber dan Sandi Negara (Poltek SSN) Badan Siber dan Sandi Negara (BSSN) dan Universitas Indonesia (UI)


**PELINDUNG:**
Kepala Badan Siber dan Sandi Negara
Letnan Jenderal TNI (Purn) Hinsa Siburian

**PENGARAH:**
Hokky Situngkir
R. Tjahjo Kurniawan , S.T., M.Si.
Prof. Ari Kuncoro, S.E., M.A., Ph.D

**TIM PENELITI:**
Dr. Amiruddin, S.Kom., M.T.I.
Ir. Setiadi Yazid, M.Sc., Ph.D.
Bayu Anggorojati, S.T., M.Sc., Ph.D.
Hermawan Setiawan , S.Si., M.TI.
Rahmat Purwoko, S.T., M.T.
Herman Kabetta, M.T.
R. Budiarto Hadiprakoso, M.M.S.I.
I Komang Setia Buana, M. T.

"Ingatlah bahwa **kechilafan satu orang sahaja** tjukup sudah menyebabkan keruntuhan negara".

(dr Roebiono Kertopati)

# KATA PENGANTAR

**Letjen TNI (Purn) Hinsa Siburian**

*Kepala Badan Siber dan Sandi Negara*

Seiring dengan pesatnya transformasi digital dan pertumbuhan ekonomi digital di Indonesia, kebutuhan untuk melindungi kedaulatan data nasional kita menjadi semakin penting. Jaminan keamanan dunia maya sangat diperlukan untuk melindungi integritas dan kerahasiaan informasi sensitif dan menjaga stabilitas infrastruktur digital. Terkait kepentingan tersebut, buku "Tinjauan Strategis Keamanan Siber Indonesia: Teknologi *Cloud* dan Tata Kelola Data" ini dapat memberikan wawasan yang komprehensif mengenai tantangan dan peluang yang akan dihadapi dengan teknologi komputasi awan *(cloud computing),* serta tata kelola data di negara kita.

Selaku Kepala Badan Siber dan Sandi Negara (BSSN), saya turut mendukung penyusunan buku ini yang membahas pentingnya kedaulatan data dan perlunya keamanan komputasi awan. Hal ini sejalan dengan Rencana Strategis BSSN tahun 2020-2024, di mana BSSN akan melakukan penguatan regulasi keamanan siber dan sandi, termasuk tata kelola keamanan siber nasional untuk mendukung transformasi digital. Saya berharap buku ini dapat turut berkontribusi meningkatkan kesadaran akan risiko yang terkait dengan komputasi awan dan mempromosikan praktik terbaik dalam tata kelola data untuk memperkuat ketahanan siber.

Saya percaya bahwa buku ini akan bermanfaat sebagai referensi bagi pembuat kebijakan, pelaku industri, dan praktisi keamanan siber yang berkomitmen untuk menjaga infrastruktur digital dan melindungi kedaulatan data nasional. Pembahasan yang mendalam tentang kerangka hukum dan peraturan seputar komputasi awan dan tata kelola data, termasuk peraturan perlindungan data, kebijakan lokalisasi data, dan peraturan transfer data lintas batas meningkatkan wawasan tentang perjalanan transformasi digital Indonesia, pentingnya tata kelola data dan keamanan komputasi awan, serta perannya dalam menjaga kedaulatan nasional kita.

Melalui tinjauan strategis yang disajikan dalam buku ini, saya berharap akan dapat semakin mendorong dan memperkuat kolaborasi antar pemangku kepentingan yang membacanya untuk bersama-sama menjaga ruang siber yang aman bagi seluruh warga Indonesia.

Jakarta, Mei 2023

Kepala Badan Siber dan Sandi Negara

Letjen TNI (Purn) Hinsa Siburian

# PRAKATA 1

**Marsma TNI. R. Tjahjo Kurniawan, S.T., M.Si.**

*Direktur Politeknik Siber dan Sandi Negara*

Pesatnya transformasi digital telah menciptakan lanskap keamanan siber yang kompleks dan dinamis. Pertumbuhan data yang eksponensial dan hadirnya teknologi komputasi awan, memunculkan pula berbagai tantangan baru dan kompleks terkait manajemen data, privasi, dan keamanan.

Untuk menghadapi tantangan ini, para pembuat kebijakan, pelaku industri, dan praktisi keamanan siber harus bekerja sama untuk mengembangkan tata kelola data yang efektif dan kerangka kerja keamanan komputasi awan yang dapat menjamin keamanan dan privasi data, sekaligus mendorong inovasi dan pertumbuhan ekonomi digital.

Buku "Tinjauan Strategis Keamanan Siber Indonesia: Teknologi *Cloud* dan Tata Kelola Data" ini merupakan hasil kolaborasi dari akademisi, industri, komunitas, dan pemerintah untuk mengeksplorasi tren terkini dan praktik terbaik dalam tata kelola data dan keamanan komputasi awan. Melalui sejumlah studi kasus dan penelitian terkini, buku ini memberikan tinjauan komprehensif tentang kondisi tata kelola data dan keamanan komputasi awan saat ini di Indonesia, serta mengajukan wawasan praktis dan rekomendasi yang dapat diimplementasikan untuk meningkatkan postur keamanan siber.

Topik yang dibahas dalam buku ini antara lain adalah arsitektur komputasi awan, ancaman dan kerentanan keamanan komputasi awan, undang-undang dan peraturan perlindungan data, serta audit dan kepatuhan. Baik Anda seorang profesional keamanan siber, pembuat kebijakan, atau pemimpin industri, buku ini dapat dijadikan sebagai salah satu referensi untuk memahami tantangan dan peluang dalam tata kelola data dan keamanan komputasi awan di Indonesia.

Buku ini diharapkan dapat menjadi rujukan dalam pengembangan dan penerapan teknologi komputasi awan di Indonesia, khususnya dalam aspek keamanan siber. Di sisi lain, penerapan tata kelola data yang aman dan efektif, seperti yang dibahas dalam buku ini, akan bermanfaat tidak hanya bagi pemangku kepentingan, tetapi juga masyarakat luas secara keseluruhan. Akhirnya, saya mengharapkan semoga buku ini dapat memberikan panduan yang komprehensif dan praktis bagi semua pihak yang ingin menjelajahi lanskap kompleks tata kelola data dan keamanan komputasi awan di Indonesia.

Jakarta, Mei 2023

Direktur Politeknik Siber dan Sandi Negara

Marsma TNI. R. Tjahjo Kurniawan ,S.T.,M.Si

# PRAKATA 2

**Prof. Ari Kuncoro, S.E., M.A., Ph.D**.

Rektor Universitas Indonesia

Transformasi digital sudah menjadi keharusan bagi setiap negara karena digitalisasi merupakan faktor penting yang menentukan keberhasilan negara tersebut dalam persaingan global. Pandemi yang baru terjadi juga mempercepat proses transformasi ini.

Teknologi komputasi awan atau *cloud computing*, memungkinkan perusahaan lebih dinamis dalam mengikuti perkembangan pasar, lebih mudah berkolaborasi dan bisa lebih mengutamakan kebutuhan pelanggan secara dinamis. Selain itu teknologi ini juga mempermudah penerapan AI dan *machine learning* dalam proses bisnis. Kemampuan ini sangat mendukung keberhasilan proses transformasi digital yang pada gilirannya akan meningkatkan daya saing dan pendapatan masyarakat.

Di kalangan negara Asia Pasifik, Indonesia adalah salah satu negara yang diharapkan menjadi negara yang termaju dalam pertumbuhan investasi layanan *cloud*, baik layanan publik maupun privat.

Salah satu tantangan yang dihadapi dalam perkembangan sektor industri *cloud* di Indonesia antara lain adalah masih kurangnya pemahaman mengenai

keamanan dan privasi data. Untuk mengatasi tantangan ini diperlukan kerjasama dari para pemangku kepentingan, baik dari pemerintahan, dari pengguna maupun dari penyedia layanan *cloud*. Sebagai langkah awal UI telah bekerja sama dengan Politeknik SSN dan Huawei melakukan penelitian bersama yang menghasilkan buku Tata Kelola Data & Keamanan Komputasi Awan di Indonesia ini.

Berbagai masalah mendasar dibahas dalam buku ini, dimulai dari ringkasan tata kelola data dan *cloud computing*, perbandingan standar dan peraturan dari berbagai negara, sampai rekomendasi tentang keamanan *cloud* di Indonesia. Disusun melalui kerjasama penelitian yang melibatkan akademisi, industri dan pemerintah, diharapkan buku ini dapat memberikan gambaran yang seimbang tentang komputasi *cloud* dan keamanannya.

Dengan pembahasan yang komprehensif terkait dengan perkembangan teknologi *cloud* hingga praktik terbaik dan rekomendasi keamanan *cloud*, buku ini diharapkan dapat menjadi referensi serta memberi manfaat bukan hanya bagi para pemangku kepentingan tetapi juga bagi masyarakat yang lebih luas. Masukan dari semua pemangku kepentingan tentu selalu sangat diharapkan. Semoga langkah ini menjadi awal dari tumbuhnya industri *cloud computing* yang dapat mendukung suksesnya transformasi digital di Indonesia.

Depok, Mei 2023

Rektor Universitas Indonesia

Prof. Ari Kuncoro, S.E., M.A., Ph.D

# DAFTAR ISI

# DAFTAR GAMBAR

# DAFTAR TABEL

# Tinjauan Strategis

# Keamanan Siber Indonesia–

Teknologi Cloud dan Tata Kelola Data

# DAFTAR SINGKATAN

CSC - *Cloud Service Consumer*

CSP - *Cloud Service Provider*

PII - *Personally Identifiable Information*

ISO - *International Organization for Standardization*

IEC - *International Electrotechnical Commission*

CSA - *Cloud security Alliance*

CIS - *Center for Internet Security*

GDPR - *General Data Protection Regulation*

NIST - *National Institute of Standards and Technology*

HIPAA - *Health Insurance Portability and Accountability Act*

PIMS - *Privacy Information Management System*

ISMS - *Information Security Management System*

TIK - Teknologi Informasi dan Komunikasi

TI – Teknologi Informasi

UE – Uni Eropa

UAE – *Uni Arab Emirates*

KAMI – Keamanan Informasi

ZTA – *Zero Trust Architecture*

PSTE – Penyelenggara Sistem & Transaksi Elektronik

PDP – Perlindungan Data Pribadi

PDN – Pusat Data Nasional

IaaS - *Infrastructure as a Service*

PaaS - *Platform as a Service*

SaaS - *Software as a Service*

DaaS – *Data as a Service*

O&M – *Operation & Maintenance*

SPBE – Sistem Pemerintahan Berbasis Elektronik

SDI – Satu Data Indonesia

AI – *Artificial Intelligence*

IoT – *Internet of Things*

PII - *Personal Identifiable Information*

AR – *Augmented Reality*

VR – *Virtual Reality*

# RINGKASAN EKSEKUTIF

Buku Tinjauan Strategis ini memberikan wawasan tentang kondisi terkini *cloud computing* dan tata kelola data di Indonesia, baik dari aspek teknologi maupun regulasi, serta praktik terbaik yang dapat diterapkan untuk mencapai pengelolaan data yang aman dan efektif.

Indonesia merupakan negara berkembang dengan ekonomi digital yang berkembang pesat, dan dengan meningkatnya adopsi *cloud computing*, organisasi perlu mengelola data mereka secara efektif untuk memastikan keamanan dan privasi. Buku ini mengeksplorasi masalah kritis yang dihadapi organisasi, seperti pelanggaran data, masalah privasi, dan kepatuhan terhadap peraturan, serta menyajikan solusi praktis untuk mengatasinya.

Buku ini dimulai dengan memberikan ikhtisar tata kelola data dan *cloud computing*, termasuk definisi, prinsip utama, dan manfaatnya. Kemudian menggali tantangan unik yang dihadapi organisasi di Indonesia dalam mengimplementasikan *cloud computing*, seperti infrastruktur dan sumber daya yang terbatas, serta kerangka peraturan dan faktor budaya yang berdampak pada tata kelola data.

Buku ini menawarkan diskusi terperinci tentang risiko keamanan yang terkait dengan *cloud computing* dan memberikan panduan komprehensif untuk menerapkan langkah-langkah keamanan yang efektif. Ini termasuk dalam aspek penilaian risiko, perencanaan keamanan, dan pemilihan kontrol keamanan yang sesuai untuk memastikan kerahasiaan, integritas, dan ketersediaan data. Berbagai standar keamanan global serta praktik terbaik pada beberapa negara juga termasuk dalam pembahasan buku ini.

Terakhir, buku ini membahas masalah penting terkait kepatuhan dan menawarkan panduan tentang bagaimana organisasi dapat memastikan

bahwa mereka memenuhi persyaratan peraturan untuk tata kelola data dan *cloud computing* di Indonesia. Disisi lain, tinjauan mendalam terkait aspek regulasi yang berlaku saat ini, serta rekomendasi yang diberikan bagi pengambil kebijakan juga menjadi nilai lebih dari buku ini.

Secara keseluruhan, buku ini merupakan panduan penting bagi segenap pemangku kepentingan dalam mewujudkan tata kelola data dan keamanan *cloud computing* yang aman dan efektif di Indonesia. Ini menawarkan saran praktis, wawasan ahli, dan contoh dunia nyata untuk membantu organisasi menavigasi lanskap kompleks tata kelola data dan keamanan *cloud computing*, dan memastikan bahwa data mereka dikelola dengan cara yang aman, bertanggung jawab, dan berkelanjutan.

# BAB 1

# PENDAHULUAN

## 1.1 Latar Belakang

Komputasi awan (*cloud computing*) merupakan sebuah paradigma komputasi yang telah mengubah budaya organisasi dan individu dalam menyimpan, mengelola, dan mengakses data hingga aplikasi(Akhtar et al., 2021). Dengan teknologi komputasi awan, pengguna dimungkinkan untuk mengakses sumber daya komputasi melalui internet tanpa harus memiliki infrastruktur fisik sendiri, seperti server, perangkat lunak, jaringan, dan penyimpanan data(Rashid & Chaturvedi, 2019). Dengan infrastruktur yang dapat diakses secara mudah dan terjangkau, komputasi awan memiliki potensi untuk mendorong pertumbuhan ekonomi digital, menciptakan lapangan kerja baru, dan meningkatkan daya saing industri Indonesia di tingkat global. Seiring dengan perkembangan teknologi informasi dan komunikasi di Indonesia, adopsi penggunaan komputasi awan telah meningkat pesat dalam beberapa tahun terakhir, baik oleh perusahaan besar maupun UMKM (Zebua & Widuri, 2023). Data dari firma riset global IDC tahun 2022 menunjukkan, 81 persen responden dari Indonesia berencana meningkatkan pemanfaatan layanan komputasi awan di tahun 2023(Mahayana, 2023). Organisasi semakin menyadari manfaat dari teknologi komputasi awan, seperti fleksibilitas, skalabilitas dan elastisitas, efisiensi biaya, serta kemudahan akses(Abdalla & Varol, 2019)(Wang & Zhang, 2020)(Fernando et al., 2019).

Komputasi awan akan menjadi teknologi masa depan pada bidang komputasi. Hal itu karena sistem dan mekanisme dari komputasi awan yang tidak perlu mengeluarkan investasi yang besar untuk membangun

infrastruktur sumber daya teknologi informasi (*software, processing power, storage*, dan lainnya). Teknologi komputasi awan dapat meningkatkan efisiensi organisasi, pada bidang administrasi pemerintahan, solusi komputasi awan memberikan kemudahan akses bagi masyarakat (Ali et al., 2021). Pemerintah dapat menyediakan layanan Sistem Pemerintahan Berbasis Elektronik (SPBE) kepada masyarakat (Sundberg, 2019), seperti pengajuan pajak *online* (Supardianto et al., 2019), pendaftaran elektronik, atau hanya sekedar mengakses informasi publik. Sektor swasta maupun pemerintahan dapat menjalankan proyek komputasi yang membutuhkan daya komputasi tingkat tinggi, seperti analisis *big data* untuk kepentingan riset, perencanaan *smart city*, atau pemodelan kecerdasan buatan. Hal tersebut berimbas pada penghematan biaya infrastruktur untuk mengatasi tantangan yang kompleks (Aceto et al., 2020a).

Konsep revolusi industri 4.0 telah mendapatkan perhatian yang besar dalam beberapa tahun terakhir. Implementasi Industri 4.0 memerlukan integrasi beberapa teknologi, seperti CPS (*cyber physical system*), IoT (*Internet of Things*), *Big Data & analytics, Autonomous Robot, Virtual & Augmented Reality* dan komputasi awan (Gizem Erboz, 2017). Sinergi teknologi Industri 4.0 diharapkan dapat membawa manfaat dan kemudahan di berbagai sektor kehidupan, termasuk kesehatan, pertanian, energi, *smart city*, bangunan dan hunian cerdas, transportasi, industri dan manufaktur. Konsep ini juga sejalan dengan agenda transformasi digital G20 dan *Sustainable Development Goals* PBB (Drath & Horch, 2014). Visi di bidang kesehatan melibatkan penggunaan AI, *big data*, dan HPC untuk pengembangan vaksin, pencarian obat, prediksi penyakit, dan penyebaran penyakit. Teknologi IoT dan biosensor juga digunakan dalam pemantauan kesehatan dan pergeseran fokus dari pengobatan menjadi pencegahan. Di bidang pangan, inovasi digital seperti *smart farming* dan penggunaan data dan teknologi dalam rantai pasok pangan diharapkan meningkatkan produksi, keberlanjutan, dan efisiensi. Konsep *smart living* mencakup pengembangan rumah dan bangunan pintar dengan

teknologi IoT, AR, VR, dan *Metaverse*, meningkatkan efisiensi energi, kenyamanan, dan keamanan. Pada bidang transportasi, sistem transportasi didorong untuk menjadi lebih aman, efisien, dan ramah lingkungan dengan bantuan teknologi IoT, komputasi awan, *big data & analytics*, dan mobil otonom (Hofmann & Rüsch, 2017). Dalam pengembangan perkotaan, infrastruktur digital dan layanan pemerintahan terpusat diharapkan dapat meningkatkan pengelolaan lingkungan perkotaan, efisiensi sumber daya, dan kualitas hidup penduduk (Fernández-Caramés & Fraga-Lamas, 2018).

Transformasi digital di bidang industri melibatkan penggunaan robot kolaboratif, model bisnis yang berpusat pada manusia, dan pemantauan rantai pasok untuk meningkatkan ketahanan dan produktivitas. Dalam bidang energi, efisiensi dan transisi menuju sumber energi ramah lingkungan menjadi fokus dengan menggunakan teknologi *smart grid* berbasis IoT dan integrasi dengan sumber energi terbarukan. Transformasi ekonomi digital dipercepat oleh pandemi Covid-19, dan penting untuk menjaga kepercayaan (*trust*) dengan tindakan di ranah teknis, organisasi, dan regulasi seperti *blockchain*, AI, dan perlindungan data pribadi. Pentingnya lingkungan *online* yang aman dan terlindungi menuntut kombinasi teknologi seperti *blockchain* dan *fraud detection* berbasis AI, kebijakan perlindungan informasi dan privasi, serta tata kelola keamanan data dan layanan komputasi awan (Zorrilla & Yebenes, 2022).

Meskipun visi yang dikemukakan dalam berbagai bidang kehidupan tersebut menawarkan potensi yang menarik, terdapat kesenjangan antara visi tersebut dan kondisi saat ini. Salah satu permasalahan utama adalah kurangnya infrastruktur yang memadai untuk mewujudkan visi tersebut. Namun, teknologi komputasi awan muncul sebagai solusi yang mampu menjembatani kesenjangan tersebut. Dengan menggunakan komputasi awan, banyak data yang dihasilkan oleh teknologi Industri 4.0 dan IoT dapat diproses, dianalisis, dan disimpan secara efisien (Aceto et al., 2020b). Hal ini

memungkinkan akses yang lebih mudah dan cepat terhadap data tersebut, serta memungkinkan kolaborasi antara berbagai sektor dan pemangku kepentingan. Dengan adopsi yang luas terhadap teknologi komputasi awan, potensi visi di bidang kesehatan, pangan, *smart living*, transportasi, perkotaan, industri, energi, ekonomi, dan kepercayaan digital dapat lebih cepat terwujud, membawa manfaat yang signifikan bagi masyarakat dan perekonomian secara keseluruhan.

Komputasi awan menjadi pilar penting dalam mewujudkan industri 4.0 dan keamanan siber merupakan komponen yang tak terpisahkan dalam mendukung visi di berbagai sektor kehidupan. Namun, perkembangan teknologi juga membawa kerawanan yang semakin besar. Dalam konteks transformasi digital, keamanan siber menjadi fondasi yang penting untuk mencapai tujuan yang spesifik, baik bagi lembaga pemerintahan maupun sektor swasta.

Di Indonesia, komputasi awan menjadi infrastruktur kunci untuk mendukung Sistem Pemerintahan Berbasis Elektronik (SPBE) melalui Pusat Data Nasional (PDN) sesuai dengan Perpres 95/2018. Keadaan geografis Indonesia yang kepulauan dan tersebar menjadikan komputasi awan sebagai alternatif yang prospektif. Dalam transformasi digital dan SPBE, penggunaan komputasi awan menjadi penting. Infrastruktur tradisional dan sistem lokal sering kali tidak mampu memenuhi tuntutan skalabilitas, fleksibilitas, dan efektivitas biaya. Komputasi awan memberikan solusi dengan menyediakan akses ke sumber daya komputasi melalui internet, seperti penyimpanan, daya pemrosesan, dan aplikasi perangkat lunak. Dengan memanfaatkan komputasi awan, pemerintah dapat mengoptimalkan sumber daya mereka dan memberikan layanan yang lebih cepat dan mudah diakses kepada warga negara.

Selain itu, komputasi awan juga memungkinkan pemerintah untuk memanfaatkan analitik data, kecerdasan buatan, dan pembelajaran mesin,

yang membuka peluang pengambilan keputusan inovatif berbasis data. Secara keseluruhan, adopsi komputasi awan dalam SPBE memungkinkan pemerintah merangkul transformasi digital dan memenuhi kebutuhan warga negara di era digital yang terus berkembang.

Namun, perkembangan terkini juga menunjukkan bahwa transformasi digital semakin penting dan mendesak. Pandemi COVID-19 yang berkepanjangan telah mempercepat digitalisasi produk dan layanan secara global. Perusahaan-perusahaan bergerak jauh lebih cepat daripada yang diharapkan dalam menerapkan digitalisasi. Selain itu, respons terhadap emisi karbon dan pemanasan global semakin meningkat, dan teknologi digital menjadi kunci untuk mengurangi emisi di semua industri. Kompleksitas lingkungan bisnis global juga mendorong pemerintah dan perusahaan untuk memprioritaskan ketahanan sebagai strategi bisnis, dengan transformasi digital sebagai pendukung utama.

*European Commission Directorate-General for Informatics* menyebutkan bahwa komputasi awan membawa perubahan kunci pada lanskap TI, memungkinkan konsumsi sumber daya TI secara *on-demand* tanpa investasi di infrastruktur TI. Selain itu, pengembangan sistem informasi berbasis komputasi awan dapat mengurangi kompleksitas dan meningkatkan fokus pada nilai bisnis. Namun, manajemen keamanan dalam konteks komputasi awan memerlukan perhatian khusus agar terhindar dari risiko keamanan informasi.

Namun demikian, meskipun komputasi awan menawarkan potensi yang besar, masih terdapat tantangan yang harus dihadapi dalam mengelola penggunaan teknologi ini di Indonesia. Beberapa tantangan yang muncul termasuk regulasi yang belum matang, kekhawatiran tentang keamanan data, kurangnya pemahaman tentang manfaat dan risiko komputasi awan, serta ketersediaan sumber daya manusia yang terlatih dalam bidang ini (Butarbutar, 2020). Dalam konteks perlindungan data dan privasi,

penggunaan komputasi awan melibatkan penyimpanan data di luar kendali langsung penggunanya, sehingga kebijakan dan tata kelola yang tepat diperlukan untuk melindungi data dan privasi yang sensitif. Menurut data perusahaan keamanan siber Surfshark yang dipublikasikan dalam laman situs Katadata, disebutkan terdapat 1,04 juta akun yang mengalami kebocoran data pengguna di Indonesia selama kuartal II 2022. Jumlah tersebut melonjak 143% dari kuartal I 2022 (Dihni, 2022). Kebutuhan akan keamanan siber yang kuat juga harus diperhatikan, mengingat adanya risiko serangan siber yang semakin kompleks dan meluas. Untuk mengatasi tantangan ini dan memanfaatkan potensi komputasi awan dengan sebaik-baiknya, maka perlu adanya tata kelola yang efektif.

Tata kelola komputasi awan mengacu pada kerangka kerja dan proses yang diterapkan untuk mengelola penggunaan komputasi awan dalam suatu organisasi atau negara. Di Indonesia, perlu dilakukan penelitian untuk memahami status tata kelola komputasi awan saat ini, tantangan yang dihadapi, dan peluang-peluang yang ada. Penelitian ini diharapkan akan memberikan pemahaman yang lebih baik tentang cara mengatur dan mengelola komputasi awan di Indonesia, serta memberikan rekomendasi untuk meningkatkan tata kelola yang ada.

Penelitian ini melibatkan analisis kebijakan dan regulasi terkait komputasi awan di Indonesia, penelusuran praktik terbaik dalam tata kelola komputasi awan di negara lain, dan survei atau wawancara dengan para pemangku kepentingan di Indonesia, termasuk perwakilan pemerintah, perusahaan, dan akademisi. Data yang terkumpul akan dianalisis untuk mengidentifikasi kekuatan dan kelemahan tata kelola komputasi awan saat ini, serta mengevaluasi kecocokannya dengan kebutuhan dan tantangan khusus Indonesia. Regulasi terkait komputasi awan di Indonesia juga masih terus berkembang dan belum matang. Oleh karena itu, penelitian ini akan membantu mengidentifikasi kekosongan regulasi yang perlu diisi dan

memberikan rekomendasi kebijakan yang tepat untuk memfasilitasi penggunaan komputasi awan yang aman dan berkelanjutan di Indonesia.

Begitu pentingnya peranan komputasi awan sebagai tulang punggung pada berbagai layanan di era digital saat ini sehingga perlu dilakukan tinjauan terhadap definisi, cara kerja, standar dan regulasi, serta tantangan dan berbagai permasalahan lain pada komputasi awan. Dengan demikian, hasil tinjauan diharapkan dapat memberikan pemahaman dan menjadi referensi bagi para pemangku kepentingan. Hasil dari penelitian ini diharapkan dapat memberikan panduan dan rekomendasi kepada pemerintah, perusahaan, dan organisasi di Indonesia untuk mengoptimalkan penggunaan komputasi awan dengan mengatasi tantangan dan memanfaatkan peluang yang ada. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan tata kelola komputasi awan di Indonesia dan mendorong pertumbuhan dan inovasi di berbagai sektor.

## 1.2 Rumusan Permasalahan

Dengan berbagai manfaat yang diberikannya, komputasi awan bukan tanpa kekurangan. Kekurangan utama pada komputasi awan adalah ancaman keamanan. Karena data yang disimpan bersifat sensitif, maka isu keamanan menjadi hal yang sangat dekat dengan komputasi awan. Untuk itu, pengguna perlu memastikan memilih penyedia layanan komputasi awan yang sudah terbukti memiliki keamanan yang tinggi. Selain itu, belum tegasnya regulasi beserta pengukuran dan penegakkannya turut pula menjadi tantangan bagi penerapan komputasi awan terutama di Indonesia. Pada tataran pengguna, pemahaman terhadap definisi, cara kerja, dan berbagai aspek lain pada komputasi awan tentu juga menjadi permasalahan tersendiri yang perlu mendapatkan jawaban.

Berdasarkan rumusan permasalahan tersebut, dibuatlah secara garis besar tiga pertanyaan penelitian yang akan dijawab dalam tinjauan strategis ini, yaitu:

a. Bagaimana pemanfaatan komputasi awan saat ini?
b. Bagaimana potensi dan risiko pemanfaatan komputasi awan dikaitkan dengan tata kelola data di Indonesia?
c. Bagaimana strategi mewujudkan keamanan komputasi awan dan tata kelola data di Indonesia?

## 1.3 Tujuan Kajian

Berdasarkan rumusan permasalahan yang telah disebutkan, tujuan dari kajian ini adalah sebagai berikut:

a. Mendeskripsikan pemanfaatan komputasi awan saat ini di lingkup global secara umum dan di Indonesia khususnya. Hal ini termasuk sejauh mana layanan tersebut digunakan dalam berbagai sektor industri dan pemerintahan.
b. Menganalisis potensi dan risiko yang terkait dengan pemanfaatan komputasi awan, terutama dalam konteks tata kelola data di Indonesia, dan menganalisis dampaknya terhadap keamanan dan privasi data.
c. Mengembangkan strategi dan rekomendasi yang dapat mewujudkan keamanan komputasi awan dan tata kelola data yang efektif di Indonesia.

## 1.4 Sistematika Penulisan Kajian

Bab I Pendahuluan:

Pada bab ini dijelaskan latar belakang penelitian mengenai keamanan komputasi awan di Indonesia, rumusan permasalahan yang ingin dipecahkan, yakni pemanfaatan komputasi awan saat ini, peluang dan risiko

terkait tata kelola data di Indonesia, serta strategi untuk mewujudkan keamanan komputasi awan dan tata kelola data yang efektif.

Bab II Metode Kajian:
Bab ini menjelaskan metode penelitian yang digunakan dalam penelitian yang meliputi teknik pengumpulan data, teknik analisis data dan dilengkapi dengan kerangka penelitian. Kerangka penelitian disusun sebagai landasan kerja untuk mengumpulkan, menganalisis, dan menginterpretasi data yang diperoleh hingga mendapatkan simpulan dan rekomendasi.

Bab III Teknologi Komputasi Awan:
Bab ini menjelaskan secara mendalam tentang definisi dan karakteristik komputasi awan, termasuk model layanan dan model *deployment* yang digunakan dalam komputasi awan. Infrastruktur global publik komputasi awan dan konsep *cloud native*. Fokusnya akan ditujukan pada keamanan teknologi komputasi awan, termasuk model tanggung jawab bersama, manajemen akses identitas, *zero trust architecture*, dan *compliance*. Bab ini memberikan pengetahuan konsep-konsep dasar terkait teknologi komputasi awan.

Bab IV Pemanfaatan Komputasi Awan di Dunia:
Bab ini membahas pemanfaatan komputasi awan di berbagai negara di dunia, pangsa pasar komputasi awan global dan standar internasional terkait keamanan data dan perlindungan privasi. Bab ini membahas kebijakan tata kelola keamanan siber di Uni Eropa dan beberapa negara di Asia, persyaratan keamanan komputasi awan dalam berbagai industri serta memberikan jawaban pada rumusan masalah poin 1 terkait pemanfaatan komputasi awan secara umum di dunia.

Bab V Pemanfaatan Komputasi Awan di Indonesia:
Pada bab ini dilakukan analisis pemanfaatan komputasi awan di Indonesia, termasuk pangsa pasarnya, kebijakan terkait komputasi awan di Indonesia

seperti Undang-Undang Informasi dan Transaksi Elektronik, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan Undang-Undang Perlindungan Data Pribadi (UU PDP). Indeks KAMI menjadi fokus dalam penjelasan bab ini. Bab ini memberikan jawaban pada rumusan masalah poin 1 terkait pemanfaatan komputasi awan secara spesifik di Indonesia.

Bab VI Potensi dan Risiko Pemanfaatan Komputasi Awan:
Bab ini membahas secara rinci masalah-masalah terkait keamanan komputasi awan di Indonesia. Risiko keamanan komputasi awan, isu terkait tata kelola data seperti kedaulatan data, keamanan dan privasi data, klasifikasi data serta peluang pemanfaatan komputasi awan juga dijelaskan dengan terperinci. dengan analisis SWOT terhadap layanan keamanan komputasi awan. Bab ini memberikan jawaban terhadap rumusan permasalahan poin 2.

Bab VII Strategi Mewujudkan Keamanan Komputasi Awan dan Tata Kelola Data di Indonesia:
Bab ini merumuskan strategi untuk mewujudkan keamanan komputasi awan dan tata kelola data yang efektif di Indonesia dengan menyusun: rancangan kerangka kerja dan tata kelola keamanan komputasi awan Indonesia, rancangan Indeks Keamanan Informasi yang mengacu pada ISO/IEC 27001:2022, serta kerangka kerja audit keamanan layanan komputasi awan beserta kontrol domain, metode audit, metode pengukuran, dan penilaian maturitas. Bab ini memberikan jawaban terhadap rumusan permasalahan poin 3.

Bab VIII Simpulan dan Rekomendasi:
Bab terakhir pada buku tinjauan strategis ini menyajikan simpulan dari penelitian dan rekomendasi untuk para pemangku kepentingan terkait langkah-langkah yang perlu diambil untuk meningkatkan keamanan komputasi awan dan tata kelola data di Indonesia.

# BAB 2

# METODE KAJIAN

## 2.1 Pendekatan Kajian

Pendekatan dalam kajian yang dilakukan adalah pendekatan kualitatif. Pendekatan kualitatif dipilih karena tidak ada hal yang perlu dibuktikan dalam kajian ini atau tidak ada hipotesis penelitian Pemanfaatan pendekatan kualitatif telah berkembang di beberapa bidang. Metode kualitatif memberikan penjelasan deskriptif tentang hipotesis yang diteliti.. Pendekatan ini menawarkan pemahaman yang lebih kaya dan lebih baik tentang masyarakat yang sedang diselidiki. Setiap studi perlu menuntut metode yang spesifik, terorganisir, dan terstruktur untuk menemukan hasil yang lebih efektif. SWOT (*Strength, Weakness, Opportunity, Threat*) dan FGD (*Focus Group Discussion*) termasuk dalam pendekatan kualitatif ini.

Secara ringkas tahapan tinjauan strategis ini adalah sebagai berikut:

1. Identifikasi masalah
2. Menetapkan pertanyaan kajian
3. Pengumpulan referensi kajian literatur
4. *Focused Group Discussions* (FGD) dengan pemerintah
5. Analisis SWOT
6. *Focused Group Discussion* (FGD) dengan Industri
7. Perbaikan penulisan draf buku
8. *Review* oleh pakar dan pemangku kepentingan
9. Penyelesaian buku dan diseminasi

Tinjauan strategis ini menggunakan pendekatan kualitatif dengan kajian literatur dan diskusi kelompok terfokus (FGD). Kajian literatur dilakukan

dengan mempelajari literatur terkait komputasi awan dan berbagai aspeknya seperti standar, kerangka kerja, regulasi, penerapan, penilaian, dan permasalahan yang ditemukan. FGD dilakukan beberapa kali dengan menghadirkan pemangku kepentingan dan pakar terkait keamanan komputasi awan. Pada FGD tersebut tim tinjauan memaparkan hasil-hasil studi literatur yang kemudian ditanggapi oleh peserta FGD terutama oleh pemangku kepentingan dan pakar. Pada akhirnya dari kajian literatur dan FGD didapatkan kesepakatan jawaban terhadap pertanyaan penelitian yang diajukan. Selain itu, hasil tinjauan strategis berupa draf buku ditinjau kembali pakar dan pemangku kepentingan untuk mendapatkan masukan. Dan pada akhirnya Ketika sudah tidak ada lagi masukan dan dianggap sudah layak, maka draf buku disetujui untuk disahkan dan didiseminasikan.

## 2.2 Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini dilakukan dengan menggunakan beberapa metode yang meliputi studi literatur, wawancara dengan pakar, dan *focus group discussion* (FGD). Studi literatur digunakan untuk mengumpulkan informasi yang relevan mengenai keamanan komputasi awan di Indonesia, termasuk perkembangan terkini, peraturan yang berlaku, dan isu-isu yang muncul.

Wawancara dengan pakar dilakukan untuk mendapatkan pandangan dan pemahaman mendalam dari para ahli keamanan komputasi awan, termasuk perspektif mereka terhadap masalah-masalah yang dihadapi dan rekomendasi solusi yang dapat diimplementasikan. Sementara FGD di sisi lain, lebih menguntungkan menyediakan lingkungan yang lebih otentik di mana peserta saling mempengaruhi dan dipengaruhi. Interaksi kelompok adalah keuntungan lain menciptakan efek sinergi pada peserta. Selain itu, ketika ada kesempatan terbatas untuk pengumpulan data, kelompok fokus lebih disukai dibandingkan dengan wawancara individu. Oleh karena itu, FGD digunakan untuk mengumpulkan data berkualitas tinggi maka FGD

harus didefinisikan dan dipahami dengan baik untuk melaksanakannya dengan benar.

FGD melibatkan sekelompok orang yang memiliki pengetahuan dan pengalaman dalam penggunaan layanan komputasi awan. FGD bertujuan untuk mendapatkan beragam pandangan, pemikiran, dan masukan dari peserta diskusi mengenai masalah-masalah keamanan yang mereka hadapi, tantangan yang dihadapi, dan ide-ide untuk meningkatkan keamanan komputasi awan. Teknik pengumpulan data dalam penelitian ini melibatkan dua sesi FGD. FGD pertama diadakan dengan melibatkan pihak pemerintah, khususnya Badan Siber dan Sandi Negara (BSSN), yang memiliki peran penting dalam pengaturan keamanan komputasi awan di Indonesia. FGD ini bertujuan untuk mendapatkan perspektif pemerintah terkait isu-isu keamanan yang dihadapi, langkah-langkah yang telah diambil, dan tantangan yang dihadapi dalam mengimplementasikan kebijakan keamanan komputasi awan.

FGD kedua melibatkan komunitas asosiasi industri komputasi awan Indonesia. Dalam FGD ini, berbagai perwakilan dari penyedia layanan komputasi awan dan industri terkait lainnya berkumpul untuk berbagi pengalaman, pemikiran, dan masukan terkait keamanan komputasi awan. Diskusi ini melibatkan topik-topik seperti kebijakan keamanan, praktik terbaik, kendala yang dihadapi, serta peluang dan tantangan dalam meningkatkan keamanan layanan komputasi awan di Indonesia.

Dengan menggunakan kombinasi metode ini, data yang diperoleh dapat memberikan wawasan yang komprehensif dan mendalam mengenai masalah-masalah terkait keamanan komputasi awan di Indonesia, serta rekomendasi strategis untuk peningkatan keamanan yang dapat diimplementasikan oleh pemerintah, penyedia layanan, dan pengguna layanan komputasi awan.

## 2.3 Teknik Analisis Data

### 2.3.1 Analisis Komparasi

Setelah data dikumpulkan, proses selanjutnya adalah analisis data. Salah satu pendekatan analisis data yang dilakukan adalah analisis komparasi. Analisis komparasi merupakan pendekatan yang digunakan untuk membandingkan standar, regulasi, dan praktik terbaik pada industri komputasi awan global dengan kondisi yang berlaku di Indonesia. Melalui analisis ini, dapat diidentifikasi kesenjangan antara praktik global dan praktik yang ada di Indonesia, serta memperoleh wawasan tentang perbedaan dalam hal keamanan komputasi awan.

Dalam analisis komparasi, aspek-aspek yang diamati meliputi kebijakan keamanan, standar keamanan, perlindungan data, regulasi privasi, dan praktik terbaik dalam industri komputasi awan. Dengan membandingkan praktik dan standar yang berlaku di Indonesia dengan yang ada di tingkat global, dapat ditemukan area-area di mana Indonesia dapat memperbaiki kebijakan dan praktiknya untuk meningkatkan keamanan komputasi awan.

Hasil analisis komparasi ini akan memberikan pemahaman yang lebih baik tentang posisi Indonesia dalam konteks keamanan komputasi awan dan membantu merumuskan langkah-langkah perbaikan yang diperlukan. Dengan memadukan praktik terbaik global dengan kebutuhan dan konteks Indonesia, dapat dibangun kerangka kerja yang kuat untuk meningkatkan keamanan komputasi awan di negara ini.

Dengan demikian, analisis komparasi merupakan salah satu pendekatan penting dalam proses analisis data yang digunakan dalam kajian ini. Hal ini memberikan pandangan yang lebih holistik tentang keadaan keamanan komputasi awan di Indonesia, serta memberikan dasar untuk merumuskan strategi dan rekomendasi yang tepat guna dalam meningkatkan keamanan layanan komputasi awan di Indonesia.

### 2.3.2 Analisis PESTLE

Teknik analisis PESTLE digunakan dalam kajian ini untuk menganalisis faktor-faktor eksternal yang dapat mempengaruhi keamanan komputasi awan di Indonesia. PESTLE adalah singkatan dari *Political* (Politik), *Economic* (Ekonomi), *Social* (Sosial), *Technological* (Teknologi), *Legal* (Hukum), dan *Environmental* (Lingkungan). Analisis PESTLE memungkinkan kita untuk memahami konteks makro di mana layanan komputasi awan beroperasi, serta mengidentifikasi ancaman dan peluang yang terkait dengan faktor-faktor tersebut.

Dalam analisis PESTLE, aspek politik melibatkan kebijakan dan regulasi pemerintah terkait keamanan dan privasi data, serta kerjasama internasional dalam hal aliran data lintas batas. Aspek ekonomi melibatkan pertumbuhan ekonomi digital, investasi dalam infrastruktur teknologi, dan dampak ekonomi dari pelanggaran keamanan. Aspek sosial melibatkan kesadaran dan persepsi masyarakat terkait privasi dan keamanan data, serta isu-isu etika dalam penggunaan komputasi awan. Aspek teknologi melibatkan perkembangan teknologi keamanan, seperti enkripsi dan kecerdasan buatan. Aspek hukum melibatkan peraturan dan undang-undang terkait keamanan data dan privasi. Sedangkan aspek lingkungan melibatkan dampak lingkungan dari infrastruktur komputasi awan dan keberlanjutan energi.

Dengan menganalisis faktor-faktor ini, analisis PESTLE membantu dalam memahami konteks yang lebih luas dan mengidentifikasi risiko dan potensi yang relevan dalam pengembangan dan penggunaan layanan komputasi awan di Indonesia. Hasil analisis ini memberikan wawasan yang berharga untuk merumuskan rekomendasi dan strategi dalam meningkatkan keamanan komputasi awan yang sesuai dengan tuntutan lingkungan eksternal.

### 2.3.3 Analisis SWOT

Selain menggunakan analisis PESTLE, dalam penelitian ini juga dilakukan analisis SWOT. Analisis SWOT adalah suatu metode analisis yang digunakan untuk mengevaluasi kekuatan (*strengths*), kelemahan (*weaknesses*), peluang (*opportunities*), dan ancaman (*threats*) yang terkait dengan suatu subjek tertentu, dalam hal ini keamanan komputasi awan di Indonesia.

Analisis SWOT membantu dalam mengidentifikasi faktor-faktor internal dan eksternal yang dapat mempengaruhi keamanan komputasi awan. Kekuatan dan kelemahan mengacu pada aspek internal, seperti keahlian teknis, sumber daya manusia, dan infrastruktur yang tersedia. Sementara itu, peluang dan ancaman mengacu pada aspek eksternal, seperti perubahan regulasi, perkembangan teknologi, dan kebutuhan pasar.

Melalui analisis SWOT, kajian ini dapat mengidentifikasi kekuatan apa yang dapat dimanfaatkan dan diperkuat, kelemahan apa yang perlu diperbaiki, peluang apa yang dapat dimanfaatkan, serta ancaman apa yang perlu diatasi dalam konteks keamanan komputasi awan di Indonesia. Hasil analisis SWOT ini memberikan dasar bagi pengembangan strategi dan rekomendasi yang tepat guna untuk meningkatkan keamanan komputasi awan dan menghadapi tantangan yang ada.

Melalui analisis SWOT, strategi-strategi yang mungkin dilakukan dapat dirumuskan dengan cara menghubungkan kekuatan internal dengan peluang eksternal, serta mengatasi kelemahan internal dengan mengantisipasi ancaman eksternal. Pendekatan ini memanfaatkan kekuatan yang ada untuk menangkap peluang yang muncul dan mengurangi risiko yang dihadapi. Sebagai contoh jika dalam analisis SWOT teridentifikasi bahwa salah satu kekuatan adalah keahlian teknis yang kuat dan salah satu peluang adalah adopsi teknologi keamanan baru, strategi yang mungkin dilakukan adalah mengembangkan dan meningkatkan keahlian teknis dalam teknologi

keamanan tersebut. Dengan demikian, kekuatan yang ada dapat dimanfaatkan untuk menangkap peluang yang muncul.

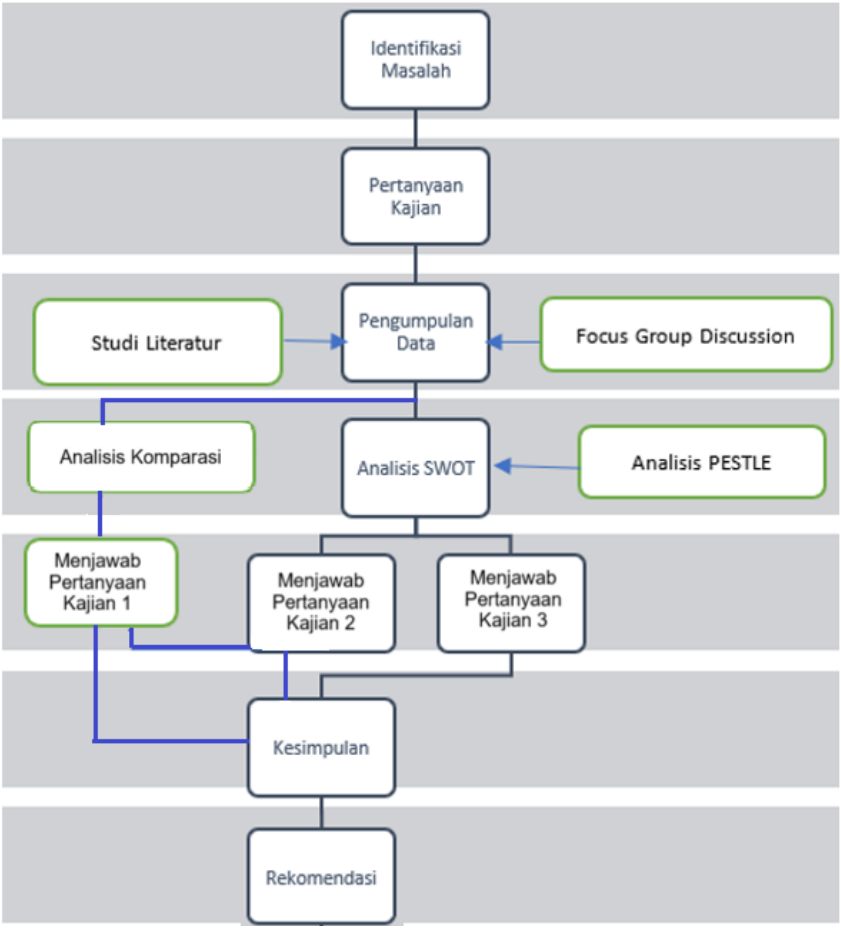
Selain itu, jika ditemukan kelemahan dalam keamanan sistem komputasi awan dan ancaman yang muncul adalah serangan keamanan yang semakin kompleks, strategi yang mungkin dilakukan adalah memperkuat keamanan sistem dengan meningkatkan lapisan perlindungan, mengadopsi teknologi keamanan yang lebih canggih, dan melibatkan pakar keamanan untuk mengurangi risiko serangan tersebut.

## 2.4 Kerangka Penelitian

Kerangka penelitian diawali dengan melakukan studi literatur untuk topik penelitian komputasi awan guna memperoleh pemahaman yang mendalam tentang konsep dasar, perkembangan terkini, dan tantangan yang terkait dengan bidang tersebut. Dalam studi literatur ini, sumber-sumber terpercaya seperti jurnal ilmiah, konferensi, buku, dan publikasi *online* akan dikaji untuk mengumpulkan informasi yang relevan.

Selanjutnya, dalam kerangka penelitian ini akan dilakukan identifikasi terhadap aspek-aspek kunci yang perlu diteliti dalam konteks komputasi awan. Hal ini mencakup pemahaman tentang arsitektur komputasi awan, model pelayanan awan, pemanfaatan komputasi di dunia, serta potensi dan risiko pemanfaatan komputasi awan di Indonesia.

Setelah itu, kerangka penelitian akan mencakup penentuan tujuan dan rumusan masalah penelitian yang spesifik, yang akan menjadi panduan untuk melaksanakan penelitian secara lebih terfokus. Selanjutnya, kerangka penelitian akan melibatkan analisis data yang telah dikumpulkan, melalui kegiatan FGD. Hasil analisis ini akan digunakan untuk menjawab pertanyaan penelitian dan mencapai tujuan yang telah ditetapkan.




*Gambar 0-1 Kerangka Penelitian*

Terakhir, kerangka penelitian akan mencakup pembahasan hasil penelitian dan kesimpulan yang diperoleh. Hasil penelitian akan dievaluasi berdasarkan tujuan penelitian, dan implikasi praktis serta rekomendasi yang ditujukan pada pemerintah, penyedia komputasi awan dan pengguna komputasi awan. Dengan demikian, kerangka penelitian yang komprehensif dan terstruktur ini akan memungkinkan peneliti untuk melakukan penelitian keamanan komputasi awan yang informatif, relevan, dan berkontribusi.

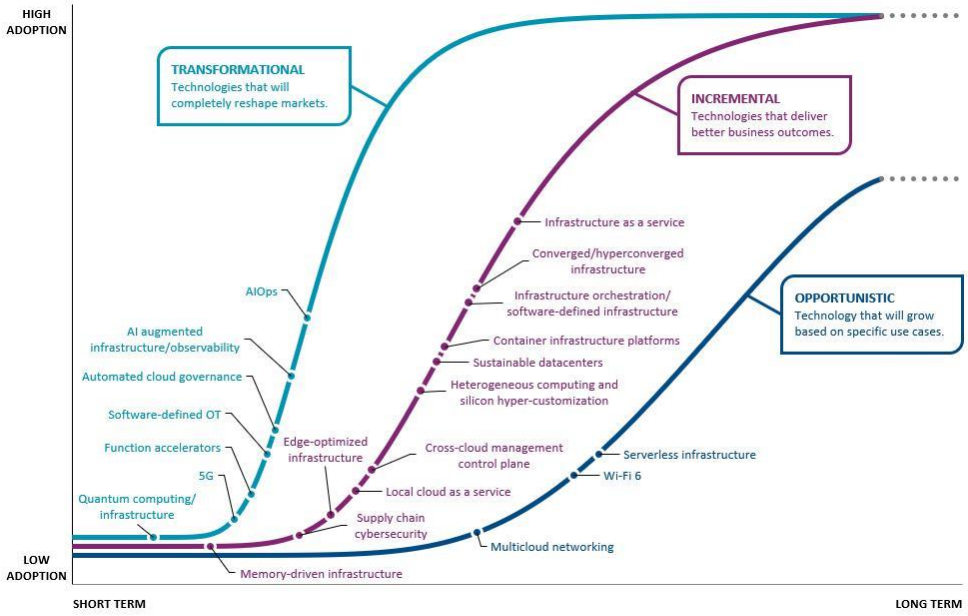
# BAB 3

# TEKNOLOGI KOMPUTASI AWAN

Komputasi awan telah berevolusi menjadi teknologi baru sebagai fondasi untuk teknologi baru lainnya seperti AI, IoT dan *blockchain*. Semua teknologi tersebut tidak akan mungkin dilakukan dalam skala besar tanpa komputasi awan sebagai fondasinya. Komputasi awan memungkinkan teknologi baru ini berkembang dikarenakan perkembangannya itu membutuhkan banyak data dan waktu pemrosesan cepat sesuai kebutuhan. Gambar 2-1 (Duncan et al., 2020) memperlihatkan bahwa semua adopsi teknologi terkini pada berbagai bidang, melibatkan komputasi awan sebagai infrastruktur dasarnya.

## 3.1 Definisi dan Karakteristik Komputasi Awan

Komputasi awan (*cloud computing)* memiliki berbagai definisi. Namun definisi yang sering dirujuk berasal dari *National Institute of Standards and Technology* (NIST) yang menyatakan bahwa komputasi awan adalah model yang menyediakan akses ke sumber daya komputasi terpusat yang luas dan dapat disesuaikan dengan kebutuhan, termasuk jaringan, server, *storage*, aplikasi, dan layanan (The NIST Definition of Cloud computing, 2011). Dengan demikian, sumber daya tersebut dapat dengan mudah untuk digunakan atau dibatalkan, dan ini meminimalkan beban pengelolaan dan interaksi dengan penyedia layanan. *International Telecommunication Union* (ITU) mendefinisikan komputasi awan sebagai model jaringan yang dapat diakses untuk sumber daya fisik dan virtual yang dapat diskalakan dan memiliki fleksibilitas dengan menyesuaikan layanan dan mengelola kebutuhan individu (ISO/IEC, 2014).




*Gambar 0-1 Komputasi awan sebagai fondasi teknologi terkini*

*European Commission* (European Commission, 2012) coba merangkum karakteristik atau fitur yang menjadi definisi dari komputasi awan. Mereka menyoroti bahwa definisi komputasi awan bersifat sangat abstrak sehingga definisi umum menjadi sulit dipahami, namun cukup untuk meringkas karakteristik dari komputasi awan. Satu hal yang cukup identik adalah komputasi awan merupakan bentuk akses ke sumber daya yang dapat dicapai melalui akses jarak jauh. Lebih lanjut, *European Commission Directorate-General for Informatics* (EU.Commission, 2019) menuliskan definisi komputasi awan sebagai paradigma teknologi informasi (TI) yang memungkinkan akses dari mana pun terhadap sumber daya sistem yang dapat dikonfigurasi dan layanan TI tingkat tinggi yang dapat tersedia secara dinamis dengan usaha yang minimal melalui internet. Komputasi awan juga bergantung pada sumber daya berbagi pakai untuk mencapai skala ekonomi.

Beberapa karakteristik penting dari komputasi awan seperti yang didefinisikan oleh NIST (The NIST Definition of Cloud computing, 2011) adalah sebagai berikut:

a. *On-demand*: konsumen dapat secara sepihak menyediakan layanan komputasi tanpa interaksi langsung dengan manusia.
b. Akses jaringan yang luas: kemampuan komputasi tersedia melalui jaringan dan diakses menggunakan mekanisme standar melalui platform *client* yang heterogen.
c. Penggabungan sumber daya: sumber daya komputasi dari penyedia layanan komputasi awan digabungkan untuk melayani banyak konsumen menggunakan model *multi-tenant*.
d. Elastis (dan cepat): kemampuan komputasi dapat disediakan dan dilepaskan secara elastis, bahkan otomatis, untuk menskalakan dengan cepat sesuai dengan kebutuhan.
e. Layanan terukur: layanan komputasi awan mengendalikan dan mengoptimalkan sumber daya secara otomatis dengan memanfaatkan kemampuan *metering*, yang biasanya digunakan pada model pembayaran *pay-per-use* (membayar sesuai penggunaan).

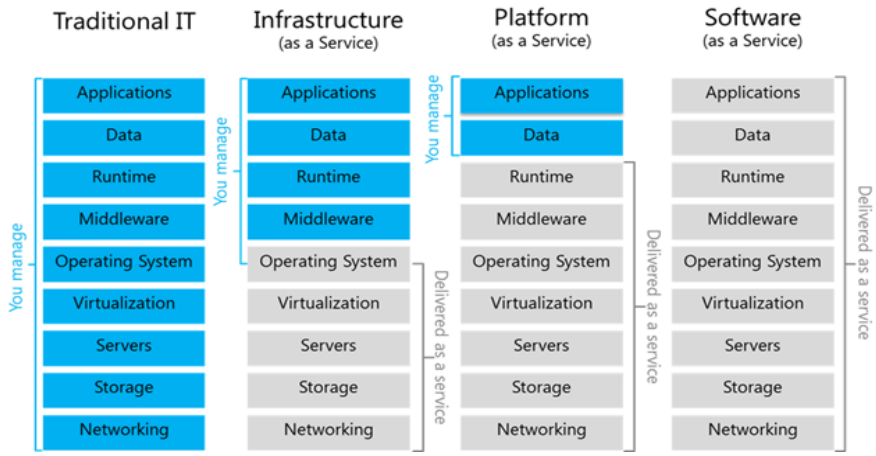
Untuk melengkapi daftar karakteristik yang dibuat oleh NIST, di antara karakteristik komputasi awan yang dirangkum oleh *European Commission* 2012 adalah:

a. Perangkat keras dimiliki oleh penyedia layanan komputasi awan dan bukan pengguna.
b. Pengoperasian perangkat keras dilakukan melalui jaringan komputer sehingga lokasi yang pasti dari data, proses, maupun *hardware* mana yang melayani seorang *user*, tidak harus menjadi perhatian *user*, walaupun mungkin ada konsekuensi terkait hukum yang berlaku.

c. Penyedia layanan komputasi awan sering kali memindahkan *workload* penggunanya untuk mengoptimalkan penggunaan perangkat keras yang tersedia.
d. Perangkat keras menyimpan dan mengolah data secara jarak jauh dan menyediakannya melalui aplikasi.
e. Pengguna dapat mengakses datanya atau aplikasi komputasi awan kapan dan di mana saja, melalui perangkat pribadi mereka, serta dapat memilih model layanan yang sesuai dengan kebutuhan mereka.
f. Biaya jasa akan disesuaikan dengan pemakaian yang sebenarnya (*pay-per-use*), serta tidak terikat dengan biaya tetap.

## 3.2 Model Layanan Komputasi Awan

Mell & Grance (2011) dari NIST mendefinisikan tiga jenis model layanan dasar dari komputasi awan, yaitu *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS), dan *Software as a Service* (SaaS), yang secara sederhana dapat dijelaskan melalui Gambar 0-2.




*Gambar 0-2 Perbandingan model layanan komputasi awan dan sistem TI tradisional* (Chou, 2018)

## 3.3 Model Deployment Komputasi Awan

Empat model *deployment* dari komputasi awan telah didefinisikan oleh NIST, yaitu *private* komputasi awan, *community* komputasi awan, *public* komputasi awan dan *hybrid* komputasi awan (The NIST Definition of Cloud computing, 2011). *Private* komputasi awan adalah layanan komputasi awan yang disediakan untuk memenuhi kebutuhan internal sebuah organisasi. Infrastrukturnya disediakan untuk penggunaan eksklusif oleh organisasi tersebut. Infrastruktur tersebut dapat dimiliki, dikelola dan dioperasikan oleh organisasi yang bersangkutan, pihak ketiga, atau kombinasi keduanya, serta dapat berlokasi di tempat organisasi tersebut berada atau di tempat lain.

*Community* komputasi awan adalah layanan komputasi awan yang dibangun eksklusif untuk komunitas tertentu, terdiri atas beberapa organisasi yang memiliki perhatian atau kepentingan yang sama, misalnya dalam hal standar keamanan, kebijakan, *compliance*, dan sebagainya. Kepemilikan, pengelolaan, operasional dan lokasi dari *infrastruktur community* komputasi awan hampir sama dengan *private* komputasi awan, akan tetapi dapat melibatkan satu atau lebih organisasi di dalam komunitas tersebut.

*Public* komputasi awan merupakan layanan komputasi awan di mana infrastruktur komputasi awan disediakan secara terbuka oleh masyarakat umum. Infrastruktur publik komputasi awan dapat dimiliki, dikelola, dan dioperasikan entitas bisnis, akademia, atau pemerintah, atau beberapa kombinasi dari ketiganya, serta berlokasi di tempat penyedia layanan komputasi awan.

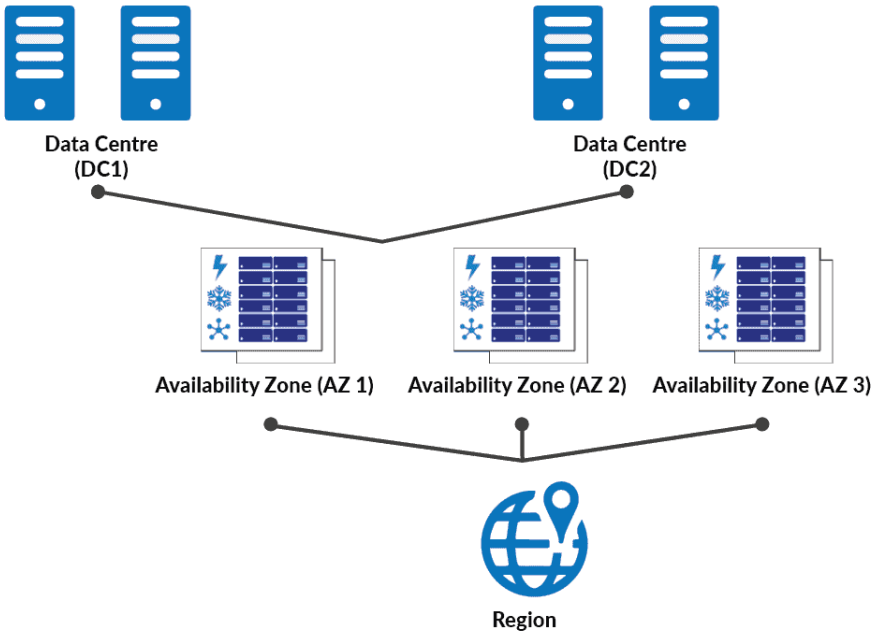
Komputasi awan hibrid merupakan kombinasi publik komputasi awan dengan *private* atau *community* komputasi awan yang diimplementasikan oleh suatu organisasi atau komunitas. Dalam hal ini, organisasi dapat memilih proses bisnis mana yang bisa dipindahkan ke publik komputasi awan dan mana yang ada di *private* atau *community* komputasi awan.

## 3.4 Infrastruktur Global Publik Komputasi Awan

Agar dapat melayani pengguna yang berasal dari seluruh belahan dunia, layanan yang diberikan oleh para penyedia layanan publik komputasi awan perlu dibangun di atas infrastruktur global yang masif, andal, kokoh, dan tersebar di berbagai bagian bumi. Infrastruktur global dari penyedia layanan *publik* komputasi awan pada dasarnya dibentuk oleh dua komponen penting, yaitu infrastruktur fisik dan konektivitas jaringan. Komponen infrastruktur fisik terdiri atas banyak pusat data yang tersebar di beberapa belahan dunia, tersusun menjadi beberapa region dan saling terhubung oleh jaringan. Dengan konektivitas jaringan global yang dimiliki penyedia layanan publik komputasi awan, setiap pusat data tersebut dapat beroperasi dengan ketersediaan tinggi (*high availability*), latensi rendah, dan *scalable*. Selain itu, trafik yang melintas antar pusat data tersebut tidak memasuki jaringan internet publik, atau tetap berada di dalam jaringan milik penyedia layanan publik komputasi awan tersebut (Azure, 2023).

Seperti telah disebutkan sebelumnya, infrastruktur fisik global dari penyedia layanan publik komputasi awan tersusun atas beberapa region. Region merupakan lokasi fisik di berbagai belahan dunia di mana penyedia layanan publik komputasi awan memiliki kluster dari beberapa pusat data. Setiap region itu terdiri atas beberapa *Availability Zones* (AZ) yang saling terisolasi dan terpisah secara fisik pada suatu area geografis. AZ itu sendiri merupakan satu atau lebih pusat data yang berbeda secara fisik dengan sumber daya, jaringan dan konektivitas yang redundan dalam sebuah region (AWS, 2023).

Tiap-tiap pusat data yang tergabung dalam sebuah AZ memiliki sumber daya, pendingin, dan jaringan yang mandiri dan tidak saling bergantung satu sama lain. Gambar 0-3 menggambarkan secara sederhana posisi dan hubungan antara region, *availability zone* dan pusat data (*datacenter*) dalam infrastruktur global yang dimiliki oleh sebuah penyedia layanan publik komputasi awan.




*Gambar 0-3 Posisi region, availability zone, dan pusat data dalam infrastruktur komputasi awan*

## 3.5 Cloud Native

Selama dekade terakhir, sejak ide komputasi awan pertama kali diajukan, teknologi TI memasuki era baru yang menampilkan konektivitas, digitalisasi, dan kecerdasan. Layanan seluler terbuka untuk konsumen dan layanan TI tertutup untuk perusahaan, industri, dan pemerintah sekarang semuanya beralih ke komputasi awan. Dalam banyak praktik transformasi digital, komputasi awan, *big data*, AI, dan IoT diintegrasikan ke dalam layanan komputasi awan, terlepas dari komputasi awan publik dan privat, komputasi awan khusus industri, atau komputasi awan *e-Government*. Basis digital asli komputasi awan satu atap menangani kompleksitas yang membebani pengembang dan personel O&M, memungkinkan inovasi, operasi, pengambilan keputusan, dan produktivitas yang lebih baik dengan menyediakan layanan komputasi awan yang mudah digunakan. *Cloud Native*

merangkum atribut arsitektur komputasi awan utama, seperti skalabilitas sesuai permintaan, penyekalaan horizontal, keandalan dan redundansi tinggi, serta pemisahan status dan aplikasi, ke dalam model desain arsitektur, arsitektur referensi standar, dan metodologi untuk memandu perusahaan memindahkan aplikasi mereka ke komputasi awan.

Pendirian *Cloud Native Computing Foundation* (CNCF) (CNCF, 2023) dan Kubernetes (The Linux Foundation, n.d.) (K8s) *open source* memperkenalkan sumber daya komputasi yang ringan dan diminimalkan serta merangkum aplikasi. Praktik-praktik ini mengarah pada pemilihan teknologi modular standar. Sementara itu, metodologi *Cloud Native,* kumpulan alat, dan arsitektur referensi *full-stack* diverifikasi dan disempurnakan lebih lanjut di komunitas CNCF. Perusahaan telah dapat memigrasikan layanan TI mereka ke komputasi awan tanpa perubahan apa pun, dan sekarang mereka dapat mencoba merekonstruksi arsitektur TI mereka menjadi *Cloud Native* dengan menggunakan komponen dan platform *opensource* yang memaksimalkan kekuatan teknis komputasi awan. Namun, teknologi *Cloud Native* dalam komunitas *open source* seperti CNCF, meskipun sudah selangkah lebih maju dari desain abstrak, masih jauh dari cukup untuk merekonstruksi seluruh sistem TI. Platform terkontainerisasi belaka terbukti tidak memadai untuk mendukung logika layanan yang dikembangkan sendiri oleh perusahaan, belum lagi skalabilitas, keandalan, dan ketersediaan aplikasi *Cloud Native* dalam status penerapan dan pengoperasian untuk setiap *instance*.

Perusahaan menghadapi tantangan dalam efisiensi pengembangan *end-to-end* layanan inti dan aplikasi AI, skalabilitas lapisan data arsitektur TI vertikal tradisional, pengurangan latensi, dan perlindungan kedaulatan/privasi data (dua yang terakhir berkinerja buruk dengan kumpulan sumber daya komputasi awan terpusat). Jaringan pipa DevOps, *middleware* terdistribusi, basis data terdistribusi, perangkat *cloud computing-edge*, dan kolaborasi multi-komputasi awan, serta AI inklusif adalah semua hal penting untuk migrasi

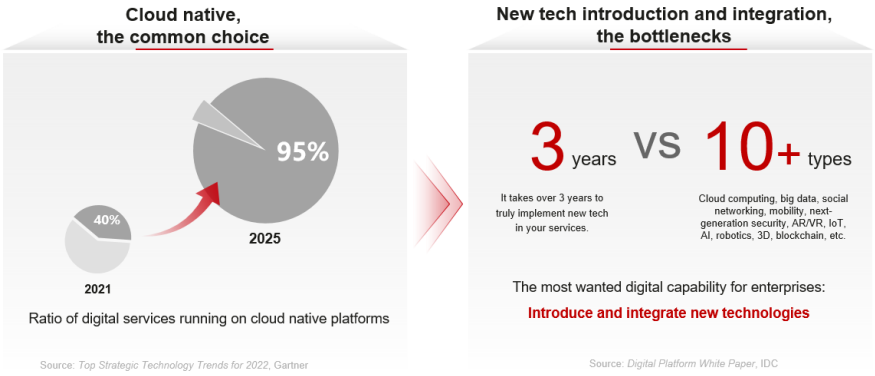
*Cloud Native full-stack*. Dalam hal ini, Huawei *Clous Computing* mengusulkan konsep dan kerangka kerja "*Cloud Native* 2.0" yang melengkapi konsep *Cloud Native* dan teknologi *open source* yang sudah ada, berdasarkan kontribusinya dan kepemimpinan komunitas, inovasi *Cloud Native* dalam kumpulan teknologi lengkap, dan pengalaman praktis dalam mendukung migrasi komputasi awan untuk ribuan pelanggan industri. Usulan ini merupakan pemikiran, saran, dan pandangan *Huawei* Komputasi awan tentang migrasi komputasi awan dan transformasi digital kepada mitra ekosistem dan pelanggan industri. *Cloud Native* 2.0 mendefinisikan komputasi awan dalam dekade berikutnya. Arsitektur dan teknologi referensi standar, terbuka, dan dapat ditiru dari fondasi komputasi awan cerdas untuk mempercepat terlaksananya ekonomi digital.

### 3.5.1 Cloud Native, Jalan Menuju Era Digitalisasi

Di era *Cloud Native* 2.0, migrasi komputasi awan telah bergeser dari "*On* Komputasi awan" menjadi "*In* Komputasi awan" dan dari berorientasi sumber daya menjadi berorientasi aplikasi. Layanan lahir dan tumbuh di dalam komputasi awan. Aplikasi *Cloud Native* di berbagai industri seperti Internet, keuangan, pemerintahan, dan manufaktur membawa nilai dan pengalaman baru dalam berbagai aspek. *Cloud Native* menjadi pilihan bagi pelanggan pemerintah dan perusahaan swasta untuk mewujudkan transformasi digital. *Cloud Native* merupakan jalan menuju transformasi digital yang nyata. Menurut Gartner, pada tahun 2025, proporsi layanan digital yang berjalan di platform *Cloud Native* akan meningkat dari 40% pada tahun 2021 menjadi 95% (Gartner, 2021).

Dalam beberapa tahun terakhir, semakin banyak teknologi baru yang berbasis *Cloud Native*, seperti *big data*, AI, AR/VR, IoT, dan *blockchain*. Dibutuhkan setidaknya tiga tahun atau lebih lama bagi sebuah organisasi untuk sepenuhnya menguasai teknologi baru, apalagi untuk mengintegrasikan teknologi tersebut ke dalam sistem TI mereka. Menurut

survei IDC terhadap 360 perusahaan di seluruh dunia, kemampuan digital yang paling diinginkan perusahaan adalah terus menggunakan dan mengintegrasikan teknologi baru (Huawei Enterprise, n.d.). Perkembangan *Cloud Native* seperti yang terungkap dari penelitian Gartner dan IDC (Gartner, 2021) dirangkum pada Gambar 0-4.




*Gambar 0-4 Perkembangan Cloud Native* (Gartner, 2021)

### 3.5.2 Berpikir dan Bertindak Cloud Native

Konsep *Cloud Native* pertama kali diusulkan oleh WSO2, sebuah vendor *middleware* integrasi aplikasi, pada tahun 2010 (Freemantle, 2010). Fitur utama dari *Cloud Native* adalah sebagai berikut:

a. Terdistribusi, terhubung dinamis: Aplikasi dan *middleware* komputasi awan harus mendukung beberapa *node* yang berjalan secara bersamaan yang berbagi konfigurasi dan berbagi status sesi. Aplikasi komputasi awan tidak hanya akan ditulis dalam satu bahasa.
b. Hasilnya adalah aplikasi harus disambungkan secara dinamis.
c. Elastis: *Subnode* terdistribusi dari aplikasi berbasis komputasi awan dan *middleware* harus dapat diperkecil (*scale-down*) maupun diperbesar (*scale-up*), berdasarkan beban, termasuk memanggil

API untuk memulai dan menghentikan VM *image*.

d. *Multi-tenant*: Ada dua mode *multi-tenant* untuk aplikasi dan *middleware* berbasis komputasi awan. Salah satunya adalah *multi-tenancy* fisik yang diimplementasikan dengan menyalin *instance* aplikasi ke beberapa VM atau kontainer, dan yang lainnya adalah *multi-tenancy* logis yang berfokus pada isolasi multi-penyewa logis intrinsik dari aplikasi dan *middleware* berbasis komputasi awan. Disarankan agar *multi-tenancy* logis digunakan karena menggunakan sumber daya yang lebih sedikit daripada *multi-tenancy* fisik ketika persyaratan *multi-tenant* aplikasi dan *middleware* berbasis komputasi awan terpenuhi.
e. Swalayan: Penyediaan dan pengelolaan swalayan adalah kunci untuk mendapatkan hasil maksimal dari sistem komputasi awan.
f. Jika mengandalkan administrator untuk mengaturnya, mengonfigurasinya, dan mengelolanya, maka itu bukanlah perangkat lunak, platform, atau infrastruktur "*as-a-Service*".
g. Pada tingkat infrastruktur, layanan mandiri berarti mengelola mesin virtual (VM). Di tingkat platform, swalayan berarti mengelola dan menerapkan aplikasi produksi dan *middleware*.
h. Terukur dan ditagih secara terperinci: Satu poin penting dari komputasi awan adalah bayar per penggunaan (*pay-per-use*). Namun hal ini haruslah terperinci. Bayar per tahun tidak sama dengan bayar per jam. Bahkan dalam komputasi awan pribadi, pengukuran sangat penting. Dalam sistem swalayan, *multi-tenant*, dan elastis, penggunaan aktual adalah biaya yang sebenarnya. Oleh karena itu, memahami, mengukur, dan memantau penggunaan tersebut sangatlah penting.
i. Diterapkan dan diuji secara bertahap: Dalam lingkungan bervolume tinggi yang sangat skalabel, bahkan setelah

sepenuhnya dilakukan uji unit dan sistem (*unit & system testing*) pada versi baru, mungkin ada keinginan untuk menguji versi baru "di tempat" di lingkungan komputasi awan langsung.

j. Mengalihkan lalu lintas antar versi bukan hanya keputusan biner.
k. *Cloud Native* meningkatkan pemanfaatan sumber daya, efisiensi penyediaan, dan tata kelola aplikasi. Fitur-fitur *Cloud Native* sebelumnya mungkin mirip dengan elemen kunci komputasi awan yang didefinisikan oleh NIST. Komputasi awan didefinisikan dari perspektif komputasi awan platform, sedangkan *Cloud Native* diusulkan berdasarkan aplikasi berbasis komputasi awan.

### 3.5.3 Fitur Teknis Cloud Native 1.0

Berdasarkan pengaruh *Cloud Native* terhadap manajemen siklus hidup penuh suatu aplikasi perusahaan, selama migrasi komputasi awan dan pada penambangan nilai layanan komputasi awan *full-stack*, fitur teknis *Cloud Native* dapat diringkas menjadi dua aspek berikut.

Fitur 1: Berorientasi *container* dan *microservice*

Mengambil NetFlix sebagai contoh, NetFlix digunakan di AWS dan dipisahkan serta dipecah menjadi beberapa *microservice* (Varshneya, n.d.). Setiap *microservice* mendukung satu fungsi dan satu atau lebih kontainer yang berjalan. Semua *microservice* membuka API REST atau gRPC deklaratif sebagai satu-satunya antarmuka untuk berinteraksi dengan *microservice* lainnya. Pengembangan *microservice* tidak rumit dan dapat diselesaikan oleh sekitar 10 orang. Semua *microservice* memiliki basis data dan lapisan data persistensi mereka sendiri secara independen. Hal ini memastikan bahwa semua *microservice* dapat dipisahkan sepenuhnya dalam kondisi berjalan untuk memperbarui secara mandiri, mendukung bahasa pengembangan yang berbeda, dan mengimplementasikan penskalaan sesuai permintaan dalam hitungan detik berdasarkan kontainer. (Kontainer lebih ringan

daripada VM dan mudah dimulai dan dihentikan dalam hitungan detik). Paket rilis kontainer berisi *image* aplikasi dan dependensi pustaka yang diperlukan serta variabel lingkungan. Selain itu, kerangka kerja *microservice* (*Spring* Komputasi awan (VMware, 2023), *ServiceComb* (Apache ServiceComb, 2023) dan CSE (Co., 2018)) dari bahasa *open source* tertentu dapat mengelola *microservice* terdistribusi menggunakan *sidecar* (Velichko, 2021) dan *service logic binding* dalam mode non-intrusif, serta *Istio service mesh* (Istio, 2023) yang menyediakan *service discovery*, rilis bertahap (*grayscale release*), deteksi pencilan (*outlier detection*), kontrol aliran, dan manajemen lalu lintas.

Fitur 2: Merekonstruksi dan mengembangkan perusahaan

Aplikasi atau layanan berbasis komputasi awan *middleware*, *database*, dan *reusable services* setelah tantangan dalam mengkontainerisasi logika layanan diatasi, *middleware* dan *database* yang bergantung perlu dipindahkan dari ruang aplikasi ke komputasi awan. Mengambil contoh *Salesforce*, logika layanan umum dari aplikasi perusahaannya dipindahkan ke platform aplikasi untuk mengimplementasikan pembagian lintas penyewa (Bobrowski, n.d.). Untuk lebih menyederhanakan isolasi sumber daya antar penyewa, *Salesforce* mengabstraksikan logika aplikasi di seluruh penyewa menggunakan *Model-Driven Architecture* (MDA) dan mengimplementasikan berbagi *database* (menyesuaikan dan memetakan kembali tabel data penyewa berdasarkan templat *database* terpadu) pada lapisan platform. Singkatnya, kemampuan berbagi lintas penyewa (*logical multi-tenancy*) pada lapisan aplikasi dan layanan data melindungi isolasi antara lapisan sumber daya penyewa komputasi awan.

Migrasi komputasi awan juga dapat dilakukan dengan menggunakan *high-control application PaaS* (*hcaPaaS*) dan *high-productivity application PaaS* (*hpaPaaS*) untuk melindungi sumber daya yang mendasari aplikasi penyewa komputasi awan dan mengimplementasikan penskalaan tingkat aplikasi dan DB pada platform aplikasi. *hcaPaaS* merupakan platform *PaaS* yang

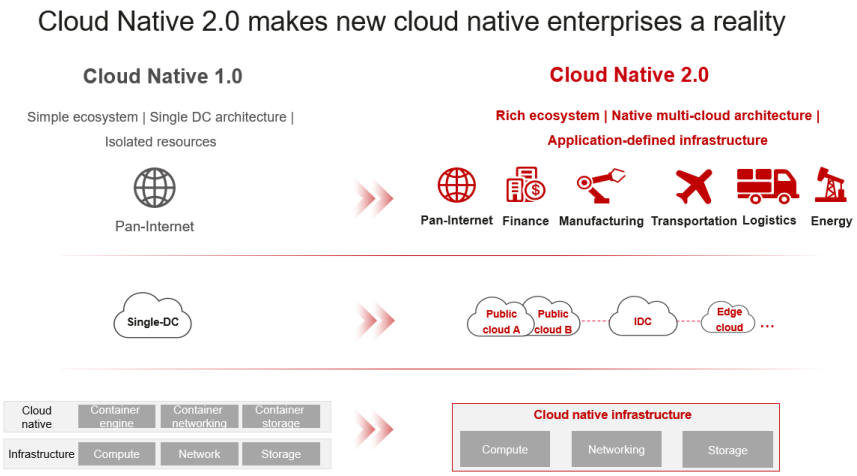
digabungkan dengan sumber daya yang mendasarinya dan di mana aplikasi mengetahui penskalaan sumber daya yang elastis. Fitur lain dari hpaPaaS adalah *low/no code*, yang berarti penyebaran lingkungan produksi aplikasi dapat dilakukan dengan menggunakan *template*/DSL pada fase pengembangan berdasarkan logika aplikasi.

### 3.5.4 Cloud Native 2.0

Teknologi *Cloud Native*, meskipun berkembang dengan cepat, menghadapi lebih banyak tantangan seiring dengan munculnya permintaan layanan baru. Pencarian solusi akan mengantarkan pada *Cloud Native* generasi berikutnya, yaitu *Cloud Native* 2.0 (Huawei, 2022a). *Cloud Native* 2.0 diawali dengan pendirian *Cloud Native Computing Foundation* (CNCF) dan evolusi teknologi *open source* yang bercabang dari kontainer, *microservice*, dan *DevOps* ke infrastruktur Cloud Native, orkestrasi dan manajemen, keamanan komputasi awan, pemantauan dan analisis, data besar, AI, *database*, dan aplikasi untuk skenario khusus, rantai teknologi siklus hidup penuh dikembangkan untuk mengubah aplikasi menjadi Cloud Native. Lanskap *Cloud Native* CNCF telah berkembang dari satu proyek (*Kubernetes* untuk orkestrasi kontainer) menjadi lebih dari 100 proyek dalam lima kategori.

*Cloud Native* 2.0 memaksimalkan keunggulan teknologi komputasi awan full-stack, membebaskan para insinyur TI dari pengembangan dan O&M infrastruktur komputasi awan dan *middleware* yang membosankan dan memberatkan, serta membantu organisasi membangun atribut arsitektur utama non- fungsional, seperti skalabilitas, kelincahan, otomatisasi, penskalaan horizontal sesuai permintaan, keamanan, kepercayaan, ketahanan, ketersediaan tinggi, dan keandalan yang tinggi, di lapisan pemberdayaan platform dasar. Dengan cara ini, organisasi dapat mendedikasikan energi dan sumber daya mereka pada daya saing inti, mengejar efisiensi input dan output tertinggi dalam transformasi digital dan

cerdas. Gambar 0-5 memperlihatkan perbedaan ekosistem dan infrastruktur antara *Cloud Native* 1.0 dengan *Cloud Native* 2.0.




*Gambar 0-5 Cloud Native 2.0* (Huawei, 2022b)

Fitur utama 1: Komputasi awan terdistribusi

Komputasi awan terdistribusi mendistribusikan layanan komputasi awan ke berbagai wilayah geografis. Operasi, tata kelola, dan evolusi dapat disediakan oleh penyedia layanan komputasi awan. Saat ini, solusi komputasi awan terdistribusi sebagian besar disediakan oleh dan di-*hosting* ke penyedia layanan komputasi awan secara terpadu. Komputasi awan terdistribusi memungkinkan layanan komputasi awan lebih dekat dengan pengguna akhir, mendukung skenario latensi rendah, mengurangi biaya data, dan membantu organisasi mematuhi hukum dan peraturan yang mengharuskan data tetap berada di wilayah tertentu. Ketika perusahaan terjun lebih dalam ke dalam transformasi digital, infrastruktur komputasi awan menjadi lebih kompleks dan skalanya menjadi lebih besar, sehingga membutuhkan lebih banyak investasi O&M. Untuk mengatasi masalah ini, platform komputasi awan terdistribusi disediakan bagi organisasi untuk melakukan penerapan

terpusat dan O&M yang di-*hosting*. Dengan cara ini, organisasi dapat fokus pada layanan mereka.

Dalam hal cakupan geografis, komputasi awan terdistribusi mengelola layanan yang digunakan di seluruh jaringan: di area inti, area *hotspot*, ruang peralatan lokal, dan lokasi layanan, sehingga memberikan pengalaman yang optimal bagi pengguna yang berbeda.

Dalam hal infrastruktur, infrastruktur yang membawa layanan lapisan atas dapat disediakan oleh satu vendor untuk membentuk arsitektur tunggal. Atau bisa juga disediakan oleh beberapa vendor. Dalam hal ini, platform manajemen *Cloud Native* terpadu diperlukan untuk mengelola layanan lintas komputasi awan. Apa pun bentuk yang digunakan, platform *Cloud Native* lapisan atas harus disatukan. Gartner memprediksi bahwa pada tahun 2025, lebih dari 50% organisasi akan menggunakan komputasi awan terdistribusi. Pengembangan dan mempopulerkan terminal seluler, *Internet of Things* (IoT), dan penyebaran layanan lintas wilayah perusahaan telah menyebabkan permintaan yang kuat untuk komputasi awan terdistribusi. Video interaktif (seperti AR, VR, dan *game* komputasi awan) dan aplikasi organisasi yang membutuhkan latensi rendah (aplikasi OT) serta penyimpanan data lokal (kepatuhan) dan pemrosesan (pengawasan video) mendorong pengembangan infrastruktur *rendering* dan komputasi lokal. Penyebaran infrastruktur akan berevolusi dari penyebaran terpusat ke penyebaran terdistribusi, mencapai cakupan komputasi awan last-mile.

Fitur utama 2: Infrastruktur berbasis aplikasi

Komputasi awan telah menjadi tempat yang populer untuk penerapan aplikasi. Mulai dari *microservice* , data besar, dan AI, hingga *middleware*, standar infrastruktur komputasi awan terus meningkat. *Microservice* adalah aplikasi berbasis komputasi awan yang khas. Permintaan sumber daya *microservice* sangat berfluktuasi berdasarkan penggunaan pengguna. Oleh

karena itu, layanan komputasi awan harus menyediakan sumber daya yang cukup dan dapat memulai *instance* dengan cepat. *Microservice* juga memiliki persyaratan yang tinggi pada latensi dan SLA. *Big data* dan AI membutuhkan sumber daya berkinerja tinggi dalam jumlah besar untuk membantu perusahaan mengatasi lingkungan bisnis yang kompleks. Hal yang sama berlaku untuk *middleware*.

Layanan *Cloud Native* berskala besar membutuhkan sumber daya jaringan yang memadai, isolasi jaringan di mana-mana, fleksibilitas jaringan yang optimal, dan QoS jaringan yang halus (*granular*). Dalam hal pasokan sumber daya, satu VPC (*Virtual Private* Komputasi awan) dapat memiliki beberapa *cluster* dengan jutaan kontainer dan migrasi *cluster* dalam skenario DR (*Disaster Recovery*) memerlukan jaringan dan isolasi tingkat kontainer, seperti QoS dan pembatasan *bandwidth*. Sejumlah besar kontainer dapat disediakan dengan cepat (100.000 kontainer per menit). Dalam hal fleksibilitas jaringan, layanan *Cloud Native* yang ringan, seperti *serverless* dan fungsi-fungsi yang dapat dibuat dalam hitungan mili detik dan dimulai dalam hitungan detik (termasuk perampingan jaringan *end-to-end*). Dalam hal isolasi jaringan, isolasi tingkat kontainer dan ACL yang langsung berlaku diperlukan untuk jaringan *Cloud Native* yang memiliki fitur di mana-mana, tanpa kepercayaan, kontainer masif, dan sangat dinamis. Dalam hal perincian sumber daya, QoS dari port jaringan kontainer (termasuk jaminan *bandwidth* dan dukungan prioritas) diperlukan untuk penerapan hibrida layanan *online* dan *offline*. Arsitektur jaringan komputasi awan terus berkembang untuk memenuhi kebutuhan yang terus berubah.

Fitur utama 3: *Hybrid deployment* dan penjadwalan terpadu

Sebelumnya, daya komputasi dan granularitas dipilih berdasarkan kebutuhan aplikasi dan direncanakan secara terpisah, sehingga sangat memengaruhi pemanfaatan sumber daya dan O&M aplikasi yang menantang. Di era Cloud Native, kontainer, *microservice*, dan orkestrasi

dinamis telah membentuk standar industri terpadu. Teknologi seperti penjadwalan cerdas menyediakan kumpulan sumber daya terpadu untuk aplikasi, memungkinkan *hybrid deployment* dari beberapa aplikasi dan kolaborasi yang efisien dengan sumber daya.

Fitur utama 4: *Serverless*

Komputasi awan muncul pada tahun 2006, diikuti oleh teknologi seperti komputasi dan virtualisasi jaringan dan OpenStack. Manajemen infrastruktur juga berevolusi untuk membebaskan kita dari pembangunan dan pemeliharaan ruang alat berat. Vendor komputasi awan menyediakan server virtual dan sumber daya jaringan, serta memigrasikan aplikasi dari server fisik ke server virtual untuk mengurangi biaya manajemen. *Docker* dan *Kubernetes* menjadi populer, dan kerangka kerja pengembangan Cloud Native, seperti Spring Komputasi awan dan Dubbo muncul. Vendor komputasi awan menyediakan alat seperti kontainer, kontrol dan manajemen kode, pipa kompilasi, pengujian otomatis, dan *middleware*. Alat-alat ini menyetandarkan lingkungan aplikasi, mendukung DevOps, menyederhanakan migrasi dan *hosting* aplikasi, serta meningkatkan orkestrasi dan O&M. *Serverless* menggabungkan pembuatan aplikasi dengan layanan komputasi awan untuk memanfaatkan sepenuhnya penskalaan elastis, penagihan bayar per penggunaan, dan fitur bebas O&M dari platform komputasi awan. Pada tahun 2019, vendor komputasi awan besar lainnya juga menambahkan produk *serverless* ke dalam portofolio mereka. *Serverless* memiliki tiga elemen dasar:

- Abstraksi dengan perincian kecil atau besar: Hal ini menghilangkan kerumitan pemrograman dan bekerja dengan server.
- Penagihan bayar per penggunaan: Pengguna tidak perlu membayar untuk sumber daya yang tidak digunakan.
- Pennyekalaan sesuai permintaan: Penggunaan sumber daya disesuaikan secara otomatis dan cepat.

Dengan menggunakan *serverless*, vendor komputasi awan secara fleksibel mengelola sumber daya yang menganggur, meningkatkan pemanfaatan sumber daya sistem, dan mencapai kesuksesan bersama. (Jonas et al., 2019) menyimpulkan bahwa platform komputasi awan yang ada saat ini masih belum memuaskan dalam hal O&M dan pemanfaatan perangkat keras. Para pengembang ditantang untuk mengelola keandalan VM, penyeimbangan beban, pemulihan bencana, perluasan dan pengurangan kapasitas, pemantauan, log, dan peningkatan sistem. Perusahaan kecil merasa sulit untuk mempekerjakan personel O&M atau *DevOps* yang terampil dan tidak dapat menyelesaikan masalah melalui alat otomatisasi, skrip, atau layanan.
Komputasi *serverless* diharapkan dapat menutupi kekurangan ini. *Serverless* melemahkan hubungan antara penyimpanan dan komputasi, membuat komputasi menjadi tanpa status, penjadwalan dan penskalaan menjadi lebih mudah, serta data menjadi lebih aman. Pengembang tidak perlu lagi membuat VM secara manual atau mengelola sumber daya lainnya, seperti *bandwidth* jaringan. Sebaliknya, mereka hanya perlu fokus pada pengkodean. Selain itu, penagihan lebih masuk akal, karena fungsi ditagih berdasarkan jumlah pemanggilan dan *overhead* sumber daya dari setiap permintaan pemanggilan.

Fitur utama 5: Pemisahan penyimpanan dan komputasi

Semakin banyak perusahaan yang beralih ke sistem pemrosesan data komputasi awan dengan penyimpanan dan komputasi terpisah dari *cluster* lokal konvensional dengan penyimpanan dan komputasi yang digabungkan. Dengan sistem seperti itu, perusahaan meng-*host* layanan mereka di komputasi awan, menggunakan sumber daya penyimpanan dan komputasi platform pemrosesan data milik vendor komputasi awan, dan hanya berfokus pada pengembangan dan pemeliharaan bisnis mereka. Sistem pemrosesan data dengan penyimpanan dan komputasi yang digabungkan memiliki beberapa kekurangan berikut ini:

- Pemanfaatan sumber daya komputasi yang rendah: Seiring dengan meningkatnya volume data, kapasitas *cluster* diperluas, tetapi permintaan komputasi tidak meningkat secara signifikan dan konsumsi komputasi berfluktuasi.
- Akibatnya, pemanfaatan sumber daya komputasi menjadi rendah, misalnya, pemanfaatan CPU rata-rata lebih rendah dari 50%, sehingga meningkatkan biaya secara keseluruhan.
- Salinan data yang mahal: Komputasi *pipeline* di seluruh siklus hidup data membutuhkan komputasi di beberapa *cluster*.
- Namun, data hampir tidak dapat dibagi di antara *cluster*, dan menyalin data serta menyimpan banyak salinan data membutuhkan biaya yang mahal. Selain itu, pemrosesan transaksi data *online* membutuhkan kemampuan baca yang lebih baik dan salinan lengkap data, sedangkan menyalin data itu memakan waktu serta menyimpan data itu mahal.
- Risiko keandalan yang tinggi: Kluster besar dengan penyimpanan dan sumber daya komputasi yang digabungkan memiliki risiko O&M dan keandalan yang tinggi. Misalnya, peningkatan beberapa komponen dapat memengaruhi semua layanan, menyebabkan *preemption* sumber daya yang parah di antara layanan dan meningkatkan risiko keandalan O&M.
- *Deployment* lintas AZ yang sulit: Aplikasi dan data biasanya digunakan di seluruh AZ untuk memastikan ketersediaan sistem yang tinggi. Dalam sistem pemrosesan data dengan penyimpanan dan komputasi yang digabungkan, konsistensi data antara AZ dijamin oleh lapisan komputasi. Khususnya dalam penerapan basis data lintas AZ untuk memproses transaksi online, visibilitas transaksi perlu dicapai pada lapisan komputasi, yang kompleks dan

berdampak signifikan pada kinerja.

Di sisi lain, pelanggan pemerintah dan perusahaan menghadapi tantangan berikut dalam tata kelola data:

- Jumlah yang sangat besar dan berbagai jenis data: Sebagai contoh, sebuah pusat layanan kesehatan memiliki 100 data inventaris PB dan 40 TB data tambahan per hari. Pengurutan gen lengkap untuk seseorang berisi 100 GB data, dan data perawatan kesehatan presisi suatu negara dapat mencapai exabyte.
- Data waktu nyata *(real time*): Ada sejumlah besar titik pengukuran data deret waktu IoT yang sering melaporkan data. Sebagai contoh, sebuah perusahaan besi dan baja memiliki lebih dari 20.000 titik pengukuran sensor yang melaporkan data setiap 100 ms hingga 1 detik untuk analisis tren dan pemantauan pengecualian waktu nyata. Ini merupakan tantangan untuk memungkinkan kolaborasi perangkat-*edge*-komputasi awan untuk mengompresi, menganalisis, dan memprediksi data deret waktu.
- Berbagai macam data: analisis korelasi dan pemrosesan data multi-modal menjadi hal yang biasa, misalnya, investigasi keamanan publik melibatkan berbagai jenis data, seperti lokasi, hubungan sosial, perilaku dunia maya, dan sejumlah besar data tak terstruktur, seperti audio, video, dan arsip kasus. Teknologi AI dapat digunakan untuk menambang data tidak terstruktur dan secara otomatis mengaitkan data tidak terstruktur dengan catatan terstruktur.
- Komputasi terkonvergensi: Inovasi bisnis membutuhkan konvergensi data lintas domain. Sebagai contoh, pembuatan profil pelanggan Internet yang tepat dan pemasaran yang presisi membutuhkan konvergensi data termasuk lokasi, perilaku konsumsi, hubungan sosial, dan opini publik, serta analisis data kolaboratif lintas sumber dan lintas domain.

- Penyebaran data lintas AZ: Data bisnis perlu disebarkan di seluruh AZ untuk meningkatkan keandalan. Misalnya, simpul data dari situs asuransi kesehatan harus digunakan di setidaknya dua AZ.

## 3.6 Keamanan Teknologi Komputasi Awan

Keamanan teknologi komputasi awan mengacu pada tindakan yang dilakukan untuk melindungi data, aplikasi, dan infrastruktur layanan komputasi awan dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran yang tidak sah. Keamanan komputasi awan merupakan aspek penting dari komputasi awan karena memastikan bahwa informasi sensitif dilindungi dari ancaman serangan siber.

Keamanan siber di pusat data tradisional bertugas melindungi semua aset teknologi pusat data tersebut sehingga semua aplikasi dan layanan dapat beroperasi tanpa risiko pemadaman dengan cara yang stabil, aman, dan berkinerja tinggi. Namun, terdapat perbedaan signifikan antara pusat data yang menjalankan layanan komputasi awan dan layanan TI tradisional. Salah satu perbedaan utama antara layanan komputasi awan dan layanan TI tradisional adalah sifat model tanggung jawab bersama untuk keamanan. Di pusat data tradisional, tanggung jawab untuk mengamankan infrastruktur, aplikasi, dan data hanya terletak pada organisasi yang memiliki dan mengoperasikan pusat data. Namun, dalam lingkungan komputasi awan, tanggung jawab keamanan dibagi antara penyedia komputasi awan dan pelanggan

Perbedaan utama lainnya adalah tingkat visibilitas dan kontrol yang dimiliki pelanggan atas keamanan aplikasi dan data mereka di lingkungan komputasi awan. Penyedia komputasi awan biasanya menawarkan berbagai layanan dan alat keamanan untuk membantu pelanggan mengamankan sumber daya

komputasi awan mereka, tetapi pelanggan harus bergantung pada penyedia untuk memantau dan menanggapi insiden keamanan.

Untuk itu, *Cloud Service Provider* (CSP) perlu mendukung penyesuaian variasi pengaturan keamanan lanjutan sesuai kebutuhan keamanan masing-masing pelanggan. Layanan keamanan ini menawarkan integrasi yang mendalam dengan fitur keamanan, pengaturan, dan kontrol di seluruh arsitektur. Dalam hal desain keamanan keseluruhan dan praktik keamanan sehari-hari, pusat data berorientasi layanan komputasi awan lebih memprioritaskan aspek-aspek berikut daripada pusat data TI tradisional, aspek tersebut di antaranya (Mobo, 2018):

a. Kelengkapan dan pengoptimalan solusi keamanan komputasi awan (terutama melalui otomatisasi);
b. Menyediakan arsitektur yang sangat adaptif, multi-layer, pertahanan mendalam yang mencakup infrastruktur, platform, aplikasi, dan keamanan data;
c. Keanekaragaman dan ekstensibilitas teknologi;
d. Konfigurasi, integrasi, dan orkestrasi kemampuan keamanan dan perlindungan privasi yang dapat disesuaikan untuk O&M (*Operation & Maintenance*) CSP dan O&M pengguna.

### 3.6.1 Model Tanggung Jawab Bersama

Ketika lingkungan komputasi berpindah dari *data center* yang dikendalikan pengguna ke *data center* komputasi awan, tanggung jawab keamanan juga bergeser. Ketika terjadi sebuah insiden keamanan siber pada layanan komputasi awan, maka siapakah yang bertanggung jawab atas keamanan? Apakah pelanggan atau penyedia layanan? Jawaban yang tepat adalah Keduanya. Baik *Cloud Service Consumer* (CSC) maupun CSP bertanggung jawab untuk memastikan lingkungan komputasi awan yang aman.

Keamanan sekarang menjadi perhatian kedua pihak baik bagi CSC maupun CSP.

Untuk setiap sumber daya pada komputasi awan, penting untuk memahami apa tanggung jawab CSC dan apa tanggung jawab CSP. Pembagian tanggung jawab ini digambarkan seperti pada Gambar 0-6.


*Gambar 0-6 Model tanggung jawab bersama*

*Shared responsibility* model berguna untuk memastikan, baik CSP ataupun CSC memahami tugasnya masing-masing dengan tepat. Pada dasarnya, CSP bertanggung jawab atas "*security of the cloud*" (keamanan dari komputasi awan) seperti infrastruktur fisik, jaringan. Pada sisi lain pelanggan bertanggung jawab atas *security in the cloud* (keamanan pada komputasi awan) seperti data, aplikasi dan sistem operasi. Berikut merupakan bagian-bagian yang menjadi pada model tanggung jawab bersama.

a. Keamanan data: Manajemen keamanan data termasuk otentikasi, integritas data, enkripsi, dan kontrol akses.
b. Keamanan aplikasi: Manajemen keamanan sistem aplikasi yang mendukung O&M dan layanan pengguna di komputasi awan CSP, yang mencakup desain, pengembangan, rilis, konfigurasi, dan penggunaan aplikasi.
c. Keamanan platform: Manajemen keamanan layanan mikro, manajemen, *middleware*, dan platform lain di komputasi awan CSP,

yang mencakup desain, pengembangan, rilis, konfigurasi, dan penggunaan platform.

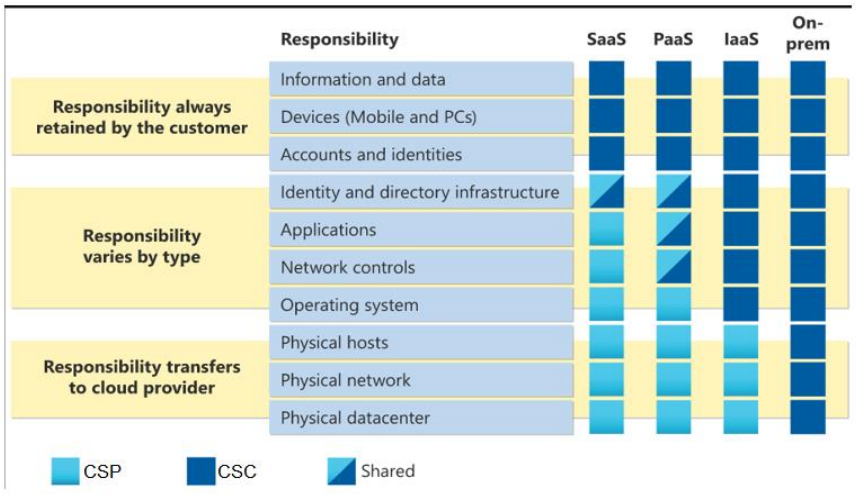
d. Keamanan Jaringan & Hipervisor: Manajemen keamanan komputasi, jaringan, dan penyimpanan yang disediakan oleh CSP, termasuk manajemen dasar (seperti lapisan kontrol virtualisasi) dan manajemen penggunaan (seperti manajemen VM) komputasi awan , penyimpanan komputasi awan , dan layanan basis data komputasi awan , serta pengelolaan jaringan virtual, *load balancing*, *gateway*, VPN, dan jalur pribadi.
e. Keamanan infrastruktur fisik: Manajemen keamanan ruang peralatan dan lingkungan untuk wilayah komputasi awan CSP, zona ketersediaan (*Availability Zone*) serta manajemen server fisik dan perangkat jaringan.

Pergeseran pertama yang akan CSC lakukan dari *data center* adalah menggunakan *Infrastructure as a Service* (IaaS). Dengan IaaS, CSC memanfaatkan layanan tingkat terendah dan meminta CSP untuk membuat VM dan jaringan virtual. Pada level ini CSC tetap bertanggung jawab untuk melakukan *patching*, mengamankan sistem operasi dan perangkat lunak CSC, serta mengonfigurasi jaringan CSC agar aman. CSC mengambil keuntungan dari IaaS ketika CSC mulai menggunakan CSP VM alih-alih server fisik di tempat CSC. Keuntungan lainnya adalah perhatian terhadap bagian fisik jaringan dapat dialihkan ke CSP.

Pada *Platform as a Service* (PaaS), lebih banyak masalah keamanan yang di-*outsource* atau dialihdayakan. Pada level ini, CSP merawat sistem operasi dan sebagian besar perangkat lunak dasar seperti sistem manajemen basis data. Semuanya diperbarui dengan *patch* keamanan terbaru dan dapat diintegrasikan dengan CSP *Active Directory* untuk kontrol akses. PaaS juga

dilengkapi dengan banyak keuntungan operasional. Daripada membangun seluruh infrastruktur dan *subnet* untuk lingkungan CSC secara manual, CSC dapat melakukan "*point and click*" dalam portal CSP atau menjalankan skrip otomatis untuk membawa sistem yang kompleks dan aman diskalakan sesuai kebutuhan.

Dengan *Software as a Service* (SaaS), CSC mengalihdayakan hampir semuanya. SaaS adalah perangkat lunak yang berjalan dengan infrastruktur internet. Kode dikendalikan oleh vendor tetapi dikonfigurasikan untuk digunakan oleh CSC. Penjabaran mendetail terkait model tanggung jawab bersama diilustrasikan seperti pada Gambar 0-7.

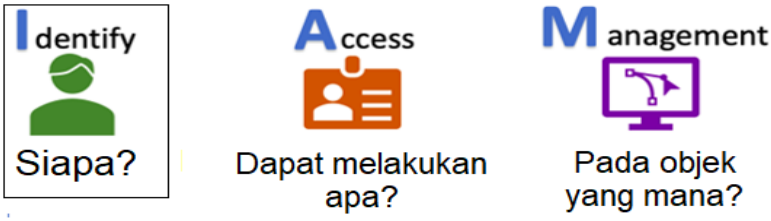



*Gambar 0-7 Detail model tanggung jawab bersama* (Microsoft, 2022)

## 3.6.2 Manajemen Akses Identitas

*Identity Access Management* (IAM) adalah sistem yang dibangun untuk mengelola hak akses pengguna dalam sumber daya di CSP. Pengelolaan ini ditujukan untuk mengidentifikasi "siapa" yang dapat melakukan "apa" pada sumber daya "mana".

IAM mengatur identitas (*identity*) atau akun mana saja yang akan diberikan sebuah peran (*role*) dalam pekerjaannya. Di dalam *role* tersebut terdapat beberapa hak akses (*access*) tertentu untuk mengizinkan pemilik akun mengelola sumber daya tertentu (*Management*). Hubungan antara *Identity, Access* dan *Management* ini diilustrasikan pada Gambar 0-8.




*Gambar 0-8 Hubungan antara Identity, Access dan Management*

Terlihat pada Gambar 0-8, IAM akan mengatur tiga komponen penting yakni (Yang et al., 2020):

a. *Identity*: Identitas merujuk pada siapa dalam hal ini akun mana yang dapat mengelola sumber daya.
b. Access: Kumpulan hak akses (*permission*) yang bisa kita tetapkan (*assign*) pada sebuah *identity*.
c. *Management*: Merujuk pada pengelolaan sumber daya yang bisa diatur berdasarkan *access* yang dimiliki oleh sebuah akun.

Identitas telah menjadi batas keamanan utama baru. Oleh karena itu, otentikasi dan penetapan hak yang tepat sangat penting untuk menjaga kontrol data. Dua konsep dasar yang perlu dipahami ketika berbicara tentang identitas dan kontrol akses adalah otentikasi dan otorisasi. Kedua konsep ini mendukung segala sesuatu yang terjadi secara berurutan dalam setiap proses identitas dan akses:

a. Otentikasi adalah proses menetapkan identitas seseorang atau layanan

yang ingin mengakses sumber daya. Otentikasi melibatkan tindakan memastikan kredensial yang sah, dan memberikan dasar untuk menciptakan prinsip keamanan untuk identitas dan penggunaan kontrol akses. Sederhananya otentikasi memastikan jika orang yang masuk adalah siapa yang mereka katakan.

b. Otorisasi adalah proses menetapkan tingkat akses yang dimiliki orang atau layanan yang diotentikasi. Otorisasi menentukan data apa yang orang boleh akses dan apa yang dapat mereka lakukan dengannya.

c. *Multi-factor authentication* (MFA) memberikan keamanan tambahan untuk identitas seseorang dengan mengharuskan dua elemen atau lebih untuk otentikasi penuh. Elemen-elemen ini terbagi dalam tiga kategori (P. K. Das et al., 2019):

   - Sesuatu yang Anda tahu
   - Sesuatu yang Anda miliki
   - Sesuatu tentang Anda

   "Sesuatu yang Anda tahu" dapat merupakan kata sandi atau jawaban untuk pertanyaan keamanan. "Sesuatu yang Anda miliki" bisa berupa aplikasi *mobile* yang menerima pemberitahuan atau token. "Sesuatu tentang Anda" biasanya semacam properti biometrik, seperti sidik jari atau pemindaian wajah yang digunakan pada banyak perangkat *mobile*.

   Menggunakan MFA meningkatkan keamanan dengan membatasi dampak paparan kredensial. Penyerang yang memiliki kata sandi pengguna juga perlu memiliki ponsel atau wajah untuk dapat mengotentikasi sepenuhnya. Otentikasi dengan hanya satu faktor yang diverifikasi tidak cukup, dan penyerang tidak akan dapat menggunakan kredensial tersebut untuk mengotentikasi.

d. *Roles* atau peran merupakan kumpulan dari *permissions*, seperti "*Read-only*" atau "*Contributor*", yang dapat diberikan kepada pengguna untuk mengakses sumber daya layanan komputasi awan. Identitas dapat

dipetakan ke *roles* secara langsung. Saat memberikan *permission* pada sebuah role, praktik terbaik dalam hal keamanan adalah mengikuti "*principle of least privilege*". Maksudnya, berikanlah akses sesuai dengan kebutuhan saat itu saja. Setiap *role* hanya diberikan hak akses sesuai yang dibutuhkan untuk menyelesaikan pekerjaannya.

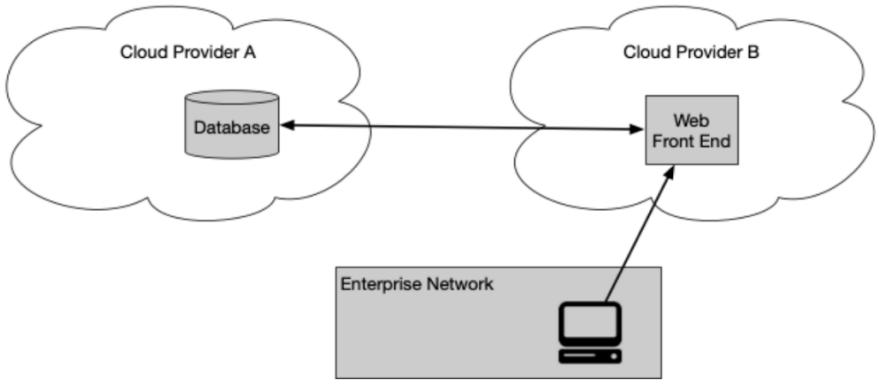
Selain itu *best practice* terkait data kredensial adalah penggunaan enkripsi (Yang et al., 2020). Data pribadi pelanggan seperti *username, password*, dan biodata pelanggan aplikasi perlu kita amankan dengan cara dienkripsi. Enkripsi adalah metode mengubah sebuah informasi atau data dari *plaintext* (teks biasa yang terbaca manusia) menjadi *ciphertext* (teks yang tidak bisa dibaca dan dimengerti manusia) menggunakan algoritma tertentu sehingga metode ini dapat mencegah pihak yang tidak berwenang mengetahui informasi yang dikirim, diterima, ataupun disimpan. Memisahkan prinsip keamanan, izin akses, dan sumber daya menyediakan manajemen akses yang sederhana dan kontrol yang baik.

### 3.6.3 Zero Trust Architecture

*Zero Trust Architecture* (ZTA) adalah pendekatan keamanan siber yang mengasumsikan bahwa semua perangkat, pengguna, dan jaringan, baik di dalam maupun di luar perimeter jaringan organisasi, harus dianggap tidak terpercaya dan memerlukan otentikasi dan otorisasi sebelum akses diberikan ke sumber daya apa pun (Hamad et al., 2022). ZTA dirancang untuk mencegah pelanggaran data dan membatasi potensi kerusakan yang disebabkan oleh serangan dunia maya. Prinsip dasar ZTA adalah meminimalkan permukaan serangan dengan membatasi akses ke sumber daya berdasarkan identitas dan konteks pengguna, daripada hanya mengandalkan perimeter jaringan. Arsitekturnya didasarkan pada konsep mikro-segmentasi, yang melibatkan pembagian jaringan menjadi segmen-

segmen kecil untuk meminimalkan kerusakan yang dapat disebabkan oleh serangan dunia maya.

Salah satu kasus penggunaan yang semakin umum untuk menerapkan ZTA adalah perusahaan yang menggunakan banyak penyedia komputasi awan (Saxena et al., 2021) (lihat Gambar 0-9). Dalam kasus penggunaan ini, perusahaan memiliki jaringan lokal tetapi menggunakan dua atau lebih penyedia layanan komputasi awan untuk meng-*hosting* aplikasi/layanan dan data. Terkadang, aplikasi/layanan di-*hosting* di layanan komputasi awan yang terpisah dari sumber data. Untuk kinerja dan kemudahan pengelolaan, aplikasi yang di-*hosting* di Penyedia Komputasi awan A harus dapat terhubung langsung ke sumber data yang di-*hosting* di Penyedia Komputasi awan B.




*Gambar 0-9 ZTA dengan komputasi awan multi provider* (Rose et al., 2020)

Saat perusahaan beralih ke lebih banyak aplikasi dan layanan yang di-*hosting* pada komputasi awan, menjadi jelas bahwa mengandalkan perimeter perusahaan untuk keamanan menjadi kewajiban. Seperti yang telah dibahas prinsip-prinsip ZTA berpandangan bahwa seharusnya tidak ada perbedaan antara infrastruktur jaringan yang dimiliki dan dioperasikan oleh perusahaan dan infrastruktur yang dimiliki dan dioperasikan oleh penyedia layanan

lainnya. Salah satu tantangannya adalah penyedia komputasi awan yang berbeda memiliki cara unik untuk mengimplementasikan fungsi serupa.

ZTA dapat membangun mentalitas "jangan pernah percaya, selalu verifikasi". *Zero Trust* memerlukan visibilitas yang konsisten, penerapan dan kontrol akses yang dapat mencegah akses tidak sah atau kehilangan data. Untuk metode mendekati strategi seperti itu, prinsip-prinsip berikut harus dilibatkan (Rose et al., 2020):

a. Identifikasi dan pahami semua sumber daya serta titik aksesnya, data, dan jenis aplikasi yang dimiliki organisasi, serta lokasi penyimpanannya, dan siapa yang mengakses dan menggunakannya.
b. Gambarkan alur semua transaksi dan aliran data di seluruh aplikasi.
c. Rancang infrastruktur komputasi awan kemudian buat batasan segmen antara pengguna dan aplikasi.
d. Menentukan kebijakan, kontrol, dan batasan *zero trust* yang sederhana dan mudah dipahami berdasarkan siapa yang harus memiliki akses ke apa dan menerapkan kontrol akses kontekstual berdasarkan *principle of least privilege*.
e. Mendidik pengguna tentang kebijakan keamanan komputasi awan yang ditentukan dan apa yang diharapkan dari mereka saat mereka mengakses dan menggunakan aplikasi dan data di komputasi awan.
f. Secara berkelanjutan, terus-menerus memeriksa - menganalisis dan mencatat semua lalu lintas, menerapkan kebijakan keamanan dengan rencana mitigasi, dan mengoptimalkan kebijakan berdasarkan pengalaman.

Dengan menerapkan ZTA organisasi dapat mengurangi risiko pelanggaran data dan serangan dunia maya dengan menerapkan kontrol akses yang ketat dan menyegmentasi jaringan mereka untuk membatasi potensi kerusakan yang disebabkan oleh serangan. ZTA juga menyediakan model keamanan yang lebih *agile* dan fleksibel, karena memungkinkan organisasi beradaptasi

dengan cepat terhadap perubahan di lingkungan mereka dan merespons ancaman baru yang muncul.

### 3.6.4 Compliance

Di setiap industri ada standar tertentu yang perlu ditegakkan. CSP akan diaudit atau diperiksa untuk memastikan bahwa standar tersebut telah dipenuhi. Jadi, jika aplikasi yang kita buat ingin diakses dan digunakan di suatu wilayah baik dengan cakupan negara atau benua tertentu, kita harus mematuhi peraturan hukum yang berlaku di wilayah tersebut. Untuk itu, kita harus mendapatkan izin dari pemegang peraturan di wilayah tersebut dengan mematuhi segala peraturan yang berlaku yang biasa kita kenal sebagai *compliance* (kepatuhan).


*Gambar 0-10 Domain compliance*

*Compliance* adalah sebuah upaya yang dilakukan oleh suatu usaha untuk memenuhi peraturan hukum (regulasi), prosedur, dan standar yang ada pada layanan yang disediakan ke masyarakat luas di suatu wilayah . Kepatuhan atas segala peraturan yang ada di wilayah berwenang di mana lokasi bisnis beroperasi itu sangat penting bagi sebuah bisnis karena:

a. Kepatuhan bersifat wajib sehingga harus dilakukan;
b. Menunjukkan kredibilitas sebuah bisnis;
c. Menciptakan kepercayaan kepada semua pemangku kepentingan;

d. Membantu upaya pengelolaan risiko untuk bisnis;

Berikut beberapa contoh *compliance* yang harus dipatuhi oleh berbagai pelaku bisnis di dunia yang menyimpan, mengolah dan menggunakan data penggunanya, di antaranya:

***General Data Protection Regulation* (GDPR)**

GDPR adalah peraturan yang mengatur perlindungan data pribadi pengguna yang ada di seluruh negara Uni Eropa (EU) (Proton AG, 2023). Pelaku bisnis yang memiliki pengguna di wilayah EU tidak boleh semena-mena mengolah data dalam bentuk apa pun tanpa seizin pemegang regulasi (regulator). GDPR ini wajib dipatuhi oleh semua orang di seluruh dunia yang mengolah, menyimpan, atau memproses data pribadi penduduk negara Uni Eropa (EU).

***Health Insurance Portability and Accountability Act* (HIPAA)**

Peraturan ini mewajibkan pelaku bisnis untuk melindungi informasi kesehatan pasien seperti nama, alamat, riwayat sakit, informasi pembayaran dan lain-lain yang tidak boleh dipublikasikan ke publik atau diakses oleh pihak yang tidak berwenang di negara Amerika Serikat (AS). Jadi, pelaku bisnis yang aplikasinya bersangkut pautan dengan data pasien seluruh warga negara AS di bidang pelayanan kesehatan seperti rumah sakit atau aplikasi kesehatan harus mematuhi peraturan yang ditetapkan dalam HIPAA.

***Payment Card Industry Data Security Standard* (PCI-DSS)**

Semua pihak, baik pengguna maupun pelaku bisnis, yang menyimpan, memproses, atau meneruskan data, termasuk lembaga keuangan, *merchant*, serta penyedia layanan wajib mematuhi PCI-DSS. Sebagai contoh kasusnya, industri perbankan yang mengeluarkan kartu debit/kredit atau aplikasi pembayaran *online* harus dapat memenuhi segala peraturan dan standarisasi yang telah ditetapkan dalam peraturan PCI-DSS.

**Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE)**

Di Indonesia terdapat Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71) mencabut PP 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE). PP 71 ini mengatur kegiatan PSTE, secara umum didefinisikan sebagai setiap orang, penyelenggara pemerintahan, badan usaha, atau anggota masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik secara individu atau kolektif untuk pengguna. Mulai 10 Oktober 2019, PP 71 ini memberikan kejelasan lebih lanjut seputar persyaratan lokalisasi data, termasuk fleksibilitas tambahan bagi PSTE sektor swasta untuk menyimpan sistem dan data di luar Indonesia, tunduk pada PSTE tertentu. PP 71 ini juga mencakup persyaratan pendaftaran untuk ESO, persyaratan perlindungan dan keamanan data umum, hak penghapusan dan penghapusan untuk pemilik data, dan larangan konten, di antara persyaratan lainnya.

### 3.6.5 Kolaborasi CSP dan CSC

Salah satu masalah teratas untuk penyediaan layanan CSP adalah mengurangi kekhawatiran CSC dengan menyelesaikan masalah keamanan layanan komputasi awan dan tantangan yang dihadapi CSP itu sendiri. CSP perlu menemukan cara yang lebih baik untuk mengatasi potensi risiko keamanan terkait layanan komputasi awan publik, ancaman keamanan internal dan eksternal organisasi, dan risiko kepatuhan keamanan komputasi awan. Mereka juga perlu meningkatkan pemahaman tentang model tanggung jawab keamanan bersama. Untuk itu, CSP harus:

a. Mengintegrasikan layanan keamanan yang disediakan oleh pemasok keamanan pihak ketiga untuk platform komputasi awan mereka agar dapat menggabungkan lebih banyak produk dan kemampuan keamanan terbaru dengan cepat.
b. Memperkuat manajemen akses, tinjauan log, pelatihan keamanan, dan

langkah-langkah lain bagi personel internal untuk memitigasi risiko keamanan internal.

c. Memperkuat manajemen kerentanan, perlindungan mendalam, dan lebih banyak tindakan untuk mempertahankan diri dari ancaman eksternal.
d. Mendapatkan pemahaman mendalam tentang persyaratan kepatuhan, tingkatkan kemampuan kepatuhan, dan hindari penalti, tuntutan hukum, dan kerusakan reputasi yang disebabkan oleh pelanggaran.
e. Memperkuat komunikasi dan pandu pelanggan untuk memahami dengan jelas tanggung jawab keamanan mereka.

CSP perlu membuat sistem manajemen keamanan komputasi awan yang mencakup semua proses layanan komputasi awan, menerapkan persyaratan kontrol keamanan untuk setiap domain bisnis berdasarkan fungsinya, dan membantu perusahaan/organisasi lebih memahami persyaratan manajemen keamanan komputasi awan. Pada akhirnya, tindakan ini dapat membantu CSP menyediakan pelanggan dengan layanan komputasi awan yang aman dan sesuai untuk membangun dan meningkatkan kepercayaan pelanggan.

CSP dan CSC berbagi tanggung jawab keamanan komputasi awan, artinya CSC juga perlu mempertimbangkan cara mengelola keamanan di lingkungan komputasi awan. CSC mungkin tidak memiliki pengetahuan manajemen keamanan komputasi awan yang komprehensif, atau metode manajemen keamanan aslinya tidak berlaku untuk komputasi awan. Oleh karena itu, CSC dapat menggunakan produk layanan yang disediakan oleh CSP untuk meningkatkan kemampuan manajemen keamanan komputasi awan mereka.

**Kemampuan perlindungan keamanan**

CSC dapat menggunakan layanan dan produk perlindungan keamanan yang disediakan oleh CSP untuk jaminan keamanan yang tepat waktu dan efektif. Pada saat yang sama, CSP dapat memberikan kemampuan pemantauan dan perlindungan keamanan yang divisualisasikan khusus untuk lingkungan

komputasi awan untuk membantu CSC mendeteksi dan memblokir kerentanan keamanan, mendeteksi perilaku yang mencurigakan, dan segera merespons kemungkinan serangan intrusi; kemampuan keamanan ini mencakup perlindungan infrastruktur, perlindungan data, deteksi dan analisis penyusupan, otentikasi dan manajemen identitas, dan *firewall*.

**Solusi keamanan yang dapat disesuaikan dengan berbagai skenario**

Selama transformasi digital, CSC dapat menerapkan banyak teknologi baru dan mengembangkan skenario bisnis baru. Penerapan teknologi baru dan transformasi proses bisnis membawa risiko keamanan baru, yang dapat menimbulkan masalah bagi CSC dan membangkitkan kekhawatiran mereka tentang penerapan teknologi baru. Transformasi digital suatu perusahaan tidak dapat pergi ke mana pun tanpa layanan komputasi awan.

CSP memanfaatkan kemampuan inovasi dengan mengintegrasikan produk dan teknologi terkini untuk merancang solusi keamanan dunia maya di berbagai skenario bisnis. Menjaga transformasi digital CSC agar berinvestasi lebih banyak dalam perubahan teknologi baru.

**Ekosistem keamanan komputasi awan yang kaya**

Ekosistem keamanan komputasi awan yang kaya sangat memperluas kategori layanan keamanan komputasi awan, memungkinkan CSC memilih produk dan layanan yang tepat untuk konteks khusus mereka. Ini membantu CSC meningkatkan keamanan sistem TI mereka.

**Layanan keamanan komputasi awan lainnya**

CSP juga dapat menyediakan konsultasi keamanan dan kepatuhan, *hosting* keamanan, dan layanan lainnya kepada CSC, sehingga CSC dapat dengan cepat memperoleh kemampuan manajemen keamanan tingkat tinggi dengan memanfaatkan kemampuan dan pengalaman CSP. Dengan bantuan CSP, CSC dapat meningkatkan kemampuan manajemen keamanan multi-komputasi awan dengan lebih sedikit upaya dan efisiensi yang lebih tinggi.

# BAB 4

# PEMANFAATAN KOMPUTASI AWAN DI DUNIA

## 4.1 Pangsa Pasar Komputasi Awan di Dunia

Menurut beberapa organisasi industri, pasar layanan komputasi awan akan terus berkembang pesat dalam dua atau tiga tahun ke depan. Gartner memperkirakan bahwa pada tahun 2023, 40% dari seluruh beban kerja perusahaan akan ditempatkan di infrastruktur komputasi awan dan layanan platform, naik dari 20% pada tahun 2020 (Gartner, 2022). Pada saat yang sama, sebuah survei dari Cybersecurity Insider (Cybersecurity insiders, 2022) yang ditugaskan oleh Fortinet menunjukkan bahwa 33% organisasi telah menjalankan lebih dari 50% beban kerja mereka di komputasi awan, angka yang diproyeksikan akan tumbuh menjadi 56% dalam 12 hingga 18 bulan ke depan. Pandemi COVID-19 juga telah memacu pertumbuhan industri ini; teknologi, industri, dan aplikasi komputasi awan global berkembang menuju tren baru. Aplikasi internet seperti *telecommuting*, edukasi *online*, dan *game online* telah menjadi semakin populer, dan volume komputasi meningkat tajam. Akibatnya, perusahaan ingin beralih ke digital lebih cepat, menghadirkan layanan secara *online*, dan bermigrasi ke komputasi awan dalam waktu dekat. Bisnis mencari komputasi awan untuk merevitalisasi bisnis mereka ke tingkat sebelum pandemi. Sementara itu, pandemi telah memaksa banyak negara dan wilayah untuk memberlakukan larangan perjalanan dan melarang pertemuan massal. Dalam konteks ini, mayoritas perusahaan telah mendorong telekomunikasi, yang telah mendorong inovasi dalam kolaborasi layanan. Orang-orang mulai menyadari bahwa akses

perusahaan jarak jauh tidak nyaman dengan VPN tradisional. Sebagai gantinya, kolaborasi perangkat komputasi awan memungkinkan penggunaan aplikasi kantor secara masif, yang efisien dan nyaman. Sebuah survei baru-baru ini menunjukkan bahwa sejak wabah COVID-19, penggunaan layanan komputasi awan di perusahaan telah meningkat sebesar 50% sementara penggunaan layanan kantor kolaborasi telah meningkat hampir enam kali lipat.

Pengeluaran pengguna akhir di seluruh dunia untuk layanan komputasi awan publik diperkirakan akan tumbuh 20,4% pada tahun 2022 hingga mencapai $494,7 miliar, naik dari $410,9 miliar pada tahun 2021, menurut perkiraan terbaru dari Gartner, Inc. Pada tahun 2023, pengeluaran pengguna akhir diperkirakan akan mencapai hampir $600 miliar.

"Komputasi awan adalah kekuatan yang menggerakkan organisasi digital saat ini," tutur Sid Nag, wakil presiden bidang riset di Gartner (Gartner, 2022). "Para CIO telah melampaui era kegembiraan yang tidak rasional dalam pengadaan layanan komputasi awan dan menjadi lebih bijaksana dalam memilih penyedia layanan komputasi awan publik untuk mendorong hasil bisnis dan teknologi yang spesifik dan diinginkan dalam perjalanan transformasi digital mereka."

*Infrastructure-as-a service* (IaaS) diperkirakan akan mengalami pertumbuhan belanja pengguna akhir tertinggi pada tahun 2022 sebesar 30,6%, diikuti oleh *Data-as-a-service* (DaaS) sebesar 26,6% dan *Platform-as-a-service* (PaaS) sebesar 26,1% (lihat Tabel 4-1)**.** Realitas baru dari pekerjaan hibrid mendorong organisasi untuk beralih dari memberdayakan tenaga kerja mereka dengan solusi komputasi klien tradisional, seperti desktop dan perangkat fisik lainnya di kantor, menuju DaaS, yang mendorong pengeluaran mencapai $2,6 miliar pada tahun 2022. Permintaan akan kemampuan *Cloud Native* oleh pengguna akhir membuat PaaS tumbuh menjadi $109,6 miliar dalam pembelanjaan.

*Tabel 4-1 Perkiraan Pengeluaran Pengguna Akhir Layanan* Komputasi awan *Publik di Seluruh Dunia (Jutaan Dolar AS)* (Gartner, 2022)

| **Layanan** Komputasi awan | **2021** | **2022** | **2023** |
|---|---|---|---|
| Komputasi awan ***Business Process Services*** **(BPaaS)** | 51,410 | 55,598 | 60,619 |
| Komputasi awan ***Application Infrastructure Services*** **(PaaS)** | 86,943 | 109,623 | 136,404 |
| Komputasi awan ***Application Services*** **(SaaS)** | 152,184 | 176,622 | 208,080 |
| Komputasi awan ***Management and Security Services*** | 26,665 | 30,471 | 35,218 |
| Komputasi awan ***System Infrastructure*** **Services (IaaS)** | 91,642 | 119,717 | 156,276 |
| ***Desktop as a Service*** **(DaaS)** | 2,072 | 2,623 | 3,244 |
| ***Total Market*** | 410,915 | 494,654 | 599,84 |

"*Kemampuan Cloud Native seperti containerization, database platform-as-a-service (dbPaaS), dan kecerdasan buatan/pembelajaran mesin memiliki fitur-fitur yang lebih kaya dibandingkan komputasi yang dikomoditaskan seperti IaaS atau network-as-a-service*," ujar Nag. "Akibatnya, layanan-layanan tersebut umumnya lebih mahal sehingga mendorong pertumbuhan pengeluaran."

SaaS tetap menjadi segmen pasar layanan komputasi awan publik terbesar, yang diperkirakan akan mencapai $176,6 miliar dalam pengeluaran pengguna akhir pada tahun 2022. Gartner memperkirakan kecepatan yang stabil dalam segmen ini karena perusahaan mengambil beberapa rute ke pasar dengan SaaS, misalnya melalui pasar komputasi awan, dan terus memecah aplikasi yang lebih besar dan monolitik menjadi beberapa bagian yang dapat dikomposisikan untuk proses DevOps yang lebih efisien.

Teknologi yang muncul dalam komputasi awan seperti komputasi *edge hyperscale* dan *secure access service edge* (SASE) mengganggu pasar yang berdekatan dan membentuk kategori produk baru, sehingga menciptakan aliran pendapatan tambahan bagi penyedia komputasi awan publik. "*Didorong oleh pematangan layanan* komputasi awan *inti, fokus diferensiasi secara*

*bertahap bergeser ke kemampuan yang dapat mengganggu bisnis digital dan operasi di perusahaan secara langsung*," kata Nag. "Layanan komputasi awan publik telah menjadi sangat integral sehingga penyedia layanan kini dipaksa untuk mengatasi tantangan sosial dan politik, seperti keberlanjutan dan kedaulatan data. "*Para pemimpin TI yang melihat* komputasi awan *sebagai enabler dan bukan sebagai tujuan akhir akan menjadi yang paling sukses dalam perjalanan transformasi digital mereka,*" ujar Nag. "Organisasi yang menggabungkan komputasi awan dengan teknologi lain yang berdekatan dan sedang berkembang akan mendapatkan hasil yang lebih baik." Pada saat yang sama, kita dapat membandingkan pertumbuhan yang cepat dari berbagai segmen pasar yang berbeda seperti di Tabel 4-2 berikut:

*Tabel 4-2 Pertumbuhan layanan* komputasi awan *pada segmen pasar berbeda (Juta Dollar U.S.)* (Gartner, 2021)

| Item | 2020 | 2021 | Pangsa 2020 (%) | Pangsa 2021 (%) | Pertumbuhan 2021 (%) |
|---|---|---|---|---|---|
| *Application Software as a Service Market(SaaS)* | 104,494.6 | 126,825.3 | 100.0% | 100.0% | 21.4% |
| Komputasi awan *Infrastructure and Platform Services Market(CIPS)* | 91,672.1 | 129,552.3 | 100.0% | 100.0% | 41.3% |
| *Infrastructure as a Service Market(IaaS)* | 64,285.9 | 90,894.3 | 100.0% | 100.0% | 41.4% |
| *dbPaaS Market Share* | 26,764.6 | 39,170.4 | 100.0% | 100.0% | 46.4% |
| *AIM-Related PaaS Market* | 17,820.3 | 22,934.0 | 100.0% | 100.0% | 28.7% |
| *Business Analytics Platform as a Service Market* | 8,382.5 | 10,847.3 | 100.0% | 100.0% | 29.4% |

| Item | 2020 | 2021 | Pangsa 2020 (%) | Pangsa 2021 (%) | Pertumbuhan 2021 (%) |
|---|---|---|---|---|---|
| *Application Development Platform as a Service Market* | 3,540.9 | 4,339.3 | 100.0% | 100.0% | 22.5% |

Definisi layanan komputasi awan yang digunakan oleh Gartner:

a. Komputasi awan *Infrastructure and Platform Services* (CIPS): Dalam konteks laporan ini, CIPS didefinisikan sebagai seperangkat penawaran yang terstandardisasi dan sangat otomatis, di mana sumber daya infrastruktur seperti komputasi, jaringan, dan penyimpanan dilengkapi dengan layanan platform terintegrasi, seperti aplikasi terkelola, basis data, dan fungsi-fungsi sebagai penawaran layanan. Sumber daya dapat diskalakan dan elastis dalam waktu yang hampir seketika, dan diukur berdasarkan penggunaan. Antarmuka swalayan diekspos langsung ke pelanggan, termasuk antarmuka pengguna (UI) berbasis web dan API. Sumber daya dapat berupa penyewa tunggal atau *multitenant*, dan di-*host* oleh penyedia layanan atau di lokasi di pusat data pelanggan. CIPS mencakup platform infrastruktur sebagai layanan (IaaS) dan platform terintegrasi sebagai layanan (PaaS). Ini termasuk aplikasi PaaS (aPaaS), *database PaaS* (dbPaaS), pengembang aplikasi PaaS (adPaaS), dan penawaran komputasi awan *privat* industri yang sering digunakan di pusat data perusahaan.
b. IaaS: *Infrastruktur as a Service* adalah penawaran terstandardisasi dan sangat otomatis di mana sumber daya komputasi yang dimiliki oleh penyedia layanan, dilengkapi dengan kemampuan penyimpanan dan jaringan, ditawarkan kepada pelanggan sesuai permintaan. Sumber daya dapat diskalakan dan elastis dalam waktu yang hampir nyata

dan diukur berdasarkan penggunaan. Antarmuka (*interface*) swalayan, termasuk API dan *Grafical User Interface* (GUI), diekspos secara langsung kepada pelanggan. Sumber daya atas kebijaksanaan penyedia layanan dapat berupa penyewa tunggal atau *multitenant* dan di-*host* oleh penyedia layanan.

c. dbPaaS: *Database platform as a Service* adalah sistem manajemen basis data (DBMS) atau penyimpanan data yang direkayasa sebagai layanan langganan yang dapat diskalakan, elastis, dan *multitenant* dengan tingkat pengelolaan mandiri, dan dijual serta didukung oleh penyedia layanan komputasi awan, atau vendor perangkat lunak pihak ketiga pada infrastruktur komputasi awan.
d. *AIM-Related PaaS: AIM-related PaaS* mencakup layanan infrastruktur aplikasi spesialis, seperti *API Management Services* (apiPaaS), Application Platform Services (aPaaS), Business Process Management Services (bpmPaaS), dan Integration Platform Services (iPaaS).
e. baPaaS: *Business analytics PaaS* mencakup platform yang menyediakan infrastruktur dan alat untuk memungkinkan pengguna membangun aplikasi yang memfasilitasi pengambilan keputusan dan membantu organisasi mempelajari, memahami, dan meningkatkan bisnis mereka.
f. adPaaS: solusi *application development platform as a service* (adPaaS) didefinisikan sebagai alat pengembangan yang disediakan oleh komputasi awan, yang dirancang untuk mendukung rantai alat DevOps dan menunjukkan kemampuan diperluas melalui pasar dan layanan mitra, acara, dan API. Platform ini dirancang untuk mendorong kolaborasi dan memungkinkan proses yang berkelanjutan.

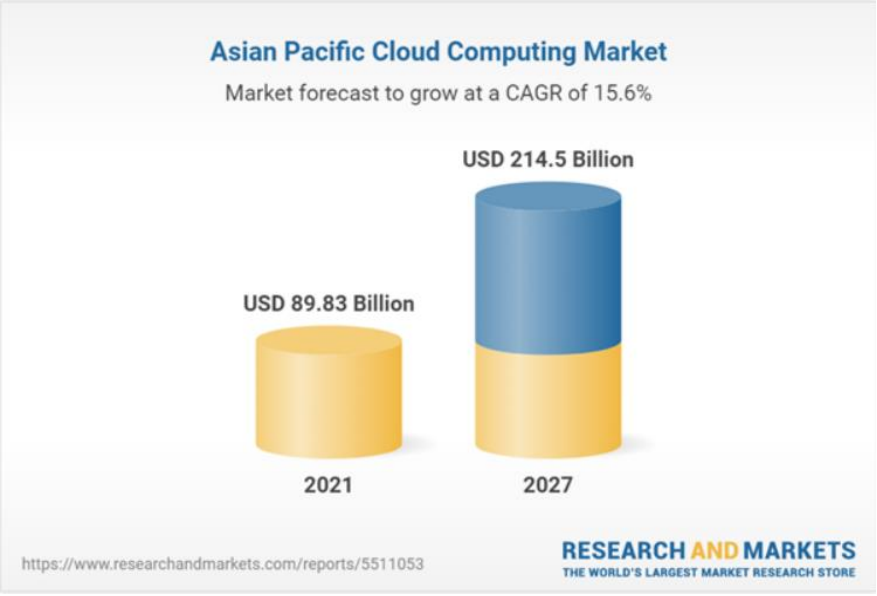
Pasar komputasi awan Asia Pasifik diperkirakan akan tumbuh dengan CAGR (*Compound Annual Growth Rate*) sekitar 15,5% selama 2021-2027 (KBV Research, 2022). Laporan pasar komputasi awan Asia Pasifik ini memberikan

pemahaman holistik tentang pasar bersama dengan ukuran pasar, perkiraan, pendorong, tantangan, dan lanskap kompetitif. Laporan ini menyajikan gambaran yang jelas tentang pasar komputasi awan Asia Pasifik dengan mengelompokkan pasar berdasarkan layanan, beban kerja, mode penerapan, ukuran organisasi, vertikal, dan negara. Selain itu, profil rinci perusahaan yang beroperasi di pasar komputasi awan juga disediakan dalam laporan ini. Laporan ini dapat membantu para profesional dan pemangku kepentingan industri dalam mengambil keputusan yang tepat. Selain itu berdasarkan survei yang dilakukan oleh IDC, rata-rata, lebih dari 80% perusahaan di ASEAN memprioritaskan investasi program ketahanan infrastruktur digital sebagai akibat dari ketidakpastian di dunia untuk mengakomodasi agenda bisnis seperti pengalaman pelanggan, keunggulan operasional, dan ketahanan bisnis (Digital News Asia, 2022). Seiring dengan semakin banyaknya organisasi yang menyadari dan memberikan nilai lebih pada komputasi awan, maka jelaslah bahwa komputasi awan akan terus ada dan akan menjadi bagian yang semakin penting dalam strategi mereka.

Permintaan dan adopsi komputasi awan di Asia Pasifik diperkirakan akan melebihi negara-negara lain di dunia, dengan pengeluaran komputasi awan secara keseluruhan diperkirakan akan mencapai USD200 miliar di kawasan ini pada tahun 2024, menurut Gartner, seiring dengan masih berlanjutnya dampak COVID-19 dan bisnis yang ingin membangun fondasi untuk meningkatkan kelincahan dan ketangguhan.

Terdapat pergeseran yang kuat menuju teknologi komputasi awan di Asia Pasifik. Pengeluaran komputasi awan secara keseluruhan diperkirakan akan mencapai USD200 miliar di kawasan ini pada tahun 2024, dengan investasi ke komputasi awan yang tumbuh dengan laju CAGR lebih dari 20% sejak tahun 2018. *Cloud*ifikasi terjadi pada komputasi awan publik maupun privat dan merupakan strategi transformasi teknologi dan bisnis. Tren ini

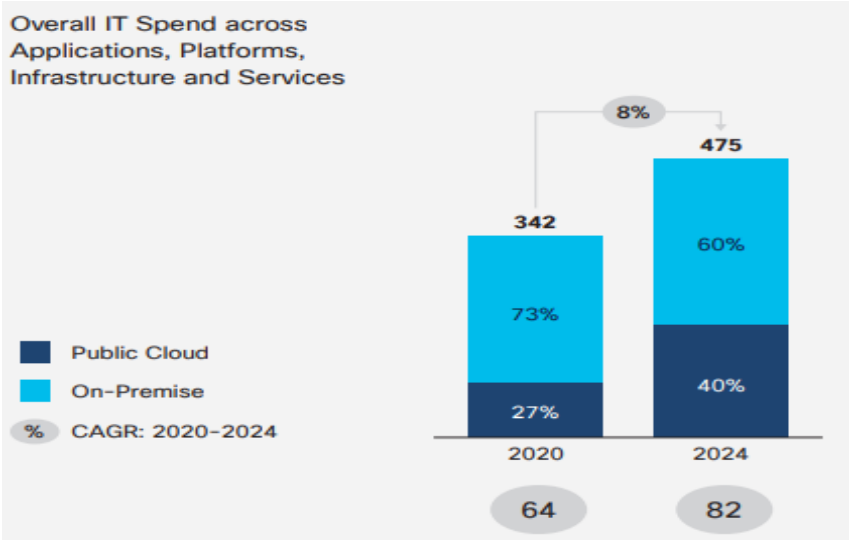
diperkirakan akan terus berlanjut, dengan pergeseran yang kuat ke arah komputasi awan di seluruh lapisan teknologi.




*Gambar 0-1 Pasar komputasi awan di Asia Pasifik* (KBV Research, 2022)

Di seluruh pasar yang menjadi fokus penelitian kami, tingkat pertumbuhan dua digit yang kuat diperkirakan terjadi pada kategori perangkat keras yang mendorong penerapan komputasi awan privat dan hibrid. ANZ, India, dan Singapura merupakan pasar terbesar untuk belanja TI dan diperkirakan akan mendorong lebih dari USD50 miliar belanja komputasi awan pada tahun 2024. Di Australia misalnya, diperkirakan 50% dari total pengeluaran TI akan digunakan untuk layanan komputasi awan publik pada tahun 2024.

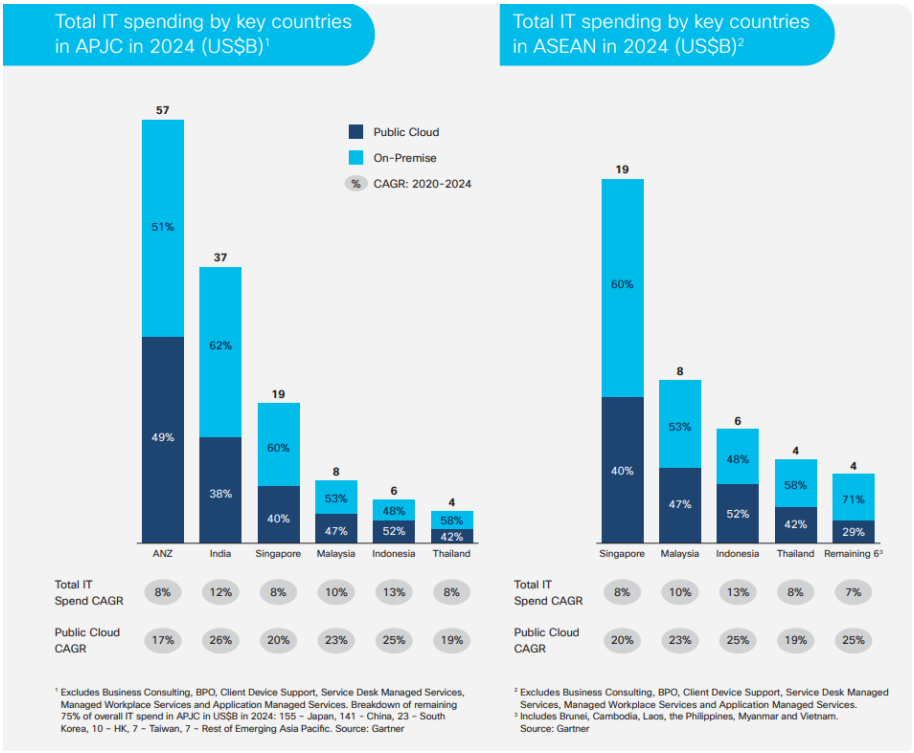
India, Indonesia, dan Malaysia merupakan pasar utama di mana belanja komputasi awan diperkirakan akan tumbuh dengan laju yang jauh lebih cepat, dengan CAGR sebesar 25%; ini lebih cepat daripada perkiraan di negara maju seperti ANZ dan Singapura.




*Gambar 0-2 Pengeluaran keseluruhan TI yang mencakup aplikasi, platform, infrastruktur dan layanan (Menon & Santhanam, 2021)*

Pertumbuhan akan relatif lebih lambat di pasar-pasar yang lebih maju, meskipun mereka masih diperkirakan akan tumbuh masing-masing sebesar 17% dan 20% di ANZ dan Singapura. India, Indonesia dan Malaysia akan memimpin dalam hal pertumbuhan belanja TI secara keseluruhan dan investasi ke dalam layanan komputasi awan publik dan privat.

Standar dan tata kelola keamanan data pada buku ini, mengacu pada kebijakan, prosedur, dan praktik terbaik yang digunakan organisasi untuk melindungi data sensitif dan rahasia mereka dari akses, penggunaan, pengungkapan, atau penghancuran yang tidak sah. Sedangkan tujuan dari standar dan tata kelola keamanan data adalah untuk memastikan bahwa data dilindungi sepanjang siklus hidupnya, mulai dari pembuatan dan penyimpanan hingga penggunaan dan pembuangan.




*Gambar 0-3 Total pengeluaran TI di beberapa negara penting di ASEAN* (Gartner, 2020a)

Tata kelola data, di sisi lain, mengacu pada keseluruhan pengelolaan data dalam suatu organisasi. Ini melibatkan penentuan kebijakan dan prosedur untuk manajemen data, menentukan peran dan tanggung jawab individu yang terlibat dalam manajemen data, dan memastikan bahwa data akurat, lengkap, dan konsisten. Tata kelola data terkait erat dengan keamanan data, karena praktik tata kelola data yang efektif dapat membantu organisasi menjaga kerahasiaan, integritas, dan ketersediaan data mereka. Kerangka tata kelola data yang kuat dapat membantu organisasi untuk:

a. Mengidentifikasi dan mengklasifikasikan data sensitif.
b. Memastikan bahwa data dikumpulkan, disimpan, dan digunakan sesuai dengan hukum dan peraturan yang relevan.
c. Tentukan kontrol akses dan izin untuk data.

d. Tetapkan proses untuk penyimpanan dan pembuangan data.
e. Memantau dan audit penggunaan data untuk mendeteksi dan mencegah akses tidak sah.

Secara keseluruhan, standar dan tata kelola keamanan data sangat penting bagi organisasi yang ingin melindungi data sensitif mereka dan mempertahankan kepercayaan pelanggan dan pemangku kepentingan mereka. Dengan menerapkan langkah-langkah keamanan data yang sesuai dan menerapkan praktik tata kelola data yang efektif, organisasi dapat memastikan bahwa data mereka dilindungi sepanjang siklus hidupnya dan digunakan dengan cara yang bertanggung jawab dan etis.

## 4.2 Standar Internasional Keamanan Data pada Komputasi Awan

ISO/IEC 38505-1:2017 (ISO/IEC, 2017b) memberikan prinsip panduan bagi anggota badan pengatur organisasi (yang dapat terdiri dari pemilik, direktur, mitra, manajer eksekutif, atau yang serupa) tentang penggunaan data yang efektif, efisien, dan dapat diterima dalam organisasi tersebut. Hal ini dapat dicapai dengan:

a. Menerapkan prinsip dan model tata kelola ISO/IEC 38500 untuk tata kelola data;
b. Meyakinkan pemangku kepentingan bahwa, jika prinsip dan praktik yang diusulkan oleh dokumen ini diikuti, mereka dapat memiliki kepercayaan terhadap tata kelola data organisasi;
c. Menginformasikan dan membimbing badan pengatur dalam penggunaan dan perlindungan data di organisasi mereka, dan
d. Membangun kosakata untuk tata kelola data.

ISO/IEC 38505-1:2017 juga dapat memberikan panduan kepada masyarakat luas, antara lain untuk:

a. Manajer eksekutif,
b. Bisnis eksternal atau pakar teknis, seperti pakar hukum atau akuntansi, asosiasi ritel atau industri, atau badan profesional,
c. Penyedia layanan internal dan eksternal (termasuk konsultan), dan
d. Auditor.

ISO/IEC 38505-1:2017 melihat tata kelola data dan penggunaannya dalam suatu organisasi, sementara panduan pengaturan implementasi untuk tata kelola TI yang efektif secara umum ditemukan dalam ISO/IEC/TS 38501. Konstruk dalam ISO/ IEC/TS 38501 dapat membantu mengidentifikasi faktor internal dan eksternal yang berkaitan dengan tata kelola TI dan membantu menentukan hasil yang bermanfaat dan mengidentifikasi bukti keberhasilan. ISO/IEC 38505-1:2017 berlaku untuk tata kelola penggunaan data saat ini dan di masa mendatang yang dibuat, dikumpulkan, disimpan, atau dikendalikan oleh sistem TI, dan berdampak pada proses dan keputusan manajemen terkait data. ISO/IEC 38505-1:2017 mendefinisikan tata kelola data sebagai subset atau domain tata kelola TI, yang merupakan subset atau domain organisasi, atau dalam kasus korporasi, merupakan domain tata kelola perusahaan. ISO/IEC 38505-1:2017 berlaku untuk semua organisasi, termasuk perusahaan publik dan swasta, entitas pemerintah, dan organisasi nirlaba. Dokumen ini berlaku untuk organisasi dari semua ukuran dari yang terkecil hingga terbesar, terlepas dari sejauh mana ketergantungan mereka pada data. Standar ISO/IEC 38505-1:2017 memuat manfaat tata kelola data yang baik, tanggung jawab dari badan pengelola data, dan mekanisme-mekanisme bagi badan pengelola. Standar ini merupakan ekstensi dari standar ISO/IEC 38500 yang menekankan enam prinsip dasar dalam tata kelola data TI yaitu:

a. Prinsip 1 — *Responsibility* (tanggung jawab)
b. Prinsip 2 — *Strategy* (strategi)
c. Prinsip 3 — *Acquisition* (akuisisi)

d. Prinsip 4 — *Performance* (kinerja)
e. Prinsip 5 — *Conformance* (kesesuaian)
f. Prinsip 6 — *Human behaviour* (perilaku manusia)

Prinsip-prinsip ini memberikan kerangka kerja bagi organisasi untuk mengelola data mereka secara efektif, dan dapat digunakan untuk memandu pengembangan kebijakan, prosedur, dan kontrol yang terkait dengan tata kelola data. Dengan mematuhi prinsip-prinsip ini, organisasi dapat memastikan bahwa data mereka dikelola dengan cara yang bertanggung jawab, transparan, dan efektif, sekaligus mematuhi undang-undang dan peraturan yang relevan. ISO/IEC 38505-1:2017 ini juga menjelaskan akuntabilitas data yang meliputi tahapan sebagai berikut:

a. *Collect* (mengumpulkan)
b. *Store* (menyimpan)
c. *Report* (melaporkan)
d. *Decide* (memutuskan)
e. *Distribute* (mendistribusikan)
f. *Dispose* (menghapus)


*Gambar 0-4 Tahapan akuntabilitas data menurut ISO/IEC 38505-1:2017*

Model tata kelola data dalam ISO/IEC 38505-1:2017 menjelaskan tentang bagaimana menerapkan model tata Kelola data, persyaratan internal, tekanan eksternal, evaluasi, pengarahan, dan *monitoring*. ISO/IEC 38505-1:2017 ini juga berisi panduan tata kelola data yang menjelaskan aspek khusus data yang terdiri dari:

a. Nilai terdiri dari: kualitas, ketepatan waktu, konteks, dan volume.
b. Risiko terdiri:umum, manajemen, skema kalsifikasi data, dan keamanan.

**c.** Kendala terdiri dari: umum, regulasi dan legislasi, kebijakan sosial, dan kebijakan organisasional.

## 4.3 Standar Internasional Pelindungan Privasi Informasi Pribadi

### 4.3.1 ISO/IEC 27701:2019

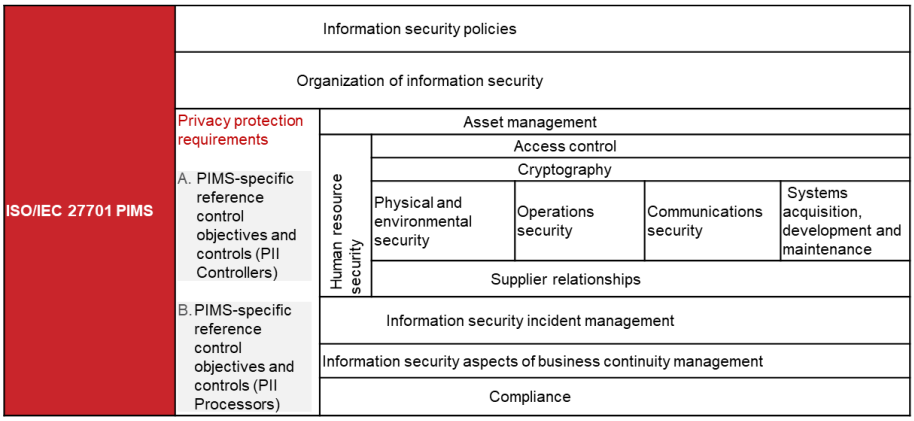
ISO/IEC 27701:2019 (ISO/IEC, 2019) menetapkan persyaratan dan memberikan panduan untuk menetapkan, menerapkan, memelihara, dan terus meningkatkan *Privacy Information Management System* (PIMS) dalam bentuk perpanjangan ISO/IEC 27001 dan ISO/IEC 27002 untuk manajemen privasi dalam konteks organisasi dan memberikan panduan bagi pengendali *Personally Identifiable Information* (PII) dan pengolah PII yang memegang tanggung jawab dan akuntabilitas pemrosesan PII. ISO/IEC 27701 berlaku untuk semua jenis dan ukuran organisasi, termasuk perusahaan publik dan swasta, entitas pemerintah, dan organisasi nirlaba, yang merupakan pengontrol PII dan/atau pemroses PII yang memproses PII dalam *Information Security Management System* (ISMS).

ISO/IEC 27701:2019 adalah perpanjangan privasi pada ISO/IEC 27001. Tujuan desainnya adalah meningkatkan ISMS yang ada dengan persyaratan tambahan untuk menetapkan, menerapkan, memelihara, dan terus meningkatkan PIMS. Standar tersebut menguraikan kerangka kerja untuk Pengontrol PII dan pemroses PII untuk mengelola kontrol privasi guna mengurangi risiko terhadap hak privasi individu.

ISO/IEC 27701 dimaksudkan sebagai perpanjangan yang dapat disertifikasi pada sertifikasi ISO/IEC 27001. Dengan kata lain, organisasi yang berencana mencari sertifikasi ISO/IEC 27701 juga harus memiliki sertifikasi ISO/IEC 27001.

PIMS yang tangguh memiliki banyak manfaat potensial untuk Pengontrol PII dan Prosesor PII:

a. Mengurangi beban dalam pemenuhan kepatuhan terhadap persyaratan privasi dengan adanya kontrol privasi tunggal yang dapat memenuhi beberapa persyaratan GDPR. Petugas proteksi data atau privasi dapat menyediakan bukti yang diperlukan untuk meyakinkan para pemangku kepentingan bahwa persyaratan privasi yang berlaku telah dipenuhi.
b. Sertifikasi PIMS dapat bermanfaat dalam mengomunikasikan kepatuhan privasi kepada pelanggan dan mitra. Kerangka kerja bukti yang seragam berdasarkan standar internasional dapat sangat menyederhanakan komunikasi transparansi kepatuhan tersebut, terutama ketika bukti tersebut divalidasi oleh auditor pihak ketiga yang terakreditasi.




*Gambar 0-5 ISO/IEC 27701 PIMS*

## 4.3.2 ISO/IEC 27018:2019

ISO/IEC 27018:2019 (ISO/IEC, 2019a) menetapkan tujuan kontrol, kontrol, dan pedoman yang diterima secara umum dalam menerapkan langkah-langkah untuk melindungi Informasi Identifikasi Pribadi (PII} sejalan dengan prinsip privasi dalam ISO/IEC 29100 untuk lingkungan komputasi awan publik.

Secara khusus, ISO/IEC 27018:2019 menetapkan pedoman berdasarkan ISO/IEC 27002, dengan mempertimbangkan persyaratan peraturan untuk perlindungan PII yang dapat diterapkan dalam konteks lingkungan risiko keamanan informasi pada penyedia layanan komputasi awan publik.

ISO/IEC 27018:2019 berlaku untuk semua jenis dan ukuran organisasi, termasuk perusahaan publik dan swasta, entitas pemerintah, dan organisasi nirlaba, yang menyediakan layanan pemrosesan informasi sebagai pemroses PII melalui komputasi awan berdasarkan kontrak dengan organisasi lain.

ISO/IEC 27018:2019 mengusulkan persyaratan kontrol pada data privasi pribadi untuk menangani perlindungan informasi identitas pribadi dan prinsip privasi dalam layanan komputasi awan. Sejumlah 37 tujuan kontrol pada ISO 27002 memperluas kontrol dan panduan terkait PII dalam layanan komputasi awan publik. Standar tersebut mengusulkan persyaratan kontrol pada data privasi pribadi untuk menangani perlindungan informasi identitas pribadi dan prinsip privasi di layanan komputasi awan.

ISO 27018 dianggap sebagai seperangkat pedoman dan kontrol yang meningkatkan ISO 27001 (standar untuk membangun sistem manajemen keamanan informasi atau ISMS), daripada standar untuk sertifikasi organisasi.

Berdasarkan dokumen ini, Penyedia layanan komputasi awan harus melakukan sertifikasi terhadap ISO 27001 menggunakan pedoman 27018 jika mereka memproses PII.

Berikut adalah empat cara tambahan kepatuhan ISO 27018 yang menguntungkan bisnis.

- Meningkatkan operasi secara global
- Meningkatkan keamanan dan perlindungan hukum
- Merampingkan proses penjualan
- Menjadikan keamanan yang lebih baik untuk dunia pasca pandemi

### 4.3.3 ISO/IEC 29101:2018

**ISO/IEC 29100:2011**

ISO/IEC 29100:2011 (ISO/IEC, 2011) menyediakan kerangka kerja privasi:

a. Menentukan terminologi privasi umum;
b. Mendefinisikan aktor dan peran mereka dalam memproses pii;
c. Menjelaskan pertimbangan perlindungan privasi; dan
d. Menyediakan referensi untuk prinsip privasi yang diketahui untuk teknologi informasi.

ISO/IEC 29100:2011 berlaku untuk orang perseorangan dan organisasi yang terlibat dalam menentukan, mengadakan, mengarsiteki, merancang, mengembangkan, menguji, memelihara, mengelola, dan mengoperasikan sistem atau layanan teknologi informasi dan komunikasi di mana kontrol privasi diperlukan untuk pemrosesan PII.

Standar ini bersifat umum dan menempatkan aspek organisasi, teknis, dan prosedural dalam kerangka kerja privasi secara keseluruhan, serta memberikan kerangka kerja tingkat tinggi untuk perlindungan PII dalam sistem teknologi informasi dan komunikasi (TIK).

Kerangka kerja privasi dimaksudkan untuk membantu organisasi menentukan persyaratan perlindungan privasi terkait PII dalam lingkungan TIK dengan:

a. Menentukan terminologi privasi umum;
b. Mendefinisikan aktor dan peran mereka dalam memproses pii;
c. Menjelaskan persyaratan perlindungan privasi; dan
d. Mereferensikan prinsip-prinsip privasi yang diketahui.

Di beberapa yurisdiksi, referensi Standar Internasional ini untuk persyaratan perlindungan privasi dapat dipahami sebagai pelengkap persyaratan hukum untuk perlindungan PII dan dimaksudkan untuk meningkatkan standar keamanan yang ada dengan menambahkan fokus yang relevan dengan pemrosesan PII. Penggunaan Standar Internasional ini akan:

a. Membantu dalam desain, implementasi, pengoperasian, dan pemeliharaan sistem TIK yang menangani dan melindungi PII;
b. Memacu solusi inovatif untuk mengaktifkan perlindungan PII dalam sistem TIK; dan
c. Meningkatkan program privasi organisasi melalui penggunaan praktik terbaik.

Kerangka kerja privasi yang disediakan dalam Standar Internasional ini dapat berfungsi sebagai dasar untuk inisiatif standarisasi privasi tambahan, seperti untuk:

a. Arsitektur referensi teknis;
b. Penerapan dan penggunaan teknologi privasi khusus dan manajemen privasi secara keseluruhan;
c. Kontrol privasi untuk proses data yang dialihdayakan;
d. Penilaian risiko privasi; atau
e. Spesifikasi teknis tertentu.

Elemen dasar dari kerangka kerja privasi meliputi:

a. Aktor dan peran
b. Interaksi
c. Mengenali PII
d. Persyaratan perlindungan privasi
e. Kebijakan privasi
f. Kontrol privasi

Prinsip privasi ISO/IEC 29100 meliputi:

a. Persetujuan dan pilihan
b. Legitimasi dan spesifikasi tujuan
c. Batasan pengumpulan
d. Minimisasi data
e. Batasan penggunaan, retensi, dan pengungkapan
f. Akurasi dan kualitas

g. Keterbukaan, transparansi dan pemberitahuan
h. Partisipasi dan akses individu
i. Akuntabilitas
j. Keamanan informasi
k. Kepatuhan privasi

**ISO/IEC 29101:2018**

ISO/IEC 29101:2018 (ISO/IEC, 2018) mendefinisikan kerangka kerja arsitektur privasi yang:

a. Menentukan masalah untuk sistem TIK yang memproses PII;
b. Membuat daftar komponen untuk penerapan sistem tersebut; dan
c. Memberikan pandangan arsitektur yang mengontekstualisasikan komponen-komponen ini.

ISO/IEC 29101:2018 berlaku untuk entitas yang terlibat dalam menentukan, mengadakan, mengarsiteki, merancang, menguji, memelihara, mengelola, dan mengoperasikan sistem TIK yang memproses PII. Dokumen ini menjelaskan kerangka kerja arsitektur tingkat tinggi dan kontrol terkait untuk perlindungan privasi dalam sistem TIK yang menyimpan dan memproses informasi yang dapat diidentifikasi secara pribadi (PII). Kerangka kerja arsitektur privasi yang dijelaskan dalam dokumen ini:

a. menyediakan pendekatan tingkat tinggi yang konsisten untuk penerapan kontrol privasi untuk pemrosesan PII dalam sistem TIK;
b. memberikan panduan untuk merencanakan, merancang, dan membangun arsitektur sistem TIK yang melindungi privasi prinsipal PII dengan mengontrol pemrosesan, akses, dan transfer informasi identitas pribadi; Dan
c. menunjukkan bagaimana teknologi peningkatan privasi dapat digunakan sebagai kontrol privasi.

Dokumen ini disusun berdasarkan kerangka kerja privasi yang disediakan oleh ISO/IEC 29100 untuk membantu organisasi menentukan persyaratan

perlindungan privasinya karena terkait dengan PII yang diproses oleh sistem TIK mana pun. Di beberapa negara, persyaratan perlindungan privasi dipahami sebagai sinonim dengan perlindungan data/persyaratan privasi dan tunduk pada undang-undang perlindungan/privasi data.

Dokumen ini membahas tinjauan terhadap kerangka kerja arsitektur privasi yang meliputi elemen-elemen dan hubungannya dengan sistem-sistem manajemen, aktor dan PII, fase siklus hidup pemrosesan PII (yang meliputi *Collection, Transfer, Use, Storage,* dan *Disposal*), prinsip-prinsip privasi, persyaratan perlindungan privasi, dan pandangan arsitektur (yang meliputi *Component view, Actor view, Interaction view*, beserta rincian masing-masing *view*) serta beberapa lampiran berupa contoh perhatian sistem TIK terkait PII, sistem agregasi PII dengan komputasi aman, dan sistem pseudonim yang ramah privasi untuk manajemen identitas dan kontrol akses.

### 4.3.4 ISO/IEC 29151:2017

ISO/IEC 29151:2017 (ISO/IEC, 2017) menetapkan tujuan kontrol, kontrol, dan pedoman untuk menerapkan kontrol, untuk memenuhi persyaratan yang diidentifikasi pada penilaian risiko dan dampak terkait dengan perlindungan PII. Secara khusus, rekomendasi atau standar ini menetapkan pedoman berdasarkan ISO/IEC 27002, dengan mempertimbangkan persyaratan untuk memproses PII yang mungkin berlaku dalam konteks lingkungan risiko keamanan informasi organisasi.

ISO/IEC 29151:2017 berlaku untuk semua jenis dan ukuran organisasi yang bertindak sebagai pengontrol PII (sebagaimana didefinisikan dalam ISO/IEC 29100), termasuk perusahaan publik dan swasta, entitas pemerintah, dan organisasi nirlaba yang memproses PII. Spesifikasi ini menawarkan panduan bagi pengontrol PII tentang berbagai kontrol keamanan informasi dan perlindungan PII yang umum diterapkan di banyak organisasi berbeda yang berurusan dengan perlindungan PII. Bagian keluarga standar ISO/IEC

lainnya memberikan panduan atau persyaratan pada aspek lain dari keseluruhan proses perlindungan PII yaitu:

a. ISO/IEC 27001 menentukan proses manajemen keamanan informasi dan persyaratan terkait, yang dapat digunakan sebagai dasar perlindungan PII.
b. ISO/IEC 27002 memberikan panduan untuk standar keamanan informasi organisasi dan praktik manajemen keamanan informasi termasuk pemilihan, penerapan dan pengelolaan kontrol, dengan mempertimbangkan lingkungan risiko keamanan informasi organisasi.
c. ISO/IEC 27009 menetapkan persyaratan untuk penggunaan ISO/IEC 27001 di sektor tertentu (bidang, area aplikasi atau sektor pasar). Ini menjelaskan cara memasukkan persyaratan tambahan untuk yang ada di ISO/IEC 27001, cara menyempurnakan persyaratan ISO/IEC 27001, dan cara menyertakan kontrol atau rangkaian kontrol selain Lampiran A ISO/IEC 27001.
d. ISO/IEC 27018 menawarkan panduan untuk organisasi yang bertindak sebagai pemroses PII saat menawarkan kemampuan pemrosesan sebagai layanan komputasi awan.
e. ISO/IEC 29134 memberikan panduan untuk mengidentifikasi, menganalisis, dan menilai risiko privasi, sedangkan ISO/IEC 27001 bersama dengan ISO/IEC 27005 menyediakan metodologi untuk mengidentifikasi, menganalisis, dan menilai risiko keamanan.

Kontrol harus dipilih berdasarkan risiko yang teridentifikasi sebagai hasil analisis risiko untuk mengembangkan sistem kontrol yang komprehensif dan konsisten. Kontrol harus disesuaikan dengan konteks pemrosesan PII tertentu. Standar ini membahas hal-hal sebagai berikut: tinjauan (terhadap tujuan perlindungan PII, persyaratan untuk perlindungan PII, kontrol, pemilihan kontrol, pengembangan pedoman khusus organisasi, pertimbangan siklus hidup, struktur dari spesifikasi ini) , kebijakan keamanan informasi, organisasi keamanan informasi, keamanan sumber

daya manusia, manajemen aset, kontrol akses, kriptografi, keamanan fisik dan lingkungan, keamanan operasi, keamanan komunikasi, data uji, hubungan pemasok, manajemen insiden keamanan informasi, aspek keamanan informasi manajemen kelangsungan bisnis, kepatuhan, serta lampiran berupa (kebijakan umum penggunaan dan perlindungan PII, persetujuan dan pilihan, legitimasi dan spesifikasi tujuan, batasan pemungutan, minimisasi data, pembatasan penggunaan, penyimpanan, dan pengungkapan, akurasi dan kualitas, keterbukaan, transparansi dan pemberitahuan, partisipasi dan akses utama PII, akuntabilitas, keamanan informasi, kepatuhan privasi).

### 4.3.5 Kode Etik CSA untuk Kepatuhan GDPR

Kode Etik CSA (*Cloud security Alliance*) untuk Kepatuhan GDPR menyediakan (*Cloud security Alliance*, 2018):

a. Fleksibilitas: Dapat diterapkan ke model pengiriman komputasi awan apa pun - IaaS/PaaS/SaaS.
b. Transparansi: Memberi pelanggan komputasi awan pemahaman yang jelas dan pandangan transparan tentang apa yang dilakukan Penyedia Layanan Komputasi awan.
c. Ketelitian: Kode etik CSA menyediakan *template* yang ketat dan terbukti untuk mematuhi persyaratan privasi GDPR.
d. Utilitas: Pelanggan komputasi awan dengan berbagai ukuran dapat menggunakan alat ini untuk mengevaluasi tingkat perlindungan data pribadi yang ditawarkan oleh berbagai CSP (sehingga mendukung keputusan yang tepat).
e. Kelengkapan: Memungkinkan CSP dengan berbagai ukuran dan lokasi geografis dengan panduan untuk mematuhi undang-undang perlindungan data pribadi Uni Eropa (UE) dan untuk mengungkapkan

tingkat perlindungan data pribadi yang mereka tawarkan kepada pelanggan.

Kode Etik *Cloud security Alliance* (CSA) untuk Kepatuhan GDPR adalah program sukarela yang dirancang untuk membantu CSP mematuhi GDPR Uni Eropa. (UE) GDPR adalah peraturan yang mewajibkan perusahaan untuk melindungi data pribadi warga negara UE dan mengenakan denda jika tidak mematuhinya. Kode Etik CSA untuk kepatuhan GDPR menyediakan kerangka kerja yang dapat diikuti oleh CSP untuk menunjukkan kepatuhan mereka terhadap GDPR. Kerangka tersebut mencakup 16 tujuan kontrol berbeda yang mencakup berbagai aspek perlindungan dan keamanan data, termasuk:

a. Perlindungan dan keamanan data: CSP harus menerapkan tindakan teknis dan organisasional yang sesuai untuk melindungi data pribadi dari akses, penggunaan, pengungkapan, atau penghancuran yang tidak sah.
b. Perjanjian pemrosesan data: CSP harus memiliki perjanjian pemrosesan data dengan pelanggan mereka yang mematuhi persyaratan GDPR.
c. Transparansi: CSP harus transparan tentang praktik pemrosesan data mereka dan memberikan informasi yang jelas kepada pelanggan tentang bagaimana data pribadi mereka digunakan.
d. Hak subjek data: CSP harus memberi pelanggan kemampuan untuk menggunakan hak mereka berdasarkan GDPR, seperti hak untuk mengakses, memperbaiki, atau menghapus data pribadi mereka.
e. Manajemen insiden: CSP harus memiliki prosedur manajemen insiden untuk mendeteksi dan merespons pelanggaran data.
f. Pemantauan kepatuhan: CSP harus secara teratur memantau kepatuhan mereka terhadap GDPR dan melakukan audit untuk memastikan bahwa mereka memenuhi persyaratan kode etik CSA.

Dengan mematuhi kode etik CSA untuk Kepatuhan GDPR, CSP dapat menunjukkan kepada pelanggan dan regulator mereka bahwa mereka mengambil tindakan yang tepat untuk melindungi data pribadi dan mematuhi GDPR. Kode etik CSA memberikan pendekatan standar dan transparan untuk kepatuhan GDPR yang dapat membantu CSP membedakan diri mereka di pasar yang ramai dan membangun kepercayaan dengan pelanggan mereka.

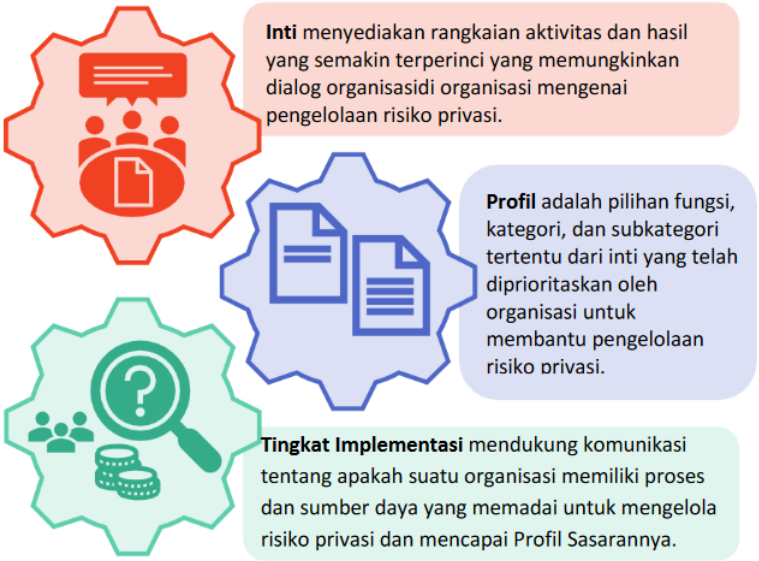
### 4.3.6 Kerangka Kerja Privasi NIST

Kerangka Kerja Privasi NIST (NIST, 2020b) merupakan alat untuk meningkatkan privasi melalui manajemen risiko perusahaan untuk memungkinkan praktik rekayasa privasi yang lebih baik yang mendukung privasi dengan konsep desain dan membantu organisasi melindungi privasi individu. Kerangka Privasi dapat mendukung organisasi dalam:

a. Membangun kepercayaan pelanggan dengan mendukung pengambilan keputusan yang etis dalam desain atau penerapan produk dan layanan yang mengoptimalkan penggunaan data yang bermanfaat sambil meminimalkan konsekuensi yang merugikan bagi privasi individu dan masyarakat secara keseluruhan;
b. Memenuhi kewajiban kepatuhan saat ini, serta produk dan layanan yang siap untuk masa depan memenuhi kewajiban ini dalam lingkungan teknologi dan kebijakan yang berubah; dan
c. Memfasilitasi komunikasi tentang praktik privasi dengan individu, mitra bisnis, penilai, dan regulator.

Kerangka privasi dimaksudkan agar dapat digunakan secara luas oleh organisasi dari semua ukuran, terlepas dari peran mereka dalam ekosistem pemrosesan data. Ini juga dirancang untuk agnostik terhadap teknologi, sektor, hukum, atau yurisdiksi tertentu, dan untuk mendorong kolaborasi

lintas organisasi antara berbagai bagian tenaga kerja organisasi, termasuk eksekutif, hukum, dan keamanan dunia maya.




*Gambar 0-6 Komponen kerangka kerja privasi NIST*

Kerangka privasi mengikuti struktur kerangka kerja untuk meningkatkan keamanan siber infrastruktur kritis untuk memfasilitasi penggunaan bersama kedua kerangka ini. Sama halnya dengan kerangka kerja keamanan siber, kerangka kerja privasi terdiri dari tiga bagian: *Core* (inti), *Profiles (*Profil*)*, dan *Implementation Tiers* (Tingkat implementasi) (lihat Gambar 0-6). Setiap komponen memperkuat manajemen risiko privasi melalui hubungan antara penggerak bisnis dan misi, peran dan tanggung jawab organisasi, dan aktivitas perlindungan privasi. Penjelasan ketiga bagian tersebut adalah sebagai berikut:

a. **Inti**: Inti terdiri dari lima fungsi - Identifikasi-P, Atur-P, Kontrol-P, Komunikasikan-P, dan Lindungi-P - yang harus diterapkan organisasi untuk mengelola risiko privasi. Setiap fungsi terdiri dari kategori dan sub kategori yang memberikan panduan lebih detail tentang aktivitas manajemen risiko privasi tertentu.

b. **Profil**: Profil adalah implementasi yang disesuaikan dari fungsi,

kategori, dan sub kategori Inti yang disesuaikan dengan kebutuhan, sasaran, dan tujuan manajemen risiko privasi spesifik organisasi.

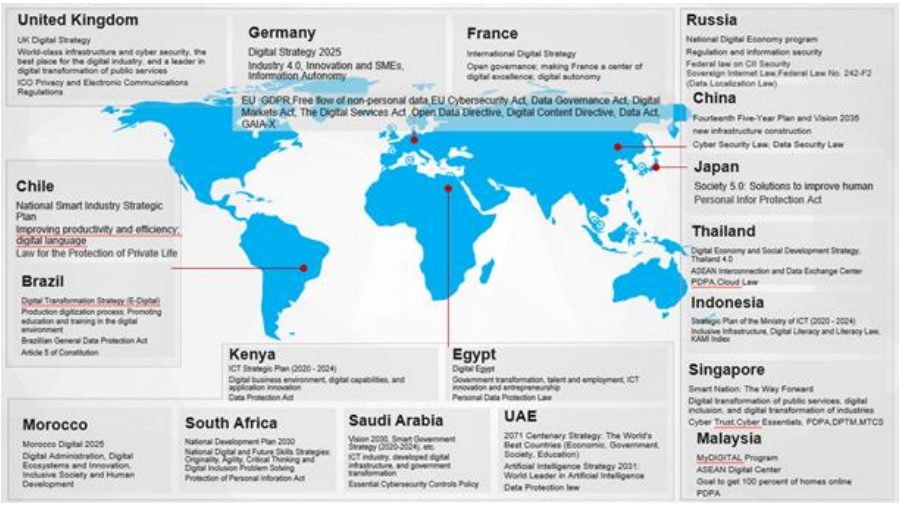
c. **Tingkat Implementasi**: Tingkat Implementasi menggambarkan tingkat ketelitian dan kecanggihan yang dengannya organisasi telah mengimplementasikan fungsi dan sub kategori Inti. Ada empat Tingkatan – *(1) Partial, (2) Risk Informed, (3) Repeatable,* dan *(4) Adaptive* - yang mencerminkan peningkatan tingkat kematangan dalam praktik manajemen risiko privasi organisasi.

Kerangka Kerja Privasi NIST dirancang agar kompatibel dengan kerangka kerja, undang-undang, dan peraturan privasi lainnya, dan dapat digunakan untuk melengkapi atau meningkatkan program privasi yang ada. Ini dimaksudkan untuk membantu organisasi membangun kepercayaan dengan pelanggan dan pemangku kepentingan mereka dengan menunjukkan komitmen mereka untuk melindungi informasi pribadi dan menghormati hak privasi individu. Secara keseluruhan, Kerangka Privasi NIST adalah alat yang berharga bagi organisasi yang mengumpulkan, menggunakan, menyimpan, atau membagikan informasi pribadi dan ingin mengelola risiko privasi secara efektif dan bertanggung jawab. Dengan mengikuti panduannya dan mengintegrasikan manajemen risiko privasi ke dalam keseluruhan praktik manajemen risiko mereka, organisasi dapat membangun hubungan yang lebih kuat dengan pelanggan dan pemangku kepentingan serta melindungi privasi individu yang mereka layani.

## 4.4 Kebijakan Tata Kelola Keamanan Siber Negara Uni Eropa

Lebih dari 170 negara telah mengembangkan perlindungan privasi/informasi pribadi, kebijakan, undang-undang, peraturan, dan aturan tata kelola komputasi awan dan data (Gartner, 2020b). Mereka juga mulai

menggunakan, seperti seri standar ISO/IEC, CSA CCM, SOC 1/2/3 , NIST CSF , PCI DSS, PCI 3DS dan sebagainya. Pada Gambar 0-7 mengilustrasikan berbagai negara yang telah memperhatikan keamanan siber dan juga keamanan komputasi awan.




*Gambar 0-7 Aturan tata kelola data di berbagai belahan negara di dunia*

Eropa menjaga kedaulatan nasional dan kedaulatan data melalui kebijakan dan peraturan, dan mempromosikan cloudifikasi, aliran data, dan berbagi di dalam UE, serta membuka kunci nilai data dengan data yang andal. Kedaulatan data yang bermula pada keamanan data digital telah bergeser ke standardisasi dan sertifikasi produk-produk dan jasa-jasa teknologi digital (Watubun, 2022). Selanjutnya adalah gambaran tentang peraturan keamanan siber atau keamanan komputasi awan yang berlaku di Uni Eropa.

### 4.4.1 GDPR

Bermula pada laporan investigasi pelanggaran data pada waktu itu mengungkapkan bahwa lebih dari 100.000 insiden keamanan dilaporkan dari 82 negara, termasuk 3.141 pelanggaran data yang dikonfirmasi. Untuk

meningkatkan perlindungan, pada 27 April 2016 Uni Eropa mengesahkan peraturan perlindungan data Eropa yang baru, *General Data Protection Regulation* (GDPR), sebagai penerus dari *Privacy Data Directive* 1995 (Magnusson & Iqbal, 2018).

Ke-27 negara anggota Uni Eropa (UE) memiliki peraturan sendiri hingga tahun 2016 yang mencakup pengumpulan, kompilasi, dan perencanaan tentang data pribadi warganya. Pada tanggal 27 April 2016, Komisi UE menerima GDPR tambahan yang akan berdampak penuh pada 25 Mei 2018. GDPR menghapus semua aturan keamanan data nasional di sekitar semua negara anggota UE bahkan dalam konteks DPD (Germanos et al., 2020).

Dalam GDPR ada pedoman baru untuk mengajukan kerangka kerja mengenai denda. Kerangka kerja ini menyatakan bahwa setiap perusahaan yang tidak memenuhi aturan baru dapat dihukum hingga 4% dari keuntungan global tahunannya. Organisasi dan perusahaan harus mematuhi GDPR secepat mungkin. GDPR berisi banyak pedoman, peraturan, dan standar baru. Menurut GDPR, baik organisasi maupun otoritas publik, harus menunjuk petugas perlindungan data (DPO) mereka sendiri. Peran DPO adalah untuk memastikan bahwa organisasi menangani data pribadi staf, pelanggan, atau individu lainnya sesuai dengan peraturan perlindungan yang berlaku (Germanos et al., 2020).

Pada prinsipnya, dilarang mentransfer data pribadi warga negara UE ke negara di luar UE kecuali negara tersebut dianggap oleh Komisi memberikan perlindungan data yang memadai. Negara ketiga perlu memastikan bahwa tingkat perlindungan data mereka pada dasarnya setara dengan perlindungan UE, khususnya bahwa peraturan perlindungan data independen yang efektif sudah ada dan bahwa subjek data memiliki hak yang efektif dan dapat ditegakkan serta pemulihan administratif dan yudisial yang efektif.

Pendekatan GDPR mampu menjangkau meski secara jarak berjauhan, tidak penting apakah pengontrol non-UE yang menawarkan barang atau jasa memiliki hubungan teritorial dengan UE atau apakah warga negara dari UE benar-benar membeli barang atau jasa tersebut. Namun ada masalah yang terjadi berkaitan dengan implementasi GDPR di luar UE. GDPR hanya mensyaratkan bahwa subjek data harus ada di wilayah UE, tetapi tidak harus tinggal di UE. Oleh karena itu, penerapan GDPR ekstrateritorial yang begitu luas di wilayah negara ketiga tidak dapat ditegakkan. Terakhir, ketentuan yang bertentangan mengenai undang-undang yang berlaku dapat muncul ketika perbandingan dibuat antara Pasal 3(2)a dan perjanjian kontraktual antara perusahaan yang berbasis di UE dan CSP negara ketiga mengenai undang-undang yang berlaku dalam situasi yang bertentangan (Michels & Walden, 2020a). GDPR menjadi penting dalam penerapan kedaulatan data di Uni Eropa.

### 4.4.2 NIS *Directive* 2.0

NIS (*The Network and Information Systems*) adalah bagian komprehensif pertama dari undang-undang di Uni Eropa yang secara khusus ditujukan untuk meningkatkan keamanan siber sehubungan dengan perlindungan infrastruktur nasional yang kritis. Tidak seperti prinsip akuntabilitas di bawah GDPR, tidak ada persyaratan eksplisit di bawah *NIS Directive* bagi perusahaan untuk secara proaktif menunjukkan kepatuhan mereka secara berkelanjutan. Berbeda juga dengan GDPR, tidak ada persyaratan untuk menunjuk pakar internal dengan sumber daya dan independensi yang memadai untuk memantau dan memberi nasihat tentang kepatuhan (Michels & Walden, 2020b). *NIS Directive* membahas tantangan hilangnya layanan dalam jaringan TI dan struktur informasi di mana GDPR berurusan dengan perlindungan data pribadi. *NIS Directive* jauh lebih mendekati bagi penyedia layanan dan penyedia layanan digital yang mempekerjakan 50 atau lebih (Germanos et al., 2020).

NIS Directive memiliki tiga pilar yakni: Kemampuan Negara Anggota, Manajemen risiko, dan Kerjasama & pertukaran informasi (Kamara & Boom, 2022). UE telah menangani masalah keamanan dunia maya secara komprehensif sejak tahun 2004, ketika mendirikan ENISA (Badan Uni Eropa untuk Jaringan dan Keamanan Informasi).

NIS Directive berakar pada Komisi Komunikasi Komisi di tahun 2009, yang berfokus pada pencegahan dan kesadaran serta menetapkan rencana tindakan segera untuk memperkuat keamanan dan kepercayaan dalam masyarakat informasi. Hal ini diikuti oleh Komunikasi bersama yang dirilis oleh Komisi dan Perwakilan Tinggi Uni Eropa untuk Urusan Luar Negeri dan Kebijakan Keamanan tentang Strategi Keamanan Siber Uni Eropa pada tahun 2013.

Dari tahun 2013 hingga 2015, Komisi, dan Dewan membahas secara intensif draf yang diajukan Komisi dan pembahasan tersebut menghasilkan NIS Directive. NIS Directive mulai berlaku pada Agustus 2016. Batas waktu untuk transposisi nasional oleh Negara-negara Anggota UE adalah 9 Mei 2018 (Maliatsos et al., 2022).

Menurut NIS Directive, layanan digital berarti pasar online, mesin pencari online, dan layanan komputasi awan (Maliatsos et al., 2022). Komponen dari layanan digital terdiri dari : Titik Pertukaran Internet (IXP), Server Sistem Nama Domain (DNS), Domain Tingkat Atas (TLD), Penyedia Layanan Internet, Operator seluler, Jaringan pengiriman konten, Penyedia layanan komputasi awan, Pasar, dan Mesin pencari.

Negara-negara Anggota UE ketika mereka mempertimbangkan langkah-langkah apa yang harus diambil untuk mengelola risiko yang ditimbulkan terhadap keamanan jaringan dan sistem informasi mereka. Pertimbangan tersebut meliputi: Keamanan sistem dan fasilitas, penanganan insiden,

manajemen kesinambungan bisnis, pemantauan, audit dan pengujian serta kepatuhan dengan standar internasional.

Sejalan dengan layanan digital menurut NIS Directive yang mengajukan persyaratan langsung untuk pembangunan domain kemampuan seperti jaringan dan sistem informasi serta keamanan fasilitas. Yaitu pentingnya perlindungan Lindungi keamanan infrastruktur penting, rantai pasokan, dan keamanan nasional, perlindungan lindungi jalur hidup kehidupan ekonomi, dan membangun bangun Eropa yang tangguh, hijau, dan digital.

Kewajiban berdasarkan NIS Directive dapat dibedakan secara luas menjadi dua kategori. Pertama, kewajiban pengamanan mengharuskan operator layanan esensial (OES) untuk menerapkan langkah-langkah keamanan siber dan terlibat dalam proses manajemen risiko siber yang berkelanjutan. Kedua, kewajiban informasi mensyaratkan pembagian atau pengungkapan informasi, untuk mempromosikan transparansi dan meningkatkan kesadaran.

NIS Directive tidak dapat diterapkan secara langsung, tetapi mewajibkan negara anggota untuk mencapai hasil tertentu. Beberapa Negara Anggota memiliki ruang untuk bermanuver dalam proses transposisi, untuk mempertimbangkan karakteristik nasional tertentu. Hal ini memastikan pendekatan yang harmonis terhadap keamanan siber, dengan konsekuensi yang menguntungkan dalam hal pembentukan badan pengalaman regulasi, panduan, dan kepastian hukum.

Untuk mengatasi tantangan ketidakpastian di bawah NIS Directive, regulator dapat mengeluarkan panduan tentang cara menafsirkan dan menerapkan Arahan tersebut. Misalnya, NIS Cooperation Group telah menerbitkan serangkaian pedoman dan dokumen referensi di bawah NIS Directive. telah menetapkan prinsip-prinsip keamanan tingkat tinggi, yang dilengkapi dengan pedoman khusus sektor dari otoritas yang kompeten (Maliatsos et al.,

2022). Dan Untuk menangkal risiko OES yang hanya terlibat dalam "kepatuhan kertas", regulator harus mengambil pendekatan proaktif untuk memantau praktik keamanan *operators of essential services* (OES). Regulator perlu secara aktif menantang perusahaan untuk mendemonstrasikan bahwa sistem mereka berfungsi dalam praktiknya, memeriksa tindakan mereka, dan menilai apakah perusahaan memiliki kepemimpinan, staf, sistem, dan prosedur untuk memenuhi kewajibannya. Memusatkan perhatian pada upaya pada perusahaan-perusahaan yang menimbulkan ancaman terbesar bagi kepentingan yang dilindungi oleh NIS Directive.

### 4.4.3 EU *Cybersecurity Act*

Terdapat peran penting ENISA dalam memajukan implementasi mengimplementasikan NIS Directive dimajukan. Seperti yang didorong oleh mendorong melalui proposal untuk peraturan baru tentang ENISA (yakni EU Cybersecurity Act). Sebelum mengelaborasi hubungan yang tak terelakkan, dari antara NIS Directive dengan GDPR (Maliatsos et al., 2022).

Ada pembagian tugas antara Lembaga di UE dan Badan Uni Eropa untuk Keamanan Siber. Lembaga-lembaga UE menangani langkah-langkah perlindungan khusus, sarana teknis, konstruksi keuangan dan infrastruktur, pendidikan kesadaran keamanan dunia maya publik, dan kerja sama timbal balik antara negara-negara anggota. Badan Uni Eropa untuk Keamanan Siber (*European Union Agency for Cybersecurity*) bertugas mendukung dan memfasilitasi pengembangan dan penerapan produk TIK, layanan TIK, dan kebijakan aliansi sertifikasi keamanan siber pemrosesan TIK.

Untuk keperluan implementasi Peraturan EU Cybersecurity Act dibentuk badan independen, yang akan diberi nama "Badan Keamanan Siber UE". Badan tersebut beroperasi sebagai pusat keahlian dalam keamanan siber. Tugasnya membantu lembaga, badan dan badan Uni, mendukung pembangunan kapasitas dan kesiapan di seluruh Perhimpunan. Aturan

tersebut akan memajukan kerja sama di seluruh Perhimpunan dan akan memajukan penggunaan sertifikasi keamanan siber (Markopoulou et al., 2019).

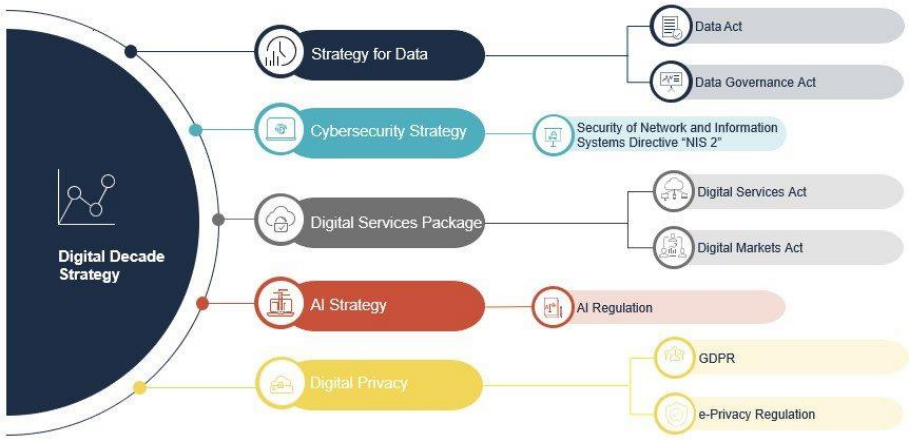
### 4.4.4 *Free Flow of Non-Personal Data*

UE memastikan pergerakan data non-pribadi lintas batas yang bebas di dalam UE dan melarang pembatasan pelokalan data. Di UE, data dibagi menjadi tiga kategori, yaitu data pribadi, data anonim, dan data non-pribadi. Yang terakhir diatur dan tunduk pada Regulasi (UE) 2018/1807 tentang *Free flow of non-personal data*. Dua yang pertama diatur oleh GDPR. Tujuan Peraturan (UE) 2018/1807 untuk memastikan aliran data yang bebas dapat berdampak buruk. Karena aliran bergantung pada gagasan data non-pribadi. Jika gagasan berbeda di seluruh Negara Anggota maka menghalangi kemungkinan untuk menciptakan lingkungan perdagangan data yang seragam di UE. Ketidakpastian juga dapat menciptakan penghalang untuk pergerakan bebas layanan, karena interpretasi yang berbeda akan menentukan perbedaan teknologi yang berlaku di seluruh Negara Anggota. Hal tersebut akan mendistorsi persaingan karena produsen dapat diberi insentif untuk memilih menawarkan barang dan jasa di beberapa Negara Anggota yang merugikan negara lain (CHERCIU, 2020) .

### 4.4.5 *Digital Services Act*

Undang-Undang Layanan Digital Services Act (DSA) melengkapi arahan e-Commerce directive yang dibentuk di tahun 2000 dan menargetkan perantara *online* (seperti pasar *online*, perusahaan komputasi awan, dan mesin telusur besar). Beberapa ketentuan utama meliputi: larangan beriklan untuk anak di bawah umur dan menggunakan kategori data khusus; larangan pola gelap; kewajiban untuk mengidentifikasi dan menghapus konten ilegal; dan serta persyaratan transparansi tambahan (Dechert LLP, 2022).

Selain itu, DSA menetapkan kerangka kerja yang transparansi untuk platform *online* dan membentuk organisasi untuk meninjau tinjauan konten. Layanan digital menurut DSA, berkisar dari situs web sederhana hingga layanan infrastruktur Internet dan platform *online*.




*Gambar 0-8 Pembagian Aturan Data Digital*

Ada Catatan berkaitan dengan DSA ini yakni membatasi "kekuatan" media sosial dan merebut kembali "hak untuk menghapus *postingan*" media digital yang berdampak besar pada perusahaan Internet. (Di balik hak untuk menghapus kiriman ada konflik besar antara proposisi hukum dan nilai).

### 4.4.6 *Digital Markets Act*

Sementara DSA berfokus pada hubungan antara layanan dan penggunanya, *Digital Markets Act* (DMA) bertujuan untuk mengatur persaingan antara bisnis "penjaga gerbang (*gatekeeper*)" (diidentifikasi dalam hal pendapatan dan jumlah pengguna, meskipun perusahaan yang lebih kecil dapat ditunjuk seperti itu. oleh Komisi UE) yang menyediakan layanan platform inti (seperti

mesin telusur *online*, layanan jejaring sosial, dan asisten virtual). Peraturan tersebut berisi serangkaian "anjuran" dan "larangan" yang dirancang untuk mencegah praktik bisnis tertentu dan untuk melindungi usaha kecil. Ada tumpang tindih dengan GDPR, khususnya sehubungan dengan ketentuan pemrosesan data pribadi di DMA, yang mengharuskan mereka yang terkena dampak untuk melihat ke beberapa undang-undang untuk menetapkan kewajiban mereka (Dechert LLP, 2022). Tujuan DMA adalah untuk melemahkan monopoli platform besar *Gatekeeper*, memutus kendali data oleh *gatekeeper*, dan mempromosikan inovasi digital di dalam UE.

### 4.4.7 *Data Governance Act*

*Data Governance Act* (DGA) bertujuan untuk mendorong pembagian dan penggunaan kembali data dengan tetap menghormati privasi data, kerahasiaan, dan hak kekayaan intelektual. Ini mencakup tiga bidang utama yaitu :Akses ke data yang dimiliki oleh badan sektor publik; Regulasi layanan intermediasi data; dan Mendorong '*altruisme data*' – menyumbangkan data untuk kebaikan bersama (misalnya untuk penelitian ilmiah).

Meskipun peraturan tersebut terutama akan berlaku untuk badan sektor publik, bisnis juga harus meninjau apakah aktivitas mereka dapat termasuk dalam layanan intermediasi data DGA (dan, jika demikian maka harus, membiasakan diri dengan ketentuan yang disyaratkan . Aturan itu yang pada prinsipnya didorong untuk memastikan independensi). Resital DGA secara khusus menyebutkan pasar data dan kumpulan data, yang mungkin sangat relevan di sektor adtech (Dechert LLP, 2022).

Undang-Undang Tata Kelola Data DGA disahkan pada Mei 2022 dan akan berlaku pada September 2023. Tujuannya adalah untuk membentuk struktur perantara dan menegakkan sertifikasi penyedia layanan perantara data.

DGA telah dengan jelas mendefinisikan subjek data (hak). Kesehatan dan mengemudi auto-kendali adalah dua industri yang paling diperhatikan oleh UE. Direkomendasikan DGA menjadi rekomendasi bagi agar data publik UE untuk dibuka sehingga untuk meningkatkan kepercayaan pada perantara data dan memperkuat mekanisme berbagi dan penggunaan kembali data di seluruh UE. UE berharap dapat menghasilkan €700 miliar pertumbuhan PDB melalui open data terbuka.

### 4.4.8 *Open Data Directive*

Dengan adanya Open Data Directive, Badan-badan sektor publik harus membuat dokumen dan data utilitas publik secara tepat waktu dan menyesuaikan format dan metadata mereka dengan standar keterbukaan formal. Selain itu, Instansi departemen dan utilitas publik harus membuat dokumen mereka tersedia dalam format atau bahasa apa pun yang ada dan, jika memungkinkan dan sesuai, melalui sarana elektronik, dokumen dan metadatanya dalam format yang tersedia untuk umum, dapat dibaca mesin, dapat diakses, dapat dicari, dan dapat digunakan kembali. Jika memungkinkan, format dan metadata harus mematuhi standar terbuka formal.

### 4.4.9 *Data Act*

*Data Act* adalah langkah logis berikutnya setelah *Data Governance Act*. Ini adalah inisiatif legislatif utama kedua setelah strategi data Eropa Februari 2020, yang menjadikan UE pemimpin dalam masyarakat berbasis data.

*Data Governance Act*, yang dipresentasikan pada November 2020 dan disetujui oleh wakil legislator pada November 2021, menciptakan proses dan struktur untuk memfasilitasi pembagian data oleh perusahaan, individu, dan sektor publik. *Data Act* mengklarifikasi siapa yang dapat menciptakan nilai dari data dan dalam kondisi apa. *Data Act* menghilangkan hambatan untuk mengakses

data, baik untuk sektor swasta maupun publik, sekaligus mempertahankan insentif untuk berinvestasi dalam pembuatan data dengan memastikan kontrol yang seimbang atas data untuk pembuatnya.

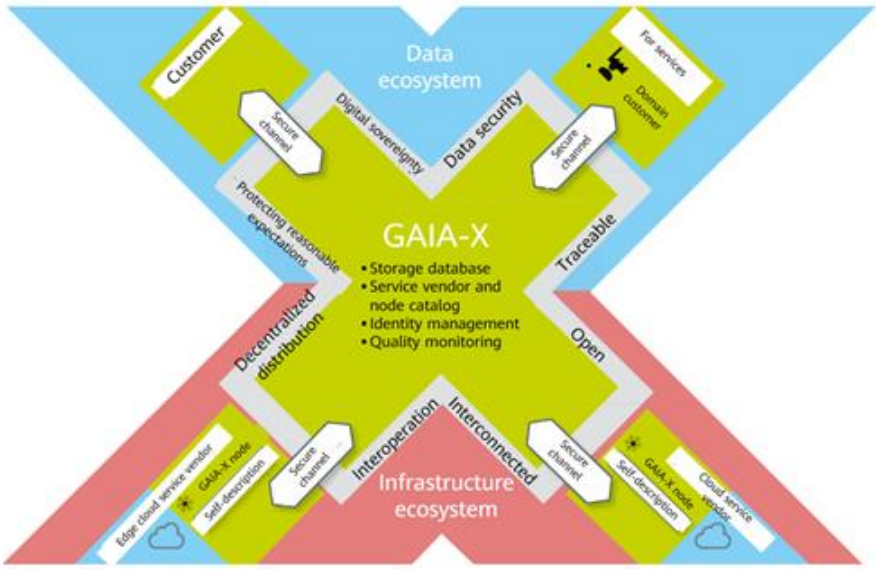
Saat membeli produk 'tradisional', maka diperoleh semua suku cadang dan aksesori dari produk tersebut. Namun, saat kita membeli produk yang terhubung (misal peralatan *smart home*) yang menghasilkan data, seringkali tidak jelas siapa yang dapat melakukan apa dengan data tersebut. Atau mungkin ditentukan dalam kontrak bahwa semua data yang dihasilkan diambil dan digunakan secara eksklusif oleh pabrikan.

*Data Act* memberi individu dan bisnis lebih banyak kontrol atas data mereka melalui hak portabilitas data yang diperkuat, menyalin atau mentransfer data dengan mudah dari berbagai layanan, di mana data dihasilkan melalui objek, mesin, dan perangkat pintar. Misalnya, pemilik mobil atau mesin dapat memilih untuk berbagi data yang dihasilkan dari penggunaannya dengan perusahaan asuransinya. Data tersebut, dikumpulkan dari banyak pengguna, juga dapat membantu mengembangkan atau meningkatkan layanan digital lainnya, misal mengenai lalu lintas, atau area dengan risiko kecelakaan tinggi (Dechert LLP, 2022).

### 4.4.10GAIA-X

GAIA-X adalah proyek yang dikembangkan federasi infrastruktur data dan penyedia layanan untuk Eropa dengan tujuan memastikan kedaulatan digital Eropa. GAIA-X adalah bagian dari strategi yang lebih luas di bawah Komisi von der Leyen dari otonomi strategis Eropa. Proyek ini pertama kali dipresentasikan kepada masyarakat umum pada Digital Summit tahun 2019 di Dortmund, Jerman dan terus dikembangkan sejak saat itu. Inisiatif Rancangan GAIA-X mengambil  diambil dari bentuk hukum AISBL, sebuah organisasi nirlaba internasional yang berbasis di Belgia. Diprakarsai oleh Perancis dan Jerman, ia yang berupaya membuat proposal untuk

infrastruktur data generasi berikutnya untuk Eropa, serta mendorong kedaulatan digital pengguna layanan komputasi awan di Eropa. Dilaporkan Pelaporannya berdasarkan nilai-nilai transparansi, keterbukaan, perlindungan data, dan keamanan Eropa. Nama proyek ini merujuk pada dewi Yunani Gaia.




*Gambar 0-9 Arsitektur GAIA-X*

Dengan adanya Gaia-X, perwakilan dari bisnis, sains, dan politik di tingkat internasional harus membuat proposal untuk infrastruktur data generasi berikutnya. Proposal yang terdiri dari yaitu : ekosistem digital yang terbuka, transparan, dan aman, penyediaan tempat data dan layanan dapat disediakan, disusun tersusun, dan terbagi dibagikan dalam sebuah lingkungan terpercaya kepercayaan.

Gaia-X adalah proyek yang diprakarsai oleh Eropa untuk Eropa dan sekitarnya. Perwakilan dari bisnis, politik, dan sains dari Eropa dan seluruh dunia bekerja sama, bergandengan tangan, untuk menciptakan infrastruktur

data yang terfederasi dan aman. Perusahaan dan warga negara akan menyusun dan berbagi data – sedemikian rupa sehingga mereka tetap dapat mengontrolnya. Mereka harus memutuskan apa yang terjadi pada data mereka, di mana disimpan, dan selalu mempertahankan kedaulatan data (Otto, 2022).

Arsitektur Gaia-X didasarkan pada prinsip desentralisasi. Gaia-X adalah hasil dari banyak platform individual yang semuanya mengikuti standar umum – standar Gaia-X. Jadi, yang muncul bukanlah komputasi awan, melainkan sistem jaringan yang menghubungkan banyak penyedia layanan komputasi awan secara bersamaan.

### 4.4.11Jerman C5

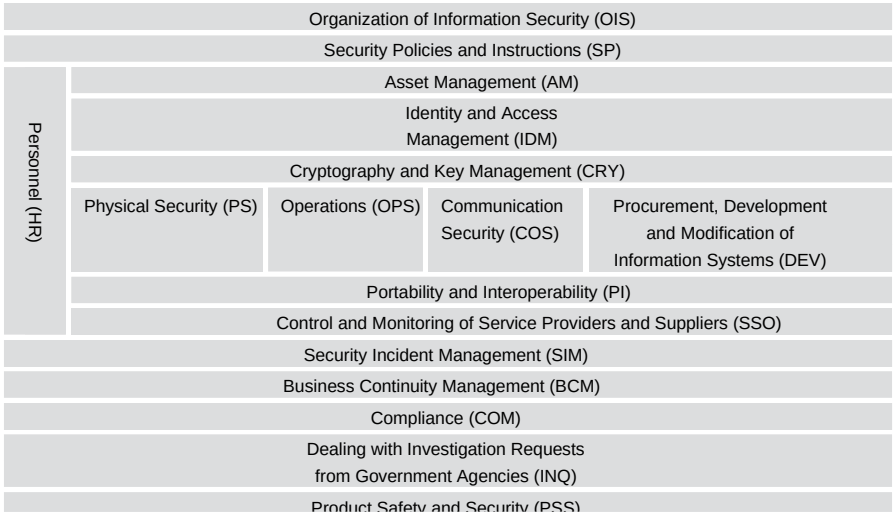
*The Federal Risk and Authorization Management Program* (FedRAMP) di AS dan *Cloud Computing Compliance Controls Catalogue* (C5) di Jerman bertujuan untuk meningkatkan tingkat perlindungan terhadap ancaman dan kerentanan yang unik pada komputasi awan. C5 adalah skema pengesahan yang didukung Pemerintah Jerman yang diperkenalkan oleh Badan untuk Keamanan Informasi di Jerman (BSI). C5 untuk membantu CSP mendemonstrasikan keamanan operasional terhadap serangan dunia maya umum saat menggunakan layanan komputasi awan dalam konteks "rekomendasi keamanan untuk penyedia komputasi awan dari pemerintah Jerman" (Giulio et al., 2017).

BSI menghadirkan C5 hanya sebagai pedoman bagi CSP untuk membangun sertifikasi lain, yang dilakukan C5 adalah menambahkan elemen lain ke lanskap standar yang umum digunakan sudah ramai untuk penyedia TI. Seperti kerangka kerja lainnya, C5 bergantung pada *control* keamanan yang diatur dalam domain kontrol. C5 menetapkan serangkaian persyaratan dasar yang wajib bagi Komputasi awan untuk dianggap sesuai dengan standar. Persyaratan tambahan ditentukan untuk memastikan tingkat keamanan yang

lebih tinggi, jika berlaku Difusi besar (Giulio et al., 2017) standar keamanan TI yang ada seperti ISO/IEC 27001 mempertanyakan perlunya membuat kerangka kerja baru daripada berfokus pada peningkatan yang sudah ada.

Tujuan C5 adalah menilai keamanan informasi layanan komputasi awan untuk membangun kepercayaan. Standar yang ditetapkan untuk keamanan informasi (misalnya, ISO/IEC 27001 dan CSA CCM) membentuk dasar kriteria dan memungkinkan auditor untuk melaksanakan audit sesuai dengan standar audit internasional.

Katalog kriteria ini berisi 17 tujuan terkait keamanan informasi layanan komputasi awan. Setiap tujuan dipecah menjadi kriteria yang diperlukan untuk mencapai tujuan. Kriteria dibagi menjadi kriteria dasar dan kriteria tambahan.




*Gambar 0-10 Germany C5:2020 Kerangka kerja manajemen keamanan komputasi awan*

Kriteria dasar mencerminkan tingkat minimum keamanan informasi yang harus ditawarkan oleh CSP saat CSC menggunakan layanan komputasi awan. Kriteria dasar menentukan ruang lingkup minimum audit menurut C5. Untuk CSC yang informasinya memiliki kebutuhan perlindungan yang lebih tinggi, kriteria tambahan memberikan titik awal untuk melakukan penilaian

ini. CSP dapat menyertakan kriteria keamanan lain saat melakukan penilaian menurut C5.

CSC tetap mendapat informasi tentang kontrol keamanan yang diterapkan oleh CSP untuk memenuhi persyaratan C5 berdasarkan informasi dalam laporan pengesahan C5, dan menilai kesesuaian desain dan efektivitas pengoperasian mekanisme kontrol.

Menetapkan kerangka kerja keamanan seperti itu mempermudah organisasi untuk memahami langkah-langkah keamanan yang perlu mereka terapkan dan keahlian yang mereka perlukan untuk melakukannya. Namun, kerangka kerja ini tidak terkait dengan proses manajemen layanan komputasi awan, dan karena itu sulit bagi departemen fungsional untuk memahami tanggung jawab keamanan dalam peran mereka. Akibatnya, beberapa tanggung jawab keamanan mungkin tidak ditetapkan.

Keamanan operasional, manajemen pengadaan rantai pasokan, manajemen aset, dan manajemen akses adalah fokus utama skema sertifikasi khusus komputasi awan yakni C527.

## 4.5 Kebijakan Tata Kelola Keamanan Siber Negara di Asia

### 4.5.1 Kazakhstan

Awal Maret 2019, Presiden Republik Kazakhstan mengadopsi Undang-Undang "Tentang ratifikasi Perjanjian kerjasama negara-negara anggota organisasi Perjanjian Keamanan Kolektif di bidang keamanan informasi". Sebelumnya, Pada November 2016, JSC "*National Infocommunication Holding* "Zerde" ditentukan oleh pemerintah Kazakhstan oleh *National Institute of development* di bidang teknologi informasi dan komunikasi. Keputusan Presiden Republik Kazakhstan pada Januari 2018 membentuk Komisi di bawah Presiden Republik Kazakhstan tentang implementasi digitalisasi di

Republik Kazakhstan. Juni 2017. Pemerintah Kazakhstan menyetujui Konsep keamanan siber "Perisai siber Kazakhstan". Tujuan utama organisasi komisi tersebut adalah untuk melakukan kegiatan tertentu dalam keamanan informasi, dan juga berkontribusi pada organisasi pembentukan, pengembangan, dan keamanan ruang informasi dan infrastruktur komunikasi Republik Kazakhstan. Menurut GCI (*draft*) di tahun 2018, Kazakhstan menaikkan peringkatnya dari posisi ke-83 ke posisi ke-40, dari tahun sebelumnya yang merupakan pencapaian luar biasa bagi Kazakhstan dalam waktu singkat. GCI dihitung setiap tahun. Integrasi GCI pertama kali dilakukan pada tahun 2013-2014. Dalam pemeringkatan ini, negara-negara seperti Kazakhstan, Tiongkok, Thailand, Hongaria, Bulgaria, Filipina, Ukraina berada pada tahap pematangan, sedangkan Singapura, AS, Rusia termasuk di antara negara-negara terkemuka di dunia (ITU, 2018).

Dengan adanya Kazakhstan Law On Communications, Operator komunikasi dan (atau) pemilik jaringan komunikasi yang beroperasi di wilayah Republik Kazakhstan berkewajiban untuk:

a. menyediakan badan yang melakukan kegiatan investigasi operasional, kontra intelijen pada jaringan komunikasi dengan kemampuan organisasi dan teknis untuk melakukan investigasi operasional , tindakan kontra intelijen di semua jaringan komunikasi, serta mengambil tindakan untuk pencegahan pengungkapan bentuk dan metode untuk melakukan tindakan tertentu;
b. mengumpulkan dan menyimpan informasi resmi dengan cara yang ditentukan oleh Pemerintah Republik Kazakhstan. Penyimpanan informasi resmi tentang pelanggan dilakukan secara eksklusif di wilayah Republik Kazakhstan. Dilarang mentransfer informasi resmi tentang pelanggan di luar Republik Kazakhstan, kecuali untuk kasus penyediaan layanan komunikasi kepada pelanggan Republik Kazakhstan yang berlokasi di luar negeri.

Catatan pada aturan ini adalah: Data tentang pelanggan layanan komunikasi hanya disimpan di Kazakhstan, dan dilarang untuk mentransfernya ke luar negeri, kecuali untuk skenario di mana layanan disediakan untuk warga negara Kazakhstan di luar negeri.

### 4.5.2 Saudi Arabia

Di Timur Tengah, Arab Saudi adalah salah satu pasar terbesar untuk produk dan layanan TI Perusahaan 14. Regulator telekomunikasi Arab Saudi, *Communications & Information Technology Commission* (CITC), mengeluarkan kerangka peraturan komputasi awan (Komputasi awan *Framework*), yang mulai berlaku pada Maret 2018. Juga pada tahun 2018, *National Cybersecurity Authority* (NCA), badan pemerintah yang bertanggung jawab atas keamanan siber, mengeluarkan *Essential Cybersecurity Controls* (ECC:2018). ECC:2018 berisi pembatasan yang sangat luas pada penggunaan layanan komputasi awan yang berbasis di luar Kerajaan. Hal ini menyebabkan kekhawatiran bagi penyedia layanan komputasi awan dan pelanggan komputasi awan. NCA adalah lembaga pemerintah yang bertanggung jawab atas keamanan siber .

Dalam penelitian di Arab Saudi sebelum penerapan komputasi awan ditemukan bahwa sebagian besar organisasi mengkhawatirkan masalah privasi, keamanan, dan kepercayaan dan ini adalah salah satu alasan utama di balik keputusan mereka untuk tidak menggunakan layanan komputasi awan. Selain itu, ada faktor lain yang disarankan oleh para ahli, seperti kompatibilitas, kepatuhan terhadap peraturan, dan penghematan biaya, dan organisasi perlu mempertimbangkannya sebelum menggunakan layanan komputasi awan (Alkhater et al., 2015).

Kerangka legislatif Kerajaan tidak secara jelas dan komprehensif mengatur komputasi awan atau penyedia layanan atau pelanggannya. Oleh karena itu, organisasi yang ingin memanfaatkan layanan Komputasi awan harus siap untuk memahami semua dimensi Komputasi awan Publik yang berdampak

dan hubungannya dengan mereka di Kerajaan, mulai dari kewajiban kontraktual hingga aspek pengembangan hubungan, dalam upaya untuk memberikan panduan yang lebih baik (O'Connell, 2019).

Pelanggan Komputasi awan tidak boleh mentransfer, menyimpan, atau memproses Konten Pelanggan Level 3 ke atau di Komputasi awan Publik, Komputasi awan Komunitas, atau Komputasi awan Hibrid mana pun, kecuali dan selama CSP terdaftar secara sah di Komisi sesuai dengan pasal 3.2.

Catatan pada aturan ini adalah: Konten pelanggan Level-3 harus disimpan secara lokal dan tidak dapat ditransfer ke luar wilayah .

### 4.5.3 UAE

PSP (penyedia layanan pembayaran digital, lembaga pemberi lisensi yang berwenang untuk menyediakan layanan pembayaran digital, termasuk PSP Ritel, PSP Pembayaran Mikro, PSP Pemerintah, dan PSP Non-penerbit) harus menyimpan dan menyimpan semua data Pengguna dan data transaksi secara eksklusif dalam batas-batas UEA, (tidak termasuk Zona Bebas keuangan UEA), untuk jangka waktu lima (5) tahun sejak tanggal transaksi awal.

UAE *Regulatory Framework for Stored Values and Electronic Payment Systems* (RVPS). Kerangka tersebut menetapkan aturan dan persyaratan untuk entitas yang menyediakan layanan tersebut, serta hak dan kewajiban konsumen dan pedagang. Kerangka kerja RVPS berlaku untuk semua jenis layanan pembayaran elektronik, termasuk kartu prabayar, dompet digital, pembayaran seluler, dan sistem serupa lainnya. Kerangka tersebut menetapkan aturan dan persyaratan untuk penerbitan dan pengelolaan sistem pembayaran elektronik, serta perlindungan dana konsumen dan informasi pribadi.

Catatan: untuk aturan ini adalah Penyedia layanan pembayaran digital harus memperhatikan persyaratan mereka untuk penyimpanan data transaksi secara lokal.

UAE Group 42 (juga dikenal sebagai G42) adalah perusahaan kecerdasan buatan dan komputasi awan yang didirikan di Abu Dhabi, Uni Emirat Arab (UEA) pada tahun 2018. Organisasi ini berorientasi pada pengembangan industri AI di sektor pemerintahan, kesehatan, keuangan, minyak dan gas, penerbangan dan perhotelan. G42 mengembangkan dan menerapkan solusi industri berdampak tinggi di sektor-sektor seperti pemerintah, perawatan kesehatan, keuangan, olahraga, energi, dan kota pintar.

Seiring waktu, G42 telah menjadi pusat paling kritis untuk kerja sama transregional China-UEA. Dari G42 sebagai simpul pusat, diidentifikasi tiga sub-jaringan berbeda yang berkembang di area masalah berbeda. Yang pertama terletak di kecerdasan buatan dan infrastruktur pengawasan. Yang kedua dalam konteks pandemi global dan mencakup infrastruktur kesehatan pada umumnya dan pengembangan serta pemantauan vaksin pada khususnya. Selanjutnya, jaringan ketiga menghubungkan pelaku dari cabang pasar tradisional (misalnya bisnis minyak dan gas) dan keamanan siber (Gurol et al., 2022).

Selain melakukan penelitian dan memberikan solusi industri yang menangani peluang jangka pendek, Grup 42 juga bekerja menuju masa depan di mana AI akan dapat menangani tugas-tugas umum, seperti yang dilakukan manusia, di zaman Kecerdasan Umum Buatan. G42 memiliki jaringan kemitraan yang aktif dan luas, menghubungkan organisasi internasional terkemuka yang melengkapi ekosistemnya dan mendukung visinya. Kemitraan G42 berkisar dari perjanjian kerja sama strategis, usaha patungan, hingga investasi langsung oleh Grup.

### 4.5.4 South Korea

*Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc Act on The Establishment, Management, Etc. of Spatial Data Amended by Act* No. 13520, (Dec. 1, 2015). Pemerintah Korea berperan besar dalam NGIS, khususnya di bidang pengembangan database spasial dan standardisasi data spasial. Pengembangan teknologi dan pelatihan spesialis GIS juga dianggap sebagai salah satu jurusan pemerintah. Bbulan Mei 1995, pemerintah Korea telah mengimplementasikan "*A Master Plan of National Geographic Information System* (NGIS)" untuk mengembangkan infrastruktur informasi pengelolaan data geo-spasial. Sejak itu, pekerjaan kompilasi data GIS di berbagai sektor berhasil membuat kemajuan. Ada pengakuan luas akan perlunya sistem pendukung hukum untuk memastikan implementasi NGIS. Oleh karena itu peraturan perundang-undangan NGIS yang diundangkan pada Januari 2000 berlaku mulai Juli 2000.

Pasal 51:

(1) Pemerintah dapat meminta penyedia atau pengguna layanan informasi dan komunikasi untuk mengambil langkah-langkah yang diperlukan untuk mencegah keluarnya informasi penting tentang industri, ekonomi, ilmu pengetahuan, teknologi, dan lain-lain ke luar negeri melalui jaringan informasi dan komunikasi. (2) Cakupan informasi penting sebagaimana dimaksud pada ayat (1) adalah sebagai berikut: 1. Informasi yang berkaitan dengan keamanan nasional dan kebijakan utama; 2. Informasi tentang detail ilmu pengetahuan dan teknologi mutakhir atau peralatan yang dikembangkan di negara ini.

Catatan pada aturan ini adalah ::

a. Untuk pelanggan layanan komunikasi, mereka harus dibantu dalam melokalisasi penyimpanan informasi penting apa pun yang berkaitan dengan industri, ekonomi, sains dan teknologi, serta informasi yang berkaitan dengan keamanan nasional dan kebijakan utama, serta

informasi terperinci tentang sains mutakhir, teknologi atau peralatan yang dikembangkan di negara mereka sendiri.

b. Peta atau foto untuk keperluan survei yang diperoleh dari survei dasar/survei publik tidak boleh dibawa ke luar negeri tanpa izin dari Menteri Pertanahan, Infrastruktur dan Transportasi.

Konstitusi Korea memberikan perlindungan umum tentang privasi, khususnya perlindungan privasi di tempat tinggal dan privasi dalam berkomunikasi. Prinsip perlindungan data pribadi di Korea Selatan termuat dalam Pasal 3 *Personal Information Protection Act* (PIPA) tahun 2011. Pemroses data pribadi harus memenuhi beberapa prinsip, antara lain:

a. Memiliki tujuan yang jelas dan spesifik
b. Memproses data pribadi hanya untuk pencapaian tujuan pengumpulan data pribadi;
c. Memastikan data pribadi akurat dan lengkap serta mukhtakhir;
d. Memperhatikan keamanan data pribadi;
e. Mengumumkan kebijakan privasi dan menjamin hak akses;
f. Mengelola dengan cara yang tidak melanggar hak subjek data;
g. Berusaha mengelola data pribadi tanpa menyerahkan nama subjek data, apabila mungkin;
h. Berusaha meningkatkan kepercayaan subjek data dengan mentaati ketentuan hukum

Untuk jangka menengah hingga jangka panjang, tindakan sistematis untuk mencegah pelanggaran privasi diperlukan dengan memperkenalkan kebijakan sertifikat, seperti ISO27001 dan, KISA-ISMS (Masyarakat Keamanan Informasi Korea – Sistem Manajemen Keamanan Informasi). Hal ini juga diimbangi dengan kebutuhan akan peningkatan partisipasi dan upaya pemerintah dan badan usaha terkait. Meskipun sistem sertifikat keamanan, seperti ISO27001 dan KISA-ISMS. akan lebih efisien dan dapat menghasilkan efek sinergi jika organisasi yang menjalankan KISA-ISMS atau

ISO27001 juga mengelola sistem sertifikasi perlindungan privasi. Ini karena sistem sertifikasi perlindungan privasi dan KISA-ISMS atau ISO27001 berbeda dalam konten implementasinya saja, bukan dalam hal kerangka operasi yang sebenarnya (Lee et al., n.d.).

K-ISMS adalah sistem sertifikasi representatif yang mengevaluasi tingkat manajemen keamanan perusahaan di Korea dan memungkinkan untuk diterapkan sebagai proses standar untuk meningkatkan manajemen keamanan. Pemerintah Korea mengoperasikan sistem manajemen keamanan informasi sistem sertifikasi "K-ISMS" untuk menilai apakah suatu organisasi telah membentuk dan mengelola lingkungan keamanan informasi yang sesuai. Oleh karena itu, K-ISMS, yang mirip dengan "ISO27001" sebagai standar internasional untuk sistem manajemen keamanan informasi, dirancang untuk meningkatkan tingkat manajemen keamanan informasi level enterprise dan melindunginya dari berbagai ancaman keamanan.

Berdasarkan Pasal 47 dalam "Undang-Undang Promosi Pemanfaatan Jaringan Informasi dan Komunikasi dan Perlindungan Informasi", pemerintah Korea memperkenalkan Sistem Manajemen Keamanan Informasi Korea (K-ISMS). Kerangka kerja ISMS khusus bagi negara, dengan menetapkan serangkaian persyaratan kontrol ketat yang dirancang untuk membantu memastikan bahwa organisasi di Korea secara konsisten dan aman melindungi aset informasi mereka.

Untuk mendapatkan sertifikasi, perusahaan harus menjalani penilaian oleh auditor independen yang mencakup manajemen keamanan informasi dan penanggulangan keamanan. Ini mencakup 104 kriteria termasuk 12 item kontrol di 5 sektor untuk manajemen keamanan informasi, dan 92 item kontrol di 13 sektor untuk penanggulangan keamanan informasi. Beberapa kriteria tersebut meliputi pemeriksaan tanggung jawab manajemen keamanan organisasi, kebijakan keamanan, pelatihan keamanan, respons

insiden, manajemen risiko, dan banyak lagi. Sebuah komite khusus memeriksa hasil audit dan memberikan sertifikasi.

Kerangka kerja K-ISMS dibangun di atas keberhasilan strategi dan kebijakan keamanan informasi yang berhasil. Hal ini juga memperhitungkan penanggulangan keamanan dan prosedur respons ancaman untuk meminimalkan dampak pelanggaran keamanan. Prosedur ini memiliki tumpang tindih yang signifikan dengan tujuan pengendalian ISO/IEC 27001 tetapi tidak identik. K-ISMS memberikan penyelidikan yang lebih terperinci terhadap persyaratan daripada penilaian ISO/IEC 27001 yang umum.

Di bawah pengawasan Kementerian Sains dan Teknologi Informasi Korea (MSIT), *Korea Internet & Security Agency* (KISA) adalah otoritas sertifikasi K-ISMS. Sertifikasi berlaku selama tiga tahun, dan entitas bersertifikat harus lulus audit tahunan untuk mempertahankannya.

### 4.5.5 Singapura

*Singapore Cybersecurity Ordinance (Cybersecurity Act 2018) And Singapore Personal Data Protection Act (Personal Data Protection Act 2012).* Singapura adalah negara yang pertama kali mengembangkan rencana induknya tentang keamanan siber pada tahun 2005 dan pada tahun 2015 menciptakan Badan Keamanan Siber, dan pada tahun 2016 strategi keamanan siber dikembangkan (Singapore`s Cybersecurity Strategy, 2016).

Singapura menjadi negara pada posisi terdepan dalam keamanan siber. dengan Singapura menempati peringkat pertama di dunia sebagai negara yang memiliki komitmen yang baik pada keamanan siber pada tahun 2017 berdasarkan *Global Security Index* yang dirilis oleh International Telecommunications Union. Singapura merupakan pihak yang menjadi target ancaman dan serangan siber. Kemudian dinyatakan juga jaringan internet pemerintah Singapura secara rutin diserang. Teo Chee Hean

menyatakan dalam *Singapore International Cyber Week* 2017 bahwa Singapura merupakan negara yang paling terpapar serangan siber dibandingkan dengan negara lainnya (Anshori & Ramadhan, 2019).

Aturan siber di Singapura berfokus pada Infrastruktur Informasi Dasar Nasional (Infrastruktur Informasi Kritis), meliputi 11 industri: Penerbangan, Perbankan & Keuangan, Energi, Pemerintahan, Kesehatan, Infokom , Transportasi Darat, Maritim, Media, Keamanan & Layanan Darurat dan Air .

Dan aturan tersebut juga mengatur Data Pribadi dimana Organisasi tidak dapat mentransfer data pribadi misi ke luar negeri kecuali jika organisasi memberikan standar perlindungan yang sama seperti yang diberikan undang-undang.

Singapura memimpin dalam pengembangan *ASEAN Data Management Framework* (DMF) dan ASEAN *Model Contracts for Cross-border Data Flows* (MCCs) untuk mempromosikan pengembangan ekonomi digital.

PDPC Singapura 2021.01.22 menerbitkan "Panduan Penggunaan Klausul Kontrak Model ASEAN untuk Aliran Data Lintas Batas di Singapura", yang mencantumkan empat klarifikasi dan amandemen utama tentang bagaimana PKS ASEAN dapat diadaptasi ke PDPA Singapura.

*Multi Tier Cloud Security* (MTCS) disiapkan di bawah arahan *Information Technology Standards Committee* (ITSC) dari *Infocomm Media Development Authority* (IMDA). Ini adalah standar keamanan komputasi awan pertama dengan berbagai tingkat keamanan, sehingga CSP bersertifikat dapat menentukan tingkat yang mereka tawarkan.

Singapura memberikan insentif kepada CSP untuk mendaftar ke Multi-Tier Keamanan Komputasi awan *Multi Tier Cloud Security Standard for Singapore* (MTCS SS), yang ditetapkan pada tahun 2013. MTCS kemudian memungkinkan pengguna komputasi awan untuk mengakses pernyataan

diri yang diajukan oleh CSP dan menawarkan perbandingan yang jelas tentang kemampuan mereka untuk memungkinkan pengguna komputasi awan memilih penyedia layanan terbaik. Pendekatan ini memungkinkan adopsi komputasi awan karena membangun kepercayaan publik pada sertifikasi CSP MTCS (Raghavan et al., 2021).

MTCS dibuat berdasarkan standar internasional yang diakui, seperti ISO/IEC 27001, dan mencakup area seperti penyimpanan data, kedaulatan data, portabilitas data, pertanggungjawaban, ketersediaan, kelangsungan bisnis, pemulihan bencana, dan manajemen insiden. MTCS bertujuan untuk menyediakan:

a. Standar umum yang dapat diterapkan CSP untuk mengatasi kekhawatiran pelanggan tentang keamanan dan kerahasiaan data di komputasi awan, dan dampak penggunaan layanan komputasi awan pada bisnis;
b. Transparansi operasional yang dapat diverifikasi dan wawasan tentang risiko bagi pelanggan saat menggunakan layanan komputasi awan.

MTCS mencakup 19 domain dari enam kategori: tata kelola komputasi awan, keamanan infrastruktur komputasi awan, manajemen operasi komputasi awan, manajemen layanan komputasi awan, hak akses pengguna komputasi awan, dan isolasi penyewa. MTCS memiliki tiga level (level-1 hingga level-3) untuk mengautentikasi penyedia layanan komputasi awan berdasarkan level persyaratan yang berbeda. Level-3 adalah yang paling menuntut dan paling aman. Penyedia layanan komputasi awan harus memiliki rencana keamanan yang ketat dan menjalani audit tahunan oleh badan sertifikasi MTCS sebelum mereka dapat lulus sertifikasi level-3 MTCS.

Banyak kontrol keamanan MTCS diinterpretasikan di bawah lingkungan komputasi awan sementara kontrol khusus terkait komputasi awan baru ditambahkan seperlunya. Rancangan MTCS disusun menurut jenis penggunaan, sensitivitas data, dan jenis aplikasi yang di-*hosting*. Tingkat

dasar, Level 1, memiliki kontrol minimal, yang dirancang untuk menampung aplikasi bisnis yang tidak penting dan data publik yang tidak sensitif. Level 2 difokuskan pada perlindungan data, dan melayani aplikasi bisnis yang lebih kritis dan data sensitif, yang mencakup spektrum penggunaan yang luas. Tingkat teratas, Level 3, paling ketat, berorientasi pada penggunaan oleh industri yang diatur, mengambil persyaratan keamanan umum di seluruh industri tersebut untuk aplikasi kritis dengan informasi yang sangat rahasia (Lee et al., n.d.).

Beberapa perbedaan mendasar antara ISO27018 dan MTCS. Yang pertama berfokus pada kode praktik CSP untuk perlindungan IIP di komputasi awan publik yang bertindak sebagai pemroses IIP, sedangkan yang terakhir mendefinisikan Sistem Manajemen Keamanan Informasi untuk CSP yang mencakup serangkaian persyaratan keamanan, perlindungan data (atau perlindungan informasi, pribadi atau lainnya) hanyalah salah satu dari banyak persyaratan kontrol. Meskipun ISO27018 tumpang tindih dengan MTCS terutama di bidang perlindungan data dalam hal menjaga kerahasiaan, mengontrol akses dan penggunaan data (dalam hal ini datanya adalah IIP), CSP harus menyediakan sarana bagi pelanggan mereka, pengguna komputasi awan, untuk memungkinkan mereka memenuhi kewajibannya untuk memfasilitasi pelaksanaan hak prinsipal IIP (subjek data) sebagai bagian dari persyaratan privasi. Selain itu, MTCS adalah standar yang dapat disertifikasi sedangkan ISO27018 adalah tambahan untuk ISO27002, untuk digunakan sebagai dokumen panduan saat mensertifikasi CSP berdasarkan standar dasar ISO27001 dengan pertimbangan perlindungan IIP di komputasi awan publik yang bertindak sebagai prosesor IIP (Giulio et al., 2017).

Ini juga mencakup mekanisme bagi pelanggan untuk membandingkan dan memberi peringkat kemampuan CSP terhadap serangkaian persyaratan keamanan dasar minimum.

### 4.5.6 Filipina

Dalam hal status keamanan siber, Filipina menduduki peringkat ke-23 sebagai negara yang paling terpengaruh di dunia jauh di bawah Vietnam, India, dan Amerika Serikat (Kaspersky, 2018). Selain itu, berada di peringkat ke-39 dari 193 negara dalam *hal Global Cybersecurity Index* atau GCI di tahun 2018. Hal ini dikaitkan dengan skor hukum yang tinggi untuk penegakan Undang-Undang Privasi Data (RA No.10173), Undang-Undang Anti Penyadapan (RA No. 4200), Undang-Undang *e-Commerce* (RA No. 8792) dan Undang-Undang Kejahatan Dunia Maya yang baru ( RA No.10175). Dibandingkan dengan tetangga ASEAN-nya, Filipina belum memberlakukan dan menerapkan hukum *anti-cybercrime* yang komprehensif.

Pada Juni 2020, *The Departement of Information and Communication Technology* (DICT) mengeluarkan dokumen No. 2020 - 010 yang mengubah kebijakan prioritas komputasi awan tersebut di atas, termasuk ruang lingkup kebijakan prioritas komputasi awan, klasifikasi data pemerintah, persyaratan keamanan data pemerintah, serta kedaulatan dan kepemilikan data pemerintah, untuk memperkuat Kontrol pemerintah Filipina atas data pemerintah.

### 4.5.7 Bangladesh

*Bangladesh Data Protection Act 2022.* Dari sedikit negara di Asia yang tidak memiliki undang-undang privasi data atau RUU Pemerintah (Korea Utara, Kamboja, Laos, Myanmar, Maladewa, dan Afghanistan), Bangladesh adalah yang paling mungkin memberlakukan undang-undang semacam itu. Bangladesh sudah memiliki undang-undang hak atas informasi, yang diatur oleh Komisi Informasi. Tidak ada aturan eksplisit yang mengatur ekspor data pribadi ke luar Bangladesh, tetapi Kantor Perlindungan Data (DPO) memiliki wewenang 'untuk memerintahkan penangguhan aliran data ke penerima di negara asing. Kewajiban pengontrol dan pemroses meliputi (pasal 5): tidak

ada pemrosesan tanpa persetujuan yang diperoleh sebelum pemrosesan; persetujuan harus 'bebas, spesifik, jelas dan dapat ditarik kembali; koleksi minimal: 'tidak berlebihan atau tidak perlu'; semua data akan dimusnahkan secara permanen ketika tidak lagi diperlukan untuk tujuan pengumpulannya; banyak kewajiban lain terkait kualitas data; tidak menggunakan data kecuali untuk tujuan pengumpulan; kewajiban untuk mengamati perlindungan keamanan data (Greenleaf, 2023).

Data sensitif, data yang dibuat atau dihasilkan pengguna, dan data rahasia harus disimpan di Bangladesh, dan akan tetap berada di luar yurisdiksi pengadilan dan penegak hukum mana pun selain Bangladesh.

### 4.5.8 Cina

**a. China GB/T 22239-2019.**

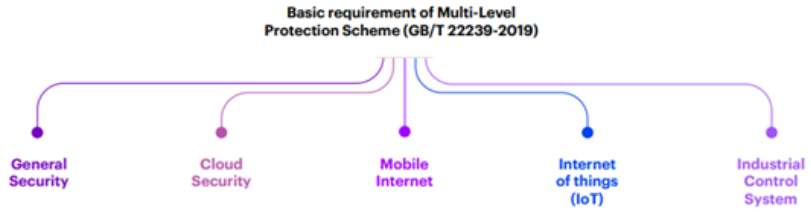
China dan Rusia mendorong "kedaulatan nasional" yang lebih kuat di dunia maya. ,Hal itu yang berarti hak untuk memastikan kontrol atas konten informasi yang dapat diakses oleh warganya dan perlindungan bidang politik nasional dari campur tangan luar melalui apa yang dilihat pemerintah mereka sebagai informasi yang mengganggu. AS dan sebagian besar negara Barat menggunakan istilah "keamanan siber" untuk membahas perlindungan jaringan dan individu dari intrusi dunia maya (Hitchens & Goren, 2017). China telah menjadi salah satu negara perdagangan terbesar di dunia (setelah AS dan Jerman), dan perdagangannya tumbuh jauh lebih cepat daripada negara ekonomi besar lainnya. Karena GDPR baru mulai berlaku pada tanggal 25 Mei 2018, tidak mungkin bagi CSP dari Cina untuk mengabaikan dampak GDPR pada aktivitas pemrosesan mereka sehubungan dengan pelanggan komputasi awan UE mereka.

Persyaratan untuk memproses data pribadi di negara ketiga memerlukan peraturan perlindungan data yang sebanding dengan standar UE. Kerangka hukum mengenai perlindungan data di Tiongkok harus memuat konten yang

sebanding dan prinsip-prinsip perlindungan data prosedural/penegakan yang telah ditetapkan oleh WP293.

**b. China GB/T 22239-2019**

Perlindungan data yang tepat tidak ada di China karena jejak perlindungan data ditemukan di banyak instrumen hukum khusus sektor dan tidak ada undang-undang perlindungan data umum. Prinsip perlindungan data umum dan mekanisme penegakan hukum yang efisien harus ada. Karena perlindungan data China sebelum Undang-Undang Keamanan Siber China tidak memiliki dua kondisi yang disebutkan di atas, diperlukan kebijakan ringkas dengan fokus pada prinsip perlindungan data, hak individu, transfer data, dan mekanisme penegakan hukum. Untuk mengetahui apakah persyaratan tersebut termasuk dalam Undang-Undang Keamanan Siber China, diperlukan suatu penilaian.




*Gambar 0-11 Skema GB/T 22239-2019*

Pada Mei 2019, China mengeluarkan serangkaian standar untuk perlindungan rahasia 2.0. Perbedaan utama antara seri baru dan seri sebelumnya meliputi:

(a) Standar baru memperluas cakupan yang menggabungkan komputasi awan, internet seluler, Internet of Things, ICS, dll. ke dalam cakupan standar.

(b) Direkomendasikan untuk menggunakan arsitektur triple protection yang didukung oleh jaringan komunikasi yang aman, batas yang aman dan lingkungan komputasi yang aman bersama dengan pusat manajemen.

(c) Persyaratan teknologi TC (Trusted Computing) diperkuat25.

Pasal CSL 21(UU Keamanan Siber (Berlaku mulai Juni 2017)) yakn berisi: Negara telah menerapkan *Multi Level Protection Scheme* (MLPS) keamanan siber. Operator jaringan harus melakukan tugas perlindungan keamanan berikut sesuai dengan persyaratan MLPS keamanan siber untuk memastikan jaringan bebas dari gangguan, kerusakan, atau akses tidak sah, dan untuk mencegah kebocoran, pencurian, atau pemalsuan data jaringan.

GB/T 22239-2019 Teknologi keamanan informasi *Baseline* untuk perlindungan rahasia keamanan siber. GB/T 22239-2019 menentukan persyaratan keamanan umum dan persyaratan ekstensi keamanan untuk proyek di bawah perlindungan rahasia dari level 1 hingga level 4 dari perlindungan rahasia keamanan siber.

Operator Jaringan berkewajiban untuk mematuhi persyaratan keamanan umum yang harus dipenuhi terlepas dari bentuk tingkat perlindungan. Persyaratan khusus lainnya untuk Komputasi awan, Internet Seluler, IoT, dan Sistem Kontrol Industri , yang disebut persyaratan perluasan keamanan. Karakteristik utama dari undang-undang ini adalah tidak memiliki efek ekstra-teritorial.

**c. China GB/T 31168-2014**

Teknologi keamanan informasi—Persyaratan kemampuan keamanan layanan komputasi awan （GB/T 31168-2014 adalah standar keamanan layanan komputasi awan yang dikeluarkan oleh Komite Teknis Standardisasi Keamanan Informasi China (SAC/TC260). Ini berorientasi pada penyedia layanan komputasi awan dan menetapkan persyaratan kemampuan keamanan yang harus dimiliki oleh penyedia layanan komputasi awan saat memberikan layanan ke departemen pemerintah. Standar ini berlaku untuk penyedia layanan komputasi awan yang menyediakan layanan komputasi awan untuk pemerintah. Berdasarkan sensitivitas dan pentingnya informasi pada platform komputasi awan, standar diklasifikasikan menjadi persyaratan

umum dan persyaratan yang ditingkatkan. Kemampuan yang dibutuhkan juga berbeda.

Standar ini berfokus pada ketersediaan dan keamanan layanan, membedakan tanggung jawab berdasarkan jenis layanan, dan mengusulkan 10 jenis persyaratan keamanan: Pengembangan sistem dan keamanan rantai pasokan, perlindungan sistem dan komunikasi, kontrol akses, manajemen konfigurasi, pemeliharaan, tanggap darurat, dan pemulihan bencana. audit, penilaian risiko dan pemantauan berkelanjutan, organisasi dan personel keamanan, serta perlindungan fisik dan lingkungan.

## 4.6 Standar Internasional Tata Kelola Keamanan Siber pada Komputasi Awan

### 4.6.1 ISO/IEC 27017:2015

ISO/IEC 27017:2015 (ISO/IEC, 2015) adalah aturan praktis untuk kontrol keamanan informasi layanan komputasi awan yang ditetapkan oleh *International Organization for Standardization* (ISO). Standar ini diturunkan dari ISO 27001 (Sistem Manajemen Keamanan Informasi) dan ISO 27002 (keamanan informasi, keamanan jaringan, dan perlindungan privasi). Standar ini merupakan kode praktik untuk kontrol keamanan informasi berdasarkan ISO/IEC 27002 untuk layanan komputasi awan. ISO 27001 merupakan standar keamanan informasi global sedangkan ISO 27002 memberikan panduan praktik terbaik yang berlaku untuk kontrol yang tercantum dalam lampiran A ISO 27001 untuk memandu standar keamanan informasi organisasi. ISO 27017 melengkapi kerangka kerja ISO/IEC 27002 untuk lingkungan komputasi awan dengan memberikan informasi tambahan, perlindungan keamanan, dan panduan implementasi. Kerangka kerja ini memberikan panduan implementasi untuk 37 kontrol dan 7 persyaratan tambahan yang terdapat dalam ISO/IEC 27001. Gol dari

ISO/IEC 27017:2015 adalah untuk membantu organisasi mengatasi tantangan keamanan yang terkait dengan adopsi layanan komputasi awan.

Aspek utama ISO/IEC 27017:2015 meliputi:

a. Cakupan: Standar ini berlaku untuk CSP dan CSC. Ini mencakup berbagai jenis layanan komputasi awan, seperti IaaS, PaaS, dan SaaS.
b. Hubungan dengan ISO/IEC 27002: ISO/IEC 27017:2015 dibangun berdasarkan kontrol keamanan informasi yang diuraikan dalam ISO/IEC 27002, mengadaptasi dan memperluasnya untuk mengatasi risiko dan tantangan khusus komputasi awan. Standar tersebut tidak menggantikan ISO/IEC 27002, melainkan melengkapinya untuk memberikan panduan yang lebih khusus untuk layanan komputasi awan.
c. Kontrol khusus komputasi awan: ISO/IEC 27017:2015 memperkenalkan kontrol khusus komputasi awan tambahan, dengan fokus pada area seperti pemisahan data, virtualisasi, dan tanggung jawab bersama antara CSP dan CSC. Kontrol ini dimaksudkan untuk mengatasi masalah keamanan unik yang muncul dari penggunaan infrastruktur virtual bersama dan lingkungan multi-penyewa.
d. Panduan implementasi: Standar ini memberikan panduan praktis tentang cara menerapkan kontrol yang direkomendasikan, dengan mempertimbangkan konteks spesifik setiap organisasi dan layanan komputasi awan yang mereka gunakan. Panduan ini dimaksudkan agar fleksibel dan dapat disesuaikan, memungkinkan organisasi untuk menyesuaikan tindakan keamanan mereka sesuai dengan kebutuhan khusus dan profil risiko mereka.
e. Model tanggung jawab bersama: ISO/IEC 27017:2015 menekankan model tanggung jawab bersama dalam komputasi awan. Model ini mengakui bahwa CSP dan CSC memiliki peran untuk memastikan keamanan layanan komputasi awan. Standar tersebut menjelaskan tanggung jawab masing-masing pihak dan membantu organisasi

memahami pembagian tugas keamanan di antara mereka.

Dengan mematuhi ISO/IEC 27017:2015, organisasi dapat meningkatkan keamanan informasi mereka dan mengurangi risiko yang terkait dengan komputasi awan. Standar ini juga membantu meningkatkan kepercayaan antara penyedia layanan komputasi awan dan pelanggan, memfasilitasi ekosistem komputasi awan yang lebih aman.

### 4.6.2 ISO/IEC 19790:2012

ISO/IEC 19790:2012 (ISO/IEC, 2012) persyaratan keamanan untuk modul kriptografi yang digunakan dalam sistem keamanan yang melindungi informasi sensitif dalam sistem komputer dan telekomunikasi. Standar Internasional ini mendefinisikan empat tingkat keamanan untuk modul kriptografi untuk menyediakan spektrum sensitivitas data yang luas (misalnya data administrasi bernilai rendah, transfer dana jutaan dolar, data perlindungan jiwa, informasi identitas pribadi, dan informasi sensitif yang digunakan oleh pemerintah) dan keragaman lingkungan aplikasi (misalnya fasilitas yang dijaga, kantor, media yang dapat dipindahkan, dan lokasi yang sama sekali tidak terlindungi). Standar Internasional ini menetapkan empat tingkat keamanan untuk masing-masing dari 11 area persyaratan dengan setiap tingkat keamanan meningkatkan keamanan di atas tingkat sebelumnya.

ISO/IEC 19790:2012 menetapkan persyaratan keamanan yang secara khusus dimaksudkan untuk menjaga keamanan yang diberikan oleh modul kriptografi. Kepatuhan terhadap standar ini tidak cukup untuk memastikan bahwa modul tertentu aman atau bahwa keamanan yang diberikan oleh modul cukup dan dapat diterima oleh pemilik informasi yang dilindungi.

Tujuan utama dari ISO/IEC 19790:2012 adalah untuk menyediakan serangkaian kriteria keamanan yang dapat digunakan untuk mengevaluasi desain dan implementasi modul kriptografi, membantu memastikan bahwa mereka memenuhi tingkat jaminan keamanan tertentu. Standar ini berlaku

untuk berbagai industri dan sektor, termasuk keuangan, kesehatan, pemerintah, dan telekomunikasi.

Aspek utama ISO/IEC 19790:2012 meliputi:

a. Persyaratan keamanan: Standar ini menguraikan serangkaian persyaratan keamanan yang harus dipenuhi oleh modul kriptografi untuk memastikan ketahanan dan keandalannya. Persyaratan ini dibagi menjadi empat kategori utama: spesifikasi modul kriptografi, antarmuka modul kriptografi, peran dan layanan, dan model keadaan terbatas.

b. Tingkat keamanan: ISO/IEC 19790:2012 mendefinisikan empat tingkat keamanan (Level 1 hingga Level 4), dengan setiap level mewakili peningkatan tingkat jaminan keamanan. Tingkatan ini memungkinkan organisasi untuk memilih tingkat keamanan yang sesuai untuk kebutuhan khusus dan profil risiko mereka. Tingkat yang lebih tinggi biasanya memberikan perlindungan yang lebih kuat terhadap berbagai ancaman, seperti perusakan fisik, serangan saluran samping, dan akses tidak sah ke kunci kriptografi.

c. Proses evaluasi: Standar memberikan pedoman untuk proses evaluasi yang dapat digunakan untuk menilai modul kriptografi terhadap persyaratan keamanan yang ditentukan. Proses ini melibatkan tinjauan menyeluruh terhadap desain, dokumentasi, dan implementasi modul, serta pengujian untuk memastikan kepatuhannya dengan tingkat keamanan yang ditentukan.

d. Evaluasi independen: Untuk memastikan kredibilitas proses evaluasi, ISO/IEC 19790:2012 merekomendasikan agar evaluasi dilakukan oleh laboratorium independen yang terakreditasi. Ini membantu membangun kepercayaan pada hasil evaluasi dan memberikan keyakinan bahwa modul kriptografi memenuhi standar keamanan yang diperlukan.

Dengan mematuhi ISO/IEC 19790:2012, organisasi dapat memastikan bahwa modul kriptografi mereka menyediakan tingkat keamanan yang tinggi, melindungi data sensitif dan komunikasi dari potensi ancaman. Kepatuhan terhadap standar ini juga dapat membantu organisasi menunjukkan komitmen mereka terhadap keamanan informasi dan membangun kepercayaan dengan pelanggan, mitra, dan regulator.

### 4.6.3 ISO/IEC 27034:2011

ISO/IEC 27034:2011 (ISO/IEC, 2011a) memberikan panduan untuk membantu organisasi dalam mengintegrasikan keamanan ke dalam proses yang digunakan untuk mengelola aplikasi. ISO/IEC 27034 berlaku bagi mereka yang merancang dan memprogram, menerapkan dan menggunakan sistem, dengan kata lain manajer bisnis dan TI, pengembang dan auditor, dan pada akhirnya pengguna akhir. Standar ini membantu organisasi menggabungkan praktik terbaik keamanan di seluruh siklus hidup aplikasi perangkat lunak mereka, mulai dari desain dan pengembangan hingga penerapan dan pemeliharaan.

Tujuan utama ISO/IEC 27034:2011 adalah untuk menetapkan pendekatan sistematis untuk mengelola risiko keamanan aplikasi, memastikan bahwa aplikasi dirancang, dikembangkan, dan dipelihara dengan cara yang aman. Standar ini berlaku untuk organisasi dari semua ukuran dan di berbagai industri yang mengembangkan, memperoleh, atau memelihara aplikasi perangkat lunak.

Aspek utama ISO/IEC 27034:2011 meliputi:

a. *Application Security Control* (ASC): Standar ini memperkenalkan konsep Kontrol Keamanan Aplikasi, yang merupakan tindakan keamanan khusus yang dapat diterapkan dalam aplikasi untuk mengatasi risiko yang teridentifikasi. ASC dapat mencakup berbagai mekanisme keamanan seperti validasi input, enkripsi, kontrol akses, dan *logging*.

b. Siklus hidup keamanan aplikasi: ISO/IEC 27034:2011 menguraikan siklus hidup keamanan aplikasi, yang merupakan pendekatan terstruktur untuk mengelola keamanan aplikasi di seluruh proses pengembangan. Siklus hidup ini terdiri dari beberapa fase, termasuk analisis kebutuhan, desain, implementasi, pengujian, penerapan, dan pemeliharaan. Standar ini memberikan panduan menggabungkan praktik terbaik keamanan ke dalam setiap fase siklus hidup.

c. Penilaian risiko: Standar ini menekankan pentingnya melakukan penilaian risiko untuk setiap aplikasi guna mengidentifikasi potensi ancaman dan kerentanan keamanan. Proses penilaian risiko ini membantu organisasi memprioritaskan upaya mereka dan berfokus pada penerapan kontrol keamanan yang paling penting untuk memitigasi risiko yang teridentifikasi.

d. Integrasi dengan sistem manajemen yang ada: ISO/IEC 27034:2011 dirancang agar kompatibel dengan standar keamanan informasi ISO/IEC lainnya, seperti ISO/IEC 27001 (Sistem Manajemen Keamanan Informasi). Hal ini memungkinkan organisasi untuk mengintegrasikan upaya keamanan aplikasi mereka dengan keseluruhan proses manajemen keamanan informasi mereka, memastikan pendekatan komprehensif untuk mengelola risiko keamanan.

e. Peningkatan berkelanjutan: Standar ini mendorong organisasi untuk terus memantau, meninjau, dan meningkatkan praktik keamanan aplikasi mereka. Hal ini melibatkan evaluasi secara berkala atas efektivitas kontrol keamanan yang diterapkan, mengidentifikasi ancaman dan kerentanan baru, dan membuat penyesuaian yang diperlukan untuk mempertahankan tingkat keamanan yang tinggi.

Dengan mematuhi ISO/IEC 27034:2011, organisasi dapat memastikan bahwa aplikasi perangkat lunak mereka dikembangkan dan dipelihara dengan aman

sebagai prioritas utama. Hal ini akan membantu melindungi data sensitif, menjaga integritas sistem, dan mengurangi kemungkinan pelanggaran keamanan, yang pada akhirnya berkontribusi pada postur keamanan informasi yang lebih kuat secara keseluruhan.

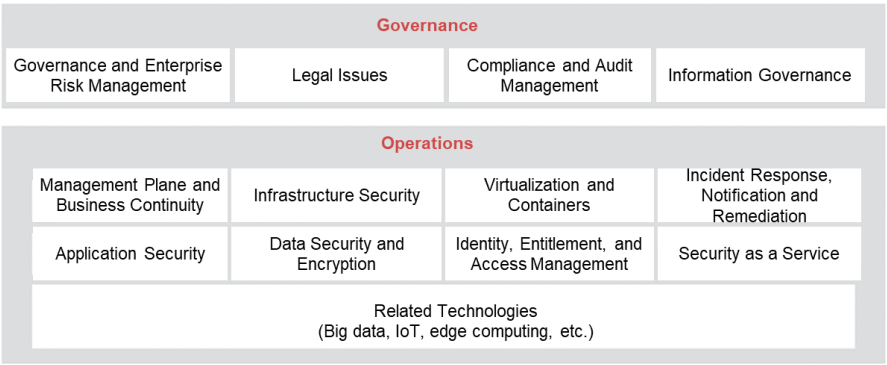
### 4.6.4 CSA STAR

CSA (*Cloud Security Alliance*) STAR (Cloud security Alliance, 2023) mencakup, penilaian mandiri, sertifikasi pihak ketiga, dan audit berkelanjutan. CSA STAR secara khusus diarahkan untuk mendukung dan mengevaluasi penyedia layanan komputasi awan (CSP). Program CSA STAR didasarkan pada pedoman berikut:

a. **CSA** Komputasi awan ***Controls Matrix*** **(CCM)**, sebuah "meta-framework" kontrol keamanan khusus komputasi awan yang dipetakan ke ISO 27001, PCI/DSS, HIPAA, COBIT, dan standar lainnya. Hal ini dimaksudkan untuk memberikan standar *de-facto* untuk jaminan dan kepatuhan keamanan komputasi awan, yang dapat memandu CSP dalam mengoptimalkan postur keamanannya, serta membantu konsumen menilai postur keamanan CSP. CSA mengembangkan S*ecurity Guidance for Critical Areas of Focus in cloud computing* v4.0 pada tahun 2017 (lihat Gambar 0-12), yang memperluas ISMS ISO/IEC 27001 dan membagi kerangka kerja keamanan komputasi awan menjadi tata kelola dan operasi berdasarkan CCM.

b. **Kuesioner Inisiatif Penilaian Konsensus** (*The Consensus Assessments Initiative Questionnaire)*, serangkaian pertanyaan ya/tidak yang dapat diajukan oleh calon pelanggan atau auditor kepada penyedia komputasi awan untuk mengukur keselarasan mereka dengan CCM.

c. **Kode Etik CSA untuk Kepatuhan GDPR**, alat untuk membantu CSP mematuhi GDPR. (lihat pada pembahasan sub bab 7.2.6)




*Gambar 0-12 Arsitektur keamanan komputasi awan di CSA Security Guidance (Cloud Security Alliance, 2020)*

### 4.6.5 CIS *Critical Security Controls*

*Center for Internet Security* (CIS) *Critical Security Controls* (CIS *Controls*) adalah (*Center for Internet Security,* 2021) rangkaian perlindungan yang diprioritaskan untuk memitigasi serangan dunia maya yang paling lazim terhadap sistem dan jaringan. Dipetakan dan dirujuk oleh berbagai kerangka kerja hukum, peraturan, dan kebijakan. Kontrol CIS versi 8 telah ditingkatkan untuk mengikuti sistem dan perangkat lunak modern. Perpindahan ke komputasi berbasis komputasi awan, virtualisasi, mobilitas, *outsourcing, Work-from-Home*, dan perubahan taktik penyerang mendorong pembaruan dan mendukung keamanan perusahaan saat mereka beralih ke lingkungan komputasi awan dan hibrid sepenuhnya.

CIS Controls adalah serangkaian tindakan yang direkomendasikan untuk pertahanan dunia maya yang menyediakan cara spesifik dan dapat ditindaklanjuti untuk menggagalkan serangan yang paling meluas. Kontrol CIS adalah daftar tindakan defensif berprioritas tinggi dan sangat efektif yang

memberikan titik awal "harus dilakukan, dilakukan pertama" untuk setiap perusahaan yang ingin meningkatkan pertahanan dunia maya mereka.
Kontrol CIS dikembangkan mulai tahun 2008 oleh konsorsium akar rumput internasional yang menyatukan perusahaan, lembaga pemerintah, institusi, dan individu dari setiap bagian ekosistem (analis dunia maya, pencari kerentanan, penyedia solusi, pengguna, konsultan, pembuat kebijakan, pembuat, eksekutif, akademisi, auditor, dll.) yang bersatu untuk membuat, mengadopsi, dan mendukung Kontrol CIS. Sukarelawan ahli yang mengembangkan kontrol menerapkan pengalaman langsung mereka untuk mengembangkan tindakan paling efektif untuk pertahanan dunia maya.

### 4.6.6 NIST CSF

*National Institute of Standards and Technology* (NIST) *Cybersecurity Framework* (CSF) diterbitkan pada Februari 2014 sebagai panduan bagi organisasi infrastruktur penting untuk lebih memahami, mengelola, dan mengurangi risiko keamanan siber mereka (NIST Cybersecurity Framework Team, 2018). CSF dikembangkan sebagai tanggapan atas Perintah Eksekutif Presiden untuk Meningkatkan Keamanan Infrastruktur Kritis, yang dikeluarkan pada Februari 2013. NIST merilis CSF Versi 1.1 pada April 2018, menggabungkan umpan balik yang diterima sejak rilis CSF asli. Adapun draf versi kedua telah dirilis pada April 2023.
*National Institute of Standards and Technology* (NIST) *Cybersecurity Framework* (CSF) adalah sistem yang diakui secara internasional untuk menilai keamanan informasi. Ini memberikan panduan bagi organisasi yang ingin meningkatkan keamanan siber. CSF NIST terdiri dari standar, pedoman, dan praktik terbaik untuk mengelola keamanan siber. Mereka mengedepankan model *Identify, Protect, Detect, Respond*, dan *Recover* (IPDRR), yang membantu organisasi meminimalkan risiko sebelum, selama, dan setelah insiden keamanan.


*Gambar 0-13 Cybersecurity Framework NIST 1.1 (NIST, 2020)*

a. Fungsi Identifikasi (*Identify*) membantu organisasi memahami cara mengelola risiko keamanan siber terhadap sistem, orang, aset, data.
b. Fungsi Lindungi (*Protect*) menguraikan perlindungan yang sesuai untuk memastikan layanan infrastruktur penting.
c. Fungsi Deteksi (*Detect*) menentukan aktivitas yang sesuai untuk mengidentifikasi terjadinya peristiwa keamanan siber.
d. Fungsi Respons (*Respond*) mencakup aktivitas yang sesuai untuk mengambil tindakan terkait insiden keamanan siber yang terdeteksi.
e. Fungsi Pemulihan (*Recover*) mengidentifikasi aktivitas yang sesuai untuk memulihkan setiap layanan yang terganggu karena insiden keamanan siber.

## 4.7 Persyaratan Keamanan Komputasi Awan pada Berbagai Industri

Pasar layanan komputasi awan global terus berkembang, perusahaan di berbagai industri merasa perlu untuk bermigrasi ke komputasi awan.

Sementara itu, perusahaan pada umumnya mengkhawatirkan keamanan komputasi awan. Menurut laporan dari (ISC, 2022), keamanan data, ketersediaan layanan, serta pemantauan dan respons adalah kebutuhan utama keamanan berbagai industri. Bagaimana pun detail dari masing-masing bidang industri dapat bervariasi. Berikut merupakan analisis persyaratan keamanan komputasi awan di empat industri utama (keuangan, perawatan kesehatan, pemerintah, otomotif).

### 4.7.1 Persyaratan Keamanan Komputasi Awan Sektor Keuangan

Dengan pesatnya perkembangan komputasi awan, lembaga keuangan telah menjadi target utama peretas baik perorangan atau organisasi baik di dalam dan luar negeri untuk melakukan serangan dunia maya, penipuan telekomunikasi, dan penetrasi rahasia. Komputasi awan untuk industri keuangan memiliki persyaratan yang tinggi pada keamanan data dan perlindungan privasi. Persyaratan keamanan industri keuangan dapat diringkas sebagai berikut (Vijaya et al., 2019):

a. Perlindungan data pelanggan: Industri keuangan memiliki persyaratan tinggi pada keamanan data pelanggan karena kekhususannya yang mengolah banyak bentuk data kredensial.
b. Manajemen O&M (*Operasional & Maintenance*) yang dioptimalkan: Industri keuangan memproses sejumlah besar data perilaku pelanggan setiap harinya. O&M tradisional membutuhkan banyak waktu dan tenaga. Oleh karena itu, teknologi informasi perlu dioptimalkan dalam mempercepat manajemen O&M.
c. Non-repudiation: Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Setiap transaksi perlu memiliki bukti log catatan yang nir-penyangkalan.

d. Pemulihan bencana secara cepat: Pelanggan di industri keuangan berada di berbagai tempat. Bencana dapat datang tiba-tiba dan memiliki dampak signifikan jika tidak ditanggapi segera. Mereka perlu menyiapkan ruang dengan peralatan pemulihan bencana di beberapa area untuk memenuhi persyaratan pemulihan bencana secara cepat.

e. Pemantauan jaringan *real-time*: Industri keuangan memerlukan pemantauan 24/7 untuk memantau sistem secara *real-time* dan menanggapi insiden secara tepat waktu.

f. Pusat data khusus: Industri keuangan perlu menyediakan pusat data khusus untuk pelanggan (pemerintah atau pelanggan VIP).

g. Memenuhi regulasi eksternal: Memenuhi persyaratan undang-undang, peraturan, dan badan pengatur di industri keuangan dan meningkatkan kepercayaan nasabah terhadap lembaga keuangan.

h. Cakupan penuh skenario persyaratan: Lembaga keuangan melibatkan beberapa skenario bisnis (AR, inventaris, dan pembayaran daring). Persyaratan keamanan harus dipenuhi dalam beberapa skenario.

i. Standar kepatuhan: PCI-DSS: *Payment Card Industry Data Security Standard* (PCI DSS) adalah standar keamanan informasi kepemilikan yang dikelola oleh PCI *Security Standards Council*, yang dibentuk oleh berbagai perusahaan keuangan internasional. PCI DSS berlaku pada entitas yang menyimpan, memproses, atau mengirimkan data pemegang kartu (CHD) atau data otentikasi sensitif (SAD), termasuk *merchant*, pengolah, pengakuisisi, penerbit, dan penyedia layanan. PCI DSS dimandatkan oleh merek kartu dan dikelola oleh PCI *Security Standards Council*.

### 4.7.2 Persyaratan Keamanan Komputasi Awan Sektor Kesehatan

Karena kekhasan industri kesehatan, jenis perangkat lunak yang perlu dijalankan di komputasi awan relatif sederhana, tetapi volume data serta kemampuan analisis dan komputasinya tinggi. Sebagai bagian penting dari komputasi awan untuk layanan kesehatan, faktor keamanan telah menarik banyak perhatian, terutama untuk keamanan data dan perlindungan privasi yang semakin ketat. Persyaratan keamanan industri kesehatan dapat diringkas sebagai berikut (Al-Issa et al., 2019; Butpheng et al., 2020):

a. Lindungi keamanan dan privasi data: Industri layanan kesehatan perlu memperkuat manajemen keamanan data di semua tingkatan, mencegah risiko keamanan dan memenuhi kepatuhan peraturan, serta meningkatkan standar.
b. Meningkatkan efisiensi pengelolaan data: Karena banyaknya *file* kecil data medis, sejumlah besar data dihasilkan di rumah sakit, dan sejumlah besar waktu dihabiskan untuk melakukan pencarian, dan persiapan data. Oleh karena itu, persyaratan untuk meningkatkan efisiensi pengelolaan data perlu ditingkatkan.
c. Kebijakan pemulihan bencana yang dioptimalkan: Solusi pencadangan dari banyak institusi medis perlu memenuhi persyaratan perlindungan data yang masif. Hal ini ditujukan untuk mencegah kecepatan pencadangan dan pemulihan yang lambat, dan efek pemulihan bencana tidak dapat diverifikasi sebelumnya. Oleh karena itu, ada lebih banyak persyaratan untuk mengoptimalkan pencadangan pemulihan bencana dan meningkatkan kemampuan pemulihan.
d. Sistem manajemen keamanan terintegrasi: Industri layanan kesehatan berharap dapat meningkatkan keamanan jaringan dan

sistem manajemen keamanan data melalui migrasi komputasi awan sehingga mereka dapat fokus memberikan layanan kesehatan pada masyarakat.

e. Standar kepatuhan HIPAA: HIPAA merupakan kerangka hukum untuk mengamankan sistem kesehatan. HIPAA mewajibkan penyelenggara layanan kesehatan untuk menetapkan aturan, pedoman, dan tindakan untuk melindungi privasi dan keamanan data kesehatan. Tujuan utama dari aturan keamanan HIPAA adalah untuk melindungi data kesehatan individu secara seimbang dengan mengizinkan penyelenggara layanan kesehatan untuk mengadopsi kemajuan teknologi informasi untuk mendapatkan keuntungan layanan kesehatan dan menghasilkan layanan berkualitas bagi individu dan penyedia layanan kesehatan.

### 4.7.3 Persyaratan Keamanan Komputasi Awan Sektor Pemerintah

Komputasi awan menghadirkan peluang untuk transformasi dan inovasi aplikasi dan model layanan teknologi informasi pemerintah. Namun, keamanan merupakan faktor paling kritis bagi sistem bisnis yang juga terlibat dalam perekonomian nasional dan hajat hidup orang banyak. Jika data dikompromikan setelah data warga negara dikumpulkan, maka akan membawa kerugian besar bagi pemerintah dan masyarakat bahkan membahayakan keamanan nasional. Oleh karena itu, persyaratan keamanan komputasi awan di industri pemerintah dapat diringkas sebagai berikut (AlAhmad et al., 2021; Salam & Investment, 2020):

a. Fokus pada privasi dan keamanan pengguna: Pemerintah sangat mementingkan privasi dan keamanan pengguna di komputasi awan, menerapkan manajemen keamanan berbasis risiko untuk

layanan komputasi awan, dan memanfaatkan sepenuhnya keunggulan komputasi awan, seperti efisiensi tinggi, kecepatan, elastisitas sambil mengendalikan risiko.

b. Pertahanan kolektif untuk mengurangi *attack vector* (jalur serangan siber): Serangan siber akan jauh lebih mudah dikendalikan jika *attack vector* serangan diminimalisir seminim mungkin. Solusi pertahanan kolektif melalui komputasi awan juga mendukung deteksi dan memitigasi serangan siber.

c. Pemantauan dan respons berkelanjutan: Industri pemerintah memerlukan arsitektur komputasi awan dengan produk komputasi awan yang menyediakan pemantauan dan respons berkelanjutan untuk membantu lembaga pemerintah mengurangi waktu pemantauan dan respons.

d. Berfokus pada keamanan informasi dan data serta mengelola informasi dan data secara terpusat: Karena data pemerintah disimpan secara luas di berbagai unit, departemen, dan sistem, departemen pemerintah mementingkan penyimpanan data dan keamanan transmisi.

### 4.7.4 Persyaratan Keamanan Komputasi Awan Pada Sektor Otomotif

Dengan tren kendaraan transportasi *online*, kendaraan swakemudi, dan kendaraan dikendalikan perangkat lunak, komputasi awan menjadi salah satu faktor kompetitif utama dalam industri otomotif. Seiring skala industri yang terus meningkat, semakin banyak perusahaan yang memulai layanan komputasi awan, teknologi produk terus diinovasi dan ditingkatkan, dan tantangan komputasi awan semakin meningkat. Persyaratan keamanan

untuk industri otomotif dapat diringkas sebagai berikut (Mondal et al., 2020; Nassif et al., 2021):

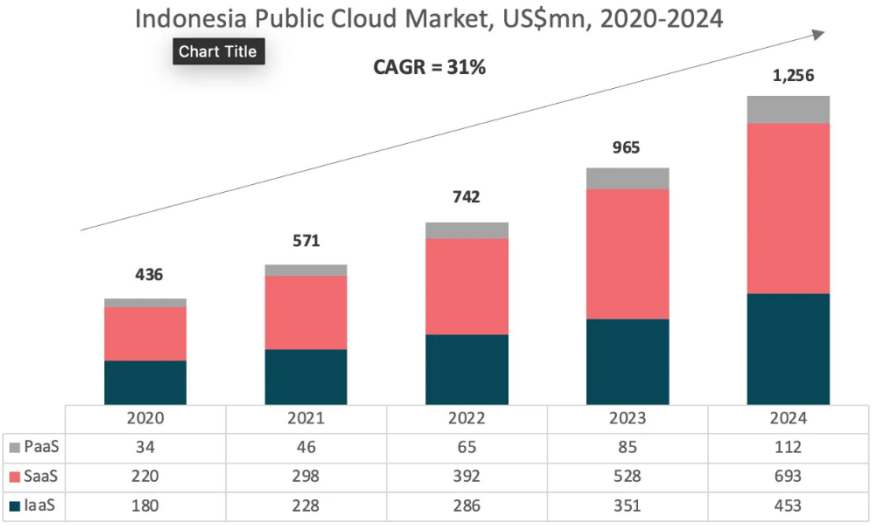
a. Membangun platform komputasi awan yang terpadu: Untuk memberikan layanan data untuk pelanggan, dan memastikan keamanan data, perusahaan otomotif perlu memiliki platform komputasi awan yang terpadu. Hal ini juga berguna untuk memastikan semua kendaraan menerima pembaruan perangkat lunak dan *firmware* dengan cara yang aman dan efisien
b. Manajemen ancaman keamanan terpusat: Seiring meningkatnya ancaman keamanan terhadap kendaraan dan jaringan kendaraan, perusahaan otomotif memiliki kebutuhan yang meningkat untuk memperkuat pemantauan ancaman dan mengelola ancaman keamanan secara terpusat.
c. Keamanan data: Memastikan enkripsi *end-to-end* untuk melindungi data sensitif dan informasi konsumen.

# BAB 5
# PEMANFAATAN KOMPUTASI AWAN DI INDONESIA

Komputasi awan adalah tren yang berkembang pesat di Indonesia, dengan bisnis dari semua ukuran mengadopsi teknologi untuk meningkatkan efisiensi, mengurangi biaya, dan mendapatkan akses ke kemampuan baru. Penggunaan komputasi awan di Indonesia didorong oleh beberapa faktor, antara lain meningkatnya ketersediaan internet berkecepatan tinggi, meningkatnya jumlah pengguna *smartphone*, dan fokus pemerintah pada transformasi digital..

## 5.1 Pangsa Pasar Komputasi Awan di Indonesia

Pasar publik komputasi awan di Indonesia sedang dalam tahap pembentukan dan merupakan salah satu pasar dengan pertumbuhan tercepat di Asia Pasifik (APAC). Berdasarkan laporan yang disusun oleh BCG (*Boston Consulting Group*) pada tahun 2019, pasar komputasi awan pada tahun 2018 bernilai US$0,2 miliar diproyeksikan akan tumbuh ke angka US$0,8 miliar pada tahun 2023 dengan CAGR 25% dalam rentang 2018 – 2023 (Boston Consulting Group, 2023). Pada studi lain yang dilakukan oleh twimbit (Zubri, 2021a) pada awal tahun 2021, pangsa pasar komputasi awan pada tahun 2020 sebesar US$436 juta diproyeksikan akan meningkat menjadi US$1,26 miliar pada tahun 2024 dengan CAGR sebesar 31% pada rentang 2020 – 2024, seperti terlihat pada Gambar 0-1, terlihat bahwa komposisi pasar komputasi awan di Indonesia di dominasi oleh SaaS dengan 51%, dan IaaS dengan 41%.




| | 2020 | 2021 | 2022 | 2023 | 2024 |
|---|---|---|---|---|---|
| PaaS | 34 | 46 | 65 | 85 | 112 |
| SaaS | 220 | 298 | 392 | 528 | 693 |
| IaaS | 180 | 228 | 286 | 351 | 453 |

*Gambar 0-1 Proyeksi pertumbuhan pasar komputasi awan di Indonesia 2020 – 2024*
(Zubri, 2021)

Twimbit juga merangkum *market matrix* dari publik komputasi awan di Indonesia pada tahun 2020, seperti dapat dilihat di Gambar 0-2. Beberapa sorotan penting dari data yang ditampilkan pada Gambar 0-2 adalah, yang pertama ukuran pasar sebesar US$435,5 juta, pertumbuhan pasar sebesar 34%, dan penetrasi pasar sebesar 3,4%. Beberapa faktor pendorong bagi pasar komputasi awan di Indonesia di antaranya adalah pertumbuhan pengguna Internet di Indonesia tahun 2020 sebesar 17%, yang setara dengan total sekitar 176 juta pengguna atau 65% dari total populasi di Indonesia.

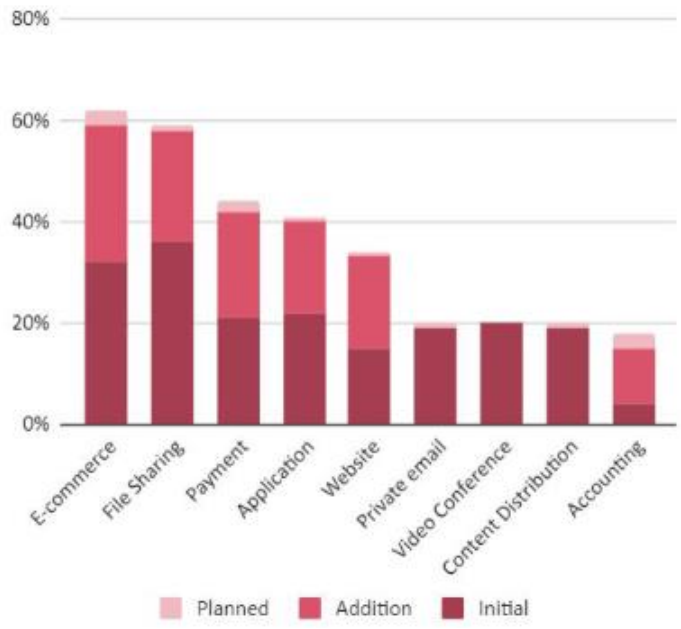
Selain itu, pertumbuhan ekonomi digital di Indonesia sebesar 11% pada nilai US$44 miliar, walaupun terjadi penurunan Produk Domestik Bruto (PDB) sebagai dampak pandemi. Selain itu, ekosistem bisnis digital *native* di Indonesia yang terdiri atas sekitar 2000 perusahaan *startup* yang aktif, berkontribusi besar pada porsi pasar dari publik komputasi awan. Seperti diketahui, Indonesia merupakan rumah bagi 5 dari 13 *unicorn* di ASEAN, yang masing-masing membelanjakan lebih dari US$10 juta pada layanan komputasi awan.

Sorotan menarik lainnya adalah terkait konsentrasi pasar sebesar 36% yang merupakan gabungan dari 3 penyedia layanan komputasi awan dengan pasar terbesar di Indonesia, yaitu *Google* Komputasi awan *Platform* (GCP), *Amazon Web Service* (AWS) dan Microsoft Azure, di mana GCP memiliki pangsa pasar tertinggi di Indonesia. Salah satu faktor yang dapat mempengaruhi tingginya pangsa pasar GCP di Indonesia karena adanya pusat data atau region GCP yang berlokasi di Indonesia sejak tahun 2020. Hal itu memberi keuntungan karena salah satu regulasi yang berlaku di Indonesia menyebutkan bahwa pusat data penyedia layanan komputasi awan harus berlokasi di Indonesia, terutama bagi instansi atau industri yang mengelola data sensitif dan ingin mengadopsi komputasi awan.

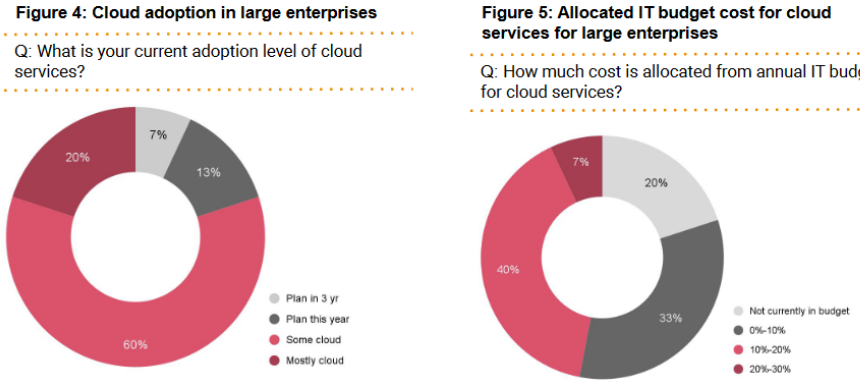

*Gambar 0-2 Market matrix dari publik komputasi awan di Indonesia tahun 2020* (Zubri, 2021)

Di sisi lain, berdasarkan survei yang dilakukan oleh PWC kepada 81 perusahaan kecil menengah (UKM) dan 15 perusahaan besar pada Maret –

Agustus 2021, terungkap bahwa 89% UKM sudah mengadopsi layanan komputasi awan secara aktif dan 9% lainnya berencana untuk segera menggunakannya (PwC Consulting Indonesia, 2021). Selain itu, hasil survei menunjukkan variasi jenis layanan komputasi awan yang digunakan oleh UKM, dengan 60% di antaranya digunakan untuk layanan komputasi awan *e-commerce*. Salah satu penjelasan adalah bahwa *e-commerce* menjadi kanal penjualan utama selama pandemi Covid-19. Di antara perusahaan besar yang disurvei oleh PWC, 80% telah mengadopsi layanan komputasi awan, 13% berencana untuk mengadopsinya pada tahun 2021 dan sisa 7% akan mengadopsi dalam jangka waktu 3 tahun sejak 2021. Akan tetapi, hanya sekitar 7% dari perusahaan besar yang mengalokasikan lebih dari 20% anggaran IT mereka untuk layanan komputasi awan, seperti yang terlihat pada Gambar 0-3 dan Gambar 0-4 (PwC Consulting Indonesia, 2021).




*Gambar 0-3 Jenis layanan komputasi awan yang digunakan oleh UKM*




*Gambar 0-4 Adopsi layanan komputasi awan dan alokasi anggaran IT untuk layanan* komputasi awan *pada perusahaan besar di Indonesia*

Tata kelola teknologi informasi di Indonesia menjadi isu penting karena pesatnya pertumbuhan teknologi dan meningkatnya penggunaan perangkat digital dalam bisnis, pemerintahan, dan kehidupan sehari-hari. Berikut adalah ikhtisar aspek kunci tata kelola TI di Indonesia:

a. Kerangka Hukum: Kerangka hukum untuk tata kelola TI di Indonesia disediakan oleh undang-undang Informasi dan Transaksi Elektronik (ITE), yang diundangkan pada tahun 2008. Undang-undang tersebut antara lain menetapkan aturan untuk transaksi elektronik, dokumen elektronik, dan tanda tangan digital.

b. Peraturan Pemerintah: Pemerintah Indonesia berperan aktif dalam tata kelola TI, dengan Kementerian Komunikasi dan Informatika (Menkominfo) bertanggung jawab atas pengembangan dan implementasi kebijakan dan peraturan terkait TI. Menkominfo mengawasi Dewan TIK Nasional, yang bertanggung jawab untuk mengembangkan strategi TI negara.

c. Perlindungan Data: Indonesia memiliki undang-undang Perlindungan Data Pribadi, yang mulai berlaku pada tahun 2022, untuk melindungi privasi dan data pribadi individu. Undang-undang ini mengharuskan

perusahaan untuk mendapatkan persetujuan sebelum mengumpulkan, memproses, atau menyimpan data pribadi.

d. Keamanan siber: Pemerintah secara aktif bekerja untuk meningkatkan keamanan siber di Indonesia. Pada 2018, pemerintah membentuk Badan Siber dan Sandi Negara (BSSN) untuk memastikan keamanan infrastruktur informasi penting negara.

e. SPBE (Sistem Pemerintahan Berbasis Elektronik): Pemerintah bekerja untuk meningkatkan penggunaan layanan SPBE untuk meningkatkan efisiensi dan transparansi dalam pelayanan publik. Dewan Teknologi Informasi dan Komunikasi Nasional (WANTIKNAS) bertanggung jawab untuk mengembangkan kebijakan dan strategi SPBE serta pelaksanaan program pengembangan TIK yang bersifat lintas kementerian.

Tata kelola TI di Indonesia adalah masalah multifaset yang melibatkan kerangka hukum, peraturan pemerintah, perlindungan data, keamanan siber dan SPBE. Pemerintah secara aktif berupaya meningkatkan tata kelola TI untuk mendorong pertumbuhan ekonomi digital negara dan memastikan keamanan di dunia siber. Bab ini kami membahas terkait bagaimana tata kelola keamanan TI di Indonesia mulai dari pandangan umum terkait aspek kerangka hukum hingga evaluasi keamanan komputasi awan.

## 5.2 Kebijakan Terkait Komputasi Awan Indonesia

Regulasi yang baik mengenai perlindungan data pribadi diharapkan dapat meminimalisir ancaman pelanggaran privasi data pribadi di berbagai bidang antara lain industri perbankan, media sosial seperti Facebook, WhatsApp, Twitter, dan Instagram, hingga program KTP elektronik. Apabila kebijakan privasi dilanggar oleh salah satu pihak, khususnya penyedia layanan, maka hal tersebut akan menimbulkan suatu kondisi yang dikenal sebagai penyalahgunaan data pribadi.

Setidaknya 3 aturan terkait kebijakan keamanan layanan komputasi awan yang berlaku di Indonesia: 1. Undang-undang perlindungan data pribadi (UU PDP), Peraturan pemerintah terkait penyelenggara sistem & transaksi elektronik dan undang-undang informasi & transaksi elektronik. Ketiga aturan ini jika dipetakan ke tanggung jawab CSP atau CSC maka dapat diilustrasikan seperti pada Gambar 0-5.


*Gambar 0-5 Pemetaan Regulasi keamanan layanan komputasi awan dengan provider dan pengguna layanan*

### 5.2.1 Undang-Undang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan undang-undang komprehensif yang mengatur transaksi elektronik di Indonesia. Berikut adalah beberapa poin penting dari UU ITE (Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik, 2016):

a. Pengakuan hukum transaksi elektronik - UU ITE mengakui validitas hukum dan keberlakuan transaksi elektronik dan tanda tangan elektronik.
b. Pengaturan transaksi elektronik - UU ITE mengatur berbagai aspek transaksi elektronik, termasuk kontrak elektronik, catatan elektronik, dokumen elektronik, dan bukti elektronik.
c. Nama domain dan merek dagang - Undang-undang ITE mengatur

pendaftaran dan penggunaan nama domain dan merek dagang dalam konteks transaksi elektronik.

d. Sistem dan fasilitas elektronik - UU ITE mencakup ketentuan terkait dengan pembentukan dan pengelolaan sistem dan fasilitas elektronik, termasuk persyaratan keamanan dan kerahasiaan.

e. Kewajiban - UU ITE mencakup ketentuan yang terkait dengan tanggung jawab atas transaksi elektronik, termasuk tanggung jawab atas kerugian akibat penggunaan sistem dan fasilitas elektronik.

Berikut beberapa perbuatan yang dilarang UU ITE:

a. Menyebarkan Video Asusila: Perbuatan pertama yang dilarang dalam UU ITE adalah orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan.

b. Judi Online: Selanjutnya, pasal 27 ayat (2) UU ITE memuat larangan perbuatan yang bermuatan perjudian. Hukuman untuk mereka yang melanggar adalah dipidana dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak satu miliar rupiah.

c. Pencemaran Nama Baik: Pasal 27 ayat (3) UU ITE juga mengatur tentang pencemaran nama baik. Pelaku yang dijerat dengan pasal ini bakal dipidana dengan pidana penjara paling lama 4 tahun dan/atau denda paling banyak tujuh ratus lima puluh juta rupiah.

d. Pemerasan dan Pengancaman: Orang yang melakukan pemerasan dan pengancaman juga berpeluang dijerat pasal 27 ayat (4) UU ITE. Hukumannya adalah dipidana dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak satu miliar rupiah.

e. Berita Bohong: Berita bohong juga dilarang dalam pasal 28 ayat (1) UU ITE yang berbunyi bahwa setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan

kerugian konsumen dalam transaksi elektronik.

f. Ujaran Kebencian: Orang yang menyebarkan informasi dengan tujuan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA) juga merupakan perbuatan yang dilarang dalam pasal 28 ayat (2) UU ITE.

g. Teror Online: Pada pasal 29 UU ITE mengatur perbuatan teror online yang dilarang. Pasal ini bakal menjerat setiap orang dengan sengaja dan tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

Undang-Undang Nomor 19 Tahun 2016 merevisi dari Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Revisi tersebut memperbaharui dan memperluas ketentuan undang-undang asli sebagai respons terhadap perkembangan teknologi dan transaksi elektronik. Revisi tersebut antara lian terkait definisi istilah, perubahan cakupan pasal, proses dan wewenang penyidik serta besaran/masa hukuman. Singkatnya, Undang-Undang Nomor 19 Tahun 2016 merevisi dan memperbaharui ketentuan UU ITE awal untuk menyikapi perkembangan baru dalam teknologi dan transaksi elektronik. Undang-undang ITE memperkenalkan ketentuan baru terkait perlindungan data pribadi, keamanan sistem elektronik, perjanjian transaksi elektronik, dan kejahatan siber.

### 5.2.2 Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Peraturan Pemerintah (PP) No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik mengatur kegiatan Penyelenggara Sistem Elektronik (PSE) (Pemerintah Republik Indonesia, 2019), secara umum

didefinisikan sebagai setiap orang, penyelenggara pemerintahan, badan usaha, atau anggota masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik secara individu atau kolektif untuk pengguna. Mulai 10 Oktober 2019, PP 71 mengamendemen Peraturan Pemerintah Indonesia sebelumnya No. 82 tahun 2012 (Pemerintah Republik Indonesia, 2012)untuk memberikan kejelasan lebih lanjut seputar persyaratan lokalisasi data, termasuk fleksibilitas tambahan bagi PSE sektor swasta untuk menyimpan sistem dan data di luar Indonesia, tunduk pada batasan tertentu. PP 71 juga mencakup persyaratan pendaftaran untuk PSE, persyaratan perlindungan dan keamanan data umum, hak penghapusan dan penghapusan untuk pemilik data, dan larangan konten, di antara persyaratan lainnya. Peraturan ini memiliki beberapa poin penting yang harus dipahami, antara lain:

**Definisi Sistem dan Transaksi Elektronik**

Peraturan ini memberikan definisi yang jelas tentang apa yang dimaksud dengan sistem dan transaksi elektronik. Sistem elektronik didefinisikan sebagai sekumpulan perangkat keras dan lunak yang saling terkait dan digunakan untuk memproses, menyimpan, dan mengirimkan informasi secara elektronik. Sedangkan transaksi elektronik didefinisikan sebagai setiap kegiatan atau proses yang melibatkan penggunaan sistem elektronik untuk membuat, mengirimkan, menerima, atau memproses informasi.

**Kewajiban Penyelenggara Sistem Elektronik (PSE)**

Peraturan ini mengatur kewajiban PSE, termasuk mengenai perlindungan data pribadi pengguna, perlindungan hak kekayaan intelektual, pengamanan sistem dan informasi, serta tata kelola yang baik. Selain itu PSE wajib memberikan edukasi yang disampaikan kepada pengguna sistem elektronik keamanan sistem elektronik.

**Tanda Tangan Elektronik**

Peraturan ini juga mengatur mengenai tanda tangan elektronik, termasuk persyaratan untuk tanda tangan elektronik yang sah, prosedur penerbitan sertifikat tanda tangan elektronik, serta tata cara verifikasi tanda tangan elektronik.

**Pelaporan Gangguan Sistem**

Peraturan ini mewajibkan penyelenggara sistem elektronik untuk melaporkan gangguan sistem yang signifikan kepada Kementerian Komunikasi dan Informatika dalam waktu 24 jam.

**Audit Keamanan dan Pengamanan Sistem**

Peraturan ini mewajibkan penyelenggara sistem elektronik untuk melakukan audit keamanan dan pengamanan sistem secara teratur untuk memastikan bahwa sistem tersebut aman dan bebas dari ancaman keamanan.

Peraturan Pemerintah No. 71 Tahun 2019 ini memiliki tujuan untuk mendorong penggunaan teknologi informasi dan komunikasi dalam sistem dan transaksi elektronik, sekaligus memperkuat perlindungan terhadap pengguna dan penyelenggara sistem elektronik. Dengan adanya peraturan ini, diharapkan dapat membantu menciptakan lingkungan yang kondusif bagi penggunaan teknologi informasi dan komunikasi di Indonesia.

PP No.71 ini bertujuan untuk meningkatkan penggunaan teknologi informasi dan transaksi elektronik di Indonesia serta memastikan bahwa penggunaannya dilakukan dengan cara yang aman dan efektif. PSE wajib menjalankan prosedur dan memiliki sarana untuk pengamanan sistem dan wajib menyediakan rekam jejak audit terhadap seluruh kegiatan. PSE wajib melindungi data pribadi pengguna dari penggunaan yang tidak sah dan melindungi kerahasiaan data pribadi tersebut. PSE untuk pelayanan publik wajib menempatkan pusat data dan pusat pemulihan bencana di wilayah Indonesia untuk kedaulatan negara terhadap data warga negaranya. Dalam

hal ini, peraturan ini juga menjadi dasar hukum bagi penggunaan teknologi informasi dan transaksi elektronik di Indonesia, sehingga penting untuk dipatuhi oleh penyelenggara dan pengguna teknologi informasi dan transaksi elektronik.

### 5.2.3 Undang-Undang Perlindungan Data Pribadi (UU PDP)

UU PDP (Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, 2022) mengatur pengumpulan, penggunaan, pemrosesan, dan penyimpanan data pribadi di Indonesia dan dalam banyak hal serupa dengan GDPR di Uni Eropa (Sinulingga, 2022). Ketentuan utama dari undang-undang tersebut meliputi:

a. Definisi data pribadi: Undang-undang mendefinisikan data pribadi sebagai setiap informasi yang berkaitan dengan individu yang dapat digunakan untuk mengidentifikasi individu tersebut, baik secara langsung maupun tidak langsung.
b. Persetujuan: Data pribadi hanya dapat diproses dengan persetujuan dari individu yang bersangkutan. Persetujuan harus diberikan secara bebas, spesifik, berdasarkan informasi, dan tidak ambigu.
c. Batasan tujuan: Data pribadi harus dikumpulkan dan diproses untuk tujuan spesifik, eksplisit, dan sah.
d. Minimalisasi data: Data pribadi yang dikumpulkan harus dibatasi pada apa yang diperlukan untuk tujuan pemrosesannya.
e. Retensi data: Data pribadi harus disimpan tidak lebih lama dari yang diperlukan untuk tujuan pemrosesannya.
f. Tindakan keamanan: Organisasi yang memproses data pribadi harus menerapkan tindakan teknis dan organisasi yang sesuai untuk memastikan keamanan data pribadi.
g. Hak subjek data: Individu memiliki hak untuk mengakses data pribadinya, meminta koreksi atas data pribadinya, meminta

penghapusan data pribadinya, dan menolak pemrosesan data pribadinya.

Peraturan PDP juga telah dimiliki negara lain, yaitu Hongkong, Malaysia, Singapura, Korea Selatan (Halim, 2022). Substansi pengaturan dalam PDP yaitu jenis data pribadi, hak pemilik data, pemrosesan data pribadi, kewajiban pengendali data dalam pemrosesan data pribadi, transfer data pribadi, sanksi administratif, larangan dalam penggunaan data pribadi, pembentukan pedoman perilaku pengendali data pribadi, penyelesaian sengketa dan hukum acara, kerja sama internasional, peran pemerintah dan masyarakat dan ketentuan pidana.

UU PDP di Indonesia berlaku untuk setiap individu atau organisasi yang mengumpulkan, memproses, atau menyimpan data pribadi di Indonesia, termasuk perusahaan dalam negeri dan luar negeri. Undang-undang memberlakukan denda yang signifikan dan hukuman pidana untuk ketidakpatuhan, termasuk denda hingga Rp 50 miliar (sekitar USD 3,5 juta) dan penjara hingga 12 tahun. Undang-undang Perlindungan Data Pribadi merupakan perkembangan penting dalam perlindungan data pribadi di Indonesia dan menyediakan kerangka kerja untuk pemrosesan data pribadi yang aman dan sah.

Selama akhir tahun 2022 terdapat berbagai pelanggaran kebocoran data yang masif terjadi di Indonesia beberapa di antaranya adalah (Andani, 2021):

a. Pada bulan Agustus 2022, sebanyak 26 juta data diduga milik pelanggan IndiHome bocor dan diperjualbelikan di BreachForums. Data-data itu berupa histori pencarian, URL, keyword, user info mencakup email, Geolocation, browser, platform, nama, jenis kelamin, hingga NIK.
b. Sebanyak 44 juta pengguna aplikasi MyPertamina dibocorkan oleh peretas Bjorka pada bulan November 2022, dan dijual seharga Rp392

juta dalam bentuk BitCoin. Data tersebut berisi dari nama, email, NIK, NPWP, nomor telepon, dan pengeluaran pengguna.

c. Sebanyak 3,2 miliar data yang diklaim sebagai pengguna aplikasi Peduli Lindungi bocor. Bocoran data tersebut dijual di forum dark web. Data berformat CSV itu berupa "Nama, Email, NIK, Nomor telepon, Tanggal lahir, *Device* ID, COVID-19 status, *Checkin History, Contact Tracing History, Vaccination*.

d. Sebanyak 1,3 miliar data pendaftaran kartu SIM diduga bocor dan dijual di forum daring pada September 2022. Data yang bocor meliputi NIK, nomor telepon, nama penyedia, dan tanggal pendaftaran dengan kapasitas data sebesar 87 GB.

e. Pada awal September 2022, peretas Bjorka mengklaim mengambil data dari KPU sebanyak 105.003.428 juta data penduduk Indonesia dengan detail NIK, KK, nama lengkap, tempat tanggal lahir, jenis kelamin dan umur.

Insiden kebocoran data skala nasional yang terjadi di tahun 2022 diakui atau tidak, telah berhasil menjadi katalis pengesahan UU PDP yang telah lama tertunda. Namun, disahkannya UU PDP bukanlah garis *finish*, melainkan semata garis start untuk mulai menata keamanan siber nasional demi terwujudnya kedaulatan data RI. Terlepas dari upaya pemerintah membuat UU PDP, pembobolan data dan serangan siber masih lazim terjadi di Indonesia, dan ada laporan data pribadi yang bocor atau dicuri dari lembaga pemerintah dan perusahaan swasta. Hal ini menunjukkan bahwa masih terdapat kesenjangan dalam penerapan dan penegakan peraturan privasi data dan keamanan siber di Indonesia.

Sebelum UU PDP telah ada Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 merupakan kebijakan penting di Indonesia yang menitikberatkan pada perlindungan data pribadi dalam sistem elektronik. Peraturan tersebut menetapkan pedoman dan persyaratan untuk pengontrol

dan pemroses data untuk memastikan privasi dan keamanan data pribadi. Akar permasalahan perlindungan data pribadi di Indonesia adalah keterbatasan kesadaran dan pemahaman: banyak individu dan organisasi di Indonesia memiliki kesadaran dan pemahaman yang terbatas akan pentingnya perlindungan data pribadi. Kurangnya kesadaran ini dapat menyebabkan langkah-langkah keamanan yang tidak memadai dan perlindungan yang tidak memadai untuk data pribadi. Kampanye pendidikan dan kesadaran sangat penting untuk meningkatkan pemahaman tentang risiko yang terkait dengan data pribadi dan mempromosikan praktik penanganan data yang bertanggung jawab.

Pada sisi lain mekanisme penegakan yang efektif sangat penting untuk memastikan kepatuhan terhadap peraturan perlindungan data pribadi. Di Indonesia, tantangan dalam penegakan hukum, seperti keterbatasan sumber daya, kurangnya koordinasi antar otoritas terkait, dan berbagai tingkat komitmen, dapat menghambat penerapan dan penegakan hukum perlindungan data yang tepat. Memperkuat kemampuan penegakan hukum dan koordinasi antar badan pengawas sangat penting untuk mengatasi tantangan ini.

UU PDP bukanlah akhir dari perjuangan melindungi data pribadi. Masih ada panjang jalan yang harus ditempuh pemerintah untuk segera mengimplementasikan regulasi, terutama dalam mendefinisikan berbagai konsep perwujudan yang masih sangat umum, memastikan implementasi dan pengawasan yang tepat, serta sinkronisasi dengan peraturan perundang-undangan lainnya.

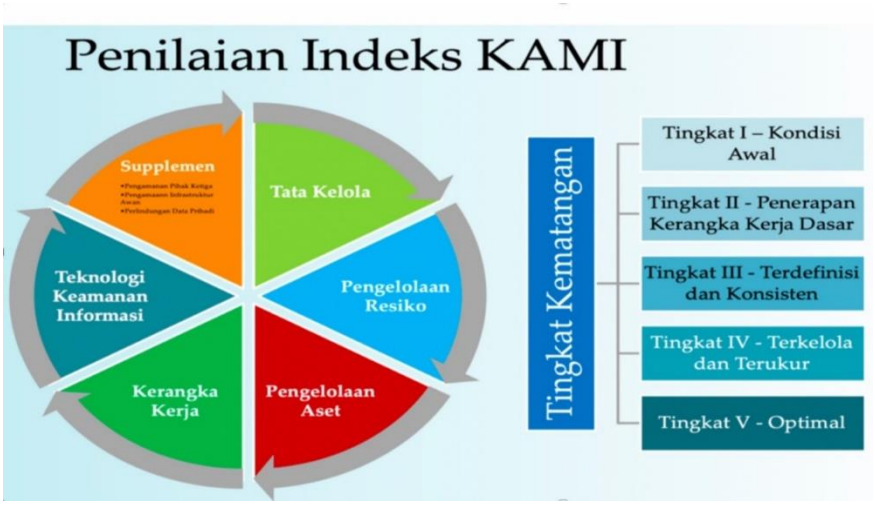
## 5.3 Indeks KAMI

Indeks Keamanan Informasi (KAMI) adalah suatu metrik atau tolok ukur yang digunakan untuk mengukur tingkat keamanan informasi pada sebuah organisasi atau perusahaan (BSSN, 2021). KAMI digunakan untuk membantu

organisasi dalam mengidentifikasi, mengevaluasi, dan memperbaiki kelemahan dalam sistem keamanan informasi mereka. KAMI terdiri dari beberapa dimensi atau aspek keamanan informasi yang harus diperhatikan oleh suatu organisasi, yaitu:

a. Kepemilikan: Menunjukkan tingkat perlindungan terhadap informasi yang dimiliki oleh organisasi dari akses yang tidak sah.
b. Kerahasiaan: Menunjukkan seberapa baik organisasi menjaga kerahasiaan informasi dan mencegah akses yang tidak sah ke informasi tersebut.
c. Integritas: Menunjukkan seberapa baik organisasi menjaga integritas informasi, yaitu keutuhan dan akurasi informasi yang dimiliki oleh organisasi.
d. Ketersediaan: Menunjukkan seberapa baik organisasi menjaga ketersediaan informasi untuk dipakai oleh pengguna yang sah.
e. Akuntabilitas: Menunjukkan seberapa baik organisasi memastikan bahwa informasi digunakan sesuai dengan peraturan dan kebijakan yang berlaku.
f. Keandalan: Menunjukkan seberapa baik sistem keamanan informasi organisasi dapat diandalkan untuk mencegah akses yang tidak sah dan mengatasi masalah keamanan informasi.

Dalam pengukuran KAMI, setiap dimensi akan diberi skor dan akan dihitung secara keseluruhan untuk memberikan nilai indeks keamanan informasi organisasi. Dengan nilai KAMI yang baik, organisasi dapat lebih percaya diri dan terhindar dari risiko keamanan informasi yang dapat membahayakan bisnis mereka. Hasil penilaian indeks KAMI menunjukkan tingkat kematangan manajemen sistem keamanan informasi seperti yang ditunjukkan pada Gambar 0-6.




*Gambar 0-6 Skema Penilaian pada indeks KAMI*

Sebagai alat untuk mengukur tingkat keamanan informasi, Indeks Keamanan Informasi (KAMI) memiliki kelebihan dan kelemahan, di antaranya (Raditya et al., 2022):

**Kelebihan KAMI:**

a. Dapat membantu organisasi untuk memprioritaskan tindakan yang diperlukan untuk meningkatkan keamanan informasi. Dengan mengetahui dimensi keamanan informasi mana yang perlu diperbaiki, organisasi dapat menentukan prioritas dan mengalokasikan sumber daya yang tepat untuk meningkatkan keamanan informasi mereka.

b. Memberikan standar untuk perbandingan dengan organisasi lain. KAMI dapat membantu organisasi untuk membandingkan tingkat keamanan informasi mereka dengan organisasi lain di sektor industri yang sama, sehingga dapat membantu dalam meningkatkan daya saing dan menjaga reputasi organisasi.

**Kelemahan KAMI:**

a. Tidak dapat mengukur keamanan informasi secara menyeluruh. KAMI hanya memberikan pengukuran terhadap dimensi-dimensi tertentu yang dianggap penting dalam keamanan informasi, sehingga tidak memberikan gambaran menyeluruh tentang keamanan informasi organisasi.
b. Tidak dapat mengatasi kebutuhan unik dari setiap organisasi. KAMI hanya memberikan pandangan umum tentang keamanan informasi dan tidak mempertimbangkan kebutuhan dan keunikan setiap organisasi, seperti jenis data yang diolah, ukuran organisasi, dan risiko spesifik yang dihadapi.
c. Penilaian KAMI cenderung bersifat subjektif, hanya memberikan gambaran dasar tanpa melakukan penilaian terhadap kesiapan menghadapi insiden serta untuk mengukur keandalan sistem informasi terhadap serangan siber
d. KAMI juga tidak memberikan rencana perbaikan apa pun yang dapat berfungsi sebagai pedoman atau rekomendasi tentang cara mengamankan, memelihara, mengelola, atau menerapkan sistem informasi.

Secara keseluruhan, KAMI dapat menjadi alat yang berguna dalam meningkatkan keamanan informasi organisasi, tetapi harus digunakan dengan bijak dan harus dipahami bahwa KAMI hanya memberikan pandangan terhadap aspek tertentu dari keamanan informasi dan bukan gambaran menyeluruh. Model KAMI seharusnya menilai secara aktif kinerja dan efektivitas sistem manajemen keamanan informasi organisasi untuk mengetahui ketahanannya dalam menahan serangan serta untuk memberikan perbaikan yang nyata.

# BAB 6

# POTENSI DAN RISIKO PEMANFAATAN KOMPUTASI AWAN

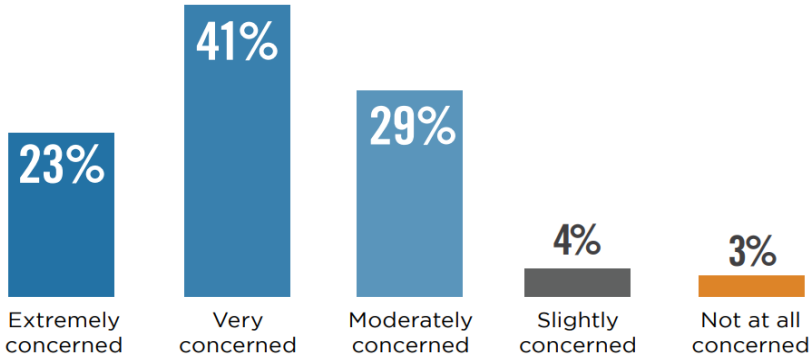
Komputasi awan telah merevolusi cara bisnis beroperasi, menghadirkan sejumlah risiko dan peluang. Di satu sisi, komputasi awan menawarkan banyak keuntungan, seperti skalabilitas, efisiensi biaya, dan peningkatan aksesibilitas. Namun, di samping manfaat ini, ada risiko yang melekat untuk dipertimbangkan. Masalah kedaulatan data, keamanan dan privasi data adalah beberapa risiko utama yang terkait dengan komputasi awan. Pada bab ini kami akan memaparkan berbagai peluang dari risiko terkait penggunaan komputasi awan.

## 6.1 CSC Memperhatikan Keamanan Komputasi Awan.

Seperti halnya banyak teknologi baru, keamanan layanan komputasi awan menjadi perhatian utama. Seiring perkembangan teknologi, masalah keamanan menimbulkan tantangan bagi penerapan dan pengembangan layanan komputasi awan secara luas. Menurut survei Ermetic terhadap lebih dari 300 *Chief Information Security Officer* (CISO), hampir 80% perusahaan yang disurvei mengalami setidaknya satu pelanggaran keamanan data pada komputasi awan dalam 18 bulan terakhir, bahkan 43% di antaranya melaporkan 10 pelanggaran atau lebih (Osterman Research, 2022).

Pada sisi lain, 70% responden survei *Barracuda* di tahun 2020 (Barracuda, 2020) menunjukkan bahwa masalah keamanan dapat menghambat adopsi layanan komputasi awan publik oleh organisasi. Aspek keamanan ini mencakup keamanan infrastruktur komputasi awan publik, dampak dari

serangan siber, dan keamanan aplikasi yang diterapkan pada komputasi awan publik.

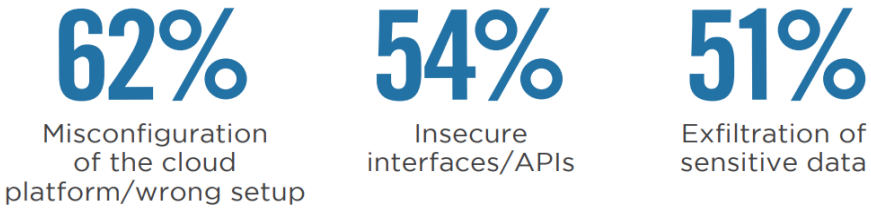



*Gambar 0-1 Survei kekhawatiran terkait layanan keamanan komputasi awan*

Laporan Keamanan Komputasi awan 2022 yang disponsori oleh ISC (ISC, 2022) juga menunjukkan bahwa 93% perusahaan yang disurvei mengkhawatirkan kekurangan profesional keamanan siber yang berkualitas. Hasil survei tersebut diilustrasikan pada Gambar 0-1. Di antaranya 29% merasa cukup khawatir, 41% sangat khawatir, dan 23% sangat khawatir. Berdasarkan laporan tersebut terdapat 3 tantangan keamanan komputasi awan teratas yakni:

a. Kehilangan/kebocoran data,
b. Privasi/kerahasiaan data,
c. Pemaparan kredensial secara tidak sengaja.

Berdasarkan laporan tersebut juga memuat hasil survei kepada profesional keamanan siber terkait ancaman keamanan komputasi awan yang paling mengkhawatirkan. Kesalahan konfigurasi keamanan komputasi awan menjadi risiko keamanan komputasi awan terbesar menurut 62% profesional keamanan siber dalam survei. Hasil ini kemudian diikuti oleh antarmuka/API yang tidak aman (54%), eksfiltrasi data sensitif (51%) dan akses tidak sah (50%), lihat ilustrasi Gambar 0-2.




*Gambar 0-2 Ancaman keamanan komputasi awan yang paling mengkhawatirkan* (ISC, 2022)

Solusi teknologi informasi berbasis komputasi awan menawarkan keuntungan yang signifikan, namun masih ada hambatan untuk adopsi komputasi awan. Survei mengungkapkan bahwa tantangan terbesar yang dihadapi CSC bukan terutama tentang teknologi, tetapi orang dan proses. Menurut survei dari ISC (ISC, 2022) faktor penghalang utama dari adopsi komputasi awan adalah: Keahlian dan pelatihan staf (52%), diikuti oleh masalah anggaran (44%) dan masalah privasi data (40%).

Serupa dengan hasil survei dari ISC, Fortinet juga membuat laporan survei di tahun 2021 (Fortinet, 2021). Laporan tersebut menyebutkan hambatan utama untuk adopsi komputasi awan yang lebih cepat, peserta survei menyebutkan kurangnya visibilitas (53%), kurangnya kontrol (46%), kurangnya sumber daya atau keahlian staf (39%), dan biaya tinggi (35%), lalu masalah privasi data (36%) sebagai faktor negatif yang paling signifikan. Kedua laporan tersebut menunjukkan bahwa calon pengguna komputasi awan masih mempersoalkan masalah keamanan komputasi awan terutama masalah privasi data.

## 6.2 Masalah Keamanan Pada Komputasi Awan

Saat ini berbagai industri mulai mengadopsi komputasi awan ke tingkat yang berbeda-beda dalam bisnis mereka. Pada sisi lain adopsi komputasi awan ini memunculkan kebutuhan untuk memastikan bahwa strategi keamanan komputasi awan industri mampu melindungi dari ancaman teratas terhadap

keamanan komputasi awan. Saat memberikan layanan, penyedia jasa layanan komputasi awan mungkin menghadapi ancaman keamanan internal (dari dalam penyedia layanan itu) dan eksternal (dari pihak selain penyedia layanan) (Gui et al., 2020). Sebagai contoh ancaman internal dan eksternal sebagai berikut:

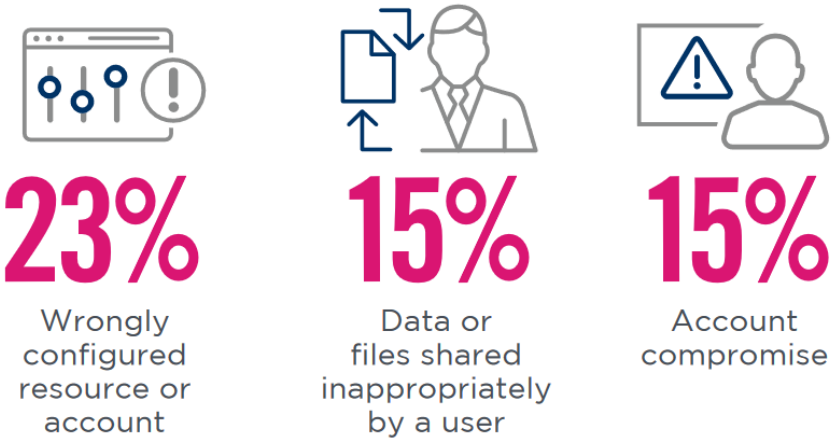
**Ancaman Internal:**

a. Aset tidak diketahui atau tidak terkendali,
b. Produk layanan komputasi awan rentan dalam desain,
c. Kebocoran data, penggunaan data yang berbahaya,
d. Penyalahgunaan izin akses karena kontrol akses yang tidak valid

**Ancaman Eksternal:**

a. Serangan peretas
b. Produk cacat dari pemasok pihak ketiga
c. Kerusakan pusat data selama bencana alam ekstrem
d. Proses bisnis dengan kerentanan yang dapat dimanfaatkan untuk penipuan.

*Check Point software* melakukan survei terhadap 775 profesional keamanan siber dilakukan pada Januari 2022 (Check Point, 2022). Menurut hasil survei tersebut seperempat organisasi (27%) pernah mengalami insiden keamanan terkait komputasi awan publik, hasil ini naik 10% dari tahun lalu. Kesalahan konfigurasi tahun ini (23%) telah menduduki posisi teratas sebagai insiden terkait keamanan nomor satu, melampaui data yang terekspos oleh pengguna (15%) di posisi kedua dan penyusupan akun (15%) merupakan insiden keamanan siber yang paling sering ketiga. Hasil ini diilustrasikan pada Gambar 0-3.

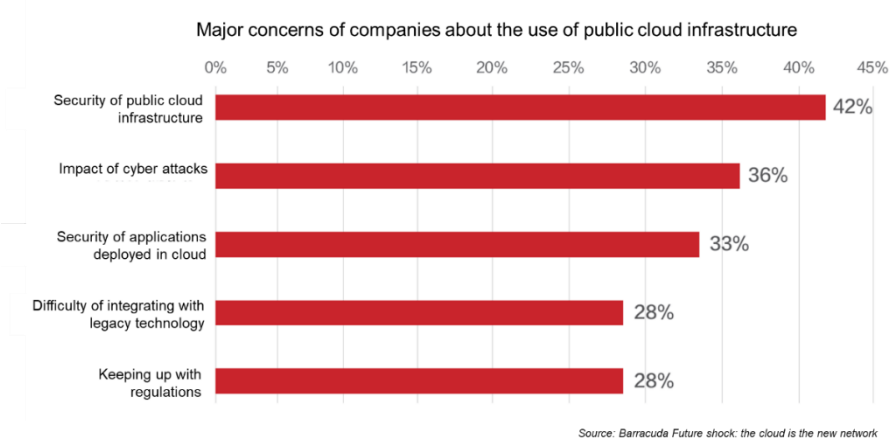



*Gambar 0-3 Insiden keamanan komputasi awan menurut Check Point Survey* (Check Point, 2022)

Mungkin tidak mengherankan mengingat skala ancaman yang dihadapi perusahaan global, masalah keamanan menempati urutan teratas dalam daftar kekhawatiran para perusahaan TI terkait penggunaan komputasi awan publik. Keamanan infrastruktur komputasi awan publik (42%) dianggap menjadi perhatian utama masalah keamanan. Hasil ini kemudian diikuti oleh dampak serangan siber (36%) dan keamanan aplikasi komputasi awan publik (33%). Namun, penting untuk diingat bahwa keamanan bukanlah satu-satunya tantangan komputasi awan publik yang dihadapi perusahaan TI dalam adopsi layanan komputasi awan publik. Selain itu masih ada masalah integrasi dengan teknologi lama (28%), kepatuhan terhadap peraturan (28%). Grafik hasil survei yang dilakukan oleh Barracuda terhadap 750 responden ini ditampilkan pada Gambar 0-4 (Barracuda, 2020).

Cloud Security Alliance (CSA) merilis laporan ancaman teratas terhadap komputasi awan pada Juni 2022 (Cloud security Alliance, 2022), dengan bertujuan untuk meningkatkan kesadaran akan ancaman, kerentanan, dan risiko di komputasi awan. Mereka menyurvei lebih dari 700 pakar industri tentang masalah keamanan di industri komputasi awan. Berdasarkan hasil

survei tersebut mereka mengidentifikasi sebelas masalah keamanan utama pada lingkungan komputasi awan di antaranya:




*Gambar 0-4 Kekhawatiran utama terhadap komputasi awan publik* (Barracuda, 2020)

a. Identitas, kredensial, akses, dan manajemen kunci yang tidak memadai: Identitas, kredensial, akses, dan manajemen kunci yang tidak memadai merupakan ancaman terhadap profil entitas baik perorangan, kelompok maupun organisasi yang dapat menyebabkan kinerja bisnis negatif dan hilangnya kepercayaan di khalayak umum.
b. Antarmuka dan API yang tidak aman: Karena antarmuka dan API digunakan secara luas di lingkungan komputasi awan untuk operasi akses dan pertukaran data, data sensitif atau pribadi yang tidak dilindungi dapat bocor secara tidak sengaja.
c. Kesalahan konfigurasi dan kontrol perubahan yang tidak memadai: Kesalahan konfigurasi atau kontrol perubahan yang tidak tepat dapat mempengaruhi kerahasiaan pengungkapan data, integritas data, ketersediaan dari operasi sistem. Semua ini akhirnya dapat berdampak pada reputasi perusahaan hingga harga saham.
d. Kurangnya arsitektur dan strategi keamanan komputasi awan:

Kurangnya kebijakan dan arsitektur keamanan komputasi awan dapat membatasi kelayakan arsitektur keamanan infrastruktur perusahaan yang efisien. Pada akhirnya masalah ini akan menyebabkan denda terkait masalah legal ataupun biaya perbaikan atau penyelesaian masalah.

e. Pengembangan perangkat lunak yang tidak aman: Pengembangan perangkat lunak yang tidak aman memiliki tiga dampak berikut: 1) Pelanggan kehilangan kepercayaan pada produk atau jasa layanan; 2) Kerusakan reputasi merek yang disebabkan oleh pelanggaran data; 3) Dampak hukum dan keuangan yang disebabkan oleh tuntutan hukum.

f. Sumber daya pihak ketiga yang tidak aman: Karena sebuah produk atau layanan adalah kombinasi dari semua produk dan layanan lain yang digunakan, maka eksploit dapat dimulai dari titik mana pun dalam rantai, dan berkembang dari sana. Peretas, untuk mencapai tujuan mereka hanya perlu mencari tautan terlemah sebagai titik masuk. Dalam dunia perangkat lunak, merupakan praktik umum untuk mencari kelemahan dari sumber daya pihak ketiga.

g. Kerentanan sistem: Kerentanan sistem merupakan kelemahan dalam platform layanan komputasi awan. Mereka dapat dieksploitasi dalam upaya untuk pelanggaran terhadap kerahasiaan, integritas, dan ketersediaan data, yang berpotensi mengganggu operasi layanan. Semua komponen dapat mengandung kerentanan yang dapat membuat layanan komputasi awan terbuka untuk diserang.

h. Pengungkapan data komputasi awan yang tidak disengaja: Basis data komputasi awan berisi data pelanggan yang sensitif, informasi karyawan, dan data produk. Kebocoran yang tidak disengaja akan menimbulkan biaya kompensasi yang tidak diharapkan.

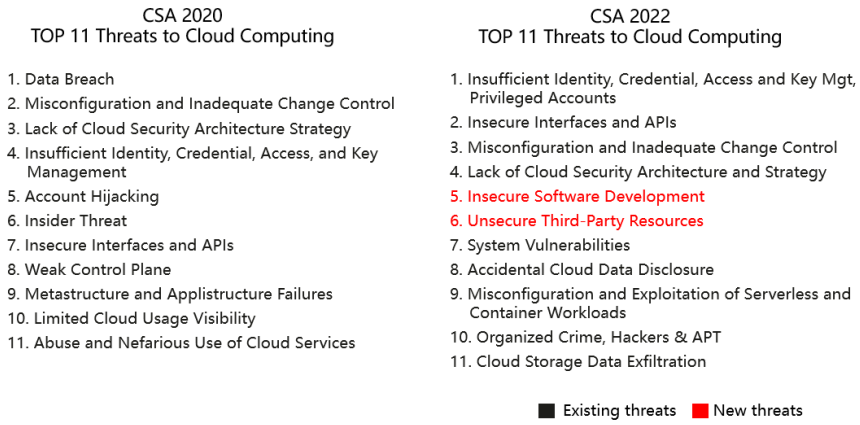
i. Kesalahan konfigurasi dan eksploitasi beban kerja dan kontainer: Tim infrastruktur lama yang terbiasa mengelola lingkungan lokal harus mempelajari keterampilan baru seperti Infrastruktur dan keamanan

komputasi awan. Beban kerja terkontainerisasi tanpa server dan *cloud-native* dapat tampak seperti solusi pamungkas (*silver bullet*) untuk masalah ini, melimpahkan tanggung jawab tersebut ke penyedia layanan komputasi awan (CSP). Namun, ini semua memerlukan tingkat komputasi awan dan kematangan keamanan aplikasi yang lebih tinggi daripada memigrasikan sebuah sistem ke komputasi awan.

j. Peretas & APT: APT (*Advanced Persistent Threats*) mengacu pada serangan yang dilakukan oleh tim penyusup yang menciptakan serangan ilegal jangka panjang pada jaringan untuk mengambil data yang sangat sensitif. Penyedia layanan harus menyadari kemungkinan dampak bisnis dari APT pada organisasi.

k. Eksfiltrasi data penyimpanan komputasi awan: Eksfiltrasi data terjadi ketika *malware* dan/atau aktor penyerang melakukan transfer data tanpa izin. Potensi ancaman terhadap eksfiltrasi data di komputasi awan adalah sebagai berikut: (1) Hilangnya hak kekayaan intelektual, yang memengaruhi kemajuan pengembangan produk. (2) Kepercayaan pelanggan, pemangku kepentingan, kehilangan mitra/karyawan, dan kesediaan organisasi lain untuk bekerja sama berkurang. (3) Pengguna kehilangan kepercayaan pada kemampuan organisasi untuk melindungi data pengguna.

Jika dibandingkan dengan 11 ancaman yang dirilis pada tahun 2020 (Cloud security Alliance, 2020b), CSA mencatat bahwa pelanggaran data (*data breach*) telah turun peringkat berkat upaya penyedia layanan komputasi awan. Kekhawatiran seperti ancaman orang dalam, pembajakan akun, dan kegagalan struktur aplikasi dan visibilitas penggunaan komputasi awan yang terbatas (Semua dari 11 potensi risiko teratas sebelumnya ada di tahun 2020) sekarang tidak lagi masuk dalam daftar ancaman teratas (lihat Gambar 0-5). Hal ini menunjukkan bahwa masalah keamanan tersebut yang menjadi tanggung jawab penyedia layanan komputasi awan tampaknya telah dikurangi secara efektif.




*Gambar 0-5 CSA top 11 Ancaman pada komputasi awan* (CSA, 2019)

Penelitian yang dilakukan oleh organisasi industri mendukung temuan CSA. Misalnya, menurut Laporan Keamanan Komputasi awan 2021 Fortinet (Fortinet, 2021) kesalahan konfigurasi keamanan komputasi awan, eksfiltrasi data sensitif, dan akses tidak sah adalah ancaman utama bagi profesional keamanan komputasi awan.

Laporan keamanan komputasi awan tahun 2022 dari Checkpoint (Check Point, 2022), organisasi ditanya tentang masalah keamanan utama mereka terkait lingkungan komputasi awan. Terlepas dari kenyataan bahwa banyak organisasi telah memutuskan untuk memindahkan data sensitif dan aplikasi penting ke komputasi awan, banyak kekhawatiran tentang bagaimana mereka dapat melindunginya.

Lingkungan berbasis komputasi awan memudahkan untuk berbagi data yang disimpan di dalamnya. Lingkungan ini dapat diakses langsung dari Internet publik dan menyertakan kemampuan untuk berbagi data dengan mudah dengan pihak lain melalui undangan email langsung atau dengan membagikan tautan publik ke data tersebut.

Kemudahan berbagi data di komputasi awan – meskipun merupakan aset utama dan kunci kolaborasi di komputasi awan – menimbulkan kekhawatiran serius terkait kehilangan atau kebocoran data. Faktanya, 69% organisasi menunjukkan ini sebagai masalah keamanan komputasi awan terbesar mereka (Netwrix, 2022). Berbagi data menggunakan tautan publik atau menyetel repositori berbasis komputasi awan ke publik membuatnya dapat diakses oleh siapa saja yang mengetahui tautan tersebut.

Menempatkan data ini di komputasi awan memiliki kelebihan, tetapi juga menimbulkan masalah keamanan utama bagi 66% organisasi. Banyak organisasi telah mengadopsi komputasi awan tetapi kurang memiliki pengetahuan untuk memastikan bahwa mereka dan pengguna mereka menggunakannya dengan aman. Akibatnya, data sensitif berisiko terpapar seperti yang ditunjukkan oleh sejumlah besar pelanggaran data komputasi awan.

## 6.3 Isu Pemanfaatan Komputasi Awan Terhadap Tata Kelola Data

Pertumbuhan koneksi internet dan digitalisasi ekonomi global, telah menyebabkan peningkatan pesat dalam pengumpulan, penggunaan, dan pengiriman data lintas batas, sebuah tren yang terus meningkat. Tidak hanya untuk perusahaan teknologi multinasional besar, tetapi juga untuk usaha mikro, kecil dan menengah, pekerja dan konsumen di semua sektor ekonomi, aturan tata kelola data harus sesuai dengan perkembangan ekonomi digital yang cepat dan sehat.

Perlindungan data adalah masalah keamanan penting bagi sebagian besar organisasi. Sebelum pindah ke komputasi awan, pengguna komputasi awan perlu mengidentifikasi objek data dengan jelas untuk dilindungi dan mengklasifikasikan data berdasarkan implikasinya pada keamanan, dan

kemudian menentukan kebijakan untuk perlindungan data serta mekanisme penegakan kebijakan.

Untuk sebagian besar aplikasi, objek data tidak hanya mencakup data yang berada di server komputasi awan (misalnya, basis data pengguna dan atau sistem *file*), tetapi juga data dalam transit antara komputasi awan dan pengguna yang dapat ditransmisikan melalui Internet atau melalui media. Berbagai jenis data akan memiliki nilai yang berbeda dan karenanya memiliki implikasi keamanan yang berbeda bagi pengguna komputasi awan. Misalnya, basis data pengguna di server komputasi awan mungkin memiliki nilai inti bagi pengguna komputasi awan dan dengan demikian memerlukan perlindungan yang kuat untuk menjamin kerahasiaan, integritas, dan ketersediaan data.

Informasi identitas pengguna dapat berisi *Personally Identifiable Information* (PII) dan berdampak pada privasi pengguna. Oleh karena itu, hanya pengguna yang berwenang harus diizinkan untuk mengakses informasi identitas pengguna. Menurut undang-undang perlindungan data pribadi no. 27 tahun 2022 data pribadi terdiri atas dua yaitu data pribadi yang bersifat spesifik dan data pribadi yang bersifat umum (Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, 2022). Data pribadi bersifat spesifik terdiri dari data dan informasi kesehatan, data biometrika, data genetika, catatan kejahatan, data anak, data keuangan pribadi dan/ atau data lainnya sesuai peraturan undang–undang. Data pribadi yang bersifat umum terdiri dari nama lengkap, jenis kelamin, agama, status perkawinan; dan atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang.

Data yang andal dapat meningkatkan standar hidup, menciptakan lapangan kerja, menaikkan pajak atas layanan data pemerintah, dan menghubungkan orang-orang dengan cara yang bermakna untuk mendukung penelitian dan penerapan kritis di berbagai bidang, serta mendorong inovasi dan

kewirausahaan. Di era ekonomi digital, data telah menjadi sumber daya yang strategis bagi suatu negara.

Tata kelola data melibatkan kedaulatan data, kedaulatan digital, transformasi digital, operasi digital, keamanan siber, dan keamanan data. Ini melibatkan banyak pemangku kepentingan, termasuk negara bagian, pemerintah, perusahaan, organisasi industri, dan konsumen. Tata kelola data lebih langsung berurusan dengan keseimbangan dan pertaruhan antara keterbukaan dan konservatif, multilateralisme dan isolasi, pembangunan ekonomi dan keamanan dunia maya, dan berdampak besar pada lanskap politik dan ekonomi global.

Tujuan akhir dari tata kelola data adalah untuk menciptakan nilai. Strategi keseluruhan adalah membuka nilai data yang andal. Pemerintah harus memimpin dalam membangun model tata kelola kolaboratif multi-*stakeholder* yang beradaptasi dengan ekonomi digital yang berkembang pesat dengan komputasi awan sebagai fondasinya. Negara, pemerintah, perusahaan, organisasi industri, dan konsumen harus lebih berpartisipasi dalam komunikasi dan kolaborasi tata kelola data global untuk membangun aturan dan berbagi nilai. Dalam implementasi layanan komputasi awan, berbagai negara telah membahas beberapa isu penting yang harus diperhatikan dalam memilih tata kelola keamanan layanan komputasi awan utama. Ini termasuk kedaulatan data, perlindungan privasi/informasi pribadi, klasifikasi data dan pedoman pemerintah, standar negara global, dan praktik terbaik untuk implementasi layanan komputasi awan.

### 6.3.1 Kedaulatan Data

Kedaulatan data mengacu pada konsep bahwa data tunduk pada hukum dan peraturan negara tempat data itu berada (Hummel et al., 2021). Artinya, pemerintah suatu negara berhak mengatur penyimpanan, pemrosesan, dan perpindahan data yang berasal dari dalam wilayahnya.

Kedaulatan data menjadi semakin penting karena semakin banyak organisasi dan individu yang menyimpan data di Komputasi awan, yang seringkali berlokasi di berbagai negara di seluruh dunia. Hal ini dapat menimbulkan tantangan bagi organisasi yang perlu mematuhi undang-undang perlindungan data yang berbeda di yurisdiksi yang berbeda. Untuk mengatasi tantangan ini, organisasi perlu mengetahui undang-undang dan peraturan perlindungan data di negara tempat mereka mengoperasikan atau menyimpan data. Mereka mungkin perlu menerapkan langkah-langkah seperti enkripsi data, residensi data, dan kontrol akses data untuk mematuhi peraturan ini. Penting juga bagi organisasi untuk bekerja sama dengan penyedia layanan komputasi awan yang mampu mematuhi undang-undang dan peraturan perlindungan data setempat.

Selanjutnya, dalam upaya perlindungan terhadap data pribadi Menurut *Privacy International* dalam (Prabowo et al., 2020) dikenal istilah perlindungan data (*data protection*). Definisi perlindungan data adalah sebuah aturan hukum yang bertujuan untuk memberikan perlindungan terhadap data pribadi yang dimiliki oleh seseorang. Bagi masyarakat modern, melindungi data dari penyalahgunaan adalah sangat penting. Itu sebabnya diperlukan hukum perlindungan data yang mengatur perusahaan dan pemerintah karena dua entitas ini memiliki peran yang signifikan untuk mencegah adanya penyelewengan oleh oknum yang tidak bisa dipertanggung jawabkan tindakannya.

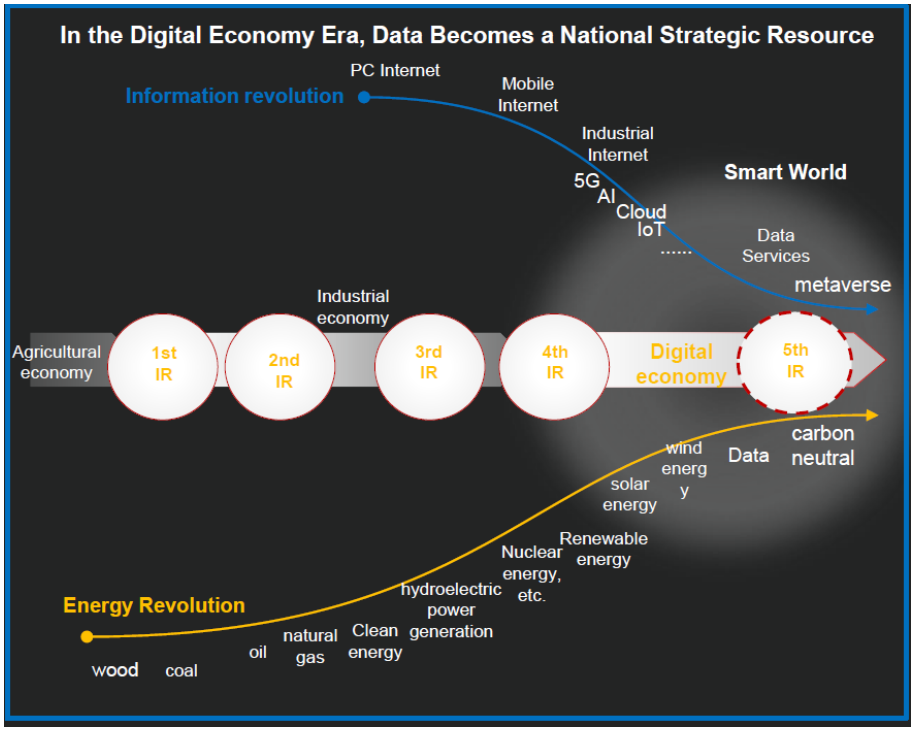
Jika tidak ada aturan hukum, banyak pihak akan dimudahkan dalam upayanya melakukan eksploitasi data. Globalisasi berjalan dengan sangat cepat dalam berbagai hal, termasuk pada aspek teknologi informasi yang di dalamnya terkait dengan keamanan siber dan kedaulatan data. Perkembangan media sosial yang begitu masif sudah tidak dapat dipisahkan dari perilaku keseharian setiap warga negara. Dalam setiap aplikasi baik media sosial maupun aplikasi lainnya di ruang siber mengandung begitu

banyak data yang harusnya terjamin keamanannya. Apabila hal ini disalahgunakan dapat menguntungkan kelompok tertentu dan merugikan sebagian kelompok lainnya (Aji, 2023).

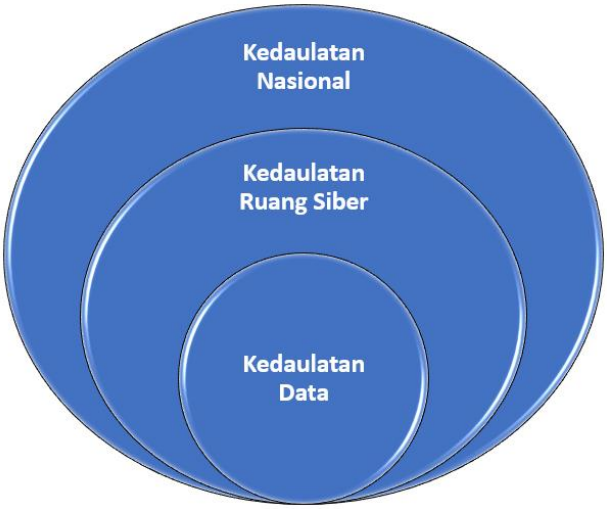
Definisi kedaulatan lebih umum berlaku untuk negara, sedangkan kedaulatan ruang siber, kedaulatan digital, dan kedaulatan data dapat memaksakan pembatasan kedaulatan pada aset informasi negara dari dimensi yang berbeda, menekankan independensi data nasional dan fasilitas terkait. Kedaulatan data dirumuskan sebagai = Kedaulatan nasional + TIK + Ruang siber + transfer data lintas batas sesuai dengan hukum, peraturan, dan standar.

Setiap negara memiliki konsep kedaulatan digitalnya masing-masing. Setiap perusahaan, institusi, organisasi, dan individu harus dengan tegas mendukung kedaulatan data nasional, serta strategi dan persyaratan kedaulatan digital nasional. Pada saat yang sama, kami menyerukan peningkatan daya saing ekonomi digital nasional melalui transfer data lintas batas sesuai dengan undang-undang, peraturan, dan standar.

Saat ini kita berada di era revolusi industri 4.0 di mana teknologi informasi terkini didorong oleh data seperti komputasi awan, AI, 5G dan IoT. Di era ekonomi digital, data menjadi sumber daya strategis nasional. Data sekarang dianggap sama berharganya dengan sumber daya alam lainnya seperti minyak atau gas, dan penting bagi bisnis untuk memanfaatkan sumber daya ini agar tetap kompetitif di pasar. Pemanfaatan data memungkinkan perusahaan untuk mendapatkan wawasan tentang perilaku pelanggan, tren pasar, dan mengoptimalkan operasi mereka. Selain itu, integrasi teknologi AI, 5G, dan IoT memungkinkan perusahaan mengotomatiskan proses, meningkatkan efisiensi, dan meningkatkan produktivitas. Hal ini akan menjadi landasan lahirnya era revolusi industri 5.0 (lihat Gambar 0-6)




*Gambar 0-6 Data sebagai sumber daya strategis sebuah negara*




Gambar 0-7 Hubungan kedaulatan data dengan kedaulatan nasional

**Kedaulatan nasional** (lihat Gambar 0-7): mengacu pada atribut paling penting yang membedakan suatu negara dari kelompok sosial lainnya. Ini adalah kekuatan tertinggi yang melekat pada suatu negara dan hak independennya di tingkat internasional. Kedaulatan nasional adalah atribut inti dari keamanan nasional, dan memastikan keamanan kedaulatan nasional adalah tugas dan misi inti dari keamanan nasional. Cakupannya darat, laut, udara, dan ruang siber, termasuk kemerdekaan, yurisdiksi, pertahanan, dan kesetaraan. Di era digital, ruang siber telah menjadi komponen kedaulatan nasional yang semakin kritis, karena keamanan infrastruktur informasi nasional dan aset data sangat penting untuk melindungi kepentingan nasional dan memastikan kesejahteraan warga negara.

**Kedaulatan ruang siber**: Merupakan perpanjangan alami dan ekspresi kedaulatan nasional di ruang siber. Secara internal, kedaulatan siber mengacu pada pengembangan, pengawasan, dan pengelolaan independen urusan Internet negara. Secara eksternal, kedaulatan siber berarti melindungi siber dari intrusi dan serangan luar.

**Kedaulatan digital**: Suatu negara memiliki kepemilikan dan yurisdiksi independen atas data, infrastruktur, dan teknologi digitalnya.

Kedaulatan data: Hak independen suatu negara untuk mengelola dan menggunakan datanya sendiri, dan bebas dari campur tangan dan intrusi negara lain, termasuk kepemilikan dan yurisdiksi.

Ciri terbesar dari kedaulatan data adalah kemerdekaan data, yaitu hak untuk sepenuhnya menguasai dan mengelola secara bebas data negara yang relevan, dan kemampuan untuk menghilangkan campur tangan asing, untuk menjamin keamanan dan stabilitas data negara terhadap negara lain, sangat erat. berkaitan dengan ketahanan nasional.

**Hak data** adalah konsep yang relatif baru, muncul sebagai tanggapan atas semakin pentingnya data dalam ekonomi dan masyarakat saat ini. Hak data

mengacu pada hak untuk memiliki, menggunakan, memanfaatkan, dan membuang properti data. Ini termasuk hak untuk mengontrol bagaimana data dikumpulkan, diproses, dan digunakan, serta hak untuk mengakses, memperbaiki, atau menghapus data pribadi. Hak data dapat dilihat sebagai bagian dari hak properti, yang secara tradisional mengacu pada hak untuk memiliki dan mengontrol properti fisik.

Hak data menjadi semakin penting karena semakin banyak data pribadi yang dikumpulkan, disimpan, dan digunakan oleh organisasi dan pemerintah. Hak data dapat membantu melindungi privasi individu, mencegah pelanggaran data, dan memastikan bahwa data digunakan dengan cara yang bermanfaat bagi masyarakat secara keseluruhan. Pada saat yang sama, hak data juga dapat menimbulkan tantangan bagi organisasi, terutama yang mengandalkan data untuk menjalankan model bisnisnya.

Untuk menyeimbangkan kebutuhan akan hak data dengan kebutuhan organisasi dan masyarakat, penting untuk menetapkan kerangka hukum dan peraturan yang jelas yang menentukan hak dan tanggung jawab pemilik, pengguna, dan regulator data. Ini termasuk mengembangkan aturan yang jelas seputar kepemilikan, penggunaan, dan pembuangan data, serta menetapkan standar untuk keamanan data dan perlindungan privasi. Selain itu, penting untuk mempromosikan literasi dan kesadaran data di antara individu, sehingga mereka dapat membuat keputusan yang tepat tentang bagaimana data mereka dikumpulkan, digunakan, dan dibagikan.

### 6.3.2 Keamanan dan Privasi Data

Menjaga keamanan dan melindungi hak privasi adalah masalah penting lainnya. Ada beberapa jenis data yang terdapat dalam basis data sektor publik, antara lain data pribadi dan bukan data pribadi. Pada saat yang sama, ini mungkin merupakan data penting pemerintah yang jika bocor atau terjatuh akan menyebabkan kerusakan serius. Jadi, seperti yang bisa dilihat,

hierarki data juga diklasifikasikan. Menjaga keamanan data itu; selain untuk menjaga privasi data pribadi mereka yang terlibat, melindungi kepentingan publik atau kepentingan sektor publik yang akan menjalankan tugasnya dan tidak dirugikan oleh fakta bahwa data tersebut bocor. Oleh karena itu, penggunaan komputasi awan merupakan bagian dari kekuatan pendorong tugas sektor publik.

Dengan demikian, ada kebutuhan untuk mengatasi masalah keamanan pemrosesan data yang terjadi di komputasi awan agar terstandarisasi dan memadai untuk menyimpan data sensitif. Namun, seperti disebutkan di atas, beberapa jenis data yang sangat sensitif menurut kebijakan atau undang-undang beberapa negara mungkin memiliki batasan untuk mengunggah data ke komputasi awan, atau dapat diunggah ke komputasi awan, tetapi ada persyaratan bahwa data tersebut harus ditempatkan dalam suatu sistem di dalam batas negara tersebut, atau yang dikenal dengan residensi data atau lokalisasi data.

Perlindungan data pribadi merupakan pertimbangan penting lainnya, terutama dalam GDPR (Proton AG, 2023). Penyedia layanan komputasi awan biasanya memiliki status pemroses data yang telah ditetapkan oleh pengontrol data. Mereka juga harus mematuhi undang-undang privasi, meskipun mereka tidak berlokasi di Eropa. Juga harus ada kontrak untuk memproses konten data pribadi sebagaimana diwajibkan oleh hukum. Selain itu, ada kewajiban hukum lainnya, misalnya hukum Eropa mengatur transfer data di luar wilayah negara anggota yang harus ada proses untuk memverifikasi bahwa tujuan memiliki tindakan perlindungan data pribadi yang memadai. Penyedia layanan komputasi awan juga harus dapat mematuhi undang-undang privasi dengan baik.

Persyaratan keamanan, termasuk perlindungan data pribadi tersebut, seringkali merupakan persyaratan dan pertimbangan yang digunakan dalam pengadaan penyedia layanan komputasi awan. Dengan demikian, ini dapat

didefinisikan sebagai kualifikasi dalam pengadaan, spesifikasi kontrak, atau bahkan kualifikasi penyedia layanan komputasi awan untuk mendapatkan akreditasi. Ini akan dapat menyediakan layanan komputasi awan untuk lembaga sektor publik juga.

Layanan keamanan dasar untuk keamanan informasi mencakup jaminan kerahasiaan, integritas, dan ketersediaan data. Dalam komputasi awan, masalah keamanan data menjadi lebih rumit karena karakteristik komputasi awan intrinsik. Untuk pengguna komputasi awan potensial dapat dengan aman memindahkan aplikasi data mereka ke komputasi awan, setelan layanan keamanan akan tersedia yang dapat diidentifikasi sebagai berikut (Yu et al., n.d.):

a. Jaminan kerahasiaan data: Layanan ini melindungi data agar tidak tertutup bagi pihak yang tidak sah. Pada komputasi awan, kerahasiaan data adalah layanan keamanan dasar yang harus ada. Meskipun aplikasi yang berbeda mungkin memiliki persyaratan yang berbeda dalam hal jenis data apa yang memerlukan perlindungan kerahasiaan, layanan keamanan ini dapat diterapkan untuk semua objek data yang dibahas di atas.
b. Perlindungan integritas data: Layanan ini melindungi data dari modifikasi berbahaya. Saat melakukan *outsourcing* data mereka ke server komputasi awan jarak jauh, pengguna komputasi awan harus memiliki cara untuk memeriksa apakah data mereka saat diam atau saat transit masih utuh atau tidak. Layanan keamanan semacam itu akan menjadi nilai inti bagi pengguna komputasi awan. Saat mengaudit layanan komputasi awan, juga merupakan kritik untuk menjamin bahwa semua data audit adalah asli karena data ini akan menjadi masalah hukum. Layanan keamanan ini juga berlaku untuk objek data lain yang dibahas di atas.
c. Jaminan ketersediaan data: Layanan ini memastikan bahwa data yang

disimpan di komputasi awan tersedia pada setiap permintaan pengambilan data dari pengguna. Jaminan ini sangat penting untuk data yang terdapat di server komputasi awan dan terkait dengan pemenuhan Layanan. Untuk layanan penyimpanan data jangka panjang, jaminan ketersediaan data lebih penting karena meningkatnya kemungkinan kerusakan atau kehilangan data dari waktu ke waktu.

d. Akses data yang aman: Layanan keamanan ini untuk membatasi pengungkapan konten data kepada pengguna yang berwenang. Dalam aplikasi praktis, mengungkapkan data aplikasi kepada pengguna yang tidak sah dapat mengancam tujuan bisnis pengguna komputasi awan. Dalam aplikasi yang sangat penting, pengungkapan data sensitif yang tidak tepat dapat menimbulkan masalah hukum. Untuk perlindungan yang lebih baik pada data sensitif, pengguna komputasi awan mungkin memerlukan kontrol akses data berbutir halus dalam arti bahwa pengguna yang berbeda mungkin memiliki akses ke kumpulan data yang berbeda.

e. Regulasi dan kepatuhan: Dalam skenario aplikasi praktis, penyimpanan dan akses data sensitif mungkin harus mematuhi kepatuhan tertentu. Untuk pemeriksaan, pengungkapan catatan kesehatan dapat dibatasi oleh *Health Insurance Portability and Accountability Act* (HIPAA) (HIPAA Home, n.d.). Selain itu, lokasi geografis data sering menjadi perhatian karena pelanggaran hukum ekspor. Pengguna komputasi awan harus meninjau masalah peraturan dan kepatuhan ini secara menyeluruh sebelum memindahkan data mereka ke komputasi awan.

f. Audisi layanan: Layanan ini menyediakan cara bagi pengguna komputasi awan untuk memantau bagaimana data mereka diakses dan sangat penting untuk penegakan kepatuhan. Dalam hal penyimpanan lokal, tidak sulit untuk mengaudit sistem. Namun, dalam komputasi

awan, diperlukan penyedia layanan untuk mendukung transparansi akses data yang dapat dipercaya (S. K. Das et al., 2012).

### 6.3.3 Klasifikasi Data

Klasifikasi data adalah proses menetapkan level data dan menentukan level sensitivitas data, level sensitivitas data ini salah satunya dapat ditentukan dari unsur kerahasiaan, integritas dan ketersediaan data (Singh et al., 2018). Data diklasifikasikan berdasarkan beberapa aspek, contohnya, nilai data atau risiko yang terkait dengan pengungkapan data. Level akan menentukan penanganan data tersebut termasuk pembuatan, modifikasi, penyimpanan, dan transmisi data. Dalam lingkungan komputasi awan, untuk memberikan akses otoritas dan kontrol, mengklasifikasikan data berdasarkan tingkatan keamanannya menjadi area penting bagi penggunanya dan penyedia layanan komputasi awan. Lebih lanjut, klasifikasi data dalam komputasi awan dapat mengurangi biaya dan waktu karena data ditangani secara berbeda berdasarkan klasifikasinya masing-masing.

Meskipun layanan komputasi awan memiliki banyak keunggulan salah satu perhatian untuk menggunakan layanan komputasi awan adalah data yang dapat disimpan atau diproses di komputasi awan. Masalah ini menimbulkan pertanyaan tentang jenis data apa yang dapat diunggah ke komputasi awan dan siapa yang dapat mengaksesnya. Organisasi harus memastikan bahwa data sensitif seperti informasi pelanggan, catatan keuangan, dan kekayaan intelektual dilindungi dan diamankan di komputasi awan. Penyedia layanan komputasi awan biasanya menawarkan fitur keamanan seperti enkripsi, kontrol akses, dan pemantauan untuk melindungi data yang disimpan di komputasi awan. Namun, merupakan tanggung jawab organisasi untuk memastikan bahwa data diamankan dengan benar dan kontrol akses diatur dengan benar untuk mencegah akses yang tidak sah.

Pertanyaan lain mungkin tentang mendapatkan data penting terkait pelaksanaan tugas sektor publik, atau bahkan data pribadi yang dapat diunggah ke komputasi awan penyedia layanan mana pun. Dalam mengikuti masalah di atas, klasifikasi tipe data dan penerapannya untuk mengakses sistem komputasi awan tertentu merupakan masalah utama dan merupakan bagian dari kebijakan atau strategi komputasi awan.

Klasifikasi tipe data dan penerapannya untuk mengakses sistem komputasi awan tertentu sangat penting untuk keamanan data. Jenis data yang berbeda memiliki tingkat sensitivitas yang berbeda, dan karena itu memerlukan tingkat kontrol keamanan yang berbeda. Misalnya, data pribadi seperti rekam medis, informasi keuangan, atau informasi rahasia lainnya memerlukan tingkat kontrol keamanan yang lebih tinggi daripada informasi publik seperti data cuaca atau catatan publik. Organisasi perlu menetapkan kebijakan atau strategi komputasi awan yang menguraikan jenis data yang dapat disimpan di komputasi awan, siapa yang dapat mengaksesnya, dan kontrol keamanan yang perlu diterapkan. Kebijakan atau strategi harus didasarkan pada penilaian risiko menyeluruh yang mengidentifikasi potensi ancaman dan kerentanan terhadap data dan sistem yang memproses dan menyimpan data.

## 6.4 Potensi Pemanfaatan Komputasi Awan

Komputasi awan telah muncul sebagai teknologi transformatif, menawarkan banyak peluang bagi bisnis dan pemerintah di seluruh dunia. Di Indonesia, pengadopsian komputasi awan menghadirkan pintu gerbang menuju peningkatan efisiensi, skalabilitas, dan inovasi di berbagai sektor industri serta sektor pemerintahan. Berikut berbagai peluang pemanfaatan komputasi awan pada berbagai sektro industry.

**Industri Manufaktur**

Komputasi awan memungkinkan produsen untuk mengoptimalkan operasi rantai pasokan mereka dengan memfasilitasi kolaborasi waktu nyata dan

berbagi data. Melalui solusi berbasis *cloud*, produsen dapat merampingkan manajemen inventaris, meningkatkan perencanaan produksi, dan meningkatkan efisiensi operasional secara keseluruhan. Skalabilitas *cloud* juga memungkinkan bisnis beradaptasi dengan permintaan pasar yang berfluktuasi dan menykalakan sumber daya komputasi mereka sesuai kebutuhan.

***E-Commerce* dan Ritel:**

Pertumbuhan pesat *e-commerce* di Indonesia membutuhkan infrastruktur yang kuat untuk mendukung bisnis online. Komputasi awan menawarkan solusi yang dapat diskalakan dan hemat biaya untuk platform e-niaga, memungkinkan pengalaman pelanggan yang mulus, pemrosesan pembayaran yang aman, dan manajemen inventaris yang efisien. Kemampuan komputasi awan untuk menangani volume data dan lalu lintas yang besar memastikan operasi tanpa gangguan selama periode puncak, berkontribusi pada pertumbuhan bisnis.

**Pendidikan:**

Komputasi awan dapat membantu institusi pendidikan untuk meningkatkan kualitas pengajaran dan pembelajaran mereka, sekaligus mengurangi biaya. Misalnya, sistem manajemen pembelajaran berbasis *cloud* dapat membantu institusi untuk menyampaikan kursus online, sementara alat kolaborasi berbasis *cloud* dapat membantu siswa untuk bekerja sama dalam proyek.

**Kesehatan**:

Komputasi awan dapat membantu penyedia layanan kesehatan untuk meningkatkan kualitas perawatan yang mereka berikan, sekaligus mengurangi biaya. Misalnya, catatan riwayat kesehatan elektronik dapat membantu penyedia untuk melacak catatan pasien, sementara sistem *telemedicine* berbasis *cloud* dapat membantu mereka memberikan perawatan kepada pasien yang tinggal di daerah terpencil.

**SPBE:**

Komputasi awan memainkan peran penting dalam mengubah sektor pemerintahan dengan memungkinkan penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE). Dengan memanfaatkan infrastruktur *cloud*, pemerintah dapat merampingkan proses administrasi, meningkatkan pemberian layanan, dan meningkatkan keterlibatan masyarakat. SPBE berbasis *cloud* menawarkan penyimpanan data terpusat, manajemen dokumen yang efisien, dan akses yang aman ke layanan publik, mendorong transparansi dan akuntabilitas.

Komputasi awan memberdayakan pemerintah untuk memanfaatkan potensi analitik data besar untuk pengambilan keputusan yang tepat. Dengan *memusatkan* penyimpanan data dan memanfaatkan alat analitik berbasis cloud, lembaga pemerintah dapat memperoleh wawasan berharga dari kumpulan data yang luas. Pendekatan berbasis data ini memungkinkan alokasi sumber daya yang efisien, perumusan kebijakan, dan tata kelola proaktif, yang pada akhirnya menguntungkan warga negara dan mendorong pembangunan sosial-ekonomi.

Komputasi awan menghadirkan peluang besar bagi Indonesia, mencakup berbagai sektor industri dan sektor pemerintah. Skalabilitas, efisiensi biaya, dan kemampuannya yang canggih memberdayakan bisnis untuk mengoptimalkan operasi, mendorong inovasi, dan mendapatkan keunggulan kompetitif. Di sektor pemerintah, SPBE berbasis *cloud* merevolusi pemberian layanan publik, meningkatkan manajemen data, dan meningkatkan ketahanan bencana. Untuk memanfaatkan sepenuhnya peluang ini, organisasi dan lembaga pemerintah harus memprioritaskan keamanan data, privasi, dan kepatuhan terhadap peraturan.

### 6.4.1 Analisis Risiko dan Peluang Keamanan Komputasi Awan di Indonesia

Analisis peluang dan risiko keamanan komputasi awan di Indonesia mengungkapkan lanskap yang menjanjikan dengan potensi pertumbuhan yang signifikan. Dukungan dan promosi pemerintah Indonesia terhadap adopsi *cloud*, seiring dengan pertumbuhan ekonomi digital, menghadirkan peluang bagi bisnis untuk memanfaatkan layanan *cloud* untuk penghematan biaya dan perluasan pasar. Kemajuan teknologi, seperti peningkatan alat keamanan siber dan solusi keamanan *cloud-native*, semakin meningkatkan langkah-langkah keamanan yang tersedia. Namun, risiko memang ada, termasuk masalah kedaulatan data dan masalah privasi. Selain itu, lanskap ancaman yang berkembang dan kompleksitas kepatuhan terhadap undang-undang dan peraturan perlindungan data menuntut kewaspadaan yang berkelanjutan. Mengatasi risiko ini melalui peraturan yang kuat, investasi dalam program pendidikan dan kesadaran, serta kemajuan berkelanjutan dalam teknologi keamanan siber akan sangat penting untuk memastikan adopsi dan pemanfaatan komputasi awan yang aman di Indonesia.

Berikut merupakan analisis PESTLE (*Political, Economic, Social, Technological, Legal and Environmental*) dari peluang dan risiko yang terkait dengan keamanan komputasi awan di Indonesia.

*Tabel 6-1 Analisis PESTLE keamanan komputasi awan di Indonesia*

| Faktor | Peluang | Risiko |
|---|---|---|
| Politik | Dukungan pemerintah dalam mempromosikan adopsi komputasi awan. | Kepemilikan data yang harus memenuhi persyaratan lokal. |
| | Kerangka regulasi yang kuat untuk perlindungan data dan keamanan siber. | Perubahan kebijakan pemerintah yang dapat |

| Faktor | Peluang | Risiko |
|---|---|---|
| | | mempengaruhi persyaratan keamanan komputasi awan. |
| Ekonomi | Penghematan biaya melalui penggunaan komputasi awan. | Ketidakstabilan ekonomi yang dapat mempengaruhi ketersediaan dan biaya layanan komputasi awan. |
| | Pertumbuhan pasar digital yang memberikan peluang bagi penyedia layanan komputasi awan. | Keterbatasan sumber daya keuangan bagi organisasi kecil yang ingin mengadopsi solusi komputasi awan yang aman. |
| Sosial | Peningkatan literasi digital dan kesadaran akan pentingnya keamanan komputasi awan. | Kekhawatiran privasi yang dapat menghambat adopsi komputasi awan. |
| | Budaya kerja jarak jauh yang meningkatkan permintaan akan alat dan solusi kolaborasi berbasis komputasi awan yang aman. | Kurangnya edukasi dan kesadaran mengenai langkah-langkah keamanan komputasi awan. |
| Teknologi | Kemajuan keamanan siber, seperti dan deteksi ancaman berbasis kecerdasan buatan. | Ancaman keamanan siber yang terus berkembang. |
| | Adopsi alat dan layanan keamanan yang dioptimalkan untuk komputasi awan. | Sistem legacy yang menghambat integrasi dan migrasi yang aman ke lingkungan komputasi awan. |
| | | infrastruktur telekomunikasi kurang merata terutama di daerah terpencil. |
| Hukum | Keberadaan UU PDP sebagai payung hukum perlindungan data | Tantangan kepatuhan terhadap regulasi dan lembaga penegak perlindungan data |

| Faktor | Peluang | Risiko |
|---|---|---|
| | | Pemerintah Indonesia belum memberlakukan undang-undang atau peraturan khusus yang mengatur keamanan komputasi awan |
| Lingkungan | Penggunaan komputasi hijau yang mengoptimalkan sumber daya dan mengurangi jejak karbon. | pemerintah belum memberlakukan peraturan khusus yang mengatur dampak lingkungan dari komputasi awan |

Analisis PESTLE tersebut menunjukkan bahwa terdapat peluang yang menjanjikan dalam keamanan komputasi awan di Indonesia, didorong oleh dukungan pemerintah, penghematan biaya, dan kemajuan teknologi. Namun, terdapat pula risiko terkait kepemilikan data, ketidakstabilan ekonomi, dan kekhawatiran privasi. Perubahan kebijakan politik, keterbatasan sumber daya bagi organisasi kecil, dan kebutuhan akan peningkatan edukasi dan kesadaran mengenai keamanan *cloud* menjadi tantangan yang harus diatasi.

Ancaman keamanan siber yang terus berkembang dan kompleksitas kepatuhan terhadap regulasi perlindungan data juga memerlukan kewaspadaan yang berkelanjutan. Dalam menghadapi risiko-risiko tersebut, regulasi yang kuat, investasi dalam program edukasi dan kesadaran, serta kemajuan teknologi keamanan siber yang berkelanjutan menjadi kunci dalam memastikan adopsi dan penggunaan komputasi awan yang aman di Indonesia.

### 6.4.2 Analisis SWOT Terhadap Keamanan Komputasi Awan di Indonesia

Keamanan layanan komputasi awan di Indonesia menjadi perhatian yang berkembang karena bisnis dan individu semakin mengandalkan teknologi berbasis komputasi awan untuk menyimpan dan mengelola data. Meskipun ada banyak penyedia layanan komputasi awan terkemuka yang beroperasi di Indonesia, ada beberapa insiden keamanan tingkat tinggi dalam beberapa tahun terakhir, yang menyoroti perlunya langkah-langkah keamanan yang lebih kuat.

Pemerintah Indonesia telah menyadari pentingnya keamanan komputasi awan dan telah mengimplementasikan regulasi seperti UU PDP, PP No. 71 Tahun 2019 tentang PSTE. Peraturan ini mengamanatkan bahwa penyedia layanan komputasi awan menerapkan langkah-langkah keamanan untuk melindungi data pribadi, termasuk enkripsi, kontrol akses, dan pencadangan data.

Terlepas dari peraturan tersebut, masih ada kekhawatiran seputar keamanan layanan komputasi awan di Indonesia. Banyak usaha kecil dan menengah mungkin tidak memiliki sumber daya atau keahlian yang diperlukan untuk menilai keamanan penyedia layanan komputasi awan secara efektif, membuat mereka rentan terhadap ancaman keamanan. Ditambah juga dengan kurangnya kepercayaan di antara klien dalam keamanan layanan komputasi awan karena insiden keamanan profil tinggi yang dilaporkan di masa lalu.

Ada beberapa kasus besar pelanggaran keamanan komputasi awan di Indonesia dalam beberapa tahun terakhir (Purnama et al., 2022). Pelanggaran data Tokopedia: pada Mei 2020, raksasa e-*commerce* Tokopedia mengumumkan bahwa data pribadi lebih dari 90 juta penggunanya telah dicuri dan dijual di *dark web*. Data yang dicuri termasuk nama, alamat email,

nomor telepon, dan kata sandi *hash*. Belakangan terungkap bahwa pelanggaran tersebut terjadi karena kerentanan pada penyedia layanan komputasi awan pihak ketiga yang digunakan oleh Tokopedia. Pelanggaran data Bhinneka: Pada tahun 2019, situs jual beli *online* Bhinneka mengalami pelanggaran data yang mengungkap informasi pribadi sekitar 2 juta pelanggannya. Pelanggaran terjadi karena kerentanan dalam penyedia layanan komputasi awan yang digunakan oleh Bhinneka, yang memungkinkan peretas mendapatkan akses tidak sah ke basis data perusahaan.

Berikut merupakan hasil analisis SWOT keamanan layanan komputasi awan di Indonesia:

**Kekuatan (*Strengths*):**

a. S1: Indonesia memiliki pasar yang berkembang untuk layanan komputasi awan, perekonomian digital Indonesia berkembang pesat, yang menciptakan permintaan untuk layanan komputasi awan.
b. S2: Ada beberapa peraturan pemerintah Indonesia, seperti UU PDP dan PP PSTE 71/2019, yang mengamanatkan penyedia layanan komputasi awan untuk menerapkan langkah-langkah keamanan dan memastikan privasi dan perlindungan data.
c. S3: Penyedia layanan komputasi awan di Indonesia dapat memanfaatkan penilaian mandiri melalui indeks KAMI untuk menunjukkan komitmen mereka terhadap keamanan komputasi awan.
d. S4: Dukungan pemerintah Indonesia mendukung adopsi teknologi dan komputasi awan melalui kebijakan seperti "*Making Indonesia 4.0*". SPBE, satu data Indonesia yang memperkuat kepercayaan dan pertumbuhan industri komputasi awan.
e. S5: Bonus demografi dari populasi Indonesia yang masih muda dan melek teknologi, yang menciptakan sejumlah besar pelanggan potensial untuk memperkuat keamanan layanan komputasi awan.

f. S6: Terdapat Standar Kompetensi Kerja Nasional Indonesia (SKKNI) di bidang komputasi awan dapat membantu meningkatkan keamanan layanan komputasi awan di Indonesia

**Kelemahan (*Weaknesses*):**

a. W1: Kekurangan tenaga ahli menerapkan langkah-langkah keamanan yang kuat, serta sumber daya manusia untuk mengimplementasikan dan memelihara keamanan komputasi awan yang memadai.
b. W2: Terdapat kurangnya kepercayaan di antara klien Indonesia dalam keamanan layanan komputasi awan karena insiden keamanan profil kebocoran data yang dilaporkan di masa lalu.
c. W3: Pemerintah Indonesia belum memberlakukan regulasi yang tegas terkait kedaulatan data, klasifikasi data, residensi data dan aliran data lintas batas.
d. W4: Pemerintah Indonesia belum memiliki indeks maturitas yang mengukur kematangan keamanan komputasi awan maupun audit keamanan untuk layanan komputasi awan.
e. W5: Undang-undang dan peraturan pemerintah Indonesia terkait perlindungan data pribadi masih relatif baru, belum ada badan independen yang ditunjuk untuk menegakkan perlindungan data pribadi.
f. W6: Kesadaran dan pemahaman masyarakat mengenai keamanan layanan komputasi awan masih relatif rendah.

**Peluang (*Opportunities*):**

a. O1: Inovasi teknologi informasi di bidang keamanan siber, seperti kecerdasan buatan dan analisis prediktif, dapat membantu mengatasi tantangan keamanan dan meningkatkan efektivitas sistem keamanan layanan komputasi awan.
b. O2: Ada sejumlah penyedia layanan komputasi awan asing terkemuka di Indonesia. Mereka memberikan peluang untuk menghadirkan

teknologi canggih, keahlian, dan praktik terbaik dalam keamanan komputasi awan di pasar Indonesia

c. 03: Pemerintah Indonesia dapat berkolaborasi dengan industri untuk membuat peraturan dan standar baru terkait keamanan layanan komputasi awan. Hal tersebut diharapkan dapat mengatasi ancaman keamanan yang muncul dan memastikan perlindungan data klien.

d. O4: Pemerintah Indonesia dapat memberikan insentif dan dukungan bagi penyedia layanan komputasi awan untuk berinvestasi dalam langkah-langkah keamanan dan meningkatkan postur keamanan mereka secara keseluruhan.

## Ancaman (*Threats*):

a. T1: Ancaman keamanan siber, seperti peretasan, pembobolan data, dan serangan *malware* yang terus meningkat secara global, dan penyedia layanan komputasi awan Indonesia masih rentan terhadap ancaman.

b. T2: Para pelaku kriminal di ruang siber dapat secara khusus menargetkan bisnis Indonesia dengan persepsi bahwa bisnis-bisnis tersebut mungkin memiliki tingkat keamanan siber yang lemah.

c. T3: Kurangnya kepercayaan masyarakat terhadap keamanan layanan komputasi awan dapat mengakibatkan bisnis Indonesia ragu untuk mengadopsi layanan komputasi awan, yang dapat membatasi peluang pertumbuhan penyedia layanan komputasi awan di Indonesia.

d. T4: Laju perkembangan teknologi yang cepat dapat mempersulit penyedia maupun pengguna layanan komputasi awan untuk mengikuti perkembangan ancaman keamanan yang muncul dan menerapkan langkah-langkah keamanan yang diperlukan.

e. T5: Undang-undang dan peraturan pemerintah Indonesia terkait keamanan komputasi awan yang kurang tegas dapat dielakkan oleh oknum jahat.

Analisis SWOT ini menyoroti kebutuhan penyedia layanan komputasi awan Indonesia untuk berinvestasi dalam langkah-langkah keamanan dan mematuhi peraturan dan standar yang relevan untuk memastikan perlindungan data pribadi konsumen. Pemerintah Indonesia dapat berperan penting dalam mendukung industri ini dengan menciptakan lingkungan peraturan yang menguntungkan, memberikan insentif dan dukungan, serta meningkatkan kesadaran akan keamanan komputasi awan di kalangan bisnis dan konsumen.

### 6.4.3 Evaluasi Keamanan Komputasi Awan di Indonesia

Analisis SWOT yang dilakukan terhadap keamanan layanan komputasi awan di Indonesia mengungkapkan beberapa temuan kunci. Dalam hal kekuatan, pasar Indonesia yang berkembang untuk layanan komputasi awan, didukung oleh ekonomi digital yang berkembang pesat, menghadirkan peluang yang signifikan bagi industri ini. Selain itu, peraturan pemerintah yang ada, seperti UU PDP dan PP PSTE 71/2019, mengamanatkan tindakan keamanan dan perlindungan privasi data, memberikan dasar yang kuat untuk meningkatkan keamanan komputasi awan. Kehadiran indeks KAMI memungkinkan penyedia layanan untuk menunjukkan komitmen mereka terhadap keamanan. Dukungan pemerintah Indonesia untuk adopsi dan inisiatif teknologi seperti "Making Indonesia 4.0" semakin memperkuat prospek pertumbuhan industri. Populasi muda dan paham teknologi di negara ini juga berkontribusi pada potensi untuk memperkuat keamanan komputasi awan.

Tidak adanya indeks kematangan atau audit keamanan untuk layanan komputasi awan, serta undang-undang yang relatif baru tentang perlindungan data pribadi, semakin menambah tantangan. Kesadaran dan pemahaman publik tentang keamanan komputasi awan ditemukan relatif

rendah. Berdasarkan analisis SWOT, dapat diambil beberapa strategi dari setiap pasangan kelemahan dan ancaman yang ada sesuai dengan tabel 6-2:

*Tabel 6-2 Strategi perbaikan dari poin-poin kelemahan dan ancaman*

| Poin Perbaikan | Strategi |
|---|---|
| W1 dan T1 | 1. Membentuk program pengembangan keterampilan dan pelatihan yang difokuskan pada keamanan komputasi awan untuk profesional TI dan pemangku kepentingan terkait.<br>2. Berkolaborasi dengan institusi pendidikan dan industri untuk mengembangkan kursus dan sertifikasi keamanan komputasi awan.<br>3. Mendorong CSP untuk menginvestasikan program pelatihan bagi karyawan dan pengguna mereka dalam menerapkan langkah-langkah keamanan yang kuat.<br>4. Memfasilitasi kemitraan antara industri dan akademisi untuk mendorong penelitian dan pengembangan dalam keamanan komputasi awan. |
| W2 dan T2 | 1. Mengimplementasikan protokol dan langkah-langkah keamanan yang ketat untuk mencegah pelanggaran data pribadi.<br>2. Meningkatkan transparansi dengan memberikan informasi yang jelas dan rinci tentang langkah-langkah keamanan, sertifikasi kepatuhan, dan praktik perlindungan data yang diimplementasikan oleh penyedia layanan komputasi awan.<br>3. Melakukan audit keamanan secara berkala untuk mengidentifikasi kerentanan dan mengatasinya dengan cepat.<br>4. Berkolaborasi dengan pihak auditor keamanan independen untuk memvalidasi praktik keamanan dan membangun kepercayaan di antara klien. |
| W3 dan T3 | 1. Berkolaborasi dengan ahli industri, pemangku kepentingan, dan organisasi internasional untuk mengembangkan regulasi dan panduan yang komprehensif terkait kedaulatan data, klasifikasi data, tempat penyimpanan data, dan aliran data lintas batas. |

| Poin Perbaikan | Strategi |
|---|---|
| | 2. Meninjau dan memperbarui regulasi yang ada untuk sejalan dengan standar internasional dan praktik terbaik.<br>3. Membentuk lembaga regulasi atau memperkuat badan yang ada untuk menegakkan dan memantau kepatuhan terhadap regulasi keamanan komputasi awan.<br>4. Mendorong dialog dan kolaborasi antara pemerintah, industri, dan masyarakat untuk memastikan regulasi menemukan keseimbangan antara keamanan dan kekhawatiran privasi. |
| W4 dan T4 | 1. Mengembangkan indeks kematangan keamanan komputasi awan yang menyediakan standar untuk menilai praktik keamanan CSP.<br>2. Berkolaborasi dengan asosiasi industri dan pakar untuk membentuk kerangka kerja audit keamanan yang mengevaluasi keamanan layanan komputasi awan.<br>3. Mendorong adopsi indeks kematangan dan kerangka kerja audit keamanan oleh CSP untuk akuntabilitas dalam praktik keamanan. |
| W5 dan T5 | 1. Mempercepat implementasi dan penegakan hukum terhadap hukum dan regulasi perlindungan data pribadi yang sudah ada. 2. Mendirikan lembaga independen atau menunjuk otoritas yang ada untuk mengawasi dan menegakkan regulasi perlindungan data pribadi.<br>3. Melakukan kampanye kesadaran publik untuk mengedukasi individu dan organisasi tentang hak dan tanggung jawab mereka terkait perlindungan data pribadi.<br>4. Berkolaborasi dengan badan dan organisasi internasional untuk menerapkan standar, praktik terbaik dan belajar dari pengalaman global dalam perlindungan data pribadi. |
| W6 | 1. Melakukan kampanye kesadaran publik untuk mengedukasi bisnis, individu, dan masyarakat umum tentang manfaat, risiko, dan aspek keamanan komputasi awan.<br>2. Mengembangkan dan mendistribusikan informasi, pedoman, dan dokumen praktik terbaik untuk meningkatkan pengetahuan dan pemahaman tentang keamanan komputasi awan. |

| Poin Perbaikan | Strategi |
|---|---|
| | 3. Membentuk kemitraan dengan media, institusi pendidikan, dan asosiasi industri untuk mempromosikan kesadaran keamanan komputasi awan melalui workshop atau seminar.<br>4. Membuat kemitraan antara pemerintah, sektor swasta, dan akademisi untuk mengembangkan kurikulum tentang keamanan komputasi awan dalam program pendidikan dan pelatihan. |

Dengan memasangkan kelemahan dengan ancaman yang teridentifikasi, strategi ini bertujuan untuk mengurangi risiko dan memperkuat keamanan layanan komputasi awan secara keseluruhan di Indonesia. Pada tabel 6-3 merupakan hasil analisis pasangan antara kekuatan dan peluang untuk menangkap atau memanfaatkan peluang melalui kekuatan yang ada. Dengan menyelaraskan kekuatan dengan peluang yang sesuai, strategi ini dapat secara efektif memanfaatkan kemampuan yang ada untuk menangkap atau memanfaatkan peluang yang teridentifikasi dalam lanskap keamanan komputasi awan di Indonesia.

*Tabel 6-3 Poin-poin strategi untuk mewujudkan sinergi antara kekuatan dan peluang*

| Poin Sinergi | Strategi |
|---|---|
| S1 dan O1 | Mendorong investasi dalam penelitian dan pengembangan teknologi keamanan yang inovatif dan memanfaatkan teknologi kecerdasan buatan dan analisis prediktif untuk meningkatkan keamanan layanan komputasi awan di Indonesia. |
| S2 dan O2 | Mendorong kolaborasi antara penyedia layanan komputasi awan asing dan lokal untuk mentransfer pengetahuan, teknologi, dan praktik terbaik dalam keamanan komputasi awan. |

| Poin Sinergi | Strategi |
|---|---|
| S3 dan O3 | Mengembangkan indeks kematangan keamanan komputasi awan yang diperoleh dari penilaian mandiri KAMI dan kolaborasi dengan penyedia layanan komputasi awan untuk menerapkan standar keamanan yang lebih tinggi. |
| S4 dan O4 | Memberikan insentif pajak atau dukungan keuangan kepada penyedia layanan komputasi awan yang aktif berinvestasi dalam keamanan dan mematuhi standar keamanan yang lebih tinggi. |
| S5 dan O1 | Melakukan kampanye pemasaran yang efektif untuk meningkatkan kesadaran dan pemahaman masyarakat tentang keamanan komputasi awan, dengan menyoroti keuntungan dan perlindungan yang ditawarkan oleh teknologi kecerdasan buatan dan analisis prediktif. |
| S6 dan O3 | Mengintegrasikan SKKNI komputasi awan dengan regulasi dan standar baru yang dikembangkan oleh pemerintah dan industri untuk memastikan adopsi praktik keamanan yang konsisten dalam layanan komputasi awan di Indonesia. |

# BAB 7

# STRATEGI MEWUJUDKAN KEAMANAN KOMPUTASI AWAN DAN TATA KELOLA DATA DI INDONESIA

Pada era digital saat ini, data telah menjadi sumber daya yang sangat berharga bagi pemerintah dan perusahaan untuk mengambil keputusan yang tepat dan mengoptimalkan kinerja mereka. Namun, penting bagi mereka untuk memastikan bahwa data yang mereka miliki andal dan dilindungi dengan baik. Oleh karena itu, dalam bab terakhir ini kami akan membahas tentang kerangka kerja dan tata kelola yang diperlukan untuk meningkatkan nilai data yang andal dan mempercepat transformasi digital di pemerintahan maupun perusahaan. Selain itu, kami akan membahas tentang pentingnya kolaborasi antara sektor publik dan swasta dalam membangun ekosistem digital yang tangguh. Kami juga akan menyoroti beberapa langkah yang dapat diambil untuk meningkatkan daya saing ekonomi digital nasional dan menjaga kedaulatan data nasional dari sisi perspektif ekonomi dan keamanan siber.

## 7.1 Rancangan Kerangka Kerja & Tata Kelola Keamanan Komputasi Awan Indonesia

Kami mengusulkan kerangka kerja dan tata kelola untuk meningkatkan nilai data yang andal serta mempercepat transformasi digital baik di pemerintahan

maupun perusahaan. Tata kelola data tersebut perlu ditimbang dari perspektif kedaulatan, pembangunan ekonomi, dan keamanan siber. Untuk mencapai hal ini, penting untuk membangun kerangka kerja tata kelola data yang kuat yang melindungi privasi, keamanan individu dan organisasi sambil memfasilitasi aliran data lintas batas. Pemerintah juga harus berinvestasi dalam infrastruktur digital dan mempromosikan adopsi teknologi baru seperti komputasi awan, 5G, AI, *blockchain*, dan IoT. Perusahaan, di sisi lain, harus mengadopsi pola pikir yang mengutamakan digitalisasi dan memanfaatkan wawasan berbasis data untuk mendorong inovasi serta meningkatkan daya saing mereka di pasar global.

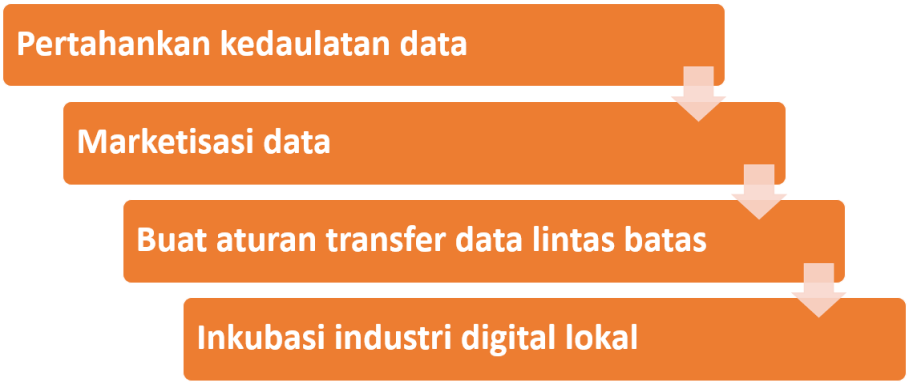
Selain itu, kolaborasi antara sektor publik dan swasta sangat penting dalam membangun ekosistem digital yang tangguh yang dapat bertahan dari ancaman dunia maya dan peristiwa yang mengganggu lainnya. Ini membutuhkan kerja sama yang erat antara lembaga pemerintah, asosiasi industri, dan akademisi untuk mengembangkan dan menerapkan kebijakan dan standar yang mendorong keamanan dunia maya dan memungkinkan inovasi digital. Dengan strategi dan investasi yang tepat, negara dan perusahaan dapat sepenuhnya mewujudkan potensi transformatif TIK dan membangun masa depan yang lebih sejahtera, berkelanjutan, dan aman untuk semua.

Untuk meningkatkan daya saing ekonomi digital nasional dan menjaga kedaulatan data nasional, mengacu pada langkah-langkah berikut:

a. **Pertahankan kedaulatan data nasional**; Terapkan undang-undang residensi data, lokalisasi data, pastikan data tidak akan diambil secara gratis dan hindari kolonisasi digital.
b. **Marketisasi data**; transformasi digital pemerintah, transformasi digital industri, dan bangun kerangka kerja, standar, dan aturan transaksi data.

c. **Rumuskan aturan untuk transfer data lintas batas**; pastikan bahwa semua pemangku kepentingan di setiap negara mendapat manfaat dari transaksi data yang andal.

d. **Inkubasi industri digital lokal**; percepat pengembangan divisi industri data lokal: pembersihan data lokal, layanan data, dan adaptasi produk cerdas lokal.




*Gambar 0-1 Langkah-langkah meningkatkan daya saing ekonomi digital dan menjaga kedaulatan data nasional*

Solusi implementasinya diuraikan dalam 7 langkah sebagai berikut:

**a.** **Pemerintah memimpin dalam merumuskan tata kelola data terlebih dahulu, strategi data, membuat undang-undang tentang residensi data, dan menjaga kedaulatan data nasional**.

Tujuan akhir tata kelola data adalah untuk menciptakan nilai. Kematangan tata kelola data pemerintah merupakan syarat mutlak untuk meningkatkan daya saing ekonomi digital suatu negara. Disarankan untuk meningkatkan daya saing ekonom digital nasional perlu menyeimbangkan perspektif ekonomi dan keamanan siber (Gambar 0-1).

**Perspektif e**konomi: Aliran data yang legal, patuh standar, dan kondusif untuk pengembangan industri. Pemerintah memimpin dalam

membangun mekanisme manajemen dan monetisasi untuk menciptakan nilai dengan menyediakan layanan data dan lebih mendukung perkembangan ekonomi digital yang sehat dan cepat.

**Perspektif keamanan siber**: Pemerintah memimpin dalam penerapan "penyimpanan lokal + pengawasan lintas batas" untuk data sensitif berdasarkan klasifikasi data, dan menetapkan mekanisme pemantauan, standar audit, standar keamanan, dan sistem sertifikasi.


*Gambar 0-2 Meningkatkan daya saing ekonomi digital nasional*

Menilik kebijakan tata kelola data di Indonesia, terdapat PP No. 71 Tahun 2019, di mana dalam pasal 21 ayat 1 menyatakan: "*PSE lingkup privat dapat melakukan pengelolaan, pemrosesan, dan/atau penyimpanan data elektronik di wilayah Indonesia dan/atau di luar wilayah Indonesia.*" Melalui PP tersebut pemerintah telah memberikan lampu hijau kepada PSE swasta dan aplikasi-aplikasi yang berasal dari negara lain untuk bisa menyimpan data di luar wilayah Indonesia. Hal ini tidak sejalan dengan konsep kedaulatan data. PP tersebut sangat kontradiktif dengan pesan-pesan yang disampaikan oleh bapak presiden Ir. H. Joko Widodo dalam berbagai pidato kenegaraan kepresidenan, yaitu:

Pidato kenegaraan pada tanggal 16 Agustus 2019, yang mana Presiden menyampaikan bahwa data termasuk jenis kekayaan baru, yang kini

data lebih berharga dari minyak. "*Kita harus siaga menghadapi ancaman kejahatan siber, termasuk kejahatan penyalahgunaan data. Data adalah jenis kekayaan baru bangsa kita, kini data lebih berharga dari minyak, karena itu kedaulatan data harus diwujudkan hak warga negara atas data pribadi harus* dilindungi. Regulasinya harus segera disiapkan tidak boleh ada kompromi".

Pidato sambutan dalam peresmian Palapa Ring tanggal 14 Oktober 2019, Presiden Jokowi meminta jajarannya berhati-hati dalam menyikapi sisi negatif dari era digital. Karena kehadiran teknologi digital bisa dimanfaatkan negara lain untuk mengintip seberapa besar peluang bisnis di Indonesia. Presiden juga mengingatkan masyarakat untuk berhati-hati karena saat ini Aplikasi yang berasal dari negara lain diam-diam telah mengumpulkan data dari masyarakat Indonesia dengan tujuan untuk mengetahui perilaku masyarakat Indonesia sebagai pasar/konsumen bagi produk-produk dari negara lain. Presiden dengan tegas menyatakan: "*Jangan sampai data kita, selera konsumen, selera pasar diketahui oleh negara lain, sehingga mereka bisa menggerojok kita dengan produk-produk sesuai selera yang kita inginkan. Hati-hati dengan ini*" tegas Presiden.

Kunci utama ketahanan siber dalam konteks geopolitik adalah kemandirian siber dan kedaulatan data. Kemandirian siber berarti bahwa suatu negara memiliki kemampuan untuk mengembangkan, mengoperasikan, dan mengamankan infrastruktur informasi penting dan layanan digitalnya sendiri tanpa bergantung pada teknologi atau keahlian negara asing. Ini termasuk kemampuan untuk membangun dan memelihara komputasi awan nasional yang aman, mengembangkan dan menggunakan teknologi keamanan siber nasional, dan menetapkan peraturan dan standar yang kuat yang mencerminkan kebutuhan dan prioritas unik negara.

Kedaulatan data, di sisi lain, mengacu pada kemampuan suatu negara untuk melakukan kontrol hukum dan teknis atas datanya sendiri, di mana pun data itu disimpan atau diproses. Ini termasuk kemampuan untuk memastikan bahwa data sensitif atau penting dilindungi dari akses tidak sah atau pencurian, dan bahwa setiap data yang ditransfer atau diproses di luar perbatasan negara dilakukan dengan cara yang aman dan transparan yang sesuai dengan undang-undang dan peraturan negara.

Tanpa kedaulatan data, transformasi digital di industri 4.0 justru akan melemahkan ketahanan siber suatu negara karena semakin bergantung pada layanan komputasi awan asing. Ini berarti bahwa data sensitif dapat disimpan dan diproses di luar perbatasan negara, berpotensi mengeksposnya data ke pihak asing atau serangan siber. Ini juga berarti bahwa infrastruktur informasi penting suatu negara mungkin rentan terhadap serangan rantai pasokan, di mana pelaku jahat mengeksploitasi kerentanan pada perangkat lunak atau perangkat keras pihak ketiga untuk mendapatkan akses tidak sah ke data atau sistem sensitif.

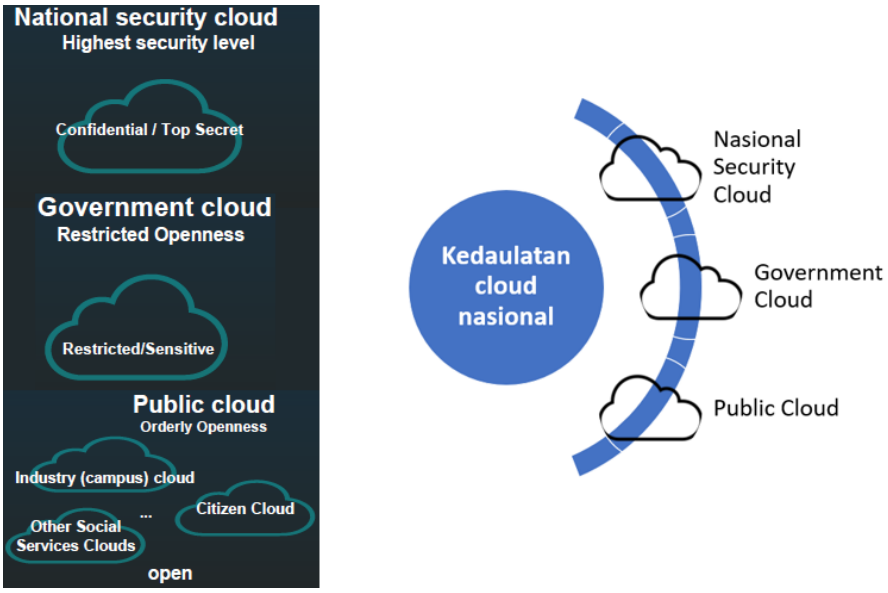
Sebaliknya, dengan memprioritaskan kedaulatan data, negara dapat mempertahankan kontrol yang lebih besar atas infrastruktur informasi dan aset data penting mereka, memastikan bahwa data sensitif dilindungi dari akses tidak sah atau pencurian dan bahwa setiap data yang ditransfer atau diproses di luar perbatasan negara dilakukan dengan cara yang sama. cara yang aman dan transparan yang konsisten dengan hukum dan peraturan negara.

**b. Pemerintah memimpin, dan industri berpartisipasi dalam membangun platform kedaulatan komputasi awan nasional**

Platform komputasi awan kedaulatan nasional bertujuan untuk membangun dan berbagi sumber daya. Platform kedaulatan komputasi awan nasional diciptakan berdasarkan sinergi antara keamanan komputasi awan nasional + komputasi awan pemerintah + komputasi awan publik seperti pada *Gambar*

*0-3* komputasi awan digunakan untuk mengelola data sangat rahasia dengan tingkat keamanan tertinggi. Komputasi awan pemerintah digunakan untuk mengelola data sensitif/terbatas sedangkan komputasi awan public untuk data publik. Keuntungannya adalah sebagai berikut:

1. Memaksimalkan efisiensi, meminimalkan biaya, dan secara efektif meningkatkan daya saing ekonomi digital nasional.
2. Data nilai nasional agregat yang dipimpin pemerintah akan memudahkan mengembangkan aplikasi penting, mempertahankan daya saing digital nasional dan mendukung transformasi digital.
3. Mendukung daerah tertinggal, UKM, dan kelompok rentan untuk menjembatani kesenjangan digital (Subsidi sumber daya, pemberdayaan kemampuan, pelatihan keterampilan dan sebagainya).




*Gambar 0-3 Platform komputasi awan kedaulatan nasional*

Dengan landasan platform nasional komputasi awan akan mendukung transisi dari pemerintahan terisolasi vertikal menuju pemerintahan

terintegrasi dan kolaboratif. Karakteristik yang membedakan keduanya antara lain adalah:

**Pemerintahan Silo Vertikal:**

Informasi terisolasi

Pemisahan korelasi layanan

Berbagi rendah dan eksploitasi terbatas

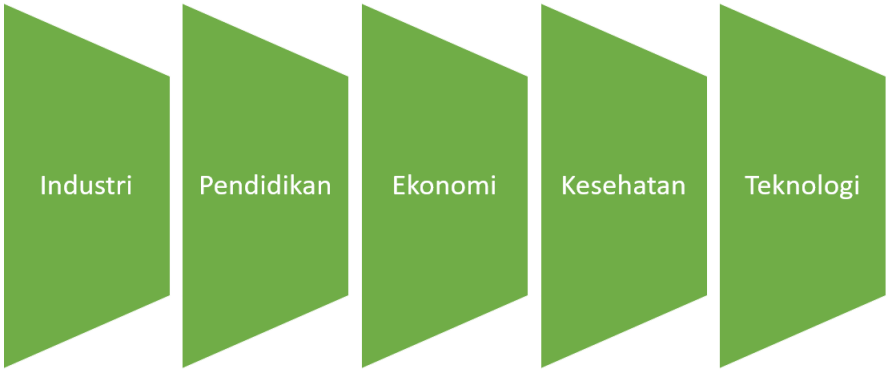
Kurangnya kemampuan berbagi elastis dan pemanfaatan rendah

**Pemerintahan yang terintegrasi dan kolaboratif:**

Platform layanan terpadu

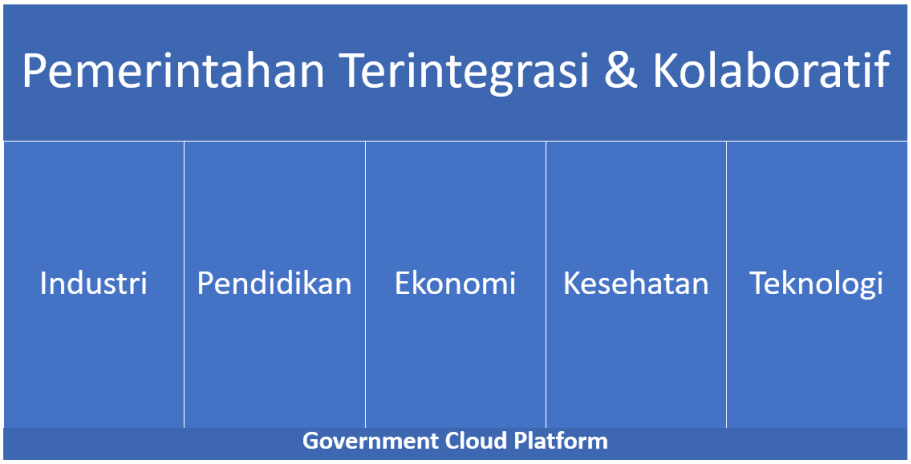
Platform pertukaran dan berbagi data dan pusat layanan data

Platform komputasi




*Gambar 0-4 Model pemerintahan silo-vertikal*

Bermigrasi dari pemerintahan silo vertikal ke pemerintahan yang terintegrasi dan kolaboratif memerlukan perubahan sistemik dalam cara lembaga dan departemen pemerintah beroperasi dan berinteraksi satu sama lain. Dengan mengikuti langkah-langkah ini, pemerintah dapat membangun sektor publik yang lebih efektif, efisien, dan responsif yang melayani kebutuhan warga negara dan pemangku kepentingan dengan lebih baik.

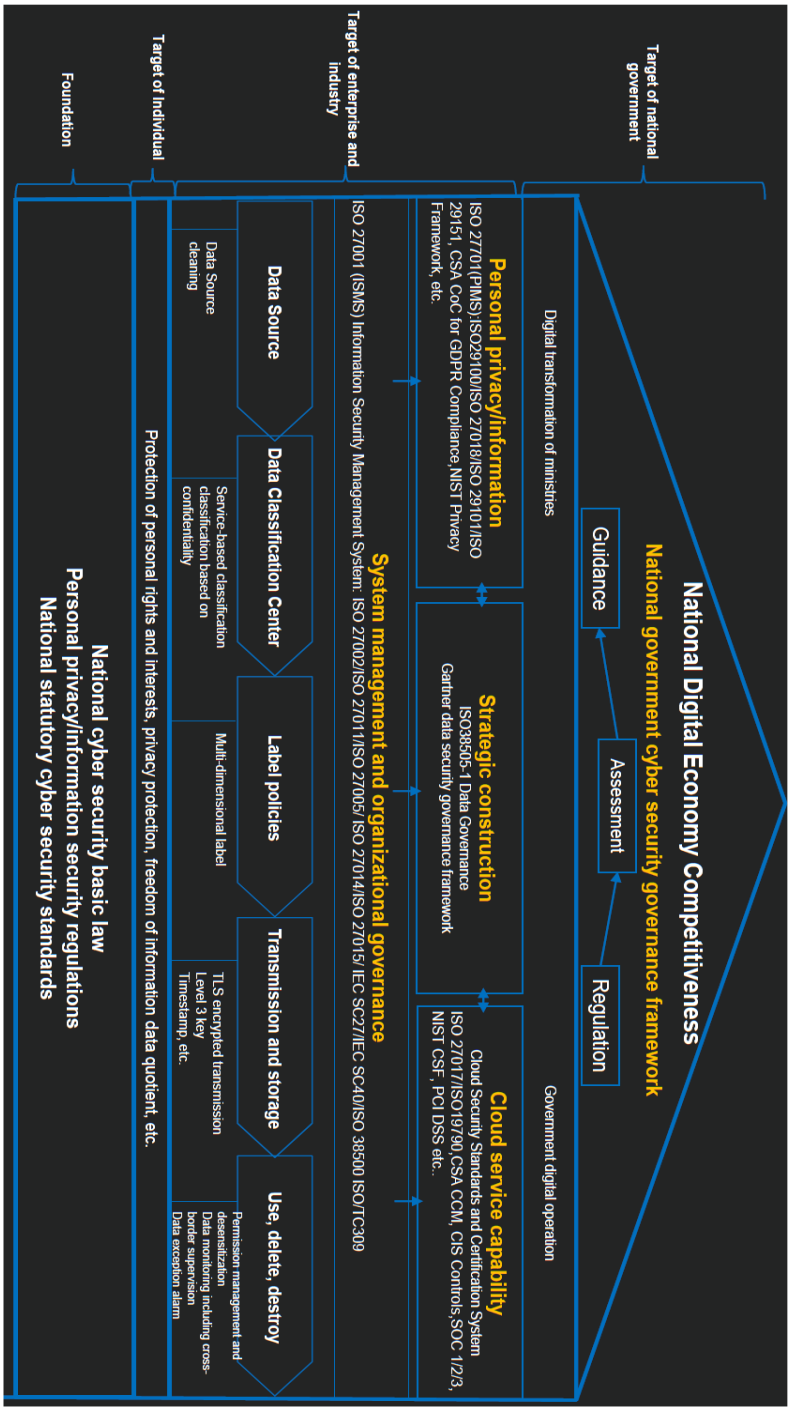



*Gambar 0-5 Pemerintahan terintegrasi dan kolaboratif*

**c. Pemerintah menetapkan mekanisme standar audit, standar keamanan dan sistem sertifikasi sesuai dengan standar internasional dan sejalan dengan situasi domestik.**

Kerangka tata kelola keamanan layanan komputasi awan & data di Indonesia dapat dipertimbangkan seperti pada *Gambar 0-6*:

*Gambar 0-6 Kerangka Tata Kelola Keamanan Layanan Komputasi awan & Data*



Pemerintah juga perlu mendukung pentingnya mengadopsi sistem standar keamanan komputasi awan yang tipikal maupun standar keamanan tata kelola secara umum seperti di bawah ini :

1. Standar konstruksi strategis seperti ISO38505-1 dsb;
2. Standar privasi/informasi pribadi seperti ISO 27701(PIMS), ISO29100, ISO 27018, ISO 29101, ISO 29151, CSA Kode etik untuk Kepatuhan GDPR, *NIST Privacy Framework*, dsb.
3. Standar keamanan layanan komputasi awan seperti ISO 27017/ISO19790, CSA CCM, Kontrol CIS, SOC 1/2/3, NIST CSF, PCI DSS, dsb.
4. Standar manajemen sistem dan tata kelola organisasi seperti: ISO 27001, ISO 27002, ISO 27011, ISO 27005, ISO 27014, ISO 27015, COBIT, IEC SC27, IEC SC40, ISO 38500, TC309 dsb.

Pemerintah Indonesia dapat menggunakan standar ini sebagai kerangka kerja keamanan komputasi awan & tata kelola data untuk menstandarkan penyedia layanan komputasi awan (CSP) dan pelanggan layanan komputasi awan (CSC) yang efektif dan memberikan tingkat keamanan tertinggi bagi pengguna. Manfaat yang paling penting adalah proses di mana semua sektor berperan dalam mendorong layanan komputasi awan yang dapat dipercaya, khususnya kolaborasi untuk mengembangkan layanan komputasi awan yang lebih aman sebagai pedoman utama.

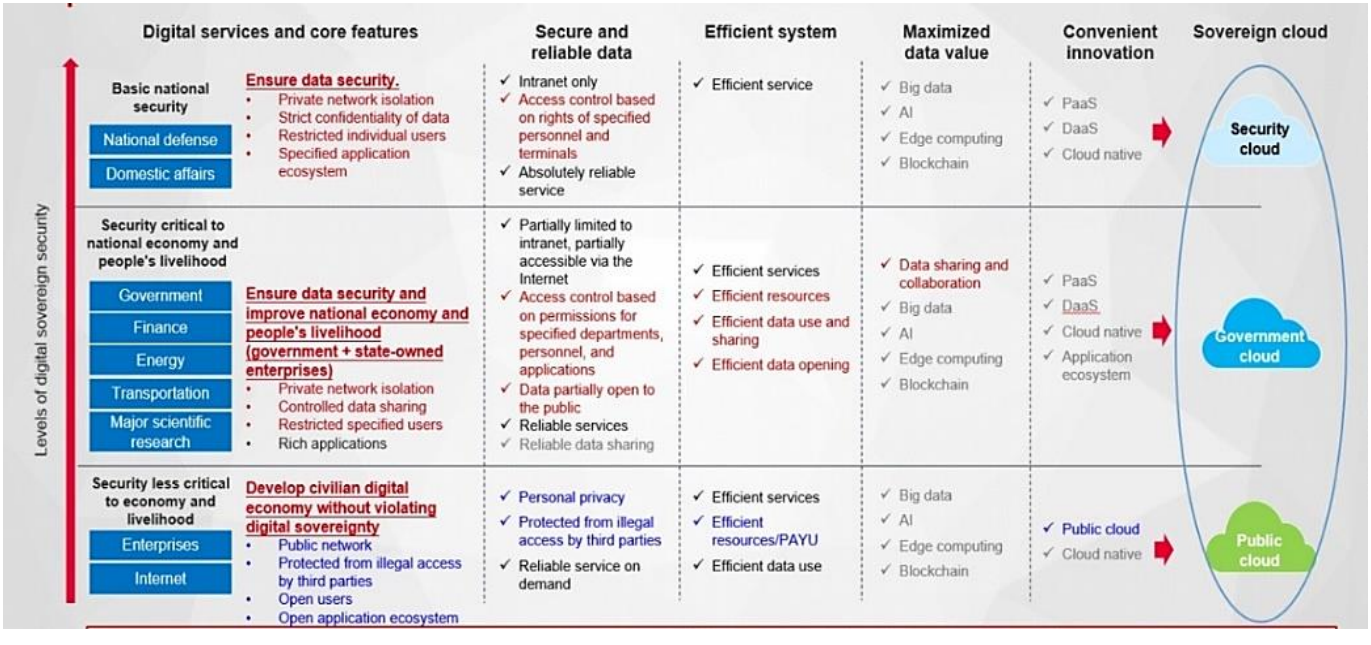
**d. Pemerintah memimpin dalam menyusun aturan klasifikasi data dan mempromosikan aturan "data *residence* + *cross-border data transfer* " untuk data sensitif**.

Klasifikasi data harus didasarkan pada kerahasiaan dan apakah merugikan keamanan nasional, kepentingan publik atau merupakan hak dan kepentingan yang sah dari warga negara atau organisasi. Disarankan agar data diklasifikasikan menjadi tiga tingkatan:

1. Data rahasia (Kritikal/Sangat Rahasia), meliputi data negosiasi internasional, pertahanan, militer, dan pemerintah nasional. Data energi nasional, data komunikasi kritis, data informasi geografis dan data infrastruktur penting seperti transportasi, keuangan, telekomunikasi dan sistem tenaga, data kependudukan dan kesehatan, data anggaran nasional dan pembiayaan pusat, data statistik, data meteorologi lingkungan, lingkungan laut data, data pendaftaran perusahaan dan data sejenis lainnya. Termasuk di dalamnya data rahasia yang pengungkapannya, seluruhnya atau sebagian, akan merugikan kepentingan nasional.
2. Data sensitif/data resmi, meliputi: data komersial, data industri kesehatan umum, data industri pendidikan umum, data pribadi, seperti data karyawan perusahaan, data industri kesehatan besar, dan data lain yang ditentukan.
3. Data non-sensitif yang dapat diungkapkan Informasi publik, basis data, dan data serupa lainnya yang menyediakan layanan yang terbuka dan dapat diakses publik secara umum.

Pemerintah dapat bekerja sama dengan industri dan pemangku kepentingan lainnya untuk mempromosikan residensi data, yang merujuk pada persyaratan bahwa data disimpan dalam lokasi geografis tertentu. Residensi data dapat membantu memastikan bahwa data sensitif tunduk pada undang-undang dan peraturan setempat, yang dapat membantu melindunginya dari akses tidak sah, penyalahgunaan, atau pencurian.

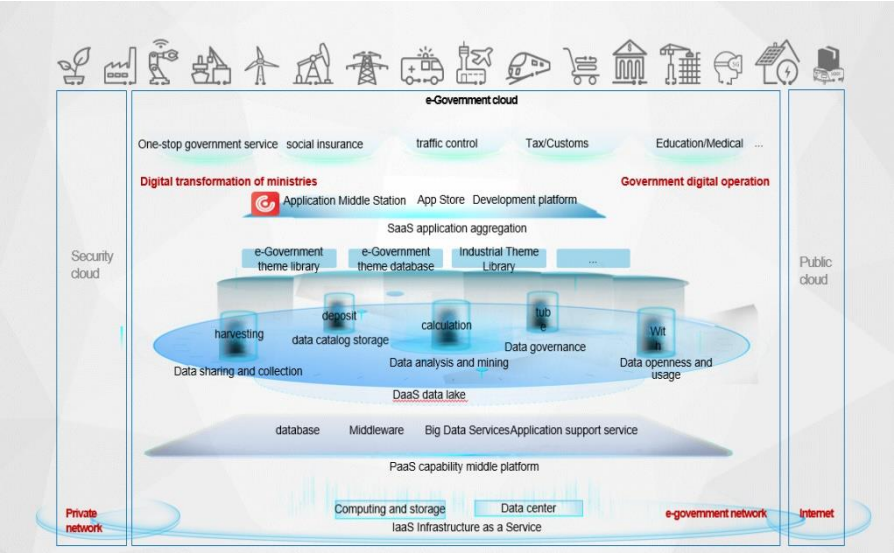
Pada saat yang sama, pemerintah juga dapat mendorong transfer data lintas batas untuk data non-sensitif, yang dapat membantu memfasilitasi pertumbuhan perdagangan dan inovasi digital. Ini melibatkan pengembangan mekanisme untuk memastikan bahwa data ditransfer dengan aman dan sesuai dengan undang-undang dan peraturan setempat, sekaligus mempromosikan interoperabilitas dan portabilitas data antara berbagai sistem dan platform.




*Gambar 0-7 Level keamanan dan kedaulatan data*

Secara keseluruhan, dengan memimpin dalam mengembangkan aturan klasifikasi dan gradasi data, mempromosikan residensi data dan transfer data lintas batas, pemerintah dapat membantu menciptakan ekosistem data yang terpercaya, aman, dan transparan yang mendukung inovasi, pertumbuhan ekonomi, dan kesejahteraan sosial, serta juga melindungi privasi individu dan kedaulatan data.

**e. Pemerintah mempercepat cloudifikasi urusan pemerintahan, transformasi digital kementerian, operasi digital pemerintah, dan mendorong transformasi digital industri.**




*Gambar 0-8 Konsep e-government cloud*

Secara keseluruhan, percepatan cloudifikasi urusan pemerintahan memerlukan upaya kolaboratif antara pemerintah, perusahaan sektor swasta, dan pemangku kepentingan lainnya. Cloudifikasi ini mencakup 4 bentuk layanan komputasi awan seperti pada *Gambar 0-8*. Keempat bentuk layanan tersebut adalah:

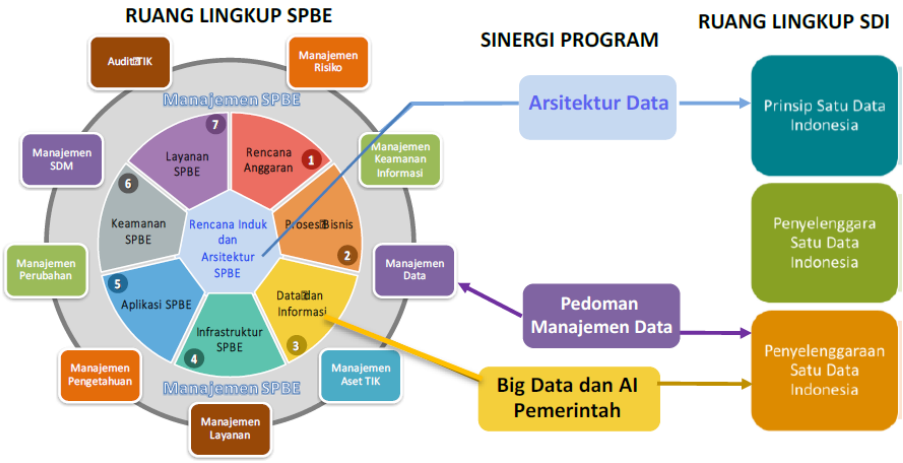
1. IaaS: Pusat data serta infrastruktur komputasi dan penyimpanan
2. PaaS: Basis data, *middleware* dsb
3. DaaS: *Data sharing, collection*, analisis, *mining* dsb
4. SaaS: *One-stop government service, traffic control*, aplikasi medis, aplikasi edukasi dsb.

Melalui *e-government cloud* kita mendapatkan berbagai keuntungan sebagai berikut (1) Memperkecil gap teknologi/infrastruktur pemerintahan pusat & daerah melalui layanan IaaS (*data center, computing & storage).* (2) Memungkinkan pengembangan teknologi seperti AI, IoT, Big Data melalui layanan PaaS (*database, middleware, big data service*). (3) Mendukung keputusan strategis berdasarkan analisis data, menambang informasi dari data melalui DaaS. (4) Mempercepat transformasi digital & layanan operasi digital pemerintahan melalui SaaS (*one-stop government service, medical apps, educational apps*).

Model *e-government cloud* ini harus disesuaikan dengan arsitektur SPBE (Perpres No.132 Tahun 2022) sehingga dapat menciptakan sinergi dengan platform satu data Indonesia (SDI). SPBE mendukung tata kelola data dalam SDI dengan cara memberi dukungan TIK baik melalui pengembangan aplikasi maupun pembangunan infrastruktur TIK berbagi pakai yang dibutuhkan. Untuk itu kolaborasi dan harmonisasi pelaksanaan penerapan SPBE dan SDI perlu diwujudkan melalui sinkronisasi pelaksanaan kegiatan SPBE dan SDI, terlihat ilustrasi pada *Gambar 0-9*.

Dengan mengadopsi kebijakan *cloud-first* (kebijakan yang mengutamakan penggunaan solusi berbasis komputasi awan), berinvestasi dalam infrastruktur komputasi awan, mendorong adopsi komputasi awan oleh lembaga pemerintah, mengembangkan standar dan pedoman komputasi awan, mengatasi hambatan yang ada, serta membina kemitraan publik-swasta, pemerintah dapat memanfaatkan manfaat komputasi awan untuk meningkatkan efisiensi dan efektivitas operasi pemerintahan dan layanan

masyarakat. Pada sisi lain hal ini juga akan mendorong transformasi digital pemerintahan dan industri.



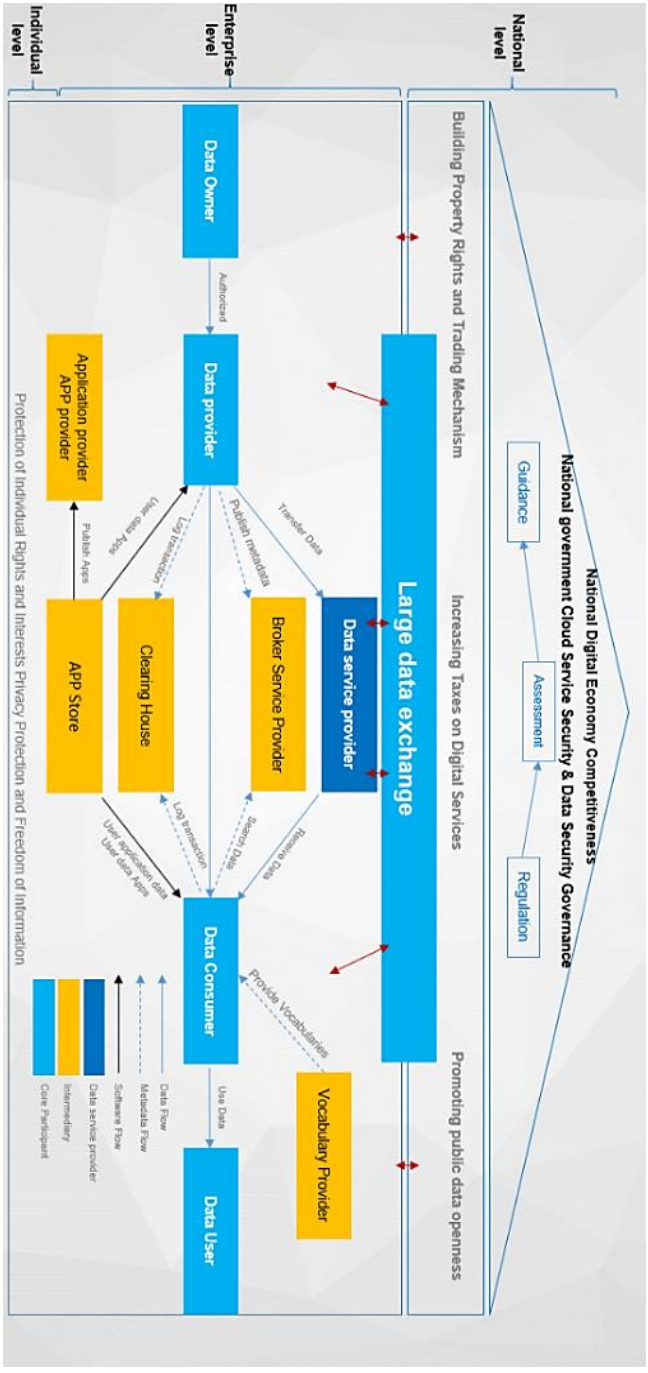

*Gambar 0-9 Sinergi antara arsitektur SPBE dan SDI*

**f. Pemerintah memimpin dalam menyiapkan mekanisme monetisasi untuk menciptakan nilai melalui layanan data serta menaikkan pajak atas layanan digital.**

Gambar 7.10 terdiri dari Penyedia kosakata (*Vocabulary provider*): Menawarkan 'kosakata' seperti ontologi, model data referensi, dan elemen metadata, yang dapat digunakan untuk membubuhi keterangan dan mendeskripsikan kumpulan data.

Hak milik dan mekanisme transaksi: Mengacu pada definisi hak milik data dan ketentuan yang relevan dari mekanisme transaksi data, seperti hak milik data eksklusif dan sistem bagi hasil data sebagai aset.

Pajak layanan digital: Mengacu pada ketentuan pajak untuk layanan digital, seperti mesin pencari, penempatan iklan bertarget pada antarmuka digital, dan penyediaan layanan perantara antarmuka digital kepada pengguna.




*Gambar 0-10 Tata kelola keamanan komputasi awan untuk meningkatkan daya saing ekonomi digital*

Keterbukaan data publik pemerintah: Mengacu pada keterbukaan data yang dimiliki oleh lembaga sektor publik di semua tingkat pemerintahan dan organisasi yang sebagian besar didanai oleh atau di bawah kendali otoritas publik.

Mekanisme monetisasi untuk menciptakan nilai melalui layanan data dapat diterapkan sebagai berikut:

- Mengembangkan kebijakan monetisasi data. Pemerintah dapat mengembangkan kebijakan monetisasi data yang memungkinkan mereka menghasilkan pendapatan dari data yang mereka kumpulkan dan kelola. Ini dapat melibatkan pembuatan pasar pertukaran data atau data lisensi ke perusahaan pihak ketiga yang dapat menggunakannya untuk mengembangkan produk dan layanan baru.
- Menerapkan kebijakan perpajakan digital. Pemerintah dapat menerapkan kebijakan perpajakan digital yang mewajibkan penyedia layanan digital untuk membayar pajak atas pendapatan yang mereka hasilkan dari layanan digital. Ini dapat membantu memastikan bahwa penyedia layanan digital membayar pajak mereka secara adil dan berkontribusi pada kas publik. Terdapat beberapa poin penting terkait aturan pajak digital ini: (1) Pajak digital diterapkan pada komoditi/barang atau jasa digital; (2) Tidak terdapat penerapan pajak ganda antara pajak digital dan pajak pertambahan nilai; (3) Harus terdapat batasan jumlah minimal pendapatan perusahaan yang dikenai pajak, dengan demikian pajak tidak membebani usaha kecil dan menengah ke bawah; (4) Besaran pajak digital sebaiknya menyesuaikan dengan besaran pajak digital di negara-negara tetangga
- Mendorong kemitraan publik-swasta: Pemerintah dapat mendorong kemitraan publik-swasta untuk mengembangkan layanan inovatif

berbasis data yang menghasilkan nilai bagi sektor publik dan swasta. Ini dapat melibatkan kerja sama dengan perusahaan sektor swasta untuk mengembangkan produk dan layanan baru, atau bermitra dengan institusi akademik untuk melakukan penelitian dan pengembangan.

- Berinvestasi dalam analitik data dan kecerdasan buatan. Pemerintah dapat berinvestasi dalam analitik data dan teknologi kecerdasan buatan yang memungkinkan mereka untuk lebih memahami dan memanfaatkan data yang mereka kumpulkan. Ini dapat membantu pemerintah membuat keputusan yang lebih tepat, mengembangkan layanan baru, dan meningkatkan efisiensi dan efektivitas operasi pemerintah.

Secara keseluruhan, dengan mengadopsi strategi ini, pemerintah dapat menciptakan nilai melalui layanan data, meningkatkan pendapatan pajak dari layanan digital, serta mendorong inovasi dan kolaborasi antara sektor publik dan swasta. Ini dapat membantu mendorong pertumbuhan ekonomi, meningkatkan layanan publik, dan meningkatkan kesejahteraan warga negara secara keseluruhan.

**Use case di Eropa: Menciptakan nilai bisnis melalui layanan data dengan GAIA-X dan IDS**

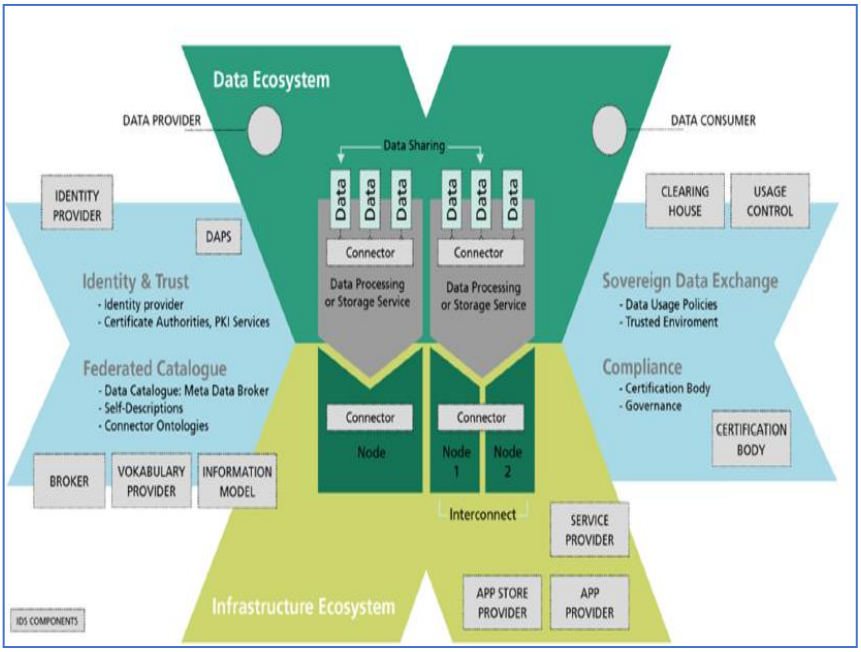
Arsitektur gabungan GAIA-X dan IDS mendukung dan memungkinkan ruang data dan layanan cerdas tingkat lanjut untuk membangun industri vertikal. GAIA-X berfokus pada layanan komputasi awan berdaulat dan infrastruktur komputasi awan, sedangkan IDS berfokus pada data dan kedaulatan data. GAIA-X berinteraksi dengan IDS dengan tiga tugas utama: penyimpanan data berdaulat, penggunaan data terpercaya, dan pertukaran data yang dapat dioperasikan.

Arsitektur IDS menyediakan kerangka kerja untuk kedaulatan data dan pertukaran data yang aman, yang memungkinkan organisasi

mempertahankan kendali atas data mereka dan membaginya secara aman dengan mitra terpercaya. Hal ini dicapai melalui penggunaan pengidentifikasi terdesentralisasi dan kredensial yang dapat diverifikasi, yang memungkinkan organisasi mengotentikasi dan mengotorisasi berbagi data dengan organisasi lain dengan cara yang aman dan dapat diaudit.

GAIA-X, di sisi lain, menyediakan kerangka kerja untuk pengembangan dan pengoperasian layanan komputasi awan berdaulat dan infrastruktur komputasi awan. Hal ini memungkinkan organisasi untuk menyimpan dan memproses data mereka di lingkungan komputasi awan yang aman dan andal yang memenuhi kebutuhan khusus mereka, sekaligus memastikan bahwa mereka mempertahankan kendali atas data mereka dan dapat memindahkannya di antara penyedia komputasi awan yang berbeda sesuai kebutuhan.

Bersama-sama, arsitektur GAIA-X dan IDS memberikan landasan yang kuat untuk pengembangan layanan cerdas tingkat lanjut yang dapat memanfaatkan data dari berbagai organisasi untuk mendorong inovasi dan menciptakan nilai baru. Dengan mengaktifkan berbagi data dan kolaborasi yang aman di lingkungan terpercaya, organisasi dapat membuka potensi penuh data mereka dan mendorong wawasan dan inovasi baru yang dapat membantu mengatasi beberapa tantangan paling mendesak di dunia.




*Gambar 0-11 Arsitektur GAIA-X dan* IDS (Thakkar & Lohiya, 2021)

Konektor (*Connector*) IDS bertanggung jawab untuk pertukaran data, karena menjalankan proses pertukaran data lengkap dari dan ke sumber daya data internal dan sistem perusahaan dari organisasi yang berpartisipasi. Konektor IDS, salah satu komponen inti yang menghubungkan komputasi awan data industri, serta komputasi awan perusahaan individual, aplikasi, dan perangkat individu yang terhubung, sehingga menyediakan akses teknis ke ekosistem IDS.

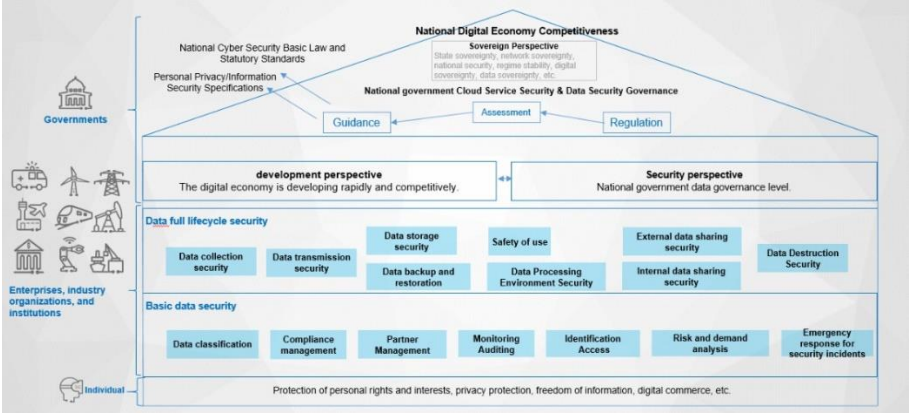
Penyedia Identitas (*Identity Provider*) menyediakan layanan otentikasi untuk semua peserta IDS. Komponen ini menawarkan layanan untuk membuat, memelihara, mengelola, memantau, dan memvalidasi informasi identitas dari dan untuk peserta dalam IDS.

Perantara (*Interconnect*) merupakan Penyedia Layanan Pialang (*Broker*), Lembaga Kliring (*Clearing house*), Penyedia App Store (*App store provider*), Penyedia Aplikasi *(App Provider*), dan Penyedia Kosakata (*Vocabularary*

*provider*). Untuk pertukaran data, Penyedia Data (*Data provider*) menyediakan metadata melalui IDS Broker. Konsumen Data (Data *Comsumer*) dapat menelusuri metadata ini untuk kumpulan data yang sesuai dengan kebutuhan mereka. Apabila syarat dan ketentuan Penyedia Data sesuai dengan kebutuhan Konsumen Data, maka pertukaran data dapat dilakukan. Untuk contoh ini, Penghubung mencatat transaksi data dan mengirimkan catatan data ke Lembaga Kliring. Selain itu, Aplikasi Data dapat memproses lebih lanjut data yang dipertukarkan. Aplikasi Data tersebut tersedia di App Store. Mereka dikerahkan dalam Konektor IDS untuk memfasilitasi alur kerja pemrosesan data. Untuk membubuhi keterangan dan mendeskripsikan kumpulan data, kosakata khusus ditawarkan oleh Penyedia Kosakata.

**7. Pemerintah memimpin dalam membangun model tata kelola kolaboratif multi-stakeholder.**

Model tata Kelola ini melibatkan kemitraan antara pemerintah, industri, akademisi, dan pemangku kepentingan lainnya untuk mengembangkan kebijakan, regulasi, dan standar yang mendorong inovasi, persaingan, dan kesejahteraan sosial dalam ekonomi digital. Melalui cara ini Indonesia dapat beradaptasi dengan pesatnya perkembangan ekonomi digital dan mempromosikan pembangunan keamanan data dasar dan keamanan data siklus penuh di tingkat perusahaan.



*Gambar 0-12 Model tata kelola kolaboratif multi-stakeholder*

Salah satu aspek utama dari model ini adalah pengembangan ruang data terpercaya dan kerangka kerja interoperabilitas yang memungkinkan berbagi data dan kolaborasi antar organisasi sembari memastikan privasi, keamanan, dan kedaulatan data. Pemerintah dapat memainkan peran penting dalam memfasilitasi pengembangan kerangka ini dengan menyediakan dana, keahlian teknis, dan panduan kebijakan.

Aspek lain dari model tata kelola kolaboratif *multi-stakeholder* adalah promosi keterampilan dan pendidikan digital. Pemerintah dapat bekerja sama dengan industri, akademisi, dan masyarakat sipil untuk mengembangkan program yang memberikan pelatihan keterampilan digital, mempromosikan literasi digital, dan mendukung pembelajaran sepanjang hayat. Dengan mempromosikan keterampilan dan pendidikan digital, pemerintah dapat membantu memastikan bahwa individu dan organisasi memiliki pengetahuan dan alat yang mereka butuhkan untuk berkembang dalam ekonomi digital.

Secara keseluruhan, membangun model tata kelola kolaboratif *multi-stakeholder* sangat penting untuk mempromosikan inovasi, persaingan, dan kesejahteraan sosial dalam ekonomi digital. Dengan bekerja sama dengan pemangku kepentingan lintas sektor dan industri, pemerintah dapat menciptakan ekosistem yang mendukung pengembangan teknologi baru, pertumbuhan bisnis digital, serta perlindungan hak dan kebebasan individu di era digital.

## 7.2 Rancangan Indeks Keamanan Informasi berdasarkan ISO/IEC 27001:2022

Pada tahun 2005, ISO/IEC *Joint Technical Committee* 1 (ISO/IEC JTC1) mengembangkan ISO/IEC 17799 berdasarkan standar negara Inggris BS7799-1: "*Information technology, Security techniques, 2005 Code of Practice for*

*Information Security Control*". Hasil pengembangan ini kemudian dikenal sebagai ISO/ IEC 27002:2005. Standar ini dimaksudkan untuk memberikan informasi berdasarkan ISO/IEC 27001: 2005 (selanjutnya disebut edisi pertama) yang digunakan sebagai panduan bagi organisasi untuk menyesuaikan kontrol keamanan. Selain itu standar ini juga sebagai referensi kontrol manajemen keamanan yang disesuaikan pada kebutuhan bisnis organisasi atau topik tertentu.

Pada tahun 2013, ISO/IEC JTC1 merevisi standar ISO/IEC 27002:2005. Dibandingkan dengan edisi pertama, edisi revisi ISO/IEC 27002:2013 "*Guide to Security Control Practices for Information Technology Security Technologies*" (selanjutnya disebut edisi kedua) sebagian besar diubah dalam terutama dua aspek yakni:

(1) Metode Seleksi Kontrol: Seleksi Kontrol kini disematkan dalam proses penilaian risiko. "Pedoman Penerapan dan Prinsip Manajemen Risiko" ISO 31000:2009, menggantikan pendekatan berbasis teknologi ISO/IEC TR 13335-3 "Panduan Manajemen Keamanan TI Bagian 3: yang diadopsi pada edisi pertama. Mengintegrasikan proses manajemen risiko keamanan informasi ke dalam keseluruhan strategi, perencanaan, manajemen, proses pelaporan, kebijakan, dan budaya nilai organisasi. Oleh karena itu, ISO/IEC JTC1 merevisi ISO/IEC 27005, Manajemen Risiko Keamanan Teknologi Informasi, sehingga metodologi penilaian risiko ISO/IEC 27005:2011 konsisten dengan ISO 31000:2009.

(2) Optimalisasi konten kontrol: Domain kontrol ditingkatkan dari 11 dalam ISO/IEC 27002:2005 menjadi 14 pada edisi kedua dengan mendekomposisi domain "kontrol manajemen komunikasi dan operasi" pada edisi kedua. Selain itu juga menambahkan dua kontrol: kontrol hubungan pemasok terkait dengan keamanan rantai pasokan dan kontrol kriptografi yang diperlukan untuk layanan Internet.

Dalam hal tujuan pengelolaan klasifikasi set kontrol dan isi dan kuantitas set kontrol, pedoman juga mengurangi tujuan edisi pertama dari 39 menjadi 35 pada edisi kedua berdasarkan saran umpan balik dan perkembangan teknologi informasi selama implementasi standar. Kontrol opsional juga dikurangi dari 133 pada edisi pertama menjadi 114 di edisi kedua, selain itu deskripsi kontrol gabungan dan juga direvisi.

Pentingnya ISO/IEC JTC1 tercermin dalam peluncuran revisi ISO/IEC 27002 yang pada Maret 2018, lima tahun setelah penerapan standar. Pada bulan Juni 2018, ISO/IEC JTC1 merilis edisi pertama Draf Kelompok Kerja ISO/IEC 27002:2018 yang menghapus "*Practice Guide*" dari judul dan mengubah judul menjadi "*Information Technology Security Technologies Information Security, Cybersecurity and Privacy Protection Information Security Control*". Perubahan ini untuk lebih mencerminkan standar ini digunakan sebagai referensi bagi organisasi untuk memilih kontrol keamanan informasi.

Untuk memenuhi persyaratan manajemen keamanan organisasi modern yang terkait dengan keamanan informasi, keamanan jaringan, dan perlindungan privasi, standar tersebut mengusulkan struktur organisasi kontrol baru yang fleksibel, menggabungkan rangkaian kontrol, dan mendefinisikan ulang struktur kontrol. Deskripsi kontrol dan panduan implementasi dilengkapi dengan panduan implementasi untuk bentuk bisnis baru yang dibawa oleh teknologi informasi baru. Draf final Standar Internasional (FDIS) untuk ISO/IEC 27002 (edisi ketiga) mulai dikomentari pada 23 Agustus 2021 dan telah dirilis secara publik pada Maret 2022. ISO/IEC JTC1 juga telah menerbitkan ISO/IEC 27001:2022 untuk menyelaraskan sertifikasinya dengan edisi ketiga pedoman implementasi ISO/IEC 27002.

Mempertimbangkan hal tersebut di atas, terutama struktur deskripsi kontrol ISO/IEC 27002 edisi ketiga maka perlu untuk membahas konsep baru revisi ISO/IEC 27002. Hali ini diperlukan untuk meringkas dan menganalisis

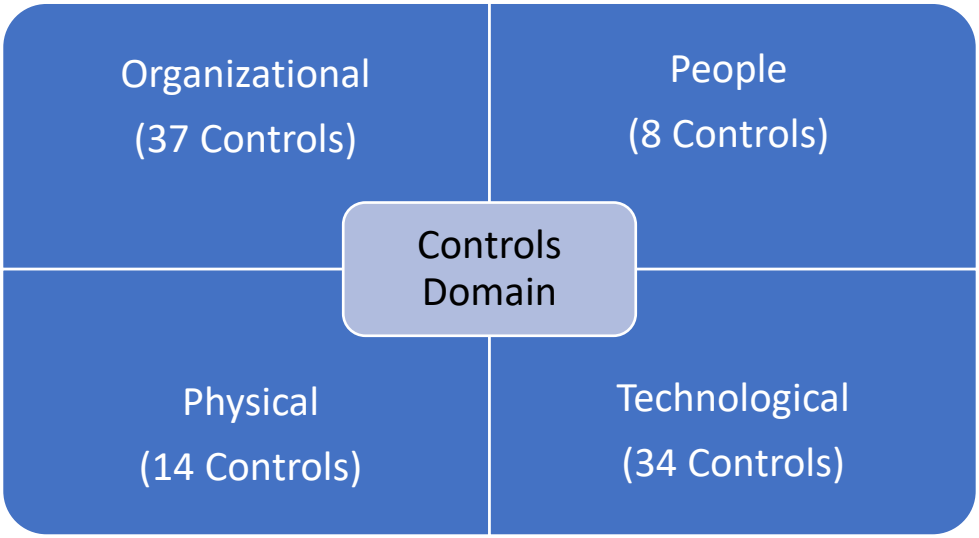
perubahan set kontrol dan konten revisi yang ada. Tujuannya agar pemilihan kontrol dalam pengelolaan risiko keamanan informasi menjadi lebih standar dan ilmiah.

Versi ketiga ISO/IEC 27002 mudah dipahami. Pemilihan domain kontrol yang ambigu dan tidak tertarget pada proses pemilihan kontrol di versi kedua dapat dihindari dengan membedakan set kontrol dengan konsep yang relatif jelas. Struktur kontrol menggunakan metode deskripsi atribut untuk membuat tampilan kumpulan kontrol dengan organisasi berbeda atau persyaratan berbeda untuk organisasi yang sama. Fleksibilitas dan operabilitas pemilihan kontrol ditingkatkan dengan mengadopsi metode pemilihan kontrol dalam tujuan mengatasi pembuangan risiko.

Deskripsi kontrol yang berorientasi pada hasil, tujuan dan presentasi konten panduan membuat standar lebih mudah dibaca dan mudah diadopsi. Beberapa istilah baru ditambahkan pada edisi ketiga, yang mencerminkan pemahaman kontrol keamanan informasi dalam keamanan informasi, keamanan jaringan dan perlindungan privasi, dan atribut serta tujuan dari struktur kontrol mencerminkan perubahan dalam penggunaan. Dalam hal set kontrol, pengaturan bab standar organisasi yang dikendalikan disesuaikan secara mendalam sesuai dengan subjek tanggung jawab. Meskipun hanya satu kontrol "perpindahan aset" yang dihapus, edisi ketiga hanya mempertahankan 58 kontrol di edisi kedua, dan kontrol lainnya digabungkan secara abstrak dalam berbagai cara, seperti ketergantungan subjek, ketergantungan entitas, dan tujuan yang sama, hal ini untuk memenuhi pernyataan tujuan pengendalian yang berorientasi pada hasil.

Terakhir, 114 kontrol dikurangi menjadi 82, dan 11 kontrol baru yang terkait dengan teknologi baru dan bentuk bisnis baru ditambahkan. Versi baru ini pada dasarnya mencakup keamanan informasi, keamanan dunia maya, dan kontrol perlindungan privasi. Untuk organisasi, meskipun jumlah persyaratan keamanan di versi ketiga dikurangi dari 114 menjadi 93, atribut

dan elemen tujuan dalam struktur kontrol membuat pemilihan kontrol , penilaian risiko dan sertifikasi keamanan lebih fleksibel, dan penerapan kontrol lebih praktis. Adaptasi terhadap filosofi manajemen risiko penciptaan nilai organisasi lebih baik. 93 kontrol pada versi ketiga mencakup 4 area domain yakni *Organizational, People, Physical* dan *Technological* (lihat *Gambar 0-13*). Adapun penggabungan (*merge*) kontrol yang ada pada versi sebelumnya dijabarkan seperti pada *Tabel 7-1*




*Gambar 0-13 Domain area kontrol pada ISO 27001:2022*

*Tabel 7-1 Perubahan domain control dari ISO/IEC 27001 versi kedua ke versi ketiga*

| No. | Kontrol Edisi Ketiga | Kontrol Edisi Kedua | Nama Kontrol | Keterangan |
|---|---|---|---|---|
| 1 | 5.1 | 5.1.1, 5.1.2 | *Information Security Policy* | Kontrol Penggabungan untuk Target yang Sama |
| 2 | 5.8 | 6.1.5, 14.1.1 | *Information Security Project Management* | Konsolidasi Kontrol Terkait Entitas: Permintaan Terkait Entitas Proyek |

| No. | Kontrol Edisi Ketiga | Kontrol Edisi Kedua | Nama Kontrol | Keterangan |
|---|---|---|---|---|
| 3 | 5.9 | 8.1.1, 8.1.2 | *Information List and Assets* | Kontrol (14.1.1) digabung menjadi 6.1.5 |
| 4 | 5.10 | 8.1.3, 8.2.3 | *Information Use and Assets* | Konsolidasi Kontrol Terkait Entitas |
| 5 | 5.14 | 13.2.1,13.2.2, 13.2.3 | *information transmission* | Konsolidasi Kontrol Terkait Entitas |
| 6 | 5.15 | 9.1.1, 9.1.2 | *Access Control* | Gabungkan kontrol target yang sama dan gabungkan kontrol yang terkait dengan entitas orang. Sistem (13.2.4) Penghapusan (6.6) |
| 7 | 5.17 | 9.2.4, 9.3.1, 9.4.3 | *discriminant information* | Kontrol Penggabungan dengan Tujuan yang Sama |
| 8 | 5.18 | 9.2.2, 9.2.5, 9.2.6 | *Access Rights* | Konsolidasi Kontrol Terkait Entitas |
| 9 | 5.22 | 15.2.1, 15.2.2 | *Supplier service monitoring, review and change management* | Kontrol Penggabungan dengan Target yang Sama |
| 10 | 5.29 | 17.1.1, 17.1.2, 17.1.3 | *Information Security During Disruption* | Kontrol Penggabungan dengan Tujuan yang Sama |
| 11 | 5.31 | 18.1.1, 18.1.5 | *Identification of laws, ordinances, regulations, and contract requirements* | Kontrol Gabung dengan Target yang Sama |
| 12 | 5.36 | 18.2.2, 18.2.3 | *Comply with information security policies and standards* | Kontrol Gabung dengan Target yang Sama |
| 13 | 6.8 | 16.1.2, 16.1.3 | *Information Security Incident Report* | Konsolidasi Kontrol Terkait Entitas |
| 14 | 7.2 | 11.1.2, 11.1.6 | *Physical Entry Control* | Konsolidasi Kontrol Terkait Entitas |
| 15 | 7.10 | 8.3.1, 8.3.2, 8.3.3 | *Storage media* | Konsolidasi Kontrol Terkait Entitas |
| 16 | 8.1 | 6.2.1, 11.2.8 | *Terminal equipment* | Konsolidasi Kontrol dengan Target dan Entitas yang Sama |

| No. | Kontrol Edisi Ketiga | Kontrol Edisi Kedua | Nama Kontrol | Keterangan |
|---|---|---|---|---|
| 17 | 8. 8 | 12.6.1, 18.2.3 | *Technology vulnerability management* | Konsolidasi kontrol terkait entitas |
| 18 | 8.15 | 12.4.1, 12.4.2, 12.4.3 | *Log* | Konsolidasi Kontrol Terkait Entitas |
| 19 | 8.19 | 12.5.1, 12.6.2 | *Software Installation in the Operating System* | Penggabungan Kontrol dengan Tujuan yang Sama dan Terkait Entitas: Kontrol (12.4.4) Lanjutkan (8.7) |
| 20 | 8.25 | 10.1.1, 10.1.2 | *Cryptographic Use* | Penggabungan Kontrol Entitas Berdasarkan Abstraksi Semantik |
| 21 | 8.26 | 14.1.2, 14.1.3 | *Application security requirements* | Kontrol Penggabungan dengan Tujuan yang Sama |
| 22 | 8.29 | 14.2.8, 14.2.9 | *Develop and accept security tests.* | Penggabungan Kontrol Terkait Entitas: Kontrol yang berbeda dari entitas (14.1.1) Dihapus (5.8) |
| 23 | 8.31 | 12.1.4, 14.2.6 | *Separation of development, testing, and running environments* | Penggabungan entitas dan tujuan berdasarkan abstraksi semantik |
| 24 | 8.33 | 12.1.2,14.2.2, 14.2.3, 14.2.4 | *Change management* | Penggabungan entitas dan tujuan berdasarkan abstraksi semantik |

Sementara beberapa kontrol lampiran A di edisi kedua telah diganti namanya dan digabungkan untuk mengurangi jumlah total kontrol, persyaratan dalam kontrol tersebut hampir semuanya sama. Perubahan terbesar di versi ketiga adalah penambahan 11 kontrol baru. Kontrol tersebut ditambahkan untuk mencerminkan area keamanan yang baru dan berkembang. Secara khusus, kategori kontrol adalah sebagai berikut:

*Tabel 7-2 Kontrol baru pada ISO 27001 edisi ketiga*

| No. | *Nama Kontrol* | *Keterangan* |
|---|---|---|
| 1 | *Threat intelligence* | Tentang mengumpulkan informasi dari sumber yang memadai untuk menghasilkan intelijen ancaman |
| 2 | *Information security for the use of* komputasi awan *services* | Tentang aspek yang harus dipertimbangkan organisasi untuk memperoleh, menggunakan, mengelola, dan keluar dari layanan komputasi awan |
| 3 | *Information and communications technology for business continuity* | Tentang mempertimbangkan keamanan informasi sebagai bagian integral dari persiapan kesinambungan bisnis, menentukan dan memenuhi persyaratan kesinambungan TIK yang relevan. |
| 4 | *Physical security monitoring* | Tentang tempat pemantauan untuk akses fisik yang tidak sah. |
| 5 | *Configuration management* | Tentang menjaga aset dalam keadaan konsisten yang diinginkan, berfungsi sebagaimana mestinya, dengan pengaturan dan fitur keamanan yang sesuai dengan manajemen kapasitas |
| 6 | *Information deletion* | Tentang memastikan bahwa setiap informasi di media penyimpanan dihapus dengan aman saat tidak diperlukan lagi. |
| 7 | *Data masking* | Tentang melindungi informasi sensitif dengan teknik penyamaran seperti psedunimisasi (identitas subjek diganti dengan nama samaran) atau anonimisasi. |
| 8 | *Data leakage prevention* | Tentang proses untuk mencegah kebocoran informasi. |
| 9 | *Monitoring activities* | Tentang memantau jaringan, sistem, dan aplikasi untuk perilaku anomali |

| No. | *Nama Kontrol* | *Keterangan* |
|---|---|---|
| 10 | *Web filtering* | Tentang mengelola akses personel ke situs web eksternal dan mengurangi paparan konten berbahaya. |
| 11 | *Secure coding* | Tentang persyaratan untuk menetapkan prinsip pengkodean yang aman untuk pengembangan perangkat lunak. |

Mengingat bahwa versi baru ISO/IEC 27001 sudah dipublikasikan, maka merupakan ide bagus untuk mempelajarinya selangkah lebih maju, dan organisasi harus mempertimbangkan hal berikut sebelum menggunakan versi kontrol yang baru:

(1) Studi kelayakan penerapan pengendalian baru: Bandingkan implementasi pengendalian saat ini dari organisasi dengan deskripsi dan tujuan pengendalian baru terhadap 93 pengendalian versi baru ISO/IEC 27001, dan evaluasi apakah pengendalian baru atau modifikasi pengendalian adalah diperlukan. Pertimbangkan kontrol yang terkait dengan peraturan keamanan data saat ini dan perlindungan informasi pribadi;

(2) Buat program sertifikasi ISO/IEC 27001 di tingkat nasional: Prioritaskan pengendalian risiko organisasi dan realisasi peluang, identifikasi sumber daya yang diperlukan dan ketergantungan lainnya, dan kembangkan program sertifikasi yang dapat ditindaklanjuti berdasarkan filosofi penciptaan nilai ISO 31000:2108.

Singkatnya, revisi ISO/IEC 27001:2022 menuntut organisasi untuk mempelajari lebih lanjut kontrol sistem manajemen keamanan informasi yang ada untuk memahami bagaimana memelihara sistem manajemen keamanan informasi organisasi dan terus mengelola risiko untuk mencapai tujuan penciptaan nilai organisasi. Versi baru dari standar mencakup pembaruan untuk mencerminkan perubahan lanskap teknologi dan ancaman yang

berkembang terhadap keamanan informasi. Versi ini juga mencakup persyaratan baru terkait pengelolaan risiko keamanan informasi, perlindungan informasi pribadi, dan pengelolaan insiden keamanan dunia maya.

## 7.3 Rancangan Kerangka Kerja Audit Keamanan Layanan Komputasi Awan

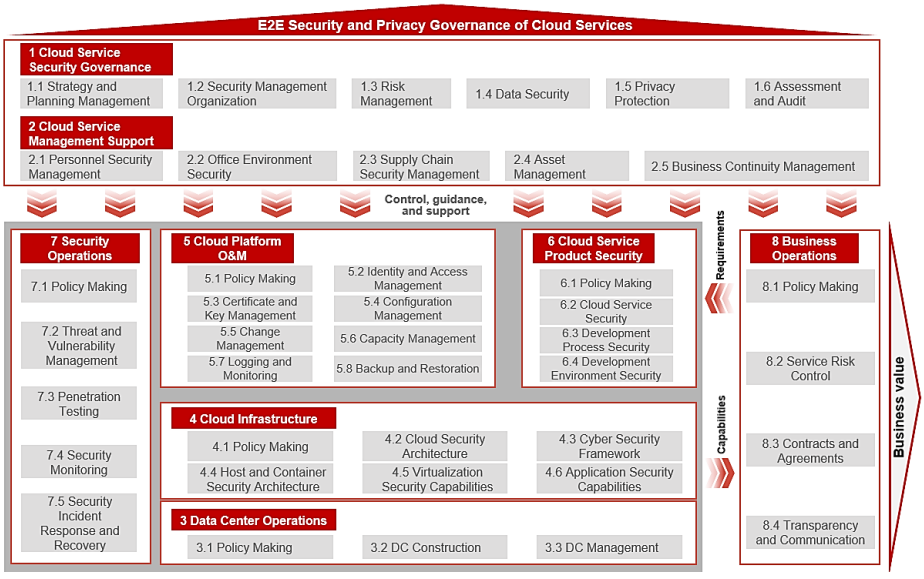
Rekomendasi kerangka kerja mengenai audit layanan komputasi awan dapat mengadopsi kerangka kerja dengan mengategorikan aktivitas kontrol keamanan yang terdiri dari tiga blok, yang mencakup delapan domain: (1) Tata Kelola Keamanan Layanan Komputasi awan, (2) Dukungan Manajemen Layanan Komputasi awan, (3) Operasi Pusat Data, (4) Infrastruktur Komputasi awan, (5) Operasi dan *Maintenance* (O&M) Platform Komputasi awan, (6) Layanan Komputasi awan Keamanan Produk, (7) Operasi Keamanan, dan (8) Operasi Bisnis.

Dengan mengadopsi kerangka kerja ini, auditor dapat menilai keefektifan kontrol keamanan yang diterapkan oleh penyedia layanan komputasi awan dan mengidentifikasi setiap celah atau kekurangan dalam kontrol keamanan yang dapat menimbulkan risiko terhadap kerahasiaan, integritas, dan ketersediaan data. Ini dapat membantu meningkatkan keamanan dan keandalan layanan komputasi awan serta membangun kepercayaan di antara pengguna layanan komputasi awan. Selain itu, kerangka kerja ini dapat memberikan sudut pandang yang sama bagi penyedia layanan komputasi awan, auditor, dan pengguna untuk mendiskusikan dan menilai kontrol keamanan, memfasilitasi komunikasi dan kolaborasi yang lebih baik terkait masalah keamanan. Penjabaran model kerangka kerja ini sebagai berikut:

Blok pertama mencakup dua domain: tata kelola keamanan layanan komputasi awan dan dukungan manajemen layanan komputasi awan.

Domain pertama "Tata Kelola Keamanan Layanan Komputasi awan" mencakup berbagai fungsi tata kelola keamanan perusahaan, termasuk pengaturan strategi dan organisasi manajemen, perencanaan manajemen keamanan berbasis risiko, tata kelola yang mementingkan keamanan data dan perlindungan privasi, serta penilaian dan audit berkelanjutan, yang membentuk tata kelola keamanan komputasi awan mekanisme siklus yang dapat terus dioptimalkan.

Domain yang kedua mencakup fungsi-fungsi manajemen seperti manajemen keamanan personel, lingkungan kantor dan keamanan fasilitas, manajemen keamanan pemasok, manajemen aset, dan rencana kesinambungan bisnis dan manajemen rencana pemulihan bencana, memberikan dukungan manajemen operasi umum untuk perusahaan. Fungsi utama tata kelola keamanan layanan komputasi awan mengontrol dan memandu manajemen keamanan siber dan perlindungan privasi. Selain itu juga mendukung manajemen keamanan di setiap domain bisnis bersama dengan proses dukungan manajemen layanan komputasi awan.




*Gambar 0-14 Kerangka Kerja Audit Keamanan Layanan Komputasi awan*

Blok kedua mencakup lima domain: Operasi Pusat Data, Infrastruktur Komputasi awan, O&M Platform Komputasi awan, Keamanan Produk Layanan Komputasi awan, dan Operasi Keamanan. Ada serangkaian aktivitas untuk mengimplementasikan platform komputasi awan dan kemampuan layanan organisasi. Hal ini termasuk membangun dan mengoperasikan pusat data, membangun infrastruktur komputasi awan dan melakukan O&M, mengembangkan dan mengoperasikan produk komputasi awan, dan mengelola kerentanan keamanan serta bertahan dari serangan. Berpusat pada setiap fase aktivitas, organisasi dapat mengidentifikasi area yang memerlukan kontrol keamanan dan menentukan kontrol keamanan yang akan diterapkan, lalu mengklasifikasikan lima domain terkait dengan kemampuan keamanan layanan komputasi awan berdasarkan modul fungsional TI yang berbeda dan proses manajemen yang sesuai. Setiap domain mencakup serangkaian tugas, dan bersama-sama membangun layanan komputasi awan yang aman dan andal.

Blok ketiga mencakup domain Operasi Bisnis. Departemen teknis menyediakan kemampuan komputasi awan sementara departemen operasi bisnis mempromosikan dan memberikan kemampuan ini kepada pelanggan bersamaan dengan mengumpulkan persyaratan baru. Hal ini membantu departemen teknis meningkatkan kemampuan layanan komputasi awan, sehingga terus meningkatkan tingkat layanan komputasi awan organisasi. Selama operasi bisnis, departemen bisnis terkait perlu menghindari atau memitigasi risiko keamanan dan kepatuhan bisnis. Domain Operasi Bisnis menentukan kontrol yang diperlukan untuk operasi bisnis yang terkait dengan layanan komputasi awan, memandu departemen bisnis untuk memastikan keamanan dan kepatuhan saat menyampaikan nilai bisnis layanan komputasi awan kepada pelanggan.

Mengikuti logika ini, organisasi dapat merujuk ke aktivitas proses khusus domain terkait kerangka kerja audit keamanan layanan komputasi awan dan

menyesuaikan sistem tata kelola keamanan yang sesuai. Kerangka kerja menyajikan hubungan hierarkis yang jelas antara domain. Organisasi dapat dengan mudah menunjuk departemen yang tepat untuk mengambil tanggung jawab manajemen keamanan, mengukur kinerja keamanan menerapkan penghargaan dan hukuman, serta memastikan tata kelola keamanan yang komprehensif dan efektif.

Kerangka kerja audit keamanan layanan komputasi awan melibatkan kontrol dalam delapan domain keamanan, termasuk Tata Kelola Keamanan Layanan Komputasi awan, Dukungan Manajemen Layanan Komputasi awan, Operasi Pusat Data, Infrastruktur Komputasi awan, O&M Platform Komputasi awan, Keamanan Produk Layanan Komputasi awan, Operasi Keamanan, dan Operasi Bisnis. Kedelapan domain ini dibagi lagi menjadi beberapa sub-domain, masing-masing dengan daftar kebutuhan dasar level-1 dan level-2. Persyaratan dasar Level-2 merinci tindakan atau aksi yang harus diterapkan organisasi untuk mencapai tujuan manajemen yang diuraikan dalam persyaratan dasar level-1 yang berisi beberapa faktor kunci yang harus dipenuhi selama implementasi.

*Tabel 7-3 Contoh satu set persyaratan kerangka kerja audit keamanan layanan* komputasi awan

| ***Subject*** | ***Level-1 Basic Requirement*** | ***Level-2 Basic Requirement*** | ***Supplementary Requirement*** | ***Note*** |
|---|---|---|---|---|
| | CSP harus mempartisi | CSP harus mengembangkan prinsip tentang cara membagi zona keamanan jaringan berdasarkan sensitivitas aset dan hasil penilaian risiko. | Divisi zona keamanan jaringan harus memenuhi persyaratan berikut:<br>• Isolasi pelanggan komputasi awan secara logis atau fisik.<br>• Hindari | Zona keamanan diklasifikasikan menjadi zona tepercaya dan tidak tepercaya. |

| *Subject* | *Level-1 Basic Requirement* | *Level-2 Basic Requirement* | *Supplementary Requirement* | *Note* |
|---|---|---|---|---|
| Network Partition Isolation | jaringan infrastruktur komputasi awan dan melakukan isolasi. | | penggelaran zona jaringan kritis pada batas jaringan internal dan eksternal CSP. | |
| | | CSP harus memberikan perlindungan isolasi untuk jaringan yang mengizinkan akses eksternal atau penyewa. | Perlindungan isolasi harus memenuhi persyaratan berikut:<br>• Tempatkan komponen sistem yang memungkinkan akses publik dan langsung ke subnet terisolasi (seperti DMZ) untuk memastikan isolasi dari jaringan penyewa.<br>• Isolasi lalu lintas data antara pelanggan komputasi awan. | Aktifkan pemfilteran firewall di antara VLAN untuk memastikan bahwa hanya sistem resmi yang dapat berkomunikasi dengan sistem lain yang diperlukan untuk memenuhi tanggung jawab khusus mereka. Nonaktifkan semua komunikasi workstation-ke-workstation untuk membatasi kemampuan penyerang untuk bergerak secara lateral dan |

| *Subject* | *Level-1 Basic Requirement* | *Level-2 Basic Requirement* | *Supplementary Requirement* | *Note* |
|---|---|---|---|---|
| | | | | membahayakan sistem tetangga, melalui teknologi seperti VLAN pribadi atau segmentasi mikro. |
| | | CSP harus memberikan perlindungan isolasi secara terpisah untuk jaringan penyewa, jaringan manajemen layanan komputasi awan, dan jaringan internal. | Perlindungan isolasi harus:<br>• Pastikan jaringan penyewa diisolasi dari jaringan manajemen layanan komputasi awan dan jaringan internal. Akses langsung tidak diperbolehkan.<br>• Pastikan jaringan manajemen layanan komputasi awan diisolasi dari jaringan internal. Akses jaringan hanya diperbolehkan setelah otorisasi dan | (1) Jaringan penyewa: sumber daya komputasi yang disediakan untuk CSC untuk mengakses layanan komputasi awan dan membawa data atau aplikasi mereka.<br>(2) Jaringan manajemen layanan komputasi awan: digunakan untuk melakukan tugas pengelolaan dan pemeliharaan |

| *Subject* | *Level-1 Basic Requirement* | *Level-2 Basic Requirement* | *Supplementary Requirement* | *Note* |
|---|---|---|---|---|
| | | | otentikasi dua faktor berhasil.<br>• Pastikan bahwa sumber otentikasi identitas jaringan penyewa dipisahkan dari jaringan internal.<br>• Pastikan hanya alamat IP yang ditentukan di jaringan internal yang dapat digunakan untuk mengakses jaringan manajemen layanan komputasi awan dan jaringan penyewa. | pada jaringan penyewa.<br>(3) Jaringan internal: digunakan untuk proses layanan internal dan tidak relevan dengan layanan komputasi awan.<br>(4) Untuk IaaS/PaaS, segregasi aman dipastikan dengan jaringan yang terpisah secara fisik atau melalui VLAN yang dienkripsi dengan kuat. |

### 7.3.1 Kontrol Domain

Kontrol domain dalam kerangka kerja audit keamanan layanan komputasi awan didasarkan pada berbagai standar dan panduan teknis yang diakui secara luas di seluruh dunia, serta praktik terbaik industri. Bagian berikut merangkum tujuan dan persyaratan kontrol khusus domain:

**Domain 1: Tata Kelola Keamanan Layanan Komputasi Awan**

Domain ini menjelaskan aktivitas yang harus dilakukan CSP dalam tata kelola keamanan dan perencanaan untuk menetapkan pendekatan tata kelola keamanan yang mengikuti siklus *planning-do-check-act* (PDCA) untuk peningkatan kualitas. Domain ini terutama ditujukan untuk tata kelola keamanan dan departemen perencanaan dalam CSP.

Tujuan manajemen: Memberikan arahan untuk manajemen keamanan komputasi awan berdasarkan persyaratan bisnis serta undang-undang dan peraturan, menetapkan kerangka kerja manajemen, dan memandu serta mengontrol implementasi dan operasi keamanan dan perlindungan privasi dalam organisasi; mendefinisikan dan mengatur penilaian risiko, dan segera mengidentifikasi dan menangani risiko keamanan dan perlindungan privasi; melakukan audit keamanan komputasi awan dan perlindungan privasi untuk memastikan penerapan tindakan dan kontrol manajemen yang relevan secara efektif.

Persyaratan kontrol domain:

a) Strategi dan perencanaan keamanan

   CSP harus menetapkan tujuan tata kelola keamanan siber dan perlindungan privasi, mengembangkan kebijakan manajemen keamanan siber dan perlindungan privasi, mengembangkan, dan menerapkan rencana tindakan yang relevan, dan menyediakan sumber daya yang diperlukan untuk mencapai tujuan keamanan siber dan perlindungan privasi. CSP harus memantau, mengukur, dan menilai implementasi kebijakan manajemen keamanan siber dan perlindungan privasi; secara teratur mengaudit dan memperbarui kebijakan manajemen keamanan dunia maya dan perlindungan privasi untuk peningkatan berkelanjutan.

b) Organisasi manajemen keamanan

   CSP harus membentuk organisasi manajemen keamanan dunia maya dan perlindungan privasi.

c) Manajemen risiko

CSP harus menentukan tujuan dan ruang lingkup manajemen risiko, mengembangkan kebijakan, proses, dan panduan operasi manajemen risiko, dan mendokumentasikan dan mendistribusikannya ke personel yang relevan untuk implementasi yang efektif. Selain itu, CSP harus mengidentifikasi dan menilai risiko terhadap aset informasi dan aktivitas dalam organisasi secara berkala dan menangani risiko untuk mengurangi risiko residual ke tingkat yang dapat diterima.

d) Keamanan data

CSP harus mengembangkan kebijakan, proses, dan panduan operasi tata kelola keamanan data; mengembangkan dan memelihara diagram aliran data dan inventarisasi data untuk secara akurat mengidentifikasi status data sensitif. Saat mengumpulkan data, CSP harus mengklasifikasikan dan melabeli data serta memastikan kerahasiaan, integritas, dan kepatuhannya. Untuk penggunaan data, CSP harus mengontrol penggunaan data untuk memastikan keamanan data dan penggunaan yang tepat. Untuk transmisi data, CSP harus menerapkan tindakan teknis untuk memastikan keamanan data transit. Untuk penyimpanan data, CSP harus menerapkan kontrol keamanan pada penyimpanan data untuk memenuhi persyaratan undang-undang dan peraturan setempat serta mencegah korupsi, perusakan, dan kebocoran data. Untuk pemusnahan data, CSP harus membuat proses pemusnahan data yang aman untuk memastikan bahwa data benar-benar dihapus. Selain itu, CSP harus secara teratur meninjau penerapan kontrol keamanan data dan memperbaruinya.

e) Perlindungan privasi

CSP harus mengembangkan kebijakan, proses, dan panduan operasi perlindungan privasi. CSP harus mematuhi prinsip dasar

perlindungan privasi saat menjalankan aktivitas bisnis yang melibatkan data pribadi untuk memastikan kepatuhan hukum dan peraturan mereka. CSP harus memberi tahu subjek data dalam bentuk yang lengkap, transparan, tepat waktu, dapat dipahami, dan mudah diakses sebelum pengumpulan data pribadi; mengumpulkan data pribadi berdasarkan persetujuan subjek data, pelaksanaan kontrak, atau dasar hukum lainnya. CSP harus mematuhi prinsip minimisasi data saat mengumpulkan data pribadi; memastikan bahwa penggunaan, pemrosesan, dan penyimpanan data pribadi konsisten dengan yang diizinkan. CSP harus melakukan penilaian dampak privasi (PIA) untuk mengidentifikasi risiko dan ancaman privasi yang dapat diperkirakan; menyediakan mekanisme untuk memproses permintaan sah subjek data untuk melindungi hak sahnya sambil menerapkan kontrol untuk memastikan keamanan dan privasi data yang diungkapkan kepada pihak ketiga.

f) Penilaian dan Audit

CSP harus membentuk komite audit keamanan siber dan perlindungan privasi untuk mengembangkan kebijakan penilaian dan audit, proses, dan panduan operasi. CSP harus mengembangkan dan memelihara rencana audit keamanan siber dan perlindungan privasi; melakukan audit sesuai rencana, melacak temuan audit, dan memastikan penerapan tindakan korektif yang efektif.

**Domain 2: Dukungan Manajemen Layanan Komputasi Awan**

Domain ini menjelaskan persyaratan manajemen keamanan dalam modul manajemen umum dan proses CSP. Modul manajemen ini mungkin tidak secara langsung terlibat dalam operasi layanan komputasi awan; sebaliknya, mereka menyediakan kemampuan manajemen internal untuk layanan komputasi awan. Fungsi mereka dapat dilakukan oleh kantor pusat, pusat layanan bersama, dan penyedia layanan eksternal. Domain ini terutama

ditujukan untuk departemen CSP yang bertanggung jawab untuk mengembangkan atau menjalankan proses manajemen internal.

Tujuan manajemen: Menetapkan tindakan manajemen khusus dalam hal keamanan personel, keamanan lingkungan fisik, keamanan pemasok, keamanan aset informasi, dan kelangsungan bisnis berdasarkan arahan manajemen keamanan komputasi awan dan perlindungan privasi, untuk memastikan penerapan yang efektif dari tindakan manajemen terkait.

Persyaratan kontrol domain:

a) Manajemen Keamanan Personalia

   CSP harus mengembangkan kebijakan, proses, dan panduan pengoperasian manajemen keamanan personel. Mereka harus melakukan pemeriksaan latar belakang terhadap karyawan dan menandatangani kontrak/perjanjian terkait keamanan dengan mereka sebelum dipekerjakan; memberikan pendidikan kesadaran keamanan dan pelatihan keterampilan keamanan di tempat kerja untuk personel internal dan eksternal. CSP harus menetapkan mekanisme pendisiplinan bagi personel internal dan eksternal yang telah melakukan pelanggaran keamanan; menerapkan kontrol keamanan untuk transfer pekerjaan atau pemutusan hubungan kerja personel internal dan eksternal dan mengomunikasikan tanggung jawab dan kewajiban keamanan mereka.

b) Keamanan Lingkungan dan Fasilitas Kantor

   CSP harus mengembangkan kebijakan, proses, dan panduan operasi untuk mengelola lingkungan kantor dan keamanan fasilitas. CSP harus menerapkan kontrol keamanan untuk lingkungan kantor untuk memastikan keamanan aset seperti dokumen dan media penyimpanan; menerapkan kontrol keamanan untuk terminal untuk memastikan keamanan dan kepatuhan sistem, perangkat lunak, dan

data yang digunakan di lingkungan kantor; mencegah penggunaan yang tidak sah dari jaringan nirkabel.

c) Manajemen Keamanan Pemasok

CSP harus mengembangkan kebijakan, proses, dan panduan operasi untuk manajemen keamanan pemasok; mengembangkan dan memelihara mekanisme manajemen keamanan pemasok; menerapkan manajemen keamanan pada pengadaan produk dan layanan untuk memastikan keamanan mereka. CSP harus mengaudit kinerja kontrak pemasok dan menetapkan mekanisme penggantian atau keluar. CSP harus meninjau dokumen, inventaris, dan kontrak/perjanjian kebijakan manajemen keamanan pemasok setidaknya setahun sekali.

d) Manajemen aset

CSP harus mengembangkan kebijakan, proses, dan panduan pengoperasian manajemen aset; mengklasifikasikan dan melabeli aset; membuat dan memelihara inventaris aset; menerapkan manajemen dan kontrol keamanan di sepanjang siklus hidup aset.

e) *Business Continuity Plan* (BCP) dan Pengelolaan *Disaster Recovery Plan* (DRP)

CSP harus mengembangkan kebijakan, standar, dan proses manajemen kesinambungan bisnis yang berkaitan dengan keamanan dunia maya dan perlindungan privasi; melengkapi infrastruktur dengan sumber daya yang berlebihan untuk memastikan operasi bisnis kritis yang berkelanjutan; mengembangkan BCP dan DRP untuk berbagai skenario; rutin melakukan latihan (*BSSN Gelar Business Continuity Plan Drill Tingkatkan Kesiapan Dan Kemampuan Respons Insiden Siber Unit Kerja BSSN*, 2020) dan perbaikan untuk BCP dan DRP.

**Domain 3: Operasi Pusat Data**

Domain ini menjelaskan persyaratan manajemen keamanan untuk manajemen operasi DC (Data Center) CSP. Selain mengelola DC mereka sendiri, CSP dapat memilih untuk menyewa banyak DC eksternal. Dengan demikian, kontrol terpisah perlu dikembangkan untuk menerapkan manajemen keamanan terpadu untuk DC yang disediakan oleh CSP berbeda. Domain ini terutama ditujukan untuk departemen manajemen operasi DC dari CSP.

Tujuan pengelolaan domain ini adalah untuk menentukan keamanan organisasi DC dan persyaratan perlindungan privasi dalam hal lingkungan, kontrol akses, pemantauan, dan untuk mencegah akses yang tidak sah, kerusakan, dan interferensi dengan DC.

Persyaratan kontrol domain:

a) Konstruksi Data Center (DC)

   Saat memilih lokasi DC, pertimbangkan risiko yang ditimbulkan oleh lokasi dan lingkungan fisik dan lakukan tindakan keamanan lingkungan yang sesuai untuk melindungi dari bencana alam, serangan berbahaya, atau kecelakaan. CSP harus menyediakan sumber daya fisik, lingkungan, dan daya yang redundan untuk memastikan ketersediaan infrastruktur (Sidabutar & Priambodo, 2022), sekaligus mengambil tindakan kontrol akses fisik untuk mencegah akses tidak sah ke DC (Chuldun et al., 2022).

b) Manajemen DC

   CSP harus mengelola pengunjung dan izin akses fisik ke DC. Selain itu, mereka harus memantau dan mengontrol keamanan DC untuk mengurangi risiko yang berkaitan dengan kegagalan daya, kebakaran, interupsi, dan intrusi.

**Domain 4: Infrastruktur Komputasi Awan**

Domain ini menjelaskan persyaratan teknis keamanan yang harus dipertimbangkan dan dipenuhi dalam tahap perencanaan dan desain platform komputasi awan. Ini terutama ditujukan untuk departemen manajemen arsitektur CSP.

Tujuan manajemen dari domain ini adalah untuk membangun arsitektur keamanan komputasi awan, dan untuk menentukan dan membangun kapabilitas keamanan infrastruktur komputasi awan, seperti keamanan jaringan, keamanan infrastruktur (misalnya, *host*), keamanan sistem dan wadah manajemen virtualisasi, dan keamanan aplikasi yang digunakan atau dikembangkan di komputasi awan.

Persyaratan kontrol domain:

a) Arsitektur Keamanan Komputasi awan

   CSP harus menyediakan kemampuan manajemen keamanan komputasi awan terpadu untuk infrastruktur komputasi awan untuk mengelola, menjadwalkan, dan mengalokasikan sumber daya fisik dan virtual sesuai dengan kebijakan, dan untuk menyediakan keamanan komputasi awan tingkat lanjut.

b) Kerangka Kerja Keamanan Siber

   CSP harus memartisi jaringan infrastruktur komputasi awan dan melakukan isolasi serta mengambil tindakan perlindungan dan pemantauan di batas jaringan. CSP juga harus melakukan kontrol akses jaringan dan kontrol akses jarak jauh untuk mencegah akses atau operasi yang tidak sah. Mereka harus memastikan redundansi jalur komunikasi dan peralatan untuk memenuhi persyaratan ketersediaan, dan meninjau kontrol komunikasi jaringan secara teratur.

c) Arsitektur Keamanan *Host* dan Kontainer

CSP harus menerapkan penguatan keamanan dan pencegahan *malware* untuk *host* dan kontainer dan memeriksa keefektifan tindakan ini secara teratur.

d) Kemampuan Keamanan Virtualisasi

CSP harus mengimplementasikan isolasi sumber daya dan kontrol akses pada platform mesin virtualisasi (VM) , memantau status VM, dan membuat alarm. Mereka *juga* harus mengambil tindakan perlindungan keamanan untuk *image* VM guna memastikan ketersediaan, kerahasiaan, dan integritasnya.

e) Kemampuan Keamanan Aplikasi

CSP harus mengambil tindakan perlindungan keamanan aplikasi untuk mencegah serangan dunia maya dan melindungi keamanan komunikasi aplikasi.

**Domain 5: Domain Operasional & Maintenance (O&M) Platform Komputasi Awan**

Domain ini menjelaskan persyaratan manajemen keamanan yang perlu dipertimbangkan dan dipenuhi selama O&M platform komputasi awan. Hal ini terutama ditujukan untuk departemen O&M dari CSP.

Tujuan manajemen domain ini adalah untuk menentukan dan mengimplementasikan manajemen O&M keamanan platform komputasi awan berdasarkan tujuan bisnis dan keamanan organisasi. Manajemen O&M keamanan mencakup penetapan identitas dan kontrol akses untuk mencegah akses tidak sah; menerapkan manajemen sertifikat dan kunci untuk secara efektif melindungi keamanan, keaslian, dan integritas informasi; mendefinisikan dan mengimplementasikan *baseline* konfigurasi keamanan dan melakukan tinjauan rutin terhadap efektivitas implementasi; meramalkan, memantau, dan menyesuaikan penggunaan sumber daya untuk

memastikan bahwa sumber daya sistem yang diperlukan tersedia; menggunakan log dan pemantauan untuk merekam informasi situasional dan menghasilkan bukti terkait; membuat cadangan data untuk mencegah kehilangan data.

Persyaratan kontrol domain:

a) Manajemen Identitas dan Akses

CSP harus menentukan persyaratan manajemen akun berdasarkan kebutuhan bisnis dan keamanan, mengelola akun pengguna, melakukan kontrol keamanan untuk akun bersama, layanan, atau aplikasi, dan menerapkan manajemen izin (menentukan dan memelihara akun dan daftar izin dan meninjau daftar secara teratur) setelah menentukan skenario aplikasi dan mode akses akun istimewa untuk mencegah akses tidak sah ke aset serta modifikasi dan penyalahgunaan yang tidak disengaja. Selain itu, CSP harus memastikan manajemen kata sandi dan kata sandi *hash* untuk penyimpanan dan transmisi untuk memastikan kekuatan kata sandi dan keamanan penggunaan kata sandi; menerapkan otentikasi multi-faktor (MFA) untuk mencegah penggunaan identitas yang tidak sah dan memanfaatkan manajemen sesi untuk memastikan kerahasiaan sesi.

b) Manajemen Sertifikat dan Kunci

CSP harus secara eksplisit mendefinisikan algoritme kriptografi dan produk teknologi penyandian yang dapat digunakan dan mengembangkan kebijakan untuk penggunaan dan perlindungan kunci sepanjang siklus hidupnya untuk melakukan kontrol keamanan pembuatan, distribusi, penggunaan, dan penyimpanan kunci, sehingga memastikan kerahasiaan dan integritas, dan mendefinisikan kebijakan rotasi dan pemusnahan utama. CSP juga harus mengelola sertifikat secara terpusat dan menerapkan kebijakan perlindungan di sepanjang siklus hidupnya. Selain itu, CSP harus

meninjau sertifikat dan kebijakan serta teknologi manajemen kunci secara berkala.

c) Manajemen konfigurasi

CSP harus menetapkan dan menerapkan garis dasar konfigurasi keamanan sesuai dengan standar industri untuk melakukan penguatan keamanan pada aset perangkat keras dan perangkat lunak. Mereka juga harus menerapkan pemeriksaan otomatis pada keefektifan konfigurasi keamanan, dan *baseline* konfigurasi keamanan harus ditinjau secara berkala.

d) Manajemen Perubahan

CSP harus mendokumentasikan perubahan dan menilai risiko terkait. Setelah mengembangkan solusi perubahan, CSP harus menguji dan mengesahkan perubahan tersebut. Mereka juga harus memberi tahu pihak terkait berdasarkan dampak perubahan tersebut, merekam proses implementasi, dan memverifikasi keefektifan setelah perubahan dilakukan.

e) Manajemen kapasitas

CSP harus melakukan perencanaan kapasitas secara teratur dan terus memantau pemanfaatan kapasitas untuk memastikan ketersediaan dan kecukupan sumber daya.

f) Pencatatan dan Pemantauan

CSP harus mengaktifkan fungsi *logging* sistem untuk memastikan bahwa perilaku penting pengguna dan insiden keamanan dapat diaudit. CSP harus menggunakan dan mengelola log secara terpusat untuk memastikan integritas dan ketersediaannya, serta meninjau kebijakan log secara teratur.

g) Pencadangan dan Pemulihan

CSP harus mengelola pencadangan dan pemulihan, menerapkan tindakan perlindungan pencadangan, dan secara berkala melakukan

pengujian pencadangan dan pemulihan untuk memenuhi persyaratan kelangsungan bisnis.

**Domain 6: Keamanan Produk Layanan Komputasi Awan**

Domain ini menjelaskan serangkaian proses untuk produk layanan komputasi awan, termasuk analisis persyaratan, pengembangan, pengujian, dan peluncuran, serta persyaratan kontrol keamanan untuk manajemen lingkungan pengembangan. Ini terutama ditujukan untuk departemen pengembangan produk CSP.

Tujuan pengelolaan domain ini adalah untuk menentukan dan memastikan keamanan layanan komputasi awan yang disediakan untuk CSC, termasuk membangun keamanan jaringan, keamanan aplikasi, keamanan data, dan kemampuan manajemen keamanan, dan untuk menentukan dan mengontrol keamanan proses pengembangan, termasuk keamanan pengembangan persyaratan, keamanan pengodean, pengujian keamanan, keamanan lingkungan pengembangan, pengujian keamanan data, dan manajemen keamanan pihak ketiga.

Persyaratan kontrol domain:

a) Keamanan Layanan Komputasi awan

   CSP harus menyediakan kemampuan manajemen keamanan (termasuk kontrol akses, transmisi aman, perlindungan keamanan aplikasi, dan keamanan data) untuk CSC.

b) Keamanan Proses Pengembangan

   CSP harus mengidentifikasi dan menganalisis persyaratan keamanan sistem, dan kemudian mengimplementasikannya dalam solusi desain dan arsitektur. CSP harus mengelola pengodean dan keamanan konfigurasi selama proses pengembangan, memastikan kualitas dan keamanan; melakukan uji keamanan dan memastikan bahwa tidak ada kerentanan keamanan yang diketahui; melakukan tes

penerimaan setelah pengembangan perangkat lunak selesai, dan mengelola proses rilis.

c) Keamanan Lingkungan Pembangunan

CSP harus melakukan kontrol keamanan atas lingkungan pengembangan dan komponen, data, dan materi yang terlibat dalam pengembangan. Misalnya, CSP menerapkan manajemen isolasi lingkungan, melakukan kontrol akses untuk kode sumber dan dokumen pengembangan, membatasi penggunaan data pengujian, dan hanya menggunakan komponen pihak ketiga yang terpercaya.

**Domain 7: Operasi Keamanan**

Domain ini menjelaskan persyaratan manajemen operasi keamanan untuk layanan komputasi awan, termasuk manajemen kerentanan, pengujian penetrasi, serta pemantauan, respons, dan pemulihan insiden keamanan. Ini terutama ditujukan untuk pusat operasi keamanan (*Security Operational Center*) atau departemen manajemen keamanan siber dari CSP.

Tujuan pengelolaan domain ini adalah untuk membangun sistem operasi keamanan komputasi awan, meningkatkan kemampuan keamanan komputasi awan serta kemampuan untuk menemukan ancaman dan kerentanan secara *real-time* serta melacak dan menanganinya secara *loop* tertutup; menetapkan proses pengujian keamanan (seperti pengujian penetrasi) untuk mendeteksi risiko keamanan sistem dengan cepat; memantau aktivitas jaringan dan *host* serta aktivitas lain secara *real-time* untuk mengidentifikasi perilaku serangan, dan mengumpulkan statistik dan melacak perilaku abnormal; mengelola insiden keamanan untuk memastikan respons yang efektif.

Persyaratan kontrol domain:

a) Manajemen Ancaman & Kerentanan

CSP harus secara berkala memindai kerentanan di platform komputasi awan dan menganalisis serta menilai setiap kerentanan yang ditemukan; menanggapi kerentanan berdasarkan kerangka waktu yang ditargetkan untuk perbaikan kerentanan; mengembangkan solusi remediasi untuk kerentanan yang teridentifikasi untuk memastikan manajemen tertutup; secara berkala meninjau kebijakan manajemen ancaman dan kerentanan.

b) Pengujian Penetrasi

CSP harus melakukan uji penetrasi secara berkala pada objek tertentu, menganalisis hasil pengujian, dan membuat laporan pengujian, serta memperbaiki dan memverifikasi kerentanan yang teridentifikasi dalam pengujian penetrasi tersebut, dan meninjau masalah yang ditemukan.

c) Pemantauan Keamanan

CSP harus melakukan pemantauan dan analisis keamanan, menyediakan pembuatan alarm, dan merekam serta menangani serangan atau perilaku abnormal.

d) Respons & Pemulihan Insiden Keamanan

CSP harus melakukan penilaian risiko, mengklasifikasikan insiden, dan mengembangkan tindakan respons yang sesuai untuk memastikan bahwa insiden dikelola secara tertutup. Setelah mengembangkan rencana tanggap insiden keamanan, CSP harus secara berkala melakukan latihan darurat untuk insiden keamanan besar dan meringkas pengalaman mereka. Mereka juga harus meninjau kebijakan respons insiden keamanan secara berkala.

**Domain 8: Operasi Bisnis**

Domain ini menjelaskan kontrol risiko keamanan yang harus dipertimbangkan dan diterapkan oleh CSP selama operasi bisnis mereka. Ini terutama ditujukan untuk departemen manajemen operasi bisnis CSP.

Tujuan pengelolaan domain ini adalah untuk menentukan dan memastikan keamanan layanan platform komputasi awan dan mencegahnya dieksploitasi secara jahat; menetapkan kontrak/perjanjian layanan terpadu dan standar berdasarkan persyaratan bisnis dan hukum/peraturan, memperkuat komunikasi dengan pengguna, dan dengan jelas mendefinisikan tanggung jawab antara CSP dan CSC untuk menghindari risiko operasional dan hukum.

Persyaratan kontrol domain:

a) Pengendalian Risiko Layanan

   CSP harus memberikan perlindungan keamanan dan kemampuan pemantauan sesuai dengan undang-undang setempat untuk mencegah sumber daya layanan komputasi awan digunakan secara ilegal atau jahat.

b) Kontrak dan Perjanjian

   CSP harus mengembangkan dan mempertahankan kontrak dan perjanjian tingkat layanan (*Service Level Agreement* /SLA) dengan CSC untuk menentukan tanggung jawab dan kewajiban kedua belah pihak, dan secara berkala meninjau kontrak dan SLA ini.

c) Transparansi dan Komunikasi

   CSP harus menetapkan dan memelihara mekanisme untuk berkomunikasi dengan CSC dan organisasi eksternal. Mereka juga harus memastikan bahwa pemangku kepentingan memiliki akses ke informasi yang dibutuhkan secara tepat waktu dan efektif.

### 7.3.2 Metode Audit

Sangat penting bagi organisasi untuk segera mengidentifikasi kekurangan kontrolnya. Dengan demikian, organisasi harus memahami keefektifan pengendaliannya dan secara teratur melakukan audit mandiri. Temuan audit dapat membantu organisasi mendapatkan gambaran lengkap tentang kepatuhannya dan mengidentifikasi kekurangan.

Untuk membentuk tolok ukur kualitas keamanan terpadu dalam suatu organisasi, kami telah mengembangkan metode audit untuk kerangka kerja audit keamanan layanan komputasi awan berdasarkan beberapa standar audit yang diakui secara internasional, dan merujuk praktik internal untuk menentukan kriteria kelulusan audit terpadu yang dapat dengan mudah dipahami untuk departemen bisnis. Ini akan memungkinkan departemen yang menerapkan kontrol keamanan untuk lebih memahami persyaratan kontrol dan hasil yang diharapkan, sementara juga memfasilitasi pemeriksaan mandiri dan pemeliharaan rangkaian bukti. Dengan melakukan tinjauan standar yang ketat dan mendokumentasikan rantai bukti, CSP dapat memastikan bahwa mereka memenuhi persyaratan sertifikasi internasional untuk kontrol yang relevan setelah melewati tinjauan persyaratan kerangka kerja audit keamanan layanan komputasi awan.

Metode audit umum meliputi wawancara (*interview*), pengujian silang (*cross-examination*), uji penelusuran (*walkthrough test*), uji pengambilan sampel (*sampling test*), observasi di tempat (*on-site observation*), tinjauan dokumen (*document review*), jalankan ulang (*re-run*), verifikasi sistem (*system verification*), tinjauan analitik (*analytical review*), validasi data (*data validation*), dan pemindaian kerentanan (*vulnerability scanning*).

Auditor dapat mengadopsi metode yang paling tepat untuk konteks organisasi. Misalnya, wawancara dan pengujian silang dapat digunakan untuk mengumpulkan informasi dari karyawan dan pemangku kepentingan tentang pengetahuan mereka tentang kontrol keamanan dan persyaratan kepatuhan. uji penelusuran dapat digunakan untuk mengevaluasi keefektifan pengendalian dalam praktiknya. Uji pengambilan sampel dapat digunakan untuk mengevaluasi efektivitas pengendalian di seluruh sampel data. Observasi di tempat dapat digunakan untuk mengevaluasi efektivitas tindakan pengendalian. Tinjauan dokumen dapat digunakan untuk

mengevaluasi kelengkapan dan keakuratan dokumentasi yang terkait dengan kontrol dan kepatuhan.

Jalankan ulang dan verifikasi sistem dapat digunakan untuk memverifikasi keefektifan kontrol dalam lingkungan yang disimulasikan. Tinjauan analitik dan validasi data dapat digunakan untuk mengevaluasi tren dan pola data, mengidentifikasi anomali dan *outlier* yang mungkin mengindikasikan risiko keamanan. Pemindaian kerentanan dapat digunakan untuk mengidentifikasi kerentanan dalam konfigurasi sistem dan aplikasi perangkat lunak. Dengan mengadopsi berbagai metode audit, auditor dapat memastikan bahwa metode tersebut mencakup semua aspek yang relevan dari persyaratan keamanan dan kepatuhan organisasi, dan mengidentifikasi setiap kekurangan atau risiko yang perlu ditangani. Masing-masing penjelasan dari metode audit yang digunakan ditampilkan seperti pada *Tabel 7-4*.

*Tabel 7-4 Jenis-jenis metode audit*

| Metode Audit | Keterangan |
|---|---|
| Wawancara | Pelajari tentang status operasi kontrol dari personel yang tepat |
| Pengujian silang | Pelajari lebih lanjut tentang pelaksanaan kontrol dari personel lain dalam organisasi |
| Uji Penelusuran | Lacak proses penanganan dalam sistem informasi atau proses bisnis untuk memverifikasi proses dan kontrol yang dipelajari |
| Uji pengambilan sampel | Melakukan pengambilan sampel dan mengumpulkan bukti untuk memverifikasi keefektifan titik kontrol |
| Pengamatan di tempat | Amati operasi kontrol yang sebenarnya di tempat |
| Peninjauan Dokumen | Memeriksa kebijakan dan proses, serta catatan dan dokumen yang dihasilkan dari pengendalian, dan menggunakannya sebagai bukti rancangan dan pelaksanaan pengendalian |

| Metode Audit | Keterangan |
|---|---|
| Jalankan ulang | Jalankan kembali prosedur kontrol tertentu untuk membuktikan bahwa prosedur tersebut berfungsi dengan benar dan efektif |
| Verifikasi sistem | Menguji apakah pengendalian aplikasi dalam sistem informasi beroperasi sesuai rancangan |
| Tinjauan analitik | Menganalisis berbagai jenis log sistem untuk memeriksa apakah ada perilaku abnormal atau perbedaan dari ekspektasi dan informasi terkait |
| Validasi data | Ekstrak data langsung dari basis data untuk memverifikasi integritas dan akurasi |
| Pemindaian Kerentanan | Gunakan alat pihak ketiga profesional untuk memindai *host* dan jaringan penting untuk potensi risiko keamanan dan kerentanan |

### 7.3.3 Metode Pengukuran

Kerangka kerja audit keamanan layanan komputasi awan dapat mempertimbangkan untuk menyediakan persyaratan kontrol keamanan terperinci bagi CSP untuk mengimplementasikan dan mengaudit langkah-langkah keamanan. Namun, sulit untuk mengevaluasi efek dari langkah-langkah ini di luar status penerapannya melalui audit. Dengan demikian, selain mengaudit, CSP harus mengukur dampak tindakan keamanan dan perlindungan privasi mereka, dan ini memerlukan metode pengukuran keamanan komputasi awan yang efektif dan layak serta metrik yang sesuai.

KAMI baru tentang pengukuran kerangka kerja audit keamanan layanan komputasi awan terutama dilakukan dengan memantau dan mengumpulkan data pada metrik utama selama suatu periode. Data tersebut kemudian dapat digunakan oleh organisasi untuk menganalisis dan memverifikasi perubahan tren keamanan komputasi awan secara menyeluruh.

Organisasi dapat memahami dan mengevaluasi kinerjanya dengan mengumpulkan sampel metrik. Dengan mengacu pada metode pengukuran

NIST SP 800-55r1 dan ISO 27004:2016 serta praktik terbaik industri, kerangka kerja audit keamanan layanan komputasi awan mengusulkan prinsip-prinsip utama berikut untuk pengembangan metrik:

a. Aktivitas yang dapat diukur: Aktivitas manajemen keamanan harus dapat diukur.
b. Proses yang dapat ditiru: Pengukuran dapat diulang selama periode tertentu.
c. Data yang dapat diperoleh: Metode pengukuran yang ditetapkan dapat memperoleh data yang efektif.
d. Hasil yang dapat dibandingkan: Data yang diperoleh melalui pengukuran dapat digunakan untuk analisis perbandingan dan tren.
e. Ketertelusuran: Metrik harus dapat dilacak ke standar dan tolok ukur yang ditetapkan, dan memberikan jejak audit yang jelas untuk melacak perubahan dan peningkatan dari waktu ke waktu.
f. Dapat ditindaklanjuti: Metrik harus dapat ditindaklanjuti, memberikan wawasan yang jelas dan dapat ditindaklanjuti ke area risiko dan peluang untuk perbaikan.
g. Aksesibilitas: Metrik harus mudah diakses dan dipahami, memungkinkan pemangku kepentingan di semua tingkatan organisasi untuk memahami dan menindaklanjuti wawasan yang mereka berikan.

Dengan mengadopsi prinsip-prinsip utama ini, organisasi dapat mengembangkan metrik yang memberikan wawasan yang berarti tentang keefektifan kontrol keamanan dan persyaratan kepatuhan mereka, serta memungkinkan mereka meningkatkan keamanan mereka dari waktu ke waktu. Setelah menentukan prinsip pengukuran, CSP dapat merancang metrik dan metode manajemen terkait dengan mengikuti siklus pengukuran dan peningkatan kerangka kerja audit keamanan layanan komputasi awan sebagaimana *Gambar 0-15*.


*Gambar 0-15 Siklus pengukuran dan peningkatan audit keamanan layanan komputasi awan*

Organisasi dapat mempertimbangkan hal-hal berikut saat merancang dan memilih metrik:

a. Kuantitas yang sesuai: Tentukan jumlah metrik yang sesuai untuk mencegah beban kerja yang berlebihan.
b. Tujuan praktis: Pertimbangkan praktik eksternal dan kondisi internal saat menetapkan tujuan manajemen keamanan dan pilih metrik yang sesuai.
c. Kerangka waktu yang wajar: Mengevaluasi seberapa sulit pengumpulan data dan apakah periode pengumpulannya wajar serta menyesuaikan frekuensi pengumpulan data jika perlu.

d. Definisi yang jelas: Definisikan metrik dengan jelas untuk memudahkan pemahaman oleh departemen/personel yang bertanggung jawab atas pengumpulan data.

### 7.3.4 Penilaian Maturitas

Kerangka kerja audit keamanan layanan komputasi awan juga dapat mempertimbangkan untuk menyediakan metode penilaian kematangan untuk membantu organisasi mengevaluasi manajemen keamanan komputasi awan dan tingkat teknologi mereka. CSP dapat menganalisis kekuatan dan kelemahan mereka di berbagai bidang keamanan komputasi awan dan menyesuaikan serta mengoptimalkan jika diperlukan. Mereka juga dapat secara intuitif menunjukkan tingkat manajemen keamanan mereka dengan menunjukkan tingkat kematangan manajemen keamanan mereka.

a. Metode penilaian kematangan kerangka kerja audit keamanan layanan komputasi awan dirancang untuk:
b. Memfasilitasi pemahaman dan pengoperasian tanpa mengharuskan asesor untuk memperoleh pengetahuan keamanan profesional.
c. Dapat memastikan kriteria evaluasi yang objektif dan jelas untuk menghindari dampak opini subjektif.
d. Dapat membandingkan hasil kematangan kerangka kerja audit keamanan layanan komputasi awan di berbagai organisasi.

Model penilaian kematangan kerangka kerja audit keamanan layanan komputasi awan mencakup berbagai bidang keamanan komputasi awan dan perlindungan privasi, termasuk tata kelola keamanan layanan komputasi awan, dukungan manajemen layanan komputasi awan, operasi DC, infrastruktur komputasi awan, dan O&M platform komputasi awan. Berdasarkan model penilaian ini, CSP dapat menilai status kontrol aktual di setiap bidang keamanan dan perlindungan privasi di tingkat manajemen dan teknologi.

Selain itu, CSP dapat memperoleh kematangan keseluruhan dari keamanan komputasi awan dan perlindungan privasi mereka berdasarkan penilaian setiap bidang dan memberikan masukan untuk perbaikan yang diperlukan. Tingkat kematangan keamanan kerangka audit keamanan layanan komputasi awan layanan komputasi awan adalah sebagai berikut:

*Tabel 7-5 Tingkat kematangan hasil audit dan deskripsinya*

| Tingkat Kematangan | Deskripsi |
|---|---|
| Initial | · CSP telah membentuk sistem manajemen keamanan berdasarkan standar industri yang diterima secara luas (seperti ISO/IEC 27001) dan menyediakan kemampuan manajemen keamanan dasar.<br>· CSP telah menerapkan kontrol keamanan yang ditentukan oleh ISO/IEC 27001 pada tingkat dasar, yang menyediakan kerangka manajemen untuk menerapkan sistem manajemen keamanan informasi (ISMS).<br>· Proses dan alat manajemen keamanan tidak dikembangkan secara sistematis tetapi diimplementasikan berdasarkan praktik.<br>· Dokumen manajemen keamanan informasi dasar tersedia. |
| Basic | · CSP telah membentuk sistem tata kelola kepatuhan dan keamanan siber layanan komputasi awan.<br>· Kontrol keamanan CSP mencakup sebagian besar kontrol yang ditentukan dalam persyaratan dasar level-1<br>· CSP telah mengembangkan dan mempertahankan proses formal dan menyediakan alat terkait.<br>· CSP telah merilis dokumen manajemen formal dan melakukan pemeliharaan rutin melalui proses formal. |
| Advanced | · CSP memiliki kemampuan untuk memenuhi sebagian besar persyaratan dasar level-2 yang ditentukan |

| Tingkat Kematangan | Deskripsi |
|---|---|
| | · CSP telah menyediakan otomatisasi proses tertentu yang didukung oleh alat yang matang.<br>· CSP mematuhi metode peninjauan dan pengukuran yang ditentukan dan melakukan penilaian rutin dan peningkatan kemampuan tata kelola keamanan komputasi awan. |
| Enhanced | · CSP memiliki kemampuan untuk memenuhi sebagian besar persyaratan dasar level-2 yang ditentukan dan memenuhi sebagian besar persyaratan tambahan level-2.<br>· CSP secara luas menggunakan teknologi dan alat manajemen yang matang sehingga memiliki kemampuan terdepan di industri dalam domain bisnis utama tertentu.<br>· Sistem tata kelola keamanan komputasi awan terus dipantau, diukur, dievaluasi, dan dioptimalkan. |
| Leading | · CSP memiliki kemampuan untuk memenuhi semua persyaratan dasar level-2 yang ditentukan serta semua persyaratan tambahan level-2.<br>· CSP secara luas menggunakan teknologi dan alat manajemen keamanan yang matang dan mampu mengembangkan solusi inovatif.<br>· CSP telah mengembangkan metodologi tata kelola keamanan yang inovatif. |

# BAB 8

# SIMPULAN DAN REKOMENDASI

## 8.1 Simpulan

Komputasi awan telah berkembang pesat di Indonesia dan telah dimanfaatkan secara luas dalam berbagai bidang. Dengan pertumbuhan ekonomi digital yang signifikan, layanan komputasi awan telah menjadi motor penggerak transformasi digital di berbagai sektor, termasuk bisnis, pemerintahan, pendidikan, dan industri lainnya. Namun, aspek keamanan komputasi awan harus menjadi sebuah perhatian penting dalam adopsi layanan komputasi awan. Keamanan komputasi awan di Indonesia menjadi urgensi penting untuk menjaga kedaulatan data, melindungi privasi, dan membangun kepercayaan pengguna. Dengan mengatasi meningkatkan keamanan layanan komputasi awan, Indonesia dapat meraih manfaat penuh dari transformasi digital serta membangun fondasi yang kokoh untuk masa depan teknologi informasi yang aman.

Pemanfaatan komputasi awan saat ini di Indonesia telah berkembang pesat dan digunakan secara luas di berbagai sektor industri dan pemerintahan. Di sektor industri komputasi awan dimanfaatkan untuk mengelola data, mengoptimalkan infrastruktur IT, dan meningkatkan efisiensi operasional. Pada sektor pemerintahan, pemanfaatan komputasi awan termasuk dalam penyediaan layanan publik, pengelolaan data, dan pengembangan SPBE. Komputasi awan menjadi pondasi untuk memberdayakan teknologi *big data*, AI, AR/VR, *IoT* dan *Blockchain* serta integrasi data dan aplikasi dari berbagai platform. Secara keseluruhan, pemanfaatan komputasi awan di Indonesia telah mengubah cara kerja dan memberikan keuntungan dalam efisiensi,

skalabilitas, aksesibilitas, dan inovasi di berbagai sektor industri dan pemerintahan.

Potensi dan risiko pemanfaatan komputasi awan dikaitkan dengan tata kelola data di Indonesia telah dianalisis melalui pendekatan PESTLE dan SWOT. Disimpulkan bahwa terdapat kekuatan utama layanan komputasi awan di Indonesia adalah pasar yang berkembang untuk layanan komputasi awan, yang didukung oleh perkembangan ekonomi digital yang pesat. Kekuatan lainnya adalah adanya peraturan pemerintah, seperti UU PDP dan PP PSTE 71/2019, yang mewajibkan langkah-langkah keamanan bagi penyedia layanan komputasi awan guna melindungi privasi dan proteksi data pelanggan. Indeks KAMI juga memberikan kesempatan bagi penyedia layanan untuk menunjukkan komitmen terhadap keamanan komputasi awan. Namun, terdapat pula risiko terkait kepemilikan data, dan kekhawatiran privasi. Perubahan kebijakan politik, keterbatasan sumber daya bagi organisasi kecil, dan kebutuhan akan peningkatan edukasi dan kesadaran mengenai keamanan komputasi awan menjadi tantangan yang harus diatasi. Peraturan pemerintah terkait kedaulatan data, residensi data, dan aliran data lintas batas perlu diperbaiki. Dengan peraturan yang lebih jelas dan tegas, akan tercipta landasan yang kuat untuk melindungi data pelanggan, menjaga kedaulatan data nasional, dan mengatur transfer data secara aman lintas batas. Regulasi harus dapat memberikan kepastian hukum bagi penyedia dan pengguna layanan komputasi awan, serta membangun kepercayaan pelanggan terkait privasi dan keamanan data mereka.

Strategi mewujudkan keamanan komputasi awan dan tata kelola data di Indonesia pada kajian ini dihasilkan dengan sebuah kerangka kerja dan tata kelola yang bertujuan untuk meningkatkan daya saing ekonomi digital nasional, nilai data yang andal, serta mempercepat transformasi digital di sektor pemerintahan maupun industri. Kerangka kerja tersebut mencakup langkah-langkah yang perlu diimplementasikan untuk mencapai tujuan

tersebut, antara lain mempertahankan kedaulatan data nasional dengan menerapkan undang-undang residensi data, mengoptimalkan pemanfaatan data melalui transformasi digital pemerintahan dan industri, serta merumuskan aturan yang memfasilitasi transfer data lintas batas yang adil dan menguntungkan semua pemangku kepentingan. Dengan adopsi kerangka kerja dan tata kelola ini, diharapkan dapat tercipta lingkungan yang kondusif bagi pertumbuhan ekonomi digital yang berkelanjutan, perlindungan data yang memadai, serta peningkatan efisiensi dan inovasi dalam pemerintahan dan industri.

## 8.2 Rekomendasi

Tinjauan strategis ini memberikan beberapa rekomendasi kepada tiga pihak yaitu pemerintah, penyedia, dan pengguna layanan komputasi awan.

**a. Rekomendasi bagi Pemerintah**

Pemerintah dapat mempertimbangkan menerapkan regulasi yang ketat dengan mengeluarkan undang-undang dan regulasi yang jelas terkait keamanan layanan komputasi awan. Regulasi ini harus mencakup persyaratan keamanan yang harus dipatuhi oleh penyedia layanan komputasi awan untuk melindungi data pelanggan. Selain itu, perlu juga dibuat undang-undang tentang residensi data. Dalam hal ini, pemerintah harus merumuskan undang-undang yang memastikan bahwa data pelanggan disimpan dan diproses di wilayah yang diatur oleh hukum yang sama dengan pelanggan. Klasifikasi data berdasarkan tingkat kerahasiaan serta aliran data lintas batas perlu diatur pada undang-undang ini. Hal ini akan membantu menjaga privasi dan kedaulatan data.

Pemerintah dapat mempertimbangkan membentuk/menugaskan badan pengawas keamanan komputasi awan atau lembaga yang bertanggung jawab untuk mengawasi dan mengevaluasi keamanan

layanan komputasi awan. Badan ini harus dapat memastikan bahwa penyedia layanan mematuhi kepatuhan standar keamanan yang ditetapkan dan melaksanakan audit keamanan secara berkala. Perlu juga dibentuk/ditunjuk lembaga independen untuk menegakkan hukum dan peraturan perlindungan data pribadi. Lembaga ini akan memiliki peran penting dalam mengawasi implementasi dan kepatuhan terhadap regulasi yang berkaitan dengan perlindungan data pribadi. Hal ini akan memberikan keyakinan kepada pelanggan bahwa data pribadi mereka dilindungi dengan baik.

Terkait dengan kepercayaan kepada penyedia layanan, pemerintah perlu mengembangkan sertifikasi keamanan yang memastikan bahwa penyedia layanan komputasi awan memenuhi persyaratan keamanan tertentu. Sertifikasi ini dapat membantu pelanggan dalam memilih penyedia layanan yang memiliki tingkat keamanan yang tinggi.

Pemerintah perlu mempertimbangkan untuk memperbarui (*update*) indeks KAMI agar selaras dengan ISO 27001:2022. *Update* ini diharapkan dapat mengukur tingkat kematangan keamanan komputasi awan. Dengan mengadopsi standar ISO 27001:2022 ini, indeks KAMI diharapkan dapat mengevaluasi kesesuaian dan kepatuhan penyedia layanan komputasi awan yang dilakukan secara mandiri.

Pemerintah diharapkan menyediakan pendidikan dan pelatihan keamanan untuk meningkatkan kesadaran dan pemahaman masyarakat serta tenaga kerja terkait keamanan layanan komputasi awan. Hal ini akan membantu mengurangi risiko keamanan yang disebabkan oleh kurangnya pengetahuan dan kesadaran. Pemerintah juga perlu mendorong inovasi teknologi keamanan dengan memberikan insentif dan dukungan untuk penelitian dan

pengembangan teknologi keamanan yang inovatif dalam konteks komputasi awan. Ini akan membantu meningkatkan tingkat keamanan secara keseluruhan dalam industri layanan komputasi awan.

Pada lingkup global, pemerintah diharapkan mampu mendorong kerjasama internasional dengan negara lain untuk mengembangkan kerangka kerja keamanan yang seragam dan standar internasional untuk layanan komputasi awan. Hal ini akan memfasilitasi pertukaran informasi dan kerjasama dalam mengatasi ancaman keamanan yang bersifat lintas batas.

**b. Rekomendasi bagi Penyedia Layanan**

Bagi penyedia layanan komputasi awan, tinjauan strategis ini memberikan rekomendasi sebagai berikut. Penyedia layanan komputasi awan wajib mengimplementasikan praktik keamanan yang kuat yakni praktik keamanan terbaik yang relevan, seperti enkripsi data, otentikasi kuat, pengelolaan akses yang ketat, dan pemantauan keamanan siber yang terus-menerus. Hal ini akan membantu melindungi data pelanggan dari ancaman keamanan. Selanjutnya, Penyedia layanan komputasi awan wajib menyelenggarakan penyediaan infrastruktur yang aman. Harus dipastikan bahwa infrastruktur fisik dan teknis yang digunakan untuk menyediakan layanan komputasi awan telah diimplementasikan dengan langkah-langkah keamanan yang memadai. Termasuk di dalamnya adalah perlindungan fisik, keamanan jaringan, dan pemisahan yang jelas antara lingkungan komputasi pelanggan.

Penyedia layanan komputasi awan juga wajib melakukan audit keamanan reguler. Hal ini dimaksudkan untuk memastikan bahwa sistem dan proses keamanan berfungsi dengan baik. Audit ini harus mencakup pemindaian kerentanan, penilaian risiko, dan pengecekan

kepatuhan terhadap standar keamanan. Selain itu, perlu juga dilakukan peningkatan kesadaran pengguna yakni penyedia layanan harus memberikan edukasi dan pelatihan keamanan kepada pengguna layanan komputasi awan. Ini termasuk menjelaskan praktik keamanan yang disarankan, tindakan pencegahan yang dapat diambil, dan peran pengguna dalam menjaga keamanan data mereka.

Penyedia layanan komputasi awan perlu memberikan transparansi kepada pelanggan tentang praktik keamanan mereka, termasuk kepatuhan terhadap standar keamanan dan regulasi yang berlaku. Hal ini dapat meningkatkan kepercayaan dan memperkuat hubungan antara penyedia layanan dan pelanggan. Selain itu, ini juga mendorong penyedia layanan untuk terus meningkatkan praktik keamanan mereka agar sesuai dengan perkembangan teknologi dan ancaman keamanan yang baru muncul.

Penyedia layanan perlu menerapkan kebijakan "*zero trust*". Melalui pendekatan ini, setiap entitas, baik itu pengguna, perangkat, atau jaringan, dianggap tidak dapat dipercaya secara *default*, bahkan walaupun jika mereka telah memperoleh akses awal yang sah. Dengan menerapkan prinsip "*never trust, always verify*" penyedia layanan komputasi awan dapat mencegah pelanggaran keamanan.

Terkait pemulihan bencana dan rencana kontinuitas bisnis, penyedia layanan harus memiliki rencana pemulihan bencana yang komprehensif dan rencana kontinuitas bisnis. Ini akan memastikan bahwa layanan dapat dipulihkan dengan cepat setelah kejadian bencana dan menjaga ketersediaan layanan yang kontinu. Terkait kolaborasi dengan pihak ketiga, penyedia layanan dapat bekerja sama dengan pihak ketiga yang memiliki keahlian keamanan untuk melakukan audit independen, penilaian risiko, atau pengujian

penetrasi. Kolaborasi ini dapat membantu mengidentifikasi celah keamanan potensial dan memberikan saran untuk meningkatkan keamanan.

**c. Rekomendasi bagi Pengguna Layanan**

Hendaknya pengguna layanan komputasi awan memilih penyedia jasa yang terpercaya dengan melakukan riset mendalam tentang penyedia layanan komputasi awan sebelum memilihnya. Pastikan penyedia tersebut memiliki kepatuhan terhadap standar serta reputasi yang baik dalam hal keamanan dan privasi data.

Terkait akses data, pengguna perlu memastikan telah menggunakan autentikasi yang kuat, seperti penggunaan kata sandi yang kompleks, otentikasi dua faktor, dan otentikas multi-faktor. Ini akan membantu melindungi akun dari akses yang tidak sah. Selain itu, Pengguna juga perlu melakukan enkripsi data: Keamanan data aplikasi pada komputasi awan merupakan tanggungjawab bersama antara penyedia dengan pengguna. Selalu lakukan enkripsi data sebelum mengirimkannya ke *cloud* atau saat berada dalam penyimpanan *cloud*. Hal ini akan menjaga kerahasiaan data bahkan jika ada pelanggaran keamanan. Lebih lanjut, Pengguna perlu menetapkan hak akses yang tepat untuk masing-masing pengguna. Gunakan prinsip "*least of privilage*" dengan membatasi akses hanya untuk orang yang membutuhkannya dan memberikan izin seminimal mungkin sesuai dengan tugas dan tanggung jawab mereka.

Pengguna juga perlu melakukan *backup* data secara teratur. Buat kebiasaan untuk melakukan *backup* data secara teratur. Ini akan membantu dalam pemulihan data jika terjadi kehilangan atau kerusakan data. Perhatikan kebijakan privasi dan keamanan, teliti kebijakan privasi dan keamanan yang ditetapkan oleh penyedia jasa

komputasi awan. Pastikan kebijakan tersebut sesuai dengan kebutuhan dan standar keamanan. Pengguna harus selalu melakukan pemantauan dan pembaruan. Pastikan secara teratur memantau aktivitas dan log keamanan dari layanan komputasi awan yang digunakan. Selain itu, pastikan untuk menginstal pembaruan keamanan segara mungkin.

Pengguna perlu mengikuti pelatihan untuk meningkatkan kesadaran keamanan. Pengguna perlu mengikuti perkembangan terbaru dalam hal keamanan komputasi awan. Hal ini akan membantu mencegah serangan seperti *phishing* atau serangan yang dapat mengancam keamanan data. Terakhir, pengguna perlu memeriksa kontrak layanan dengan cermat berupa *service-level agreement* (SLA) yang ditawarkan oleh penyedia jasa komputasi awan. Pastikan aspek keamanan dan perlindungan data diatur dengan jelas dalam kontrak tersebut.

# DAFTAR PUSTAKA


Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Al Jum'ah, M. N. (2019). Analisa Keamanan Dan Hukum Untuk Pelindungan Data Privasi. *Cyber Security Dan Forensik Digital*, *1*(2), 39–44. https://doi.org/10.14421/csecurity.2018.1.2.1370

AlAhmad, A. S., Kahtan, H., Alzoubi, Y. I., Ali, O., & Jaradat, A. (2021). Mobile cloud computing models security issues: A systematic review. *Journal of Network and Computer Applications*, *190*, 103152. https://doi.org/10.1016/j.jnca.2021.103152

Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth Cloud Security Challenges: A Survey. *Journal of Healthcare Engineering*, *2019*, 1–15. https://doi.org/10.1155/2019/7516035

Alkhater, N., Chang, V., Wills, G., & Walters, R. (2015). Towards an Integrated Conceptual Model for Komputasi awan Adoption in Saudi Arabia. *Proceedings of the 2nd International Workshop on Emerging Software as a Service and Analytics*, 80–85. https://doi.org/10.5220/0005528400800085

Andani, S. R. (2021). Analysis of Information Security in Data Leaks in The PeduliLindungi Application. *The IJICS (International Journal of Informatics and Computer Science)*, *5*(3), 246. https://doi.org/10.30865/ijics.v5i3.3406

Anshori, M. F., & Ramadhan, R. A. (2019). Kepentingan Singapura pada Keamanan Siber di Asia Tenggara dalam Singapore International Cyber Week.

*Padjadjaran Journal of International Relations*, *1*(1), 39. https://doi.org/10.24198/padjir.v1i1.21591

Apache ServiceComb. (2023). *Apache ServiceComb*. Apache.Org. https://servicecomb.apache.org/

AWS. (2023). *Global Infrastructure Regions & AZs*. Aws.Amazon.Com. https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

Azure. (2023). *Global Infrastructure*. Azure.Microsoft.Com. https://azure.microsoft.com/en-us/explore/global-infrastructure/

Barracuda. (2020). *Future shock: The* Komputasi awan *is the New Network*.

Bobrowski, S. (n.d.). *Platform Multitenant Architecture | Salesforce Architects*. Retrieved April 17, 2023, from https://architect.salesforce.com/fundamentals/platform-multitenant-architecture

Boston Consulting Group. (2023). *Indonesia | Economic Impact of Public* Komputasi awan *in APAC | BCG*. Bcg.Com. https://www.bcg.com/publications/2019/economic-impact-public-komputasi awan-apac/indonesia

BSSN. (2021). *Indeks KAMI*. https://bssn.go.id/indeks-kami/

*BSSN Gelar Business Continuity Plan Drill Tingkatkan Kesiapan dan Kemampuan Respons Insiden Siber Unit Kerja BSSN*. (2020). Bssn.Go.Id. https://bssn.go.id/bssn-gelar-business-continuity-plan-drill-tingkatkan-kesiapan-dan-kemampuan-respons-insiden-siber-unit-kerja-bssn/

Butpheng, C., Yeh, K.-H., & Xiong, H. (2020). Security and Privacy in IoT-Komputasi awan-Based e-Health Systems—A Comprehensive Review. *Symmetry*, *12*(7), 1191. https://doi.org/10.3390/sym12071191

Center for Internet Security. (2021). *CIS Critical Security Controls, Version 8*. 59.

Check Point. (2022). *Cloud Security Report*.

CHERCIU, N. (2020). Non-personal data processing-why should we take it personally? *European Journal of Privacy Law & Technologies*.

Chou, D. (2018). Komputasi awan *Service Models (IaaS, PaaS, SaaS) Diagram*. https://dachou.github.io/2018/09/28/komputasi awan-service-models.html

Chuldun, Z. N., Marlena, D., Priambodo, D. F., & Arizal. (2022). Multilayers Physical Authentication and NoSQL PRESENT algorithm for Data Center. *2022 FORTEI-International Conference on Electrical Engineering (FORTEI-ICEE)*, 26–31. https://doi.org/10.1109/FORTEI-ICEE57243.2022.9972986

Cloud Security Alliance. (2018). *Cloud Security Alliance Code of Conduct for GDPR Compliance*. *June*, 3.

Cloud Security Alliance. (2020a). *CSA STAR*. https://cloudsecurityalliance.org/star

Cloud Security Alliance. (2020b). Top Threats to Cloud computing: Egregious Eleven Deep Dive. Cloud security *Alliance*, 1–30.

Cloud Security Alliance. (2022). *Top Threats to* Cloud computing *Pandemic Eleven*.

Cloud Security Alliance. (2023). *STAR | CSA*. https://cloudsecurityalliance.org/star/

CNCF. (2023). *Cloud Native Computing Foundation*. Cncf.Io. https://www.cncf.io/

CSA. (2019). *Top Threats to* Cloud computing*: Egregious Eleven*.

Singapore`s Cybersecurity Strategy, (2016).

Cybersecurity insiders. (2022). *Cloud Security Report 2022 2 Fortinet*. 1–25.

Dang, L. M., Piran, Md. J., Han, D., Min, K., & Moon, H. (2019). A Survey on Internet of Things and Cloud computing for Healthcare. *Electronics*, *8*(7), 768. https://doi.org/10.3390/electronics8070768

Das, P. K., Hu, B., Liu, C., Cui, K., Ranjan, P., & Xiong, G. (2019). A New Approach for Face Anti-Spoofing Using Handcrafted and Deep Network Features. *Proceedings - IEEE International Conference on Service Operations and Logistics, and Informatics 2019, SOLI 2019*, 33–38. https://doi.org/10.1109/SOLI48380.2019.8955089

Das, S. K., Kant, K., & Zhang, N. (2012). Handbook on Securing Cyber-Physical Critical Infrastructure. In *Handbook on Securing Cyber-Physical Critical Infrastructure*. Elsevier. https://doi.org/10.1016/C2011-0-04434-4

Dechert LLP. (2022). *EU Data and Digital Drive: an Overview of Forthcoming Legislation*.

Digital News Asia. (2022, June 24). *IDC reveals journey and priorities for a digital-first economy*. https://www.digitalnewsasia.com/business/idc-reveals-journey-and-priorities-digital-first-economy

Drath, R., & Horch, A. (2014). Industrie 4.0: Hit or Hype? [Industry Forum]. *IEEE Industrial Electronics Magazine*, *8*(2), 56–58. https://doi.org/10.1109/MIE.2014.2312079

Duncan, R., Burgener, E., Buss, A., Butler, B., Casemore, B., Cooke, J., Filkins, P., Johnston Turner, M., Mccarthy, D., Moohan, D., Nadkarni, A., Rau, S., Roberti, G., Rutten, P., Solis, P., Villars, R., & West, H. (2020). *IDC TechScape: Worldwide Future of Digital Infrastructure*.

EU.Commission. (2019). *The European* komputasi awan *strategy*. *May*, 6–8.

European Commission. (2012). Unleashing the Potential of Cloud computing in Europe. *Communication From the Commission To the European Parliament, the*

*Council, the European Economic and Social Committee and the Committee of the Regions*, 1–16.

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on Human-Centered IoT-Connected Smart Labels for the Industry 4.0. *IEEE Access*, *6*, 25939–25957. https://doi.org/10.1109/ACCESS.2018.2833501

Fortinet. (2021). *Cloud Security Report 2021*.

Freemantle, P. (2010). Cloud Native. https://wso2.com/library/articles/2010/05/blog-post-komputasi awan-native/

Friedlingstein, P., Jones, M. W., O'Sullivan, M., Andrew, R. M., Hauck, J., Peters, G. P., Peters, W., Pongratz, J., Sitch, S., Quéré, C. Le, DBakker, O. C. E., Canadell1, J. G., Ciais1, P., Jackson, R. B., Anthoni1, P., Barbero, L., Bastos, A., Bastrikov, V., Becker, M., … Zaehle, S. (2019). Global carbon budget 2019. *Earth System Science Data*, *11*(4), 1783–1838. https://doi.org/10.5194/ESSD-11-1783-2019

Fujitsu. (2021). Priorities in the post-pandemic world. In *Fujitsu Future Insights*.

G Ngqondi, T. (2009). The ISO / IEC 27002 and ISO / IEC 27799 Information Security Management Standards : A Comparative Analysis from a Healthcare Perspective Tembisa G . Ngqondi Magister Technologiae School of Information and Communication Technology Faculty of Engineering ,. In *Thesis*.

G-20, K. (2022). *G20 BALI LEADERS' DECLARATION* (Issue November).

Gartner. (2020a). *The State of Privacy and Personal Data Protection*. https://www.gartner.com/en/documents/3989495

Gartner. (2020b). *The State of Privacy and Personal Data Protection*.

Gartner. (2021). *Market Share: IT Services, Worldwide*. Gartner.Com. https://www.gartner.com/en/documents/4013377

Gartner, Inc. (2022). *Gartner Forecasts Worldwide Public* Komputasi awan *End-User Spending to Reach Nearly $500 Billion in 2022*. STAMFORD, Conn. https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-komputasi awan-end-user-spending-to-reach-nearly-500-billion-in-2022

Germanos, V., Zeng, W., Saqib, N., & Maglaras, L. (2020). *Mapping of the Security Requirements of GDPR and NIS Privacy-preservation View project Concurrent Interactions View project Mapping of the Security Requirements of GDPR and NIS*.

Gillwald, A., & Mothobi, O. (2019). *AFTER ACCESS 2018 A DEMAND-SIDE VIEW OF MOBILE INTERNET FROM 10 AFRICAN COUNTRIES*. https://researchictafrica.net/2019_after-access_africa-comparative-report/

Giulio, C. Di, Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R. H., & Bashir, M. N. (2017). Komputasi awan Standards in Comparison: Are New Security Frameworks Improving Cloud Security? *2017 IEEE 10th International Conference on* Cloud computing *(*KOMPUTASI AWAN*)*, *2017-June*, 50–57. https://doi.org/10.1109/KOMPUTASI AWAN.2017.16

Gizem Erboz. (2017). How to Define Industry 4.0: The Main Pillars of Industry 4.0. *Managerial Trends in the Development of Enterprises in Globalization Era*, *November 2017*, 761–767.

Granger, M.-P., & Irion, K. (2014). *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection Analysis and Reflections The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection*. http://europeanlawblog.eu/?p=2289#sthash.Ju0PiCyJ.dpufhttp://europeanlawblog.eu/?s=digital

Greenleaf, G. (2023). *Bangladesh's Data Protection Bill*.

Gui, A., Fernando, Y., Shaharudin, M. S., Mokhtar, M., Karmawan, I. G. M., & Suryanto, -. (2020). Cloud computing Adoption Using TOE Framework for Indonesia's Micro Small Medium Enterprises. *JOIV : International Journal on Informatics Visualization*, *4*(4), 237. https://doi.org/10.30630/joiv.4.4.458

Gui, A., Fernando, Y., Shaharudin, M. S., Mokhtar, M., Karmawan, I. G. M., & Suryanto, -. (2021). Drivers of Cloud computing Adoption in Small Medium Enterprises of Indonesia Creative Industry. *JOIV : International Journal on Informatics Visualization*, *5*(1), 69. https://doi.org/10.30630/joiv.5.1.461

Gurol, J., Zumbrägel, T., & Demmelhuber, T. (2022). Elite Networks and the Transregional Dimension of Authoritarianism:Sino-Emirati Relations in Times of a Global Pandemic. *Journal of Contemporary China*. https://doi.org/10.1080/10670564.2022.2052444

Halim, E. F. (2022). Perlindungan Hukum Data Pribadi Pembeli Di Perdagangan Secara Elektronik (E-Commerce) di Indonesia. *Jurnal Hukum Visio Justisia*, *2*(1).

Hamad, M., Kuwaiti, A., & Kaissi, T. M. Al. (2022). A Comprehensive Reconsideration of Cloud security Approach. *Journal of Cybersecurity*, *4*(1), 51.

Hitchens, T., & Goren, N. (2017). International Cybersecurity Information Sharing Agreements. In *Center for International & Security Studies* (pp. 1–141).

Hofmann, E., & Rüsch, M. (2017). Industry 4.0 and the current status as well as future prospects on logistics. *Computers in Industry*, *89*, 23–34. https://doi.org/https://doi.org/10.1016/j.compind.2017.04.002

Huawei. (2021). *Building a Fully Connected, Intelligent World*.

Huawei. (2022). *Cloud Native 2.0 Architecture White Paper*.

Huawei Enterprise. (2019.). *Digital Platforms Enable DX*. Retrieved April 17, 2023, from

https://e.huawei.com/es/publications/global/ict_insights/201810161444/analysts/201906101000

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, *8*(1), 205395172098201. https://doi.org/10.1177/2053951720982012

ISC. (2022). Cloud security *Report*.

ISO/IEC. (2011a). *ISO/IEC 27034-1:2011 - Information technology — Security techniques — Application security — Part 1: Overview and concepts*. https://www.iso.org/standard/44378.html

ISO/IEC. (2011b). *ISO/IEC 29100:2011 - Information technology — Security techniques — Privacy framework*. https://www.iso.org/standard/45123.html

ISO/IEC. (2012). *ISO/IEC 19790:2012 - Information technology — Security techniques — Security requirements for cryptographic modules*. https://www.iso.org/standard/52906.html

ISO/IEC. (2014). ISO/IEC 17788 -Y. 3500 SERIES Y- Information technology - Cloud computing - Overview and vocabulary. *Itu Series Y*, *ITU Y.3500*, 1–16.

ISO/IEC. (2015). *ISO/IEC 27017:2015 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for* komputasi awan *services*. https://www.iso.org/standard/43757.html

ISO/IEC. (2017a). *ISO/IEC 29151:2017 - Information technology — Security techniques — Code of practice for personally identifiable information protection*. https://www.iso.org/standard/62726.html

ISO/IEC. (2017b). *ISO/IEC 38505-1:2017 - Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data*. https://www.iso.org/standard/56639.html

ISO/IEC. (2018a). *ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management*. https://www.iso.org/standard/75281.html

ISO/IEC. (2018b). *ISO/IEC 29101:2018 - Information technology — Security techniques — Privacy architecture framework*. https://www.iso.org/standard/75293.html

ISO/IEC. (2019a). *ISO/IEC 27018:2019 - Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*. https://www.iso.org/standard/76559.html

ISO/IEC. (2019b). *ISO/IEC 27701:2019(en), Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en

ISO/IEC. (2020). *ISO/IEC 27014:2020 - Information security, cybersecurity and privacy protection — Governance of information security*. https://www.iso.org/standard/74046.html

ISO/IEC. (2022a). *ISO/IEC 27001 Standard – Information Security Management Systems*. https://www.iso.org/standard/27001#lifecycle

ISO/IEC. (2022b). *ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls*. https://www.iso.org/standard/75652.html

Istio. (2023). *Istio*. https://istio.io/

ITU. (2018). Global Cybersecurity Index 2018. In *Measuring the Digital Transformation*.

Jonas, E., Schleier-Smith, J., Sreekanti, V., Tsai, C.-C., Khandelwal, A., Pu, Q., Shankar, V., Carreira, J., Krauth, K., Yadwadkar, N., Gonzalez, J. E., Popa, R.

A., Stoica, I., & Patterson, D. A. (2019). Komputasi awan *Programming Simplified: A Berkeley View on Serverless Computing*.

Kalkan, K. ;, Kwansa, F. ;, & Cobanoglu, C. (n.d.). Journal of Hospitality Financial Management Journal of Hospitality Financial Management The Professional Refereed Journal of the International Association of Hospitality Financial The Professional Refereed Journal of the International Association of Hospitality Financial Management Educators Management Educators. In *Journal of Hospitality Financial Management* (Vol. 16, Issue 2).

Kamara, I., & Boom, J. Van Den. (2022). *Computer Security Incident Response Teams in the reformed Network and Information Security Directive: good practices*.

KBV Research. (2022). *Asia Pacific* Cloud security *Market Size, Share & Industry Trends Analysis Report By Organization Size, By Vertical, By Application, By Service Model, By Security Type, By Country and Growth Forecast, 2021-2027*. https://www.researchandmarkets.com/reports/5571264/asia-pacific-komputasi awan-security-market-size-share-and

Kirimtat, A., Krejcar, O., Kertesz, A., & Tasgetiren, M. F. (2020). Future Trends and Current State of Smart City Concepts: A Survey. *IEEE Access*, *8*, 86448–86467. https://doi.org/10.1109/ACCESS.2020.2992441

Lee, H. Y., Tao, Y.-S., & Lee, H.-Y. (n.d.). *Bridging* Cloud security *and Data Protection, using MTCS and ISO27018 Data Certification View project Technology Crowdsourcing View project Bridging* Cloud security *and Data Protection, using MTCS and ISO27018*. https://doi.org/10.13140/RG.2.2.13282.53444

Magnusson, L., & Iqbal, S. (2018). Implications of EU-GDPR in Low-Grade Social, Activist and NGO Settings. *International Journal of Business & Technology*, *6*(3), 1–7. https://doi.org/10.33107/ijbte.2018.6.3.07

Maliatsos, A. K., Lambrinoudakis, C., Menegatos, A., Lyvas, C., Kanatas, A., Kalloniatis, C., Mancilla, R. O., Vito, P. De, & Giannakoulias, A. (2022). *D2.2*

*Analysis NIS directive Cross domain threats and proof of concepts Work Package 2 Task T2.2 Cross-domain threat analysis*.

Marc, J. (2022). *Outcome of the 2022 G20 summit in Bali, Indonesia*. European Parliamentary Research Service.

Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review*, *35*(6), 105336. https://doi.org/10.1016/j.clsr.2019.06.007

McKinsey. (2020). How COVID-19 has pushed companies over the technology tipping point-and transformed business forever. *McKinsey Global Publishing*, *October*, 1–9.

The NIST Definition of Cloud computing, NIST Special Publication 800-145 7 (2011).

Menon, N., & Santhanam, P. (2021). *The Future of* Komputasi awan *in Asia Pacific* (Issue August).

Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik, Pub. L. No. 11 (2016).

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, Pub. L. No. 27, 1 (2022).

Michels, J. D., & Walden, I. (2020a). *Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?* https://www.ft.com/content

Michels, J. D., & Walden, I. (2020b). *Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?*

Microsoft. (2022). *Shared responsibility in the* komputasi awan | *Microsoft Learn*.

Mobo, F. D. (2018). Cloud computing Security, Privacy and Forensics: Issues and Challenges Ahead. *International Journal of Recent Trends in Engineering and Research*, *4*(3), 10–13. https://doi.org/10.23883/IJRTER.2018.4083.XWPNA

Mondal, A., Paul, S., Goswami, R. T., & Nath, S. (2020). Cloud computing security issues & challenges: A Review. *2020 International Conference on Computer Communication and Informatics (ICCCI)*, 1–5. https://doi.org/10.1109/ICCCI48352.2020.9104155

Nassif, A. B., Talib, M. A., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine Learning for Cloud security: A Systematic Review. *IEEE Access*, *9*, 20717–20735. https://doi.org/10.1109/ACCESS.2021.3054129

Netwrix. (2022). Komputasi awan *Data Security Report*.

NIST. (2020a). *NIST PRIVACY FRAMEWORK:* https://doi.org/10.6028/NIST.CSWP.01162020

NIST. (2020b). *Privacy Framework*. https://doi.org/10.6028/NIST.CSWP.01162020

NIST Cybersecurity Framework Team. (2018). Framework for Improving Critical Infrastructure Cybersecurity. *Proceedings of the Annual ISA Analysis Division Symposium*, *535*, 9–25.

NITDA. (2001). *NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY ACT 2007 A BILL FOR An Act to provide for the establishment of the NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY (NITDA) and related matters*.

O'Connell, N. (2019). *Saudi Arabia's* cloud computing *regulatory framework 2.0*.

Osterman Research. (2022). *State of* Cloud security *Maturity 2022 Survey Findings*. *August*.

Otto, B. (2022). Designing Data Spaces. In *Designing Data Spaces*. Springer International Publishing. https://doi.org/10.1007/978-3-030-93975-5

P C I Security Standards Council. (2023). *Official PCI Security Standards Council Site*.

Pemerintah Republik Indonesia. (2012). *Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik*.

Pemerintah Republik Indonesia. (2019). *Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik*.

Prabowo, W., Wibawa, S., & Azmi, F. (2020). Perlindungan Data Personal Siber di Indonesia. *Padjadjaran Journal of International Relations*, *1*(3), 218. https://doi.org/10.24198/padjir.v1i3.26194

Proton AG. (2023). *Complete guide to GDPR compliance*.

Purnama, A., Mayasari, D., & Abdullah, Y. (2022). News Media Text Analysis Regarding Personal Data Leakage on the Main Page of Harian Kompas. *Journal of Humanities, Social Sciences and Business (Jhssb)*, *2*(1), 317–334. https://doi.org/10.55047/jhssb.v2i1.476

PwC Consulting Indonesia. (2021). *The Impact of* Cloud computing *on The Indonesian Economy* (Vol. 6, Issue September).

Raditya, M., Dewanto, P., Oktavia, T., & Sundaram, D. (2022). Comparative Study of Information Security Evaluation Models for Indonesia Government. *Journal of Theoretical and Applied Information Technology*, *28*, 2022.

Raghavan, A., Demircioglu, M. A., & Taeihagh, A. (2021). Public health innovation through komputasi awan adoption: A comparative analysis of drivers and barriers in Japan, South Korea, and Singapore. *International Journal of Environmental Research and Public Health*, *18*(1), 1–30. https://doi.org/10.3390/ijerph18010334

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. https://doi.org/10.6028/NIST.SP.800-207

Salam, N., & Investment, S. A. (2020). Determining factors of cloud computing adoption: a study of Indonesian local government employees. *Pdfs.Semanticscholar.Org*, *21*(2). https://doi.org/10.18196/jai.2102151

Saxena, D., Gupta, R., & Singh, A. K. (2021). *A Survey and Comparative Study on Multi-*Komputasi awan *Architectures: Emerging Issues And Challenges For* Komputasi awan *Federation*.

Sidabutar, J., & Priambodo, D. F. (2022). TIA-942 Approach dengan Computational Fluid Dynamic untuk Data Center. *Jurnal Informatika Universitas Pamulang*, *6*(4), 721–726. https://doi.org/10.32493/informatika.v6i4.12874

Singh, K. P., Rishiwal, V., & Kumar, P. (2018). Classification of Data to Enhance Data Security in Cloud computing. *Proceedings - 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages, IoT-SIU 2018*. https://doi.org/10.1109/IOT-SIU.2018.8519934

Sinulingga, D. A. (2022). Legal Certainty of Aggregate Data Utilization in The Design of Personal Data Protection Bill. *Jambura Law Review*, *4*(1).

Thakkar, A., & Lohiya, R. (2021). A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges. *Archives of Computational Methods in Engineering*, *28*(4), 3211–3243. https://doi.org/10.1007/s11831-020-09496-0

The Linux Foundation. (n.d.). *Kubernetes*. Retrieved January 26, 2023, from https://kubernetes.io/

Titie, O., Natalia, S., Baturaja, U., & Anzani, E. (2022). Tanggung Jawab Bank Terhadap Penyalahgunaan Data Informasi Nasabah. *Justicia Sains: Jurnal Ilmu Hukum*, *07*(02).

Varshneya, K. (n.d.). *Understanding Design of Microservices Architecture at Netflix*. Retrieved April 17, 2023, from

https://www.techaheadcorp.com/blog/design-of-microservices-architecture-at-netflix/

Velichko, I. (2021). *Sidecar Proxy Pattern - The Basis Of Service Mesh*. https://iximiuz.com/en/posts/service-proxy-pod-sidecar-oh-my/

Vijaya, C. J., Narasimham, C., & Kiran, P. S. (2019). Authentication and Authorization Mechanism for Cloud security. *International Journal of Engineering and Advanced Technology*, *8*(6), 2072–2078. https://doi.org/10.35940/ijeat.F8473.088619

VMware, Inc. (2023). *Spring* Komputasi awan. Spring.Io. https://spring.io/projects/spring-komputasi awan

Watubun, K. (2022). *Geopolitik dan Kedaulatan Data Digital Negara*. Kompas. https://www.kompas.com/tren/read/2022/12/19/132849265/geopolitik-dan-kedaulatan-data-digital-negara

Yang, P., Xiong, N., & Ren, J. (2020). Data Security and Privacy Protection for Komputasi awan Storage: A Survey. *IEEE Access*, *8*, 131723–131740. https://doi.org/10.1109/ACCESS.2020.3009876

Yu, S., Lou, W., & Ren, K. (n.d.). Chapter 5.3: Data Security in Cloud computing. In *University of Arkansas* (pp. 1–29). Retrieved April 26, 2023, from https://www.cnsr.ictas.vt.edu/publication/chapter/BookChapter_Yu12.pdf

Zubri, N. (2021a). *insights | Google* Komputasi awan*: The Uncanny Leader in Indonesia*. Twimbit.Com. https://twimbit.com/insights/google-komputasi awan-the-uncanny-leader

Zubri, N. (2021b, January 11). *Indonesia Public* Komputasi awan *market grew to US$435.4million*. https://twimbit.com/insights/indonesias-2020-public-komputasi awan-market-is-worth-us-435-5million

# DAFTAR ISTILAH

***Cloud Computing* (Komputasi Awan):** Model sumber daya komputasi yang dapat diakses di mana pun melalui jaringan internet dan dapat digunakan sesuai kebutuhan

***Data Governance* (Tata Kelola Data)**: Serangkaian proses, kebijakan, dan kontrol yang mengatur bagaimana data dihasilkan, disimpan, diproses, ditransfer, diperbarui dan dihapus.

***Artificial Intelligence* (Kecerdasan Buata**n): Simulasi kecerdasan manusia pada mesin yang diprogram tanpa instruksi secara eksplisit

***Blockchain*:** Basis data terdesentralisasi dan transparan yang mencatat dan memverifikasi transaksi di beberapa komputer dalam jaringan terdistribusi

***Internet of Things:*** Jaringan perangkat fisik yang saling terhubung yang disematkan dengan sensor, perangkat lunak, dan kemampuan bertukar data satu sama lain melalui internet

***Compliance* (Kepatuhan):** Kepatuhan terhadap regulasi atau standar tertentu

***Augmented Reality:*** Teknologi yang mengubah objek atau data virtual ke objek dunia nyata secara real-time, memungkinkan interaksi pengguna dengan objek tersebut

***Virtual Reality:*** Simulasi lingkungan yang dihasilkan komputer yang dapat berinteraksi dengan dan dialami oleh seseorang melalui penggunaan headset atau perangkat khusus

**5G**: Generasi kelima teknologi nirkabel yang memberikan kecepatan data yang lebih cepat, latensi yang lebih rendah, kapasitas jaringan yang lebih besar.

***Data Residency* (Residensi Data):** Lokasi fisik atau geografis dari data atau informasi disimpan

***Cross-Border Data Transfer* (Transfer data lintas batas):** perpindahan data digital dari satu negara ke negara lain maupun antar organisasi yang berada pada wilayah yuridiksi hukum berbeda

***Cloud Native:*** Pendekatan dalam pengembangan dan penyebaran perangkat lunak di mana aplikasi dirancang dan dibangun khusus untuk lingkungan cloud

***Industry 4.0:*** Revolusi industri keempat yang ditandai dengan integrasi teknologi digital terkini untuk mengaktifkan otomatisasi, konektivitas, pengambilan keputusan berbasis data.

Diterbitkan oleh
Politeknik Siber dan Sandi Negara Press
Jl. Raya H. Usa, Putat Nutug, Kec. Ciseeng, Kabupaten Bogor, Jawa Barat 16120
perpustakaan@poltekssn.ac.id