

Mitigasi Risiko Komputasi Awan

Joni¹, Teguh Prasandy², Imanuel Revelino Murmanto³

¹ Information System, BINUS Online Learning, Bina Nusantara University, Jakarta, Indonesia, 11480
joni@binus.ac.id

² Information System, BINUS Online Learning, Bina Nusantara University, Jakarta, Indonesia, 11480
teguh.prasandy@binus.edu

³ Information System, BINUS Online Learning, Bina Nusantara University, Jakarta, Indonesia, 11480
imanuel.revelino@gmail.com

Diterima 21 Juli 2019

Disetujui 20 Desember 2019

Abstract—The business world is developing very dynamically along with the development of information technology (IT). The technology or system that is currently invested will become obsolete in the next few years. Companies are starting to consider using cloud computing to keep up with the latest technology and reduce the complexity of managing IT experts, so they can focus on their main business processes. But when it comes to implementing cloud computing, there are risks that cannot be avoided. The purpose of this paper is to analyze the risks of using cloud computing, so that it can provide guidelines and guidelines for companies that want to switch to cloud computing services. The method used in writing this paper uses a literature study approach through tracing journals, textbooks, and the internet. Based on these searches it is known that cloud computing can be adopted by companies that want to get agility and flexibility when businesses grow rapidly, but must still pay attention to corporate governance, risk management, and compliance with regulations.

Index Terms—cloud computing, business, corporation, risk

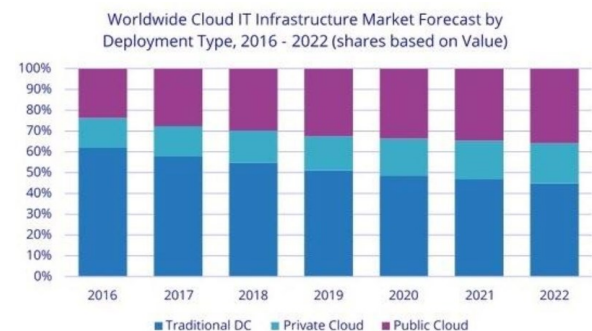
I. PENDAHULUAN

Di era digital saat ini, dunia bisnis semakin tergantung dengan teknologi dan internet. Banyak perubahan terjadi seiring dengan perkembangan teknologi dan internet. Sebuah perusahaan yang dulunya membutuhkan investasi besar untuk membangun infrastruktur teknologi informasi, kini dapat memanfaatkan komputasi awan. Penggunaan komputasi awan semakin meningkat setiap tahunnya dan diprediksi akan terus mengalami pertumbuhan dalam beberapa tahun mendatang. Laporan Gartner berjudul *The Data Center is Dead, and Digital Infrastructures Emerge* yang dipublikasikan pada tahun 2018 menyebutkan 10% perusahaan di dunia sudah beralih ke komputasi awan. Dan per tahun 2025, Gartner memprediksi 80% perusahaan akan mematikan pusat data (*data center*) mereka.

Teknologi komputasi awan (*cloud computing*) menjadi daya tarik bagi perusahaan karena mampu menyediakan kebutuhan infrastruktur TI (teknologi

informasi) secara cepat, mudah, dan dapat ditingkatkan kapasitasnya secara fleksibel sesuai perkembangan bisnis. Skema pembayaran komputasi awan juga lebih fleksibel karena perusahaan hanya membayar sesuai kapasitas yang digunakan, tanpa perlu mengeluarkan biaya besar untuk membangun infrastruktur TI di awal. Dengan demikian, perusahaan dapat menjadi lebih fokus ke bisnis utamanya tanpa harus mengembangkan kompetensi di area TI.

Meskipun pemanfaatan komputasi awan menawarkan banyak kemudahan dan fleksibilitas dari sisi biaya dan infrastruktur, namun data prediksi dari IDC (International Data Corporation) menunjukkan pengeluaran biaya TI untuk *cloud computing* belum meningkat secara signifikan karena sebagian masih menggunakan *Traditional DC (Data Center)*.



Gambar 1: *Spending on IT Infrastructure in Cloud Environments* (IDC 2019)

Hal ini tidak terlepas dari kekhawatiran akan keamanan dan risiko penempatan pusat data ke *cloud* sehingga banyak perusahaan masih enggan beralih ke *cloud*.

Tujuan dari penulisan paper ini adalah menganalisa risiko dari pemanfaatan komputasi awan, sehingga dapat memberikan panduan bagi perusahaan yang ingin beralih ke layanan komputasi awan.

II. METODOLOGI PENELITIAN

Metode yang dipergunakan dalam penulisan paper ini menggunakan pendekatan studi literatur melalui penelusuran terhadap jurnal, buku teks, dan internet. Dalam studi literatur ini dilakukan analisa karakteristik layanan komputasi awan, jenis komputasi awan, dan perbandingan model layanan komputasi awan, agar bisa dijadikan sebagai panduan atau acuan dalam mengimplementasikan komputasi awan.

Dikutip dari NIST (*National Institute of Standards and Technology*), terdapat 5 karakteristik utama dalam layanan komputasi awan:

1. *On-demand self-service*: perusahaan dapat memesan dan menentukan sendiri kemampuan komputasi yang diinginkan, serta dapat dipenuhi secara cepat. Misalnya: pengadaan sebuah server di suatu perusahaan yang membutuhkan waktu berminggu-minggu dapat dipenuhi hanya dalam hitungan menit oleh penyedia *cloud*.
2. *Broad network access*: perusahaan dapat mengakses layanan ini secara luas dari berbagai jenis perangkat seperti *smart phone*, *tablet*, *laptop*, maupun PC (*personal computer*).
3. *Resource pooling*: penyedia layanan memiliki sumber daya komputasi yang sangat besar yang dapat dialokasikan secara dinamis untuk melayani banyak perusahaan (*multi-tenant*) sesuai dengan permintaan perusahaan.
4. *Rapid elasticity*: kemampuan sumber daya komputasi yang dapat diubah secara cepat setiap saat sesuai dengan kebutuhan perusahaan. Misalnya: perusahaan penyedia aplikasi transportasi online seperti Grab yang awalnya hanya digunakan oleh sedikit pengguna, dapat meningkatkan kapasitas layanan ini secara cepat dan mudah ketika pertumbuhan penggunaannya mencapai 200 kali lipat.
5. *Measured service*: kemampuan untuk mengontrol dan mengukur pemanfaatan sumber daya sesuai dengan penggunaannya (biasanya secara *pay-per-use* atau *charge-per-use*). Misalnya: ukuran data yang tersimpan, lama penggunaan, jumlah user, dll.

Secara umum jenis *cloud* (*deployment models*) terbagi menjadi empat yaitu: *Private Cloud*, *Community Cloud*, *Public Cloud*, dan *Hybrid Cloud*:

1. *Private Cloud* – infrastruktur *cloud* yang dibangun dan dioperasikan hanya untuk kebutuhan internal suatu organisasi (tidak terjadi *sharing resource* dengan perusahaan lain). Contohnya server virtual ataupun *web application* di infrastruktur *cloud* yang dikhususkan bagi suatu perusahaan.
2. *Community Cloud* – infrastruktur *cloud* dibangun dan digunakan secara bersama oleh beberapa

organisasi dalam satu komunitas yang memiliki visi dan misi yang sama.

3. *Public Cloud* – infrastruktur *cloud* yang dibangun oleh penyedia layanan *cloud* untuk dimanfaatkan oleh masyarakat umum, baik secara gratis maupun berbayar. Contohnya seperti: Facebook, Google Mail, Office 365, Windows Azure, dll.
4. *Hybrid Cloud* – infrastruktur *cloud* yang merupakan komposisi dari dua atau lebih layanan *cloud* (*private*, *community*, atau *public*). Pada *Hybrid Cloud* ini, perusahaan bisa memilih proses bisnis mana yang akan dipindahkan ke *Public Cloud* dan proses bisnis mana yang harus tetap berjalan di *Private Cloud*

Public cloud adalah jenis *cloud* yang paling umum digunakan, sedangkan *Private Cloud* memiliki infrastruktur yang eksklusif, dan biasanya ditempatkan ke dalam server internal suatu perusahaan. Untuk perbandingan dari ketiga jenis *cloud* dapat dilihat pada tabel 1.

Tabel 1. *Cloud Deployment Models* (diolah)

Deployment Models	Infrastructure Owned by	Infrastructure Located	Cost	Security
Private Cloud	Organization or Third Party	On-site	High	High
Community Cloud	Third Party	On-site	High	High
Public Cloud	Third Party	Off-site	Low	Low
Hybrid Cloud	Both	Both	Medium	Medium

Model layanan *cloud* (*service models*) terbagi menjadi tiga yaitu IaaS (*Infrastructure as a Service*), PaaS (*Platform as a Service*), dan SaaS (*Software as a Service*).

1. *Infrastructure as a Service* (IaaS) – Perusahaan menyewa server virtual yang masih kosong sesuai kebutuhannya dan memiliki kontrol atas sistem operasi, penyimpanan data, serta aplikasi di dalamnya.
2. *Platform as a Service* (PaaS) – Perusahaan menempatkan aplikasi (*software*) pada infrastruktur dan platform yang disiapkan oleh penyedia layanan *cloud*. Perusahaan memiliki kontrol terbatas atas aplikasi yang berada pada platform dan infrastruktur tersebut. Contoh dari PaaS misalnya Amazon Web Service, Windows Azure, SQL Azure, yang dapat dimanfaatkan oleh perusahaan untuk menempatkan aplikasinya di sana.
3. *Software as a Service* (SaaS) – Perusahaan menggunakan aplikasi (*software*) yang disediakan oleh penyedia layanan *cloud*. Seluruh infrastruktur (server, sistem operasi, *security*, penyimpanan data, *update software*) dikelola oleh penyedia

layanan *cloud*. Contoh dari SaaS ini seperti Office 365, Salesforce, dll.

Pemilihan model layanan *cloud* (IaaS – PaaS – SaaS) harus disesuaikan dengan sumber daya yang dimiliki oleh perusahaan maupun kebutuhan bisnis dari perusahaan tersebut. Setiap model layanan memiliki kelebihan dan kekurangan masing-masing.

Infrastructure as a Service (IaaS) – memiliki fleksibilitas yang sangat tinggi, namun harus didukung oleh sumber daya IT yang kompeten, waktu yang cukup untuk implementasi, serta tata kelola yang baik. Untuk bisnis dengan kompleksitas yang tinggi dan membutuhkan banyak customization, maka lebih tepat untuk menerapkan model layanan IaaS.

Sebaliknya *Software as a Service* (SaaS) – memiliki keterbatasan untuk melakukan perubahan sistem yang sesuai dengan kebutuhan bisnis, karena sangat tergantung dengan fitur yang telah disediakan oleh penyedia layanan.

Namun untuk kebutuhan sistem/ aplikasi yang sudah standar, perusahaan dapat memanfaatkan model layanan SaaS karena implementasinya lebih cepat dan tidak perlu dibebani dengan pembuatan maupun pemeliharaan sistem.

Platform as a Service (PaaS) – dapat menjadi alternatif solusi bagi perusahaan yang menginginkan fleksibilitas, namun tetap mendapatkan kecepatan dalam implementasi.

Untuk perbandingan dari ketiga model layanan *cloud* ini dapat dilihat pada tabel 2.

Tabel 2. *Cloud Service Models* (diolah)

Service Models	IT/Developer Expertise	Software/patch Updates Effort	Customizability	Deployment Duration
On-premise	●●●●	●●●●	●●●●	●●●●
IaaS	●●●	●●●	●●●	●●●
PaaS	●●	●●	●●	●●
SaaS	●	●	●	●

III. HASIL DAN PEMBAHASAN

Layanan *cloud* digunakan oleh perusahaan yang tidak ingin membangun infrastruktur sendiri, seperti pengembangan pusat data (*data center*), pemeliharaan sistem, sampai dengan pengelolaan data dan aplikasi. Perusahaan dapat menentukan infrastruktur yang sesuai dengan kebutuhannya secara fleksibel dan ekonomis, karena tidak harus mengeluarkan biaya investasi yang sangat besar di awal.

Namun ketika sebuah perusahaan memutuskan untuk memanfaatkan layanan *cloud*, maka proses pengelolaan dan penyimpanan data perusahaan tersebut akan berpindah ke jaringan yang dikelola oleh

penyedia layanan *cloud*. Ini berarti data tersimpan secara eksternal dan perusahaan tidak dapat mengetahui secara fisik apa yang terjadi dengan datanya.

Karena itu, dalam mengadopsi layanan *cloud* terdapat sejumlah tantangan dan risiko yang dihadapi oleh perusahaan. Mulai dari isu kedaulatan data, aspek keamanan data, serta kurangnya kontrol dan visibilitas atas pengelolaan data atau aplikasi yang ditempatkan di *cloud*.

A. Risiko Utama Layanan Cloud

Sebelum memutuskan untuk beralih ke *cloud*, setiap perusahaan perlu mempertimbangkan 3 aspek risiko utama, yaitu:

1. Aspek Regulasi

Risiko utama terkait aspek regulasi adalah ketidakjelasan lokasi penyimpanan data. Penyedia layanan *cloud* bisa saja memecah data menjadi beberapa bagian dan menyimpannya di berbagai tempat, termasuk di luar Indonesia. Hal ini berpotensi melanggar aturan yang berlaku di Indonesia, antara lain:

- Peraturan Pemerintah Nomor 82 Tahun 2012 pasal 43 ayat 1b yang mengatur mengenai penyimpanan data transaksi elektronik di dalam negeri.
- Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 pasal 17 yang mengatur mengenai penempatan pusat data (*data center*) dan pusat pemulihan bencana (*disaster recovery center*) di wilayah Indonesia.

Secara aturan, semua transaksi elektronik, datanya wajib disimpan di dalam negeri. Sedangkan untuk data pribadi yang terkait dengan layanan publik harus disimpan di dalam negeri.

2. Aspek Keamanan Data

Risiko keamanan data ini muncul karena kontrol yang terbatas atas sistem dan infrastruktur di *cloud*. Dengan aplikasi dan data yang dikelola oleh penyedia layanan *cloud*, maka data tidak sepenuhnya di bawah kendali perusahaan sehingga rentan terhadap ancaman keamanan dan kerahasiaan data. Keamanan dan keutuhan data menjadi sangat tergantung kepada standar keamanan yang dimiliki penyedia layanan *cloud* karena perusahaan tidak memiliki kontrol langsung terhadap infrastruktur dan sistem yang telah disiapkan oleh penyedia layanan *cloud*. Selain itu infrastruktur *cloud* yang memungkinkan penggunaan secara bersama (*resource pooling*) dapat meningkatkan kerentanan data diakses oleh orang yang tidak berhak.

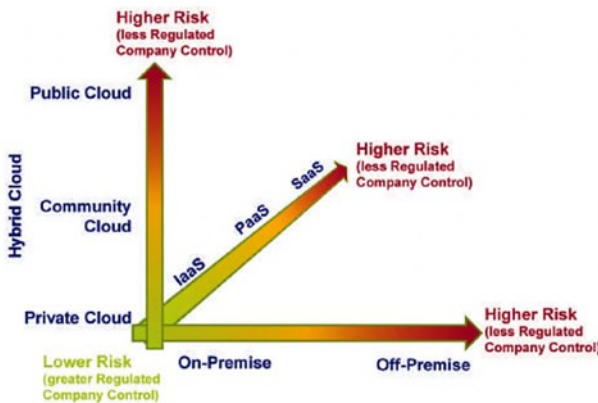
3. Aspek Vendor Dependency

Pengelolaan data yang diserahkan kepada penyedia layanan *cloud* menimbulkan ketergantungan kepada

vendor. Perusahaan tidak bisa dengan mudah mengambil data dan program yang tersimpan di cloud secara masif, misalnya ketika akan memindahkan data dan aplikasinya ke penyedia layanan cloud yang baru, ataupun ingin menempatkan datanya ke pusat data sendiri (*on-premise*). Tidak adanya standarisasi antar penyedia layanan cloud membuat data yang diperoleh harus dikonversi dan dilakukan konfigurasi ulang. Risiko ini juga dapat ditimbulkan karena penyedia layanan cloud mengalami kepailitan maupun mengalihdayakan aspek-aspek khusus dari penawaran layanannya kepada penyedia pihak ketiga.

Dari ketiga aspek risiko di atas, dapat dilihat bahwa model dari komputasi awan yang dipilih harus berdasarkan strategi *cloud* yang komprehensif dari suatu perusahaan, sehingga tidak semata-mata didorong oleh kebutuhan untuk mengurangi biaya TI.

Strategi pemilihan jenis cloud (*Private – Public – Hybrid*) maupun penentuan model layanan cloud (*IaaS – PaaS – SaaS*) akan memberikan variabel risiko yang berbeda. Oleh karena itu diperlukan perhatian ekstra dalam penilaian risiko dan mitigasi. Kurangnya kontrol oleh perusahaan akan meningkatkan kemungkinan terjadinya risiko, seperti dapat dilihat pada gambar di bawah ini.



Gambar 2: *Cloud Risk Model* (Stokes 2013)

B. Mitigasi Risiko Layanan Cloud

Untuk memastikan keamanan komputasi awan maupun perlindungan data dan aplikasi di *cloud* serta memastikan kepatuhan terhadap peraturan yang berlaku, maka perlu adanya mitigasi risiko yang memadai. Pengamanan dan perlindungan terhadap data perusahaan tetap menjadi tanggung jawab manajemen perusahaan meskipun data dan sistem dikelola oleh penyedia layanan *cloud*.

Berikut ini mitigasi risiko yang dapat dilakukan oleh perusahaan yang akan mengimplementasikan komputasi awan, dapat dilihat pada tabel 3.

Tabel 3: Mitigasi Risiko *Cloud Computing* (diolah)

Risiko Utama	Mitigasi
1. Aspek Regulasi	<ul style="list-style-type: none"> Memastikan data yang tersimpan di <i>cloud</i> sudah mematuhi ketentuan dan kebijakan suatu negara.
2. Aspek Keamanan Data	<ul style="list-style-type: none"> Memastikan penyedia layanan <i>cloud</i> memiliki sertifikasi keamanan data dan informasi. Memilih layanan <i>private cloud</i> untuk menyimpan data yang bersifat sensitif dan rahasia.
3. Aspek <i>Vendor Dependency</i>	<ul style="list-style-type: none"> Memilih penyedia layanan <i>cloud</i> yang memiliki reputasi, sejarah, dan keberlanjutan jangka panjang untuk memastikan bahwa layanan tetap tersedia dan data dapat dilacak dalam jangka waktu yang lama. Melakukan <i>off-site backup</i> secara rutin, sehingga data tetap dapat "diselamatkan" jika terjadi kepailitan pada penyedia layanan <i>cloud</i>.

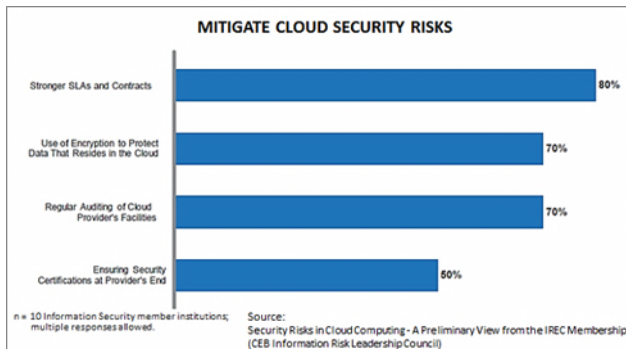
Dari sudut pandang perlindungan *data privacy*, mitigasi risiko harus dilakukan oleh kedua belah pihak, baik pengguna *cloud* maupun penyedia layanan *cloud*. Perusahaan sebagai pengguna layanan *cloud* harus memperhatikan kontrol terhadap sistem dan mengklasifikasikan data secara tepat atas informasi yang diperbolehkan diakses di *cloud*. Sedangkan dari sisi penyedia *cloud* harus menyediakan enkripsi untuk setiap data penting dan menyiapkan *secure infrastructure* secara komprehensif.

Dari sudut pandang keamanan data, beberapa penanganan risiko yang dilakukan pada komputasi *on-premise* tetap harus diterapkan pada komputasi awan seperti dapat dilihat pada tabel 4.

Tabel 4: Mitigasi Risiko Keamanan Data (diolah)

Parameter	Risiko	Mitigasi
Data Confidentiality	Unauthorized access	<ul style="list-style-type: none"> Strong passwords Strong authentication mechanism
Data Integrity	Data compromised	<ul style="list-style-type: none"> Secure data encryption algorithm Data retention & backup techniques
Data Availability	Data loss	<ul style="list-style-type: none"> Monitoring control system Disaster Recovery Plan (DRP)

Terkait *data availability*, infrastruktur di *cloud* cenderung lebih baik daripada *on-premise* karena faktor *High Availability* inilah yang biasanya menjadi layanan yang diunggulkan oleh penyedia *cloud*. Karena itu, perusahaan yang akan menggunakan layanan *cloud* harus memperhatikan *Service Level Agreement* (SLA) yang tercantum di dalam kontrak untuk mendapatkan jaminan tingkat pelayanan yang diharapkan dari penyedia *cloud*. Hasil riset dari CEB *Information Risk Leadership Council* juga menunjukkan urusan kontrak dan SLA menjadi hal penting dalam memitigasi risiko komputasi awan.



Gambar 3: Strategies for mitigate cloud security risks (CEB IREC 2010)

C. Beralih ke Layanan Cloud

Seiring perkembangan bisnis yang didukung dengan internet, maka komputasi awan sudah menjadi bagian penting bagi bisnis. Namun ketika akan mengimplementasikan komputasi awan, terdapat risiko-risiko yang tidak dapat dihindarkan. Untuk itu, sebelum mengalihkan layanan ini ke penyedia layanan *cloud*, perusahaan perlu memperhatikan beberapa rambu-rambu berikut ini:

1. *Regulation & Compliance.* Pastikan data yang akan disimpan di *cloud* telah memenuhi peraturan perundang-undangan yang berlaku, seperti jenis data yang akan ditempatkan di *cloud*, lokasi penempatan data, dll.
2. *Vendor Assurance.* Pastikan penyedia layanan *cloud* yang dipilih harus memiliki sertifikasi keamanan dan dapat menunjukkan adanya audit eksternal dari institusi independen secara berkala. Standarisasi keamanan sistem informasi dan sertifikasi yang seharusnya dimiliki oleh penyedia layanan *cloud* seperti sertifikasi ISO 27001, SOC1 – SOC2 – SOC3, maupun STAR (Security, Trust & Assurance Registry) dari Cloud Security Alliance (CSA).
3. *Gradually Implementation.* Sebaiknya pemanfaatan layanan *cloud* dilakukan secara bertahap yang dimulai dari sistem informasi yang bersifat *non-critical*. Hal ini untuk mendapatkan pengalaman dan tingkat kredibilitas akan penggunaan layanan *cloud* sebelum mengalihkan sistem lainnya ke *cloud*.
4. *Off-site Backup.* Pemanfaatan *cloud* dapat menggabungkan beberapa layanan *cloud* yang ada. Dengan demikian perusahaan tidak perlu terikat hanya kepada satu penyedia layanan *cloud*. Selain itu perusahaan dapat melakukan *backup* / replikasi data secara berkala di luar penyedia layanan *cloud*.
5. *Economical.* Melakukan kalkulasi ulang biaya penggunaan *cloud* secara cermat dan kualifikasi infrastruktur sesuai kebutuhan, khususnya pada sistem dengan frekuensi penggunaan yang sangat tinggi sehingga tetap mendapatkan manfaat penghematan finansial.

D. Tren industri yang mengadopsi cloud

Migrasi ke komputasi awan sudah menjadi solusi bagi perusahaan saat ini. Layanan komputasi awan memberikan daya tarik bagi usaha kecil dan menengah dan perusahaan rintisan (*start-up company*), karena biasanya mereka tidak ingin melakukan investasi besar di muka, tidak berminat membangun tim operasional besar, dan memerlukan skalabilitas untuk beradaptasi dengan cepat terhadap perubahan permintaan.

Komputasi awan lebih *agile* dalam menyokong kebutuhan para perusahaan rintisan, khususnya perusahaan transportasi *online* dan *e-commerce* karena seringkali membutuhkan kapasitas yang naik turun, misalnya saat menggelar diskon atau promosi.

Perusahaan di sektor keuangan juga sesuai untuk mengadopsi komputasi awan untuk mengakomodir fleksibilitas seiring dengan pertumbuhan pengguna *financial technology (fintech)*.

Pada intinya, komputasi awan dimanfaatkan oleh perusahaan yang ingin mendapatkan kelincahan dan fleksibilitas ketika permintaan meningkat ataupun bisnis bertumbuh dengan cepat. Dan ketika terjadi penurunan permintaan, komputasi awan menyediakan cara mudah untuk mengurangi kapasitas, sehingga menghindari perusahaan membangun infrastruktur di awal dengan kapasitas yang belum tentu sesuai dengan kebutuhan.

Model komputasi awan juga sesuai untuk jenis bisnis yang sering terhubung langsung dengan internet setiap saat dan tidak memiliki gedung kantor permanen, sehingga ketika perusahaan ingin berekspansi ke luar daerah bahkan luar negeri, data dan aplikasi yang ada di *cloud* dapat diakses dan digunakan kapan saja tanpa harus memindahkan server atau membangun server baru di tempat yang baru.

IV. SIMPULAN

Seiring dengan makin tingginya ketergantungan dunia bisnis terhadap teknologi informasi, menyebabkan perusahaan harus melakukan investasi untuk sistem TI. Namun tidak jarang investasi ini kurang efektif karena sistem TI segera menjadi usang akibat cepatnya transformasi dalam dunia TI.

Tetapi dengan adanya teknologi komputasi awan, perusahaan dapat menyerahkan pelayanan ini beserta perawatannya kepada penyedia layanan *cloud* sehingga perusahaan tersebut dapat berfokus pada bisnis utamanya. Hal ini membuat layanan komputasi awan menjadi alternatif solusi bagi perusahaan yang ingin mengubah investasi TI dari belanja modal (*Capital Expenditure*) menjadi biaya operasional (*Operational Expenditure*).

Meskipun demikian, sebelum beralih ke layanan *cloud*, perusahaan perlu mempertimbangkan dengan matang karena terdapat jenis-jenis layanan yang akan

lebih efisien apabila dilakukan secara *on-premise*. Beberapa jenis layanan bahkan dapat dilakukan secara bersamaan (*hybrid*) dengan menggabungkan kedua jenis model tersebut. Dan yang terutama, pemanfaatan komputasi awan tetap harus memperhatikan tata kelola perusahaan, manajemen risiko, dan kepatuhan terhadap peraturan.

DAFTAR PUSTAKA

- [1] Andersen, Brian D. (2018). *The Role of Internal Audit in a Cloud Environment*, CEB Audit Leadership Council: Gartner Inc.
- [2] Cappuccio, D. (2018). The Data Center is Dead, and Digital Infrastructures Emerge. ID G00354861 Gartner, Inc.
- [3] Heripracoyo, S. (2014). Analisa Studi Literatur Manfaat Implementasi Komputasi Awan untuk Perusahaan. *ComTech* Vol. 5 No. 1 Juni 2014: 154-162.
- [4] IDC, 2019. Cloud IT Infrastructure Revenues Continue to Expand Despite Slow Down in Spending in 2019. Framingham: International Data Corporation Corporate USA.
- [5] Ludwig, S. (2011). *Cloud 101: What the heck do IaaS, PaaS and SaaS companies do?* 14.11.2011. Accessed on 14.8.2018. <https://venturebeat.com/2011/11/14/cloud-iaas-paas-saas/>.
- [6] Permen Kominfo No.20 Tahun 2016. Perlindungan Data Pribadi Dalam Sistem Elektronik. Indonesia: Kementerian Komunikasi dan Informatika.
- [7] PP No 82 Tahun 2012. Penyelenggaraan Sistem dan Transaksi Elektronik. Indonesia: Peraturan Pemerintah Republik Indonesia.
- [8] Sharma, C. (2014). Analogous Study of Security Issues and Challenges in Cloud Environment. *International Journal of Advance Research in Computer Science and Management Studies (IJARCSMS)* Volume 2, Issue 5, May 2014.
- [9] Stokes, D. (2013). Compliant Cloud Computing – Managing the Risks. PDF-document from ISPE GAMP® July/August 2013.
- [10] Stanton, Brian., Theofanos, Mary., Joshi, Karuna P. (2015). *Framework for Cloud Usability*, NIST (National Institute of Standards and Technology).
- [11] Tandy, J., Siswono. (2013). Cloud Computing dan Dampaknya terhadap Bisnis. *ComTech* Vol.4 No. 2 Desember 2013: 687-695.
- [12] Thakare, Vaishali R., Singh, K John. (2016). A Study of Security and Privacy Issues at Service Models of Cloud Computing. *Indian Journal of Science and Technology*, Vol 9(38), DOI: 10.17485/ijst/2016/v9i38/92880, October 2016.
- [13] Williams, Mark I. (2010). *A Quick Start Guide to Cloud Computing: Moving your business into the cloud*, Kogan Page Publisher.