

## Sistem Informasi Manajemen Berbasis Cloud

Agung Wijoyo, ,Abdul Rahim Silalahi ,Achmad Raihan ,Panji Arrasyid ,Riska Diana

Ekonomi & Bisnis , Manajemen , Universitas Pamulang , Tangerang Selatan , Indonesia

Email: [dosen01671@unpam.ac.id](mailto:dosen01671@unpam.ac.id) , [abduhrahimsilalahi68@gmail.com](mailto:abduhrahimsilalahi68@gmail.com),

[achmad.raihan6666@gmail.com](mailto:achmad.raihan6666@gmail.com), [Riskachainago09@gmail.com](mailto:Riskachainago09@gmail.com), [panjiarrasyid9a@gmail.com](mailto:panjiarrasyid9a@gmail.com)

**Abstrak** Sistem Informasi Manajemen Berbasis Cloud (Cloud-Based Management Information System) adalah jenis sistem informasi manajemen (SIM) yang menjalankan fungsi-fungsi manajerial dan operasional menggunakan infrastruktur komputasi awan atau cloud computing. Dalam SIM Berbasis Cloud, data, perangkat lunak aplikasi, dan sumber daya komputasi disimpan, dikelola, dan diakses melalui internet, bukan pada perangkat keras dan infrastruktur fisik yang berlokasi di dalam perusahaan itu sendiri.

Dengan kata lain, SIM Berbasis Cloud adalah bentuk evolusi dari SIM tradisional yang berfokus pada penggunaan teknologi cloud untuk menyediakan akses lebih fleksibel, skalabilitas yang lebih baik, dan biaya yang lebih efisien dalam mengelola informasi dan mendukung proses pengambilan keputusan manajerial. SIM Berbasis Cloud memungkinkan organisasi untuk mengakses data dan aplikasi dari mana saja dengan koneksi internet, memungkinkan mobilitas dan kerja jarak jauh.

Kata kunci :

**Abstract** A Cloud-Based Management Information System (Cloud-Based Management Information System) is a type of management information system (SIM) that carries out managerial and operational functions using cloud computing infrastructure. In a Cloud-Based SIM, data, application software, and computing resources are stored, managed, and accessed over the internet, rather than on hardware and physical infrastructure located within the company itself.

In other words, Cloud-Based SIM is an evolutionary form of traditional SIM that focuses on the use of cloud technology to provide more flexible access, better scalability, and more cost efficiency in managing information and supporting managerial decision-making processes. Cloud-Based SIM allows organizations to access data and applications from anywhere with an internet connection, enabling mobility and remote working.

Keyword :

## PENDAHULUAN

Pergeseran menuju Sistem Informasi Manajemen (SIM) berbasis cloud adalah fenomena penting dalam dunia bisnis dan teknologi informasi modern. Revolusi ini mencerminkan transformasi mendalam dalam cara organisasi mengelola, menyimpan, dan mengakses data serta aplikasi mereka. Cloud computing telah mengubah paradigma tradisional di mana perusahaan harus memiliki infrastruktur IT sendiri menjadi model layanan berbasis internet yang memungkinkan akses dan penggunaan sumber daya komputasi secara fleksibel.

Sejak kemunculannya, cloud computing telah menjadi elemen kunci dalam strategi teknologi informasi banyak organisasi, dari perusahaan besar hingga bisnis kecil dan startup. Pergeseran ini mendapatkan momentum karena sejumlah alasan yang kuat, termasuk skalabilitas yang lebih baik, efisiensi biaya, akses universal, dan inovasi yang lebih cepat.

Dalam makalah ini, kami akan menjelajahi secara lebih mendalam pergeseran menuju SIM berbasis cloud. Kami akan memahami manfaat utama yang diberikan oleh cloud computing dalam konteks manajemen informasi, serta mengeksplorasi tantangan yang terkait dengan implementasi dan penggunaan SIM berbasis cloud. Selain itu, kami akan meninjau contoh-contoh kasus dan tren terkini dalam pengadopsian teknologi ini.

Dengan pemahaman yang lebih baik tentang pergeseran ini, kita dapat menggali bagaimana cloud computing telah membentuk cara organisasi beroperasi, mengambil keputusan, dan meraih keunggulan kompetitif dalam era digital yang terus berubah. Kami juga akan membahas rekomendasi dan strategi untuk mengelola dan mengatasi tantangan yang mungkin timbul dalam proses implementasi dan penggunaan SIM berbasis cloud. Dengan demikian, makalah ini akan membantu pembaca untuk mendapatkan wawasan yang lebih baik tentang bagaimana cloud computing telah mengubah lanskap bisnis dan manajemen informasi, dan bagaimana organisasi dapat mememanfaatkannya secara optimal.

Selanjutnya, makalah ini akan membahas beberapa aspek penting yang terkait dengan SIM berbasis Icloud. Disarankan bagi Penulis untuk menggunakan struktur artikel berikut: PENDAHULUAN – HASIL DAN PEMBAHASAN – KESIMPULAN.

## ANALISA DAN PEMBAHASAN

### 2.1 Pengertian Sistem Informasi Manajemen Berbasis Cloud

Sistem informasi manajemen adalah sistem perencanaan bagian dari pengendalian internal suatu bisnis yang meliputi pemanfaatan manusia, dokumen, teknologi, dan prosedur oleh akuntansi manajemen untuk memecahkan masalah bisnis seperti biaya produk, layanan, atau suatu strategi bisnis. Sistem informasi manajemen dibedakan dengan sistem informasi biasa karena SIM digunakan untuk menganalisis sistem informasi lain yang diterapkan pada aktivitas operasional organisasi. Secara akademis, istilah ini umumnya digunakan untuk merujuk pada kelompok metode manajemen informasi yang bertalian dengan otomasi atau dukungan terhadap pengambilan keputusan manusia, misalnya sistem pendukung keputusan, sistem pakar, dan sistem informasi eksekutif.

### Perbedaan Antara Sistem Tradisional Dan Berbasis Cloud

Berikut adalah perbedaan utama antara keduanya:

#### a. Infrastruktur :

Sistem Tradisional : Sistem tradisional mengandalkan infrastruktur fisik yang ada di lokasi perusahaan, seperti server, pusat data, dan perangkat keras yang harus diinvestasikan dan dikelola secara lokal.

Sistem Berbasis Cloud : Sistem berbasis cloud menggunakan infrastruktur yang dihosting oleh penyedia layanan cloud di data center mereka. Perusahaan tidak perlu mengelola perangkat keras fisik ini secara langsung.

#### a) Akses :

Sistem Tradisional : Akses ke sistem tradisional sering kali terbatas pada lokasi fisik perusahaan atau melalui jaringan VPN yang kompleks.

Sistem Berbasis Cloud : Sistem berbasis cloud memungkinkan akses dari mana saja dengan koneksi internet, memfasilitasi mobilitas dan kerja jarak jauh.

#### b) Skalabilitas :

Sistem Tradisional : Skalabilitas pada sistem tradisional sering kali memerlukan investasi tambahan dalam perangkat keras fisik dan konfigurasi yang rumit.

Sistem Berbasis Cloud : Sistem berbasis cloud memungkinkan organisasi untuk dengan mudah menambah atau mengurangi kapasitas sesuai dengan kebutuhan tanpa investasi besar.

c) Biaya :

Sistem Tradisional : Sistem tradisional memerlukan investasi modal yang signifikan untuk membeli perangkat keras, lisensi perangkat lunak, dan pemeliharaan.

Sistem Berbasis Cloud : Sistem berbasis cloud mengurangi biaya modal awal, karena organisasi membayar berdasarkan penggunaan, yang dapat mengurangi biaya operasional dalam jangka panjang.

d) Keamanan :

Sistem Tradisional : Keamanan pada sistem tradisional sepenuhnya tergantung pada perusahaan untuk melindungi data dan infrastruktur mereka. Sistem Berbasis Cloud : Penyedia layanan cloud sering kali menyediakan lapisan keamanan yang kuat, tetapi perusahaan juga memiliki tanggung jawab untuk melindungi data mereka.

e) Manajemen :

Sistem Tradisional : Manajemen infrastruktur, pemeliharaan, dan pembaruan perangkat keras dan perangkat lunak adalah tanggung jawab internal perusahaan.

Sistem Berbasis Cloud : Penyedia layanan cloud mengelola sebagian besar infrastruktur dan pemeliharaan, sementara perusahaan fokus pada penggunaan dan manajemen aplikasi.

Perbedaan ini menunjukkan bahwa sistem berbasis cloud memberikan fleksibilitas, akses yang lebih mudah, dan potensi penghematan biaya, sementara sistem tradisional mungkin lebih cocok untuk beberapa kasus penggunaan yang memerlukan kontrol penuh atas infrastruktur atau memiliki kebijakan keamanan khusus. Keputusan antara kedua jenis sistem ini harus didasarkan pada kebutuhan dan strategi bisnis organisasi.

## 2.2 Manfaat Sistem Informasi Manajemen Berbasis Cloud

1. Skalabilitas ; Bagaimana cloud memungkinkan perusahaan untuk menyesuaikan kapasitas sesuai kebutuhan.

Skalabilitas adalah salah satu fitur utama yang membuat teknologi cloud computing sangat menonjol. Ini mengacu pada kemampuan perusahaan untuk menyesuaikan kapasitas komputasi, penyimpanan, atau sumber daya lainnya sesuai dengan kebutuhan mereka dengan cepat dan efisien. Berikut adalah beberapa cara di mana cloud memungkinkan perusahaan untuk mencapai skalabilitas:

a) Pengukuran Berdasarkan Permintaan (On-Demand) :

Layanan cloud biasanya tersedia dalam mode "on-demand," yang berarti perusahaan hanya membayar untuk sumber daya yang mereka gunakan. Ini berbeda dengan infrastruktur tradisional yang harus dibeli sebelumnya. Dengan demikian, perusahaan dapat mengalokasikan sumber daya sebanyak yang mereka butuhkan saat dibutuhkan, dan kemudian mengurangnya ketika permintaan berkurang.

b) Auto-Scaling :

Cloud computing juga mendukung auto-scaling, yang berarti sistem dapat secara otomatis menyesuaikan kapasitasnya sesuai dengan lonjakan permintaan. Ketika ada beban kerja yang lebih berat, sistem secara otomatis menambah sumber daya komputasi (seperti server virtual) untuk menjaga kinerja. Ketika beban kerja berkurang, sumber daya yang tidak lagi diperlukan dapat dihentikan secara otomatis.

c) Kepuasan Pelanggan :

Dengan akses data yang fleksibel, perusahaan dapat lebih responsif terhadap kebutuhan pelanggan. Karyawan yang dapat mengakses informasi kapan saja dapat memberikan layanan yang lebih baik dan merespons pertanyaan atau permintaan pelanggan dengan cepat.

d) Kemudahan Kolaborasi :

Akses data yang fleksibel mendukung kolaborasi antara tim yang tersebar. Tim yang berbeda lokasi dapat mengakses dan berbagi data secara real-time, memfasilitasi kerja sama yang lebih baik.

e) Ketangkasan Bisnis :

Dengan akses data yang fleksibel, perusahaan dapat dengan cepat menyesuaikan operasinya dengan perubahan pasar atau keadaan yang mendadak. Kemampuan untuk mengambil keputusan berdasarkan data yang terkini dari mana saja dapat menjadi faktor kunci dalam kesuksesan bisnis.

f) Penghematan Waktu dan Biaya :

Akses data yang fleksibel mengurangi kebutuhan untuk perjalanan fisik atau waktu yang dihabiskan untuk berpindah tempat untuk mengakses data. Ini dapat menghemat biaya perjalanan dan waktu yang sebelumnya dihabiskan untuk aktivitas non-produktif.

g) Keamanan Data :

Meskipun akses yang fleksibel menawarkan manfaat besar, penting juga untuk memastikan keamanan data yang selalu terjaga. Oleh karena itu, perusahaan perlu menerapkan tindakan keamanan seperti enkripsi dan otorisasi yang kuat untuk melindungi data sensitif yang diakses dari berbagai lokasi.

Akses fleksibel ini telah menjadi norma dalam dunia bisnis modern dan merupakan salah satu alasan utama mengapa perusahaan beralih ke solusi berbasis cloud. Ini membantu organisasi menjadi lebih responsif, efisien, dan adaptif dalam menghadapi tantangan dan peluang di era digital yang terus berubah.

**3. Efisiensi biaya :** Penghematan biaya dalam hal perangkat keras dan pemeliharaan.

Efisiensi biaya dalam hal perangkat keras dan pemeliharaan adalah salah satu manfaat utama yang diberikan oleh sistem informasi berbasis cloud. Berikut adalah cara-cara di mana cloud computing membantu perusahaan menghemat biaya terkait dengan infrastruktur dan pemeliharaan :

a. Pengurangan Investasi Modal Awal :

Dalam infrastruktur tradisional, perusahaan harus mengeluarkan biaya besar untuk membeli perangkat keras, server, perangkat jaringan, dan pusat data. Dengan cloud computing, perusahaan dapat menghindari investasi modal awal ini karena penyedia layanan

cloud yang mengelola infrastruktur fisik. Ini mengurangi tekanan keuangan awal yang sering kali diperlukan untuk peralatan fisik.

b. Model Pembayaran Berbasis Penggunaan :

Cloud computing umumnya menggunakan model pembayaran berbasis penggunaan atau berbasis langganan. Artinya, perusahaan hanya membayar untuk sumber daya komputasi yang mereka gunakan. Ketika beban kerja berkurang, biaya pun turun secara proporsional. Ini memungkinkan perusahaan menghindari pemborosan sumber daya.

c. Skalabilitas yang Mudah :

Cloud computing memungkinkan perusahaan untuk dengan mudah menambah atau mengurangi sumber daya sesuai dengan kebutuhan. Ini berarti bahwa perusahaan tidak perlu mengeluarkan uang untuk perangkat keras tambahan yang mungkin hanya dibutuhkan sesekali. Penggunaan yang efisien dari sumber daya komputasi dapat menghemat biaya secara signifikan.

d. Pemeliharaan yang Dikelola oleh Penyedia :

Penyedia layanan cloud bertanggung jawab atas pemeliharaan infrastruktur fisik, perangkat keras, perangkat lunak, dan pembaruan sistem. Ini menghilangkan beban pemeliharaan yang biasanya diperlukan dalam infrastruktur lokal. Perusahaan tidak perlu lagi mempekerjakan staf IT tambahan atau mengeluarkan biaya pemeliharaan yang signifikan.

e. Reduksi Biaya Energi dan Ruang Fisik :

Dengan menggunakan infrastruktur cloud, perusahaan dapat mengurangi konsumsi energi dan ruang fisik yang diperlukan untuk server dan pusat data lokal. Ini dapat menghasilkan penghematan biaya operasional yang signifikan.

f. Manajemen Siklus Hidup yang Tidak Diperlukan :

Perangkat keras fisik memiliki siklus hidup dan perlu diganti secara berkala. Dalam lingkungan cloud, perusahaan tidak perlu khawatir tentang pembaruan perangkat keras ini, yang dapat menghemat biaya jangka panjang.

Dengan semua manfaat ini, cloud computing menjadi pilihan yang menarik bagi banyak perusahaan yang mencari cara untuk mengoptimalkan pengeluaran teknologi informasi mereka. Selain itu, ini juga memberikan fleksibilitas yang lebih besar dalam mengalokasikan sumber daya sesuai dengan kebutuhan bisnis saat ini.

#### 4. Keamanan data ; Upaya keamanan yang diterapkan dalam lingkungan cloud

Keamanan data adalah salah satu aspek yang sangat penting dalam lingkungan cloud. Saat perusahaan memindahkan data mereka ke cloud, untuk menerapkan berbagai upaya keamanan untuk melindungi informasi sensitif dan menjaga privasi pelanggan. Berikut adalah beberapa upaya keamanan yang umumnya diterapkan dalam lingkungan cloud :

a. Enkripsi Data :

Enkripsi adalah salah satu langkah keamanan paling dasar dalam lingkungan cloud. Data harus dienkripsi saat berada dalam perjalanan (misalnya, selama transfer data melalui jaringan) dan saat istirahat (data yang disimpan dalam penyimpanan cloud). Enkripsi ini menggunakan algoritma kriptografi yang kuat untuk melindungi data dari akses yang tidak sah.

b. Manajemen Identitas dan Akses :

Pengelolaan identitas dan akses adalah kunci untuk mengontrol siapa yang memiliki akses ke data dan aplikasi dalam lingkungan cloud. Ini melibatkan penggunaan otentikasi ganda, pengelolaan peran dan izin pengguna, serta pemantauan dan pemutusan akses yang tidak sah.

c. Firewall dan Filtering :

Penyedia layanan cloud biasanya menyediakan firewall dan sistem filtering untuk melindungi infrastruktur mereka dari serangan siber. Ini membantu melindungi data pelanggan yang disimpan di lingkungan cloud.

d. Pemantauan Keamanan :

Pemantauan secara terus-menerus terhadap aktivitas di lingkungan cloud adalah kunci untuk mendeteksi ancaman atau insiden keamanan secara cepat. Pemantauan ini dapat mencakup analisis log, deteksi intrusi, dan pemantauan perilaku pengguna.

e. Pemulihan Bencana dan Cadangan Data :

Upaya keamanan tidak hanya mencakup perlindungan dari ancaman siber, tetapi juga perlu mempertimbangkan pemulihan bencana. Perusahaan harus memiliki rencana pemulihan bencana yang kuat dan melakukan cadangan data secara teratur.

f. Kepatuhan Regulasi :

Banyak perusahaan harus mematuhi regulasi tertentu yang berkaitan dengan privasi data, seperti GDPR di Eropa atau HIPAA di Amerika Serikat. Penyedia layanan cloud sering kali menawarkan solusi yang mematuhi regulasi ini, tetapi perusahaan juga memiliki tanggung jawab untuk memastikan bahwa penggunaan cloud mereka sesuai dengan persyaratan hukum.

g. Pendidikan dan Pelatihan Pengguna :

Mengedukasi karyawan tentang praktik keamanan dan risiko siber adalah penting. Pengguna yang terlatih lebih mungkin menghindari perilaku yang dapat mengancam keamanan data, seperti mengklik tautan berbahaya atau mengungkapkan kata sandi.

h. Audit Keamanan Reguler :

Melakukan audit keamanan reguler dan pemeriksaan penetrasi adalah cara untuk memverifikasi keefektifan upaya keamanan yang telah diimplementasikan.

Penting untuk diingat bahwa keamanan data adalah tanggung jawab bersama antara penyedia layanan cloud dan pengguna (perusahaan atau organisasi). Ini berarti bahwa perusahaan perlu berkolaborasi dengan penyedia layanan cloud untuk memastikan bahwa semua langkah keamanan yang tepat telah diambil dalam lingkungan cloud mereka. Selain itu, keamanan data adalah proses yang terus menerus, dan perusahaan harus selalu mengikuti perkembangan teknologi dan ancaman siber terbaru untuk memastikan bahwa data mereka tetap aman.

## 2.3 TANTANGAN DAN RISIKO

### 1. **Keamanan** : tantangan yang terkait dengan keamanan data dalam lingkungan cloud

Keamanan data dalam lingkungan cloud memiliki sejumlah tantangan khusus yang perlu diperhatikan oleh perusahaan dan organisasi yang mengadopsi layanan cloud. Berikut adalah beberapa tantangan utama yang terkait dengan keamanan data dalam lingkungan cloud :

#### a. Keamanan Akses dan Identitas :

Tantangan utama adalah memastikan bahwa hanya pihak yang sah yang memiliki akses ke data dan sumber daya di lingkungan cloud. Manajemen identitas dan akses yang tepat, termasuk otentikasi ganda, pengelolaan peran, dan pemantauan akses, sangat penting untuk menghindari akses yang tidak sah.

#### b. Kebocoran Data (Data Leakage) :

Kebocoran data dapat terjadi jika data yang disimpan di cloud tidak dilindungi dengan baik. Ini bisa terjadi melalui penggunaan yang tidak sah oleh karyawan, kesalahan konfigurasi, atau serangan siber yang berhasil. Memastikan enkripsi data yang tepat dan manajemen izin yang ketat adalah langkah penting untuk menghindari kebocoran data.

#### c. Kepatuhan Regulasi :

Banyak organisasi harus mematuhi regulasi tertentu yang berkaitan dengan privasi data, seperti GDPR di Eropa atau HIPAA di Amerika Serikat. Memastikan bahwa penyimpanan dan pengelolaan data di cloud sesuai dengan persyaratan hukum adalah tantangan yang signifikan.

#### d. Keamanan API (Application Programming Interface) :

Banyak aplikasi cloud menggunakan API untuk berkomunikasi. Tantangan terkait dengan keamanan API meliputi perlindungan terhadap serangan seperti pencurian kunci API, penolakan layanan, atau serangan melalui antarmuka yang tidak aman.

#### e. Manajemen Kunci :

Keamanan data dalam cloud sering bergantung pada manajemen kunci yang tepat. Tantangan di sini adalah memastikan bahwa kunci enkripsi disimpan dengan aman dan diatur dengan baik untuk melindungi data yang disimpan di cloud.

#### f. Penggunaan Layanan Tidak Resmi (Shadow IT) :

Karyawan mungkin menggunakan layanan cloud yang tidak disetujui oleh IT, yang dapat meningkatkan risiko keamanan. Mengelola dan mengawasi penggunaan layanan ini adalah tantangan yang perlu diatasi.

g. Pemantauan dan Deteksi Ancaman :

Mengidentifikasi ancaman siber dan aktivitas yang mencurigakan dalam lingkungan cloud dapat menjadi tantangan. Pemantauan yang efektif dan pemahaman tentang perilaku normal dan anormal dapat membantu mendeteksi serangan siber dengan cepat.

h. Keamanan Bersama dengan Penyedia Cloud :

Keamanan data adalah tanggung jawab bersama antara perusahaan dan penyedia layanan cloud. Oleh karena itu, penting untuk memahami peran dan tanggung jawab masing-masing pihak serta memiliki perjanjian keamanan yang jelas.

i. Kehilangan Kontrol Fisik :

Dalam cloud, perusahaan kehilangan kendali fisik atas infrastruktur yang digunakan untuk menyimpan data mereka. Ini dapat menyulitkan untuk mengaudit keamanan dan memastikan kepatuhan.

j. Pengamanan Multi-Tenancy :

Beberapa pelanggan dapat menggunakan sumber daya yang sama dalam lingkungan cloud (multi-tenancy). Memastikan bahwa data dan aplikasi dari satu pelanggan terisolasi dengan baik dari yang lain adalah tantangan yang perlu diatasi.

Mengatasi tantangan keamanan ini dalam lingkungan cloud memerlukan perencanaan yang cermat, pelaksanaan kebijakan keamanan yang kuat, pemantauan terus-menerus, dan pendidikan bagi karyawan tentang praktik keamanan yang baik. Selain itu, perusahaan harus bekerja sama dengan penyedia layanan cloud untuk memastikan bahwa infrastruktur yang mereka gunakan memenuhi standar keamanan yang diperlukan.

**2. Kepatuhan ;** bagaimana peraturan dan kepatuhan berubah dengan penggunaan cloud

Penggunaan teknologi cloud computing telah memengaruhi dan mengubah peraturan dan kepatuhan dalam berbagai cara. Berikut adalah beberapa cara di mana peraturan dan kepatuhan telah berubah atau dipengaruhi oleh penggunaan cloud :

a. Kepatuhan Regulasi Data :

Penggunaan cloud telah menghadirkan tantangan baru dalam menjaga kepatuhan dengan regulasi data, seperti GDPR (General Data Protection Regulation) di Eropa atau HIPAA (Health Insurance Portability and Accountability Act) di Amerika Serikat. Perusahaan harus memastikan bahwa penyimpanan dan pemrosesan data yang sensitif sesuai dengan persyaratan hukum. Ini dapat mencakup persyaratan terkait privasi data, keamanan, dan pelaporan insiden.

b. Kepatuhan Pindah Batas :

Ketika data disimpan di cloud, dapat menyeberang batas negara dan yurisdiksi dengan lebih mudah. Hal ini dapat menimbulkan pertanyaan tentang bagaimana regulasi berlaku untuk data yang berpindah melintasi perbatasan. Sebagai contoh, GDPR memiliki ketentuan yang mengatur transfer data lintas batas.

c. Kepatuhan dengan Standar Keamanan Cloud :

Banyak negara dan lembaga regulasi telah mengembangkan standar keamanan khusus untuk layanan cloud, seperti ISO 27001 atau FedRAMP (Federal Risk and Authorization Management Program) di Amerika Serikat. Perusahaan harus memastikan bahwa penyedia layanan cloud mereka memenuhi standar-standar ini untuk memenuhi persyaratan kepatuhan.

d. Kontrol Akses dan Auditabilitas :

Memastikan kontrol akses yang ketat dan kemampuan untuk mengaudit aktivitas pengguna di lingkungan cloud menjadi aspek penting dalam menjaga kepatuhan. Perusahaan harus dapat memberikan bukti bahwa mereka memiliki kendali yang memadai atas data dan aplikasi mereka.

e. Keamanan Data Multi-Tenancy :

Dalam lingkungan cloud multi-tenancy, di mana beberapa pelanggan menggunakan sumber daya yang sama, keamanan data antara pelanggan harus terisolasi dengan baik. Kepatuhan harus memastikan bahwa data pelanggan tidak dapat diakses oleh pelanggan lain atau oleh penyedia layanan cloud itu sendiri.

f. Pemulihan Bencana dan Pemeliharaan Data :

Regulasi sering mengharuskan perusahaan untuk memiliki rencana pemulihan bencana yang kuat dan melakukan cadangan data secara teratur. Dalam lingkungan cloud, perusahaan harus memastikan bahwa penyedia layanan cloud juga memenuhi persyaratan ini.

g. Kepatuhan untuk Industri Khusus :

Beberapa industri, seperti perbankan, perawatan kesehatan, atau pemerintahan, memiliki regulasi khusus yang berlaku untuk mereka. Penggunaan cloud dalam industri-industri ini harus memenuhi persyaratan kepatuhan yang ketat.

h. Kepatuhan dengan Keamanan Fisik dan Operasional :

Kepatuhan tidak hanya berlaku untuk aspek-aspek digital, tetapi juga untuk keamanan fisik dan operasional pusat data yang digunakan oleh penyedia layanan cloud. Perusahaan perlu memahami bagaimana penyedia layanan cloud memenuhi persyaratan ini.

Penggunaan cloud computing dapat membantu perusahaan memenuhi kepatuhan dengan lebih efisien melalui fasilitas pemulihan bencana yang kuat, otentikasi ganda, pemantauan aktivitas, dan kemampuan untuk dengan cepat menghentikan akses yang tidak

sah. Namun, perusahaan juga perlu memahami bagaimana teknologi cloud memengaruhi kepatuhan mereka dan bekerja sama dengan penyedia layanan cloud untuk memastikan bahwa persyaratan kepatuhan dipenuhi. Selain itu, perusahaan harus selalu mengikuti perubahan dalam peraturan dan memperbarui strategi mereka sesuai dengan perubahan tersebut.

### 3. **Ketersediaan:** Risiko downtime dan ketersediaan sistem dalam cloud.

Ketersediaan sistem adalah aspek kunci dalam lingkungan cloud. Meskipun cloud computing sering kali menawarkan ketersediaan yang tinggi, risiko downtime atau ketidakterediaan sistem tetap ada. Berikut adalah beberapa risiko downtime dan ketersediaan sistem dalam cloud :

#### a. Gangguan Infrastruktur Penyedia Layanan Cloud :

Meskipun penyedia layanan cloud sering kali memiliki infrastruktur yang sangat andal, mereka juga dapat mengalami gangguan, pemadaman listrik, kerusakan perangkat keras, atau masalah teknis lainnya. Ini dapat mengakibatkan sistem menjadi tidak tersedia untuk sementara waktu.

#### b. Serangan DDoS (Distributed Denial of Service) :

Serangan DDoS adalah serangan yang bertujuan untuk menghambat ketersediaan sistem dengan melimpahkan lalu lintas internet yang sangat tinggi ke server atau infrastruktur cloud. Ini dapat mengakibatkan penurunan ketersediaan sistem atau bahkan pemadaman sementara.

#### c. Kesalahan Konfigurasi atau Pengelolaan :

Ketersediaan sistem cloud dapat dipengaruhi oleh kesalahan konfigurasi atau pengelolaan yang tidak benar oleh pengguna atau administrator. Sebuah konfigurasi yang salah atau tindakan manusia yang tidak sengaja dapat menyebabkan masalah ketersediaan.

#### d. Overload Resource :

Jika beban kerja yang digunakan melebihi kapasitas sumber daya yang dialokasikan dalam lingkungan cloud, sistem dapat menjadi tidak tersedia. Ini bisa terjadi jika perusahaan tidak memantau dan mengelola kapasitas dengan baik.

#### e. Risiko Vendor Lock-In :

Bergantung pada satu penyedia layanan cloud tertentu dapat menyebabkan risiko vendor lock-in, di mana perusahaan tidak dapat dengan mudah berpindah ke penyedia lain jika terjadi masalah ketersediaan atau jika biaya meningkat secara signifikan.

#### f. Perawatan Terjadwal :

Penyedia layanan cloud dapat memiliki jendela perawatan terjadwal di mana sistem menjadi tidak tersedia untuk pemeliharaan rutin. Sementara biasanya dilakukan pada waktu yang memungkinkan untuk pengaruh minimal, tetap merupakan risiko ketersediaan.

g. Bencana Alam atau Kegagalan Besar :

Bencana alam seperti banjir, gempa bumi, atau badai dapat mengganggu pusat data penyedia layanan cloud dan menyebabkan ketidaktersediaan sistem. Kegagalan besar dalam infrastruktur juga merupakan risiko.

Untuk mengatasi risiko-risiko ini dan meminimalkan downtime, perusahaan dapat mengambil beberapa langkah :

- 1) Redundansi : Menggunakan berbagai zona atau wilayah geografis untuk redundansi sistem dan cadangan data.
- 2) Backup Reguler: Melakukan cadangan data secara teratur dan mengujinya untuk memastikan pemulihan yang cepat.
- 3) Monitoring dan Pemantauan : Mengimplementasikan alat pemantauan dan pemantauan yang kuat untuk mendeteksi masalah ketersediaan dengan cepat.
- 4) Recovery Plan : Mengembangkan rencana pemulihan bencana yang komprehensif untuk mengatasi situasi darurat.
- 5) Diversifikasi Cloud Providers : Pertimbangkan untuk menggabungkan berbagai penyedia layanan cloud atau menggunakan strategi multi-cloud untuk menghindari risiko vendor lock-in.

Ketersediaan sistem dalam cloud tetap menjadi fokus utama untuk memastikan bahwa bisnis dapat beroperasi dengan lancar dan menghindari kerugian yang disebabkan oleh downtime yang berlebihan.

**4. Ketergantungan pada penyedia :** Bagaimana ketergantungan pada penyedia cloud dapat menjadi tantangan

Ketergantungan pada penyedia layanan cloud dapat menjadi tantangan serius bagi perusahaan dan organisasi. Meskipun cloud computing menawarkan banyak manfaat, termasuk fleksibilitas dan efisiensi, ada beberapa risiko yang terkait dengan tingkat ketergantungan yang tinggi pada penyedia layanan cloud. Berikut adalah beberapa cara di mana ketergantungan pada penyedia cloud dapat menjadi tantangan :

a. Vendor Lock-In :

Ketika perusahaan sangat tergantung pada satu penyedia layanan cloud tertentu, mereka mungkin sulit untuk berpindah ke penyedia lain jika diperlukan. Ini dapat mengikat perusahaan dengan satu penyedia dan membuat mereka bergantung pada harga, layanan, dan kebijakan penyedia tersebut.

b. Kenaikan Biaya yang Tidak Terduga :

Penyedia layanan cloud dapat mengubah harga sewaktu-waktu, dan perusahaan mungkin tidak memiliki banyak negosiasi dalam hal ini. Ini dapat mengakibatkan kenaikan biaya yang tidak terduga dan mempengaruhi margin keuntungan.

c. Ketersediaan dan Downtime :

Meskipun penyedia layanan cloud biasanya menawarkan tingkat ketersediaan yang tinggi, tidak ada jaminan bahwa sistem akan selalu tersedia. Downtime yang tidak terduga

dari penyedia cloud dapat mempengaruhi bisnis perusahaan dan menyebabkan kerugian finansial.

d. Keamanan dan Kepatuhan :

Keamanan data dan kepatuhan bisa menjadi isu saat perusahaan memindahkan data dan aplikasi ke cloud. Ketergantungan pada penyedia cloud berarti bahwa perusahaan harus mempercayai penyedia dalam hal keamanan dan kepatuhan data.

e. Penghentian Layanan atau Perubahan Layanan :

Penyedia layanan cloud memiliki hak untuk menghentikan layanan atau mengubah layanan mereka. Ini dapat menyulitkan perusahaan yang sangat tergantung pada layanan tertentu dalam operasi mereka.

f. Kontrol Terbatas :

Dalam lingkungan cloud, perusahaan memiliki kontrol terbatas atas infrastruktur fisik dan perangkat keras yang digunakan. Ini bisa menjadi tantangan ketika perusahaan ingin mengelola atau mengontrol lebih banyak aspek dari lingkungan IT mereka.

g. Ketergantungan pada Konektivitas Internet :

Cloud computing bergantung pada konektivitas internet yang andal. Ketergantungan ini dapat menjadi risiko jika ada masalah dengan koneksi internet yang mengakibatkan ketidakterediaan sistem.

h. Ketersediaan Data :

Data yang disimpan di cloud mungkin tidak selalu tersedia jika perusahaan ingin mengaksesnya atau jika penyedia layanan mengalami masalah teknis. Hal ini dapat menghambat operasi bisnis yang kritis.

Untuk mengatasi tantangan ketergantungan pada penyedia cloud, perusahaan dapat mempertimbangkan beberapa langkah :

- 1) Strategi Multi-Cloud : Menggunakan beberapa penyedia layanan cloud untuk mengurangi risiko vendor lock-in dan memberikan fleksibilitas dalam pemilihan penyedia.
- 2) Perencanaan Keluar yang Baik : Membuat rencana yang baik untuk keluar dari layanan cloud dan mengembalikan data jika perlu.
- 3) Evaluasi Keamanan dan Kepatuhan : Memastikan bahwa penyedia layanan cloud memenuhi standar keamanan dan kepatuhan yang sesuai untuk bisnis Anda.
- 4) Kontrak yang Jelas : Menyusun kontrak yang jelas dengan penyedia layanan cloud yang mencakup persyaratan tingkat layanan (SLA), kebijakan harga, dan perubahan layanan.

Sementara cloud computing dapat memberikan banyak manfaat, seperti skalabilitas dan efisiensi, perusahaan perlu memahami risiko dan tantangan yang terkait dengan

ketergantungan pada penyediaan cloud dan mengambil tindakan untuk mengelolanya dengan bijak.

## 2.4 KEPUTUSAN DALAM MENGADOPSI SIM BERBASIS CLOUD

Proses pengambilan keputusan yang bijak dalam mengadopsi sim berbasis cloud Pengambilan keputusan bijak dalam mengadopsi Sistem Informasi Manajemen (SIM) berbasis cloud memerlukan pendekatan yang hati-hati dan terencana. Berikut adalah proses pengambilan keputusan yang bijak dalam mengadopsi SIM berbasis cloud :

- a. Evaluasi Kebutuhan Bisnis : Langkah pertama adalah memahami kebutuhan bisnis Anda dengan baik. Identifikasi area atau proses yang dapat ditingkatkan melalui penggunaan SIM berbasis cloud. Pertimbangkan juga apakah ada tantangan khusus yang perlu diatasi.
- b. Analisis Manfaat vs. Risiko : Selanjutnya, lakukan analisis manfaat dan risiko dari implementasi SIM berbasis cloud. Pertimbangkan manfaat seperti skalabilitas, akses fleksibel, dan efisiensi biaya, serta risiko seperti keamanan data, ketersediaan sistem, dan ketergantungan pada penyedia.
- c. Pengembangan Kasus Bisnis : Buat kasus bisnis yang kuat untuk pengadopsian SIM berbasis cloud. Ini harus mencakup perkiraan biaya, proyeksi manfaat, dan alasan-alasan mengapa ini adalah investasi yang bijak untuk bisnis Anda.
- d. Identifikasi Penyedia Cloud : Selanjutnya, identifikasi penyedia cloud yang sesuai dengan kebutuhan bisnis Anda. Pertimbangkan faktor seperti reputasi, keamanan, kepatuhan, dan kemampuan mereka untuk memenuhi persyaratan khusus Anda.
- e. Evaluasi Keamanan : Lakukan evaluasi keamanan menyeluruh untuk memahami bagaimana data Anda akan dilindungi di lingkungan cloud. Pastikan penyedia cloud memiliki langkah-langkah keamanan yang sesuai dengan standar industri.
- f. Perencanaan Migrasi: Buat rencana migrasi yang terperinci. Tentukan bagaimana data dan aplikasi akan dipindahkan ke lingkungan cloud. Pastikan proses migrasi berjalan lancar dan minimalkan downtime.
- g. Pelatihan dan Integrasi : Persiapkan tim Anda dengan pelatihan yang diperlukan untuk bekerja di lingkungan cloud. Juga, pertimbangkan bagaimana SIM berbasis cloud akan diintegrasikan dengan sistem dan proses yang ada.
- h. Pilot dan Uji Coba : Sebelum melakukan implementasi penuh, lakukan uji coba atau pilot terbatas untuk memastikan bahwa semua sistem berjalan dengan baik dan sesuai dengan harapan.
- i. Implementasi Bertahap : Implementasikan SIM berbasis cloud secara bertahap, mulai dari area atau departemen yang lebih kecil. Ini memungkinkan Anda untuk memecahkan masalah secara progresif dan meminimalkan dampak potensial.
- j. Pemantauan dan Evaluasi Berkelanjutan : Setelah implementasi, terus monitor kinerja dan keamanan lingkungan cloud Anda. Evaluasi secara berkala apakah SIM berbasis cloud telah memenuhi ekspektasi dan melakukan perubahan jika diperlukan.
- k. Kebijakan dan Kepatuhan : Pastikan Anda memahami dan mematuhi semua kebijakan dan peraturan yang berlaku terkait dengan penggunaan cloud, termasuk privasi data dan kepatuhan.
- l. Komitmen Jangka Panjang : Akhirnya, pertimbangkan penggunaan cloud sebagai komitmen jangka panjang. Rencanakan skala dan pertimbangkan kebutuhan masa depan bisnis Anda.

Pengambilan keputusan untuk mengadopsi SIM berbasis cloud harus dilakukan dengan hati-hati dan dengan perencanaan yang matang. Ini melibatkan pemahaman mendalam tentang kebutuhan bisnis Anda, evaluasi manfaat dan risiko, serta pemilihan penyedia cloud yang tepat. Dengan perencanaan yang baik, implementasi SIM berbasis cloud dapat meningkatkan efisiensi, skalabilitas, dan fleksibilitas bisnis Anda.

## 2.5 FAKTOR YANG HARUS DI PERTIMBANGKAN OLEH PERUSAHAAN

Ketika sebuah perusahaan mempertimbangkan untuk mengadopsi Sistem Informasi Manajemen (SIM) berbasis cloud, ada sejumlah faktor yang harus dipertimbangkan dengan cermat. Faktor-faktor ini akan membantu perusahaan membuat keputusan yang bijak dan sesuai dengan kebutuhan bisnis mereka. Berikut adalah beberapa faktor yang harus dipertimbangkan :

1. **Kebutuhan Bisnis** : Pertama-tama, perusahaan harus memahami dengan baik kebutuhan bisnis mereka. Apa yang ingin dicapai dengan mengadopsi SIM berbasis cloud? Identifikasi area atau proses yang akan diintegrasikan dengan SIM berbasis cloud dan beri prioritas pada kebutuhan kritis.
2. **Manfaat dan Tujuan** : Tentukan manfaat yang diharapkan dari implementasi SIM berbasis cloud. Apakah perusahaan menginginkan efisiensi biaya, skalabilitas, akses fleksibel, atau manfaat lainnya Tujuan yang jelas akan membantu dalam mengukur kesuksesan implementasi.
3. **Biaya dan Keuangan** : Evaluasi biaya implementasi, termasuk biaya awal, biaya operasional, dan biaya pemeliharaan. Buat perbandingan antara biaya cloud dan infrastruktur on-premises. Selain itu, pertimbangkan ROI (Return on Investment) yang diharapkan dari implementasi SIM berbasis cloud.
4. **Keamanan Data** : Keamanan data adalah faktor kritis. Pastikan penyedia cloud memiliki langkah-langkah keamanan yang memadai untuk melindungi data perusahaan. Evaluasi kebijakan keamanan, enkripsi data, dan kompatibilitas dengan peraturan kepatuhan yang berlaku.
5. **Ketersediaan dan Kinerja** : Pastikan bahwa penyedia cloud memiliki layanan dengan tingkat ketersediaan tinggi dan kinerja yang memadai. Downtime yang sering atau lambatnya akses dapat berdampak negatif pada operasional bisnis.
6. **Skalabilitas** : Cloud computing memungkinkan skalabilitas yang mudah. Pertimbangkan apakah perusahaan memerlukan kapasitas yang dapat ditingkatkan secara dinamis saat diperlukan.
7. **Integrasi dengan Sistem yang Ada** : Pastikan SIM berbasis cloud dapat diintegrasikan dengan sistem yang sudah ada dalam perusahaan. Integrasi yang baik akan memungkinkan data dan proses berjalan dengan mulus.
8. **Pengelolaan dan Dukungan** : Evaluasi tingkat dukungan yang disediakan oleh penyedia cloud. Apakah mereka memiliki layanan pelanggan yang responsif dan bantuan teknis yang tersedia?
9. **Kepatuhan dan Regulasi** : Pastikan bahwa penggunaan SIM berbasis cloud mematuhi semua peraturan dan kebijakan kepatuhan yang berlaku, seperti GDPR (General Data Protection Regulation) atau HIPAA (Health Insurance Portability and Accountability Act) jika sesuai.
10. **Kapasitas Pertumbuhan** : Pertimbangkan kebutuhan kapasitas jangka panjang perusahaan. SIM berbasis cloud harus dapat mendukung pertumbuhan bisnis dan perubahan kebutuhan.
11. **Kebergantungan pada Penyedia Cloud** : Perusahaan perlu menyadari tingkat ketergantungan pada penyedia cloud tertentu. Pastikan ada rencana darurat jika perlu memindahkan data atau aplikasi dari satu penyedia cloud ke penyedia lain.
12. **Pertimbangan Lingkungan** : Selain aspek bisnis, pertimbangkan dampak lingkungan dari penggunaan cloud. Beberapa perusahaan memprioritaskan penyedia cloud yang berkomitmen pada praktik berkelanjutan dan ramah lingkungan.
13. **Keselarasan dengan Strategi TI** : Pastikan bahwa implementasi SIM berbasis cloud selaras dengan strategi TI keseluruhan perusahaan dan memiliki dukungan dari departemen TI.
14. **Pelatihan dan Kesiapan Karyawan** : Siapkan tim Anda dengan pelatihan yang diperlukan untuk menggunakan SIM berbasis cloud dengan efektif. Pastikan bahwa karyawan memahami perubahan yang akan terjadi.

Pertimbangan ini harus dijalani melalui proses evaluasi dan perencanaan yang matang. Selain itu, kolaborasi antara tim manajemen, TI, dan pihak-pihak terkait sangat penting untuk membuat keputusan yang bijak dalam mengadopsi SIM berbasis cloud.

## KESIMPULAN DAN SARAN

### 3.1 Kesimpulan

Sistem informasi berbasis cloud adalah bahwa pendekatan ini memberikan fleksibilitas, skalabilitas, dan aksesibilitas data yang tinggi. Dengan memanfaatkan teknologi cloud, organisasi dapat meningkatkan efisiensi operasional, mengurangi biaya infrastruktur, dan memfasilitasi kolaborasi tim secara global. Namun, penting untuk mempertimbangkan keamanan data dan privasi sebagai tantangan yang perlu diatasi dalam implementasi sistem informasi berbasis cloud. Dengan perencanaan dan pengelolaan yang cermat, integrasi teknologi cloud dapat memberikan manfaat strategis bagi perusahaan.

### 3.2 Saran

Demikianlah penyajian yang kami susun Pembahasan tentang Sistem Informasi Manajemen Berbasis Cloud. Kami hanyalah manusia biasa yang tidak luput dari kekesalahan. Mungkin dalam pembahasan di atas terdapat kekurangan atau tidak sesuai tema yang di bahas, maka dari itu kami selaku tim penyusun makalah ini sangat mengharapkan kritik dan saran dari teman - teman ataupun pembaca makalah ini.

## REFERENCES

[https://id.wikipedia.org/wiki/Sistem\\_informasi\\_manajemen](https://id.wikipedia.org/wiki/Sistem_informasi_manajemen)

<https://www.elitery.com/articles/aplikasi-berbasis-cloud/>

<https://www.kompasiana.com/rifqimurtiani6620/64fd993108a8b513cf30c662/sistem-informasi-berbasis-cloud-revolusi-dalam-strategi-organisasi>

<https://www.helios.id/id/blog-id/detail/pentingnya-teknologi-cloud-computing-bagi-perusahaan/>