BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

2.1.1 Manajemen Risiko Penerapan Komputasi Awan pada UMKM

Berdasakan penelitian yang dilakukan Nurmaya (2011) yang berjudul Manajemen Risiko Penerapan Komputasi Awan pada UMKM dapat disimpulkan sebagai berikut:

1. Penerapan teknologi '*cloud computing*' dengan dukungan infrastruktur jaringan dan layanan informasi dan telekomunikasi di Korea Selatan menunjukkan bahwa teknologi ini dapat memajukan *Small Medium Enterprise* (SME) di negara tersebut.
2. Kondisi geografis Indonesia yang dikelilingi laut dan terdiri dari pulau-pulau merupakan suatu tantangan tersendiri dalam penyediaan infrastruktur jaringan dan layanan informasi dan telekomunikasi yang baik secara merata.
3. Penerapan komputasi awan dapat menjadi salah satu solusi untuk meningkatkan kesejahteraan masyarakat Indonesia melalui penggunaan teknologi informasi dengan menghilangkan kendala-kendala pada pengadaan infrastuktur, *platform*, unit kerja penyedia layanan informasi berikut sumberdaya manusia yang mahal pada sisi UMKM.

4. Namun demikian, ‘cloud computing’ bukanlah solusi tunggal. Keberhasilan penerapannya untuk mencapai tujuan yang disebutkan dalam makalah ini perlu didukung oleh sejumlah faktor penting yang sebagiannya dapat diidentifikasi, dianalisis, dan disusun langkah penanganannya.

Sebagai kesimpulan dari makalah “MANAJEMEN RISIKO PENERAPAN KOMPUTASI AWAN PADA UMKM” dapat disebutkan bahwa penerapan proses-proses manajemen risiko yang baik pada penerapan komputasi awan untuk UMKM merupakan kunci penting untuk mencapai keberhasilan.

2.1.2 Beberapa Kendala Penerapan *Cloud Computing* di Indonesia

Berdasarkan hasil penelitian (Enlik, 2013) tentang berbagai kendala *Cloud Computing*, dapat diambil kesimpulan bahwa *Cloud Computing* merupakan pilihan yang dapat digunakan untuk menyediakan sumber daya TI serta efektif dan efisien dalam hubungannya dengan pemanfaatan sumber daya TI tersebut. Terlihat bahwa masih terdapat beberapa kendala yang masih erat hubungannya dengan infrastruktur di Indonesia. Solusi yang dapat dilakukan di antaranya dengan melakukan pembenahan untuk beberapa kendala yang terjadi dan belajar untuk memahami dasar-dasar *Cloud Computing* sebagai langkah awal sebelum memutuskan untuk migrasi menuju *Cloud Computing*. Dan dari pembahasan yang ada, untuk saat ini Indonesia dapat dinyatakan belum seratus persen siap dalam menerapkan *Cloud Computing* di

berbagai aspek karena untuk dapat menerapkan *Cloud Computing* dengan berhasil, ada beberapa kondisi dan faktor keberhasilan yang harus diperhatikan.

2.1.3 Analisis Keamanan Aplikasi Penyimpanan Data Pada Sistem *Cloud Computing*

Analisis yang dilakukan Oktariani (2011) ini menghasilkan kesimpulan:

Cloud computing merupakan model komputasi yang memiliki beragam keuntungan. Namun dibalik itu, *privacy* data merupakan hal penting dalam sebuah organisasi terutama pengguna *Cloud Computing* yang harus memperhatikan aspek proteksi data yang disediakan oleh *provider*. Jika *provider* mengalami *down*, data organisasi terancam hilang, tidak dapat diakses, atau dapat *direcovery* namun tidak utuh. Hal tersebut tentu saja dapat merugikan pihak user, karena itu saran untuk *user* sebelum memilih *provider* penyedia layanan adalah :

1. Memastikan reputasi, sejarah dan keberlanjutan provider memiliki pelayanan yang akan tersedia dan data dapat dilacak dalam jangka waktu yang lama.
2. Meyakinkan penanganan dari provider dalam menghadapi kegagalan *backup* atau *retrieval* informasi cukup terjamin.
3. Waktu delay yang mungkin terjadi ketika pengembalian informasi setelah *crash* atau insiden lainnya.
4. Memastikan tersedianya perlindungan hak milik intelektual dan rahasia dagang atas informasi yang kita simpan pada media penyimpanan cloud.

5. Kinerja provider dalam melakukan *backup*, respon dan pemulihan insiden harus benarbenar teruji.

Namun ancaman tersebut dapat diantisipasi dengan melakukan beberapa hal seperti berikut:

1. Memastikan telah memilih provider pengada layanan cloud computing yang memiliki standardisasi keamanan, *recovery* data, maupun *backup* rutin.
2. Melakukan proses enkripsi data-data penting yang dimiliki dengan menyimpan kunci dekripsinya di luar *cloud*.
3. Berlangganan *service* antivirus *cloud*.

2.1.4 "*The Benefits and Risks of Cloud Platform*"

Chappell (2011) dalam tulisannya yang berjudul "*The Benefits and Risks of Cloud Platform*" dapat disimpulkan bahwa penerapan *Cloud Platform* bagi suatu organisasi dapat menimbulkan keuntungan (*Benefits*) dan juga risiko (*Risks*) tergantung sejauh mana organisasi tersebut mempersiapkan penerapannya dan memahami segala keuntungan dan risiko tersebut yang akan mempengaruhi bisnis-nya. Dalam hal ini departemen TI sangat berpengaruh dalam meyakinkan organisasi / perusahaan untuk memutuskan penerapan *Cloud Platform*.

2.2 Manajemen Risiko

Risiko berhubungan dengan ketidakpastian ini terjadi oleh karena kurang atau tidak tersedianya cukup informasi tentang apa yang akan terjadi. Sesuatu yang tidak pasti *(uncertain)* dapat berakibat menguntungkan atau merugikan. menurut Wideman, ketidakpastian yang menimbulkan kemungkinan menguntungkan dikenal dengan istilah peluang (*Opportunity*). sedangkan ketidak pastian yang menimbulkan akibat yang merugikan dikenal dengan istilah risiko (*Risk*).

Risiko adalah segala sesuatu yang dapat mempengaruhi pencapaian tujuan organisasi. Australian/ NZ Standard 4360 : 1999 mendefinisikan Risk sebagai "*The chance of something happening that will have or impact upon objectives"* (perubahan dari sesuatuyang terjadi yang akan mempuyai pengaruh terhadap tujuan).

Kata *something* (sesuatu) menurut definisi risiko diatas dapat menyangkut : Komersil, legal, operasional, teknologi, karyawan, manajemen, manusia, finansial, kejadian alamiah, politik. Sedangkan kata *impact* (pengaruh) dapat menyangkut : aset, lingkungan, reputasi, komunitas, manusia, penghasilan, biaya, kinerja dan layanan. Dan kata *objectives* (tujuan) dapat menyangkut : aset, manusia, layanan, komunitas, laba, lingkungan, reputasi.

Dalam bidang investasi, menurut Jones (2004:142), risiko adalah kemungkinan pendapatan yang diterima (*actual return*) dalam suatu investasi akan berbeda dengan pendapatan yang diharapkan (*expected return*). Semakin besar

penyimpangan antara hasil sesungguhnya dengan hasil yang diharapkan, berarti semakin besar risiko yang akan ditanggung.

Dapat tidaknya risiko dialihkan kepada pihak lain, dapat dibedakan :

1. Risiko yang dapat dialihkan kepada pihak lain, dengan mempertangguhkan suatu objek yang akan terkena risiko kepada pihak asuransi.
2. Risiko yang tidak dapat dialihkan pada pihak lain.

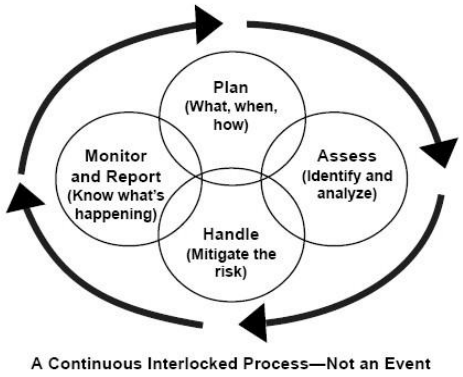
Menurut sumber/penyebab timbulnya risiko dapat dibedakan :

1. Risiko *intern* yaitu risiko yang berasal dari dalam perusahaan sendiri, seperti kecelakaan kerja, kerusakan aktiva karena karyawan, *miss*-manajemen dan sebagainya.
2. Risiko *ekstern* yaitu risiko yang berasal dari luar perusahaan, seperti penipuan, persaingan, fluktuasi harga, perubahan politik.

Manajemen risiko adalah suatu pendekatan terstruktur/metodologi dalam mengelola ketidakpastian yang berkaitan dengan ancaman, suatu rangkaian aktivitas manusia termasuk : penilaian risiko, pengembangan strategi untuk mengelolanya dan mitigasi risiko dengan menggunakan pemberdayaan/pengelolaan sumber daya. Strategi yang dapat diambil antara lain adalah memindahkan risiko kepada pihak lain, menghindari risiko, mengurangi efek negatif risiko, dan menampung sebagian atau semua konsekuensi risiko tertentu. Manajemen risiko tradisional terfokus pada risiko-risiko yang timbul oleh penyebab fisik atau legal (seperti bencana alam atau

kebakaran, kematian, serta tuntutan hukum. Manajemen risiko keuangan, di sisi lain, terfokus pada risiko yang dapat dikelola dengan menggunakan instrumen-instrumen keuangan. (Sadgrove, 2005).

Manajemen Risiko dimulai dari proses identifikasi risiko, penilaian risiko, mitigasi, *monitoring* dan evaluasi seperti pada Gambar 2.1:



Gambar 2.1 : Elemen Manajemen Risiko

sumber: Sadgrove, 2005

Manfaat adanya manajemen risiko pada perusahaan diantaranya adalah :

1. Membantu perusahaan menghindari semaksimal mungkin biaya-biaya yang terpaksa harus dikeluarkan.
2. Membantu manajemen untuk memutuskan apakah risiko yang dihadapi perusahaan akan dihindari atau diambil.
3. Jika penaksiran risiko dilakukan secara akurat maka dapat memaksimalkan keuntungan perusahaan.

Risiko dapat diminimalisir/ditanggulangi beberapa aktivitas :

1. Mengadakan pencegahan dan penanggulangan terhadap kemungkinan terjadinya peristiwa yang menimbulkan kerugian
2. Melakukan retensi artinya mentolerir terjadinya kerugian, dengan membiarkan terjadinya kerugian dan untuk mencegah terganggunya operasi dengan menyediakan dana untuk penanggulangannya.
3. Melakukan pengendalian terhadap risiko, seperti melakukan perdagangan berjangka
4. Mengalihkan/memindahkan risiko kepada pihak lain, yaitu dengan cara mengadakan kontrak pertangguhan (asuransi) dengan perusahaan asuransi terhadap risiko tertentu.

2.3 Enterprise Risk Management (ERM)

2.3.1 Pengertian ERM

Definisi ERM menurut COSO *Enterprise Risk Management – Integrated Framework.* 2004 adalah :

"suatu proses yang berpengaruh pada sebuah entitas, jajaran direksi, pihak manajemen, dan personel lain yang diaplikasikan pada penetapan strategi perusahaan, didisain untuk mengidentifikasi kejadian yang potensial yang dapat berpengaruh pada

entitas, dan mengelola risiko yang dapat diterima, dan memberikan jaminan keamanan yang beralasan dalam rangka mencapai tujuan perusahaan".

Prinsip yang melandasi ERM bahwa setiap entitas pada perusahaan seharusnya memberikan suatu nilai bagi *stakeholder*. Nilai ini sangat tergantung pada keputusan manajemen mulai dari perumusan strategi sampai dengan kegiatan operasional setiap hari.

ERM mendukung penciptaan nilai dengan memudahkan manajemen untuk :

1. Menghadapi kejadian potensial yang menciptakan ketidakpastian.
2. Memberikan respon yang tepat untuk mengurangi risiko yang dapat mempengaruhi hasil.

2.3.2 Elemen-elemen ERM

Elemen-elemen ERM meliputi :

1. Komitmen Chief Executive Officer(CEO)
2. Kebijaksanaan risiko dan misi perusahaan
3. Laporan unit bisnis, dan jajaran eksekutif
4. Pengembangan kerangka kerja (framework) risiko
5. Pengembangan bahasa risiko yang umum
6. Teknik untuk mengidentifikasi risiko
7. Perangkat untuk melaporkan dan memonitor risiko

8. Keterkaitan risiko pada pihak-pihak yang sesuai dan bertanggung jawab
9. Keterkaitan risiko dengan fungsi keuangan dan pendanaan
10. Pengintegrasian indentifikasi risiko dan perkiraan risiko ke strategi organisasi

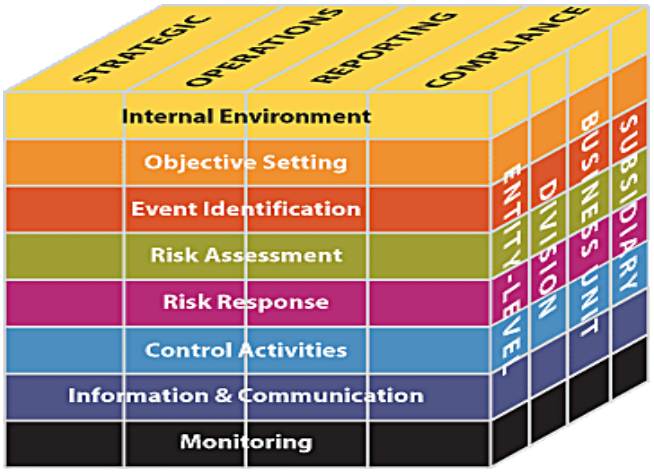
2.4 COSO Framework

Awalnya dibentuk pada tahun 1985, COSO merupakan inisiatif bersama dari lima organisasi sektor swasta dan didedikasikan untuk menyediakan panduan berpikir melalui pengembangan kerangka kerja dan pedoman manajemen risiko perusahaan (ERM), pengendalian internal, dan pencegahan risiko. Organisasi yang mendukung COSO adalah *Institute Auditor Internal* (IIA), *American Association Akuntansi* (AAA), *American Institute* Akuntan Publik (AICPA), Eksekutif Keuangan Internasional (FEI), dan Institut Akuntan Manajemen (IMA).

COSO mendefinisikan *Enterprise Risk Management* (ERM) sebagai proses yang dipengaruhi oleh unit dewan direksi, manajemen dan personil lainnya, diterapkan pada pengaturan strategi dan di seluruh perusahaan yang dirancang untuk mengidentifikasi peristiwa potensial yang dapat mempengaruhi unit/entitas, dan mengelola risiko untuk tetap berada pada *risk appetite*-nya, untuk memberikan keyakinan yang memadai mengenai pencapaian tujuan entitas.

Framework COSO ERM merupakan kubus 3-dimensi,selain sisi depan yang terdiri dari 8 komponen, sisi atas merupakan objektif manajemen risiko dan sisi

samping kubus merupakan komponen entitas organisasi seperti yang terlihat pada Gambar 2.2. ERM versi COSO terdiri dari 8 komponen yang saling terkait, yaitu: Lingkungan Internal (*Internal Environment*), Penetapan Tujuan (*Objective Setting*), Identifikasi Kejadian (*Event Identification*), Penilaian Risiko (*Risk Assessment*), Respon Risiko (*Risk Response*), Aktivitas Pengendalian (*Control Activities*), Informasi dan komunikasi (*Information and Communication*) dan Pemantauan (*Monitoring*). Framework ini mendefinisikan komponen penting, penyamaan bahasa, dan memberikan arahan dan bimbingan yang jelas bagi *enterprise risk management*.



Gambar 2.2: Kubus *Framework* COSO

Sumber: (*Committee of Sponsoring Organizations* (COSO) *of the Treadway Commission*. 2012)

2.4.1 Komponen COSO framework

Terdapat delapan komponen COSO framework yaitu :

1. Lingkungan internal (*internal environment*)

Pada tahapan ini perusahaan menetapkan :

a. Strategi bisnis
b. Objektif utama dari bisnis
c. Obektif terkait yang diturunkan ke bawah organisasi dari objktif utama bisnis
d. Menugaskan elemen organisasi dan pimpinan yang bertanggung jawab

2. Penetapan Tujuan (*objective setting*)

a. Menetapkan proses bisnis
b. Menentukan *risk appetite*

3. Identifikasi kejadian (*event identification*)

a. Kejadian yang dapat memberikan pengaruh negatif yang menggambarkan risiko
b. Termasuk dalam mengidentifikasikan kejadian, baik internal maupun eksternal yang dapat mempengaruhi strategi dan pencapaian objektif
c. Menentukan bagaimana faktor internal dan eksternal bersatu dan berinteraksi mempengaruhi profil risiko

4. Penilaian risiko (*assesment*)

a. Memperkenankan unit untuk memahami sampai di mana kejadian potensial yang dapat berpengaruh terhadap objektif
b. Penilaian risiko dari dua perspektif

- *Likelihood* (Kemungkinan terjadi)
- *Impact* (Dampak)

c. Menilai dan mengukur risiko terkait dengan objektif

5. Respon risiko (*risk response*)

a. Identifikasi dan evaluasi kemungkinan respon atas risiko

b. Evaluasi pilihan terkait dengan *risk appetite* dari perusahaan.

c. Pilih dan lakukan respon atas evaluasi dari portofolio risiko dan respon

Dalam menentukan respon terhadap risiko terdapat empat alternatif tindakan, yaitu:

1. Menerima Risiko, adalah tindakan perusahaan untuk menerima suatu risiko dengan tidak melakukan tindakan berarti yang memerlukan sumber daya yang besar. Tindakan ini biasanya diterapkan pada risiko-risiko yang tingkat risiko keseluruhan rendah (tidak signifikan) bagi perusahaan, sehingga apabila dilakukan penanganan residual risk menimbulkan biaya yang tidak sebanding dengan keuntungannya.
2. Menghindari Risiko, adalah tindakan perusahaan untuk tidak melakukan usaha tertentu yang mengandung risiko yang tidak diinginkan. Tindakan ini biasanya diterapkan pada risiko-risiko yang tingkat risiko keseluruhannya tidak dapat

diterima oleh perusahaan atau berdampak sangat tinggi bagi perusahaan, dimana penanganannya akan menimbulkan biaya yang sangat tinggi serta tidak efisien.

3. Mengurangi Risiko, adalah tindakan perusahaan dengan menggunakan semua sumber daya yang dimilikinya berusaha untuk dapat meminimalkan risiko tanpa menghilangkan peluang perusahaan untuk meraih keuntungan (*return*). Tindakan ini dapat dilakukan terhadap paling tidak salah satu dari kedua faktor, yaitu:
   a. Mengurangi kemungkinan terjadinya risiko, biasanya dengan melakukan proses perubahan desain dan *engineering*, prosedur *quality assurance* atau audit secara periodik.
   b. Mengurangi dampak akibat terjadinya suatu risiko, biasanya diterapkan pada risiko yang berdampak tinggi dan kemungkinannya rendah, antara lain dengan membuat rencana kontinjensi atau rencana evakuasi.
4. Membagi Risiko, adalah tindakan perusahaan untuk memindahkan risiko kepada pihak ketiga yang dapat mengelola risiko antara lain melalui kesepakatan kontrak dengan *cloud provider* atau asuransi.

6. Aktivitas pengendalian (*control activities*)

Aktifitas pengendalian merupakan kebijakan dan prosedur yang membantu memastikan bahwa *risk response* yang dipilih dilaksanakan dengan memadai. Meskipun aktifitas pengendalian umumnya dikenal sebagai strategi untuk mengurangi risiko, namun aktifitas pengendalian tertentu juga dipakai pada strategi

risk response lain. Aktifitas pengendalian dipasangkan di seluruh organisasi, yaitu disetiap tingkatan maupun fungsi dalam organisasi. Aktifitas pengendalian dikelompokkan dalam berbagai ccara dan mencakup areal aktifitas yang mungkin bersifat preventif atau detektif, manual atau terkomputerisasi, serta di tingkatan proses atau manajemen.

7. Komunikasi dan informasi (*information and communication*)

a. Identifikasi manajemen, mendapatkan dan mengkomunikasikan informasi yang berhubungan dalam bentuk dan jangka waktu yang memungkinan yang bertanggungjawab menjalanakan kewajibannya.

b. Komunikasi berlangsung dalam pengertian luas, mengalir ke bawah, antar dan ke atas oraganisasi.

8. Pengawasan (*Monitoring*)

Efektifitas dari komponen ERM yang lain dimonitor melalui:

a. Aktivitas monitoring terus-menerus

b. Evaluasi terpisah

c. Kombinasi dari keduanya

2.4.2 Perbandingan COSO ERM dengan ISO 31000: 2009

ISO 31000: 2009 dan COSO ERM merupakan dua rujukan praktik terbaik saat ini yang dapat digunakan dalam penerapan manajemen risiko. Dalam praktik penerapan manajemen risiko di perusahaan, penggunaan rujukan tersebut harus disesuaikan dengan kebutuhan perusahaan baik dari konteks internal maupun eksternal. Metode kuantitatif, semi kuantitatif, maupun kualitatif juga harus dipergunakan dalam mengelola risiko dan pemanfaatan peluang yang digunakan dalam rangka membantu pencapaian tujuan perusahaan.

Perbedaan mendasar antara ISO 31000:2009 dan COSO ERM:2004 adalah:

a. COSO ERM tidak memaparkan secara terpisah proses dari kerangka kerja manajemen risiko dan lebih menekankan pada pengembangan pengendalian internal perusahaan sebagai salah satu upaya perusahaan dalam memastikan risiko dapat terkelola dan masuk ke dalam area selera risiko perusahaan.
b. ISO 31000 memaparkan proses manajemen risiko (klausal 5) terpisah dari kerangka kerjanya (klausal 4) dan lebih menekan pada penerapan manajemen risiko sebagai alat penciptaan nilai dari proses bisnis perusahaan.

2.5 Komputasi Awan (*Cloud Computing*)

Menurut Peter Mell dan Timothy Grance (2012:2) definisi *Cloud Computing* adalah sebuah model yang memungkinkan untuk *ubiquitous* (Diamanapun dan kapanpun), nyaman, *On demand* akses jaringan ke sumber daya komputasi (contoh: jaringan, *server*, *storage*, aplikasi, dan layanan) yang dapat dengan cepat dirilis atau ditambahkan. *Cloud Computing* sebagai suatu layanan teknologi informasi yang dapat dimanfaatkan oleh pengguna dengan berbasis jaringan/internet. Dimana suatu sumber daya, perangkat lunak, informasi dan aplikasi disediakan untuk digunakan oleh komputer lain yang membutuhkan. *Cloud computing* mempunyai dua kata "*Cloud*" dan "*Computing*". *Cloud* yang berarti internet itu sendiri dan *Computing* adalah proses komputasi.

Konsep *Cloud computing* biasanya dianggap sebagai internet. Karena internet sendiri digambarkan sebagai awan (*Cloud*) besar (biasanya dalam skema jaringan, internet dilambangkan sebagai awan) yang berisi sekumpulan komputer yang saling terhubung. *Cloud computing* datang sebagai sebuah evolusi yang mengacu pada konvergensi teknologi dan aplikasi lebih dinamis. Dimana terdapat perubahan besar memiliki implikasi yang menyentuh hampir setiap aspek komputasi. Untuk *end user*, Komputasi awan menyediakan sarana untuk meningkatkan layanan baru atau mengalokasikan sumber daya komputasi lebih cepat, berdasarkan kebutuhan bisnis.

2.5.1 Model Layanan *Cloud Computing*

Tiga model layanan dijelaskan oleh NIST (Mell dan Grance, 2009) yang ditawarkan oleh *cloud computing*, berdasarkan kemampuan yang disediakan yaitu :

1. *Cloud Software as a Service (SaaS).* Kemampuan yang diberikan kepada konsumen untuk menggunakan aplikasi penyedia dapat beroperasi pada infrastruktur awan. Aplikasi dapat diakses dari berbagai perangkat klien melalui antarmuka seperti *web browser* (misalnya, email berbasis web). Konsumen tidak mengelola atau mengendalikan infrastruktur awan yang mendasari termasuk jaringan, server, sistem operasi, penyimpanan, atau bahkan kemampuan aplikasi individu, dengan kemungkinan pengecualian terbatas terhadap pengaturan konfigurasi aplikasi pengguna tertentu.

2. *Cloud Platform as a Service (PaaS).* Kemampuan yang diberikan kepada konsumen untuk menyebarkan aplikasi yang dibuat konsumen atau diperoleh ke infrastruktur komputasi awan menggunakan bahasa pemrograman dan peralatan yang didukung oleh *provider*. Konsumen tidak mengelola atau mengendalikan infrastruktur awan yang mendasari termasuk jaringan, server, sistem operasi, atau penyimpanan, namun memiliki kontrol atas aplikasi disebarkan dan memungkinkan aplikasi melakukan hosting konfigurasi.

3. *Cloud Infrastructure as a Service (IaaS).* Kemampuan yang diberikan kepada konsumen untuk memproses, menyimpan, berjaringan, dan komputasi

sumberdaya lain yang penting, dimana konsumen dapat menyebarkan dan menjalankan perangkat lunak secara bebas , dapat mencakup sistem operasi dan aplikasi. Konsumen tidak mengelola atau mengendalikan infrastruktur awan yang mendasari tetapi memiliki kontrol atas sistem operasi, penyimpanan, aplikasi yang disebarkan, dan mungkin kontrol terbatas komponen jaringan yang pilih (misalnya, *firewall host*).

2.5.2 Model *Deployment Cloud Computing*

Menurut NIST (Mell dan Grance, 2009), ada empat *deployment* model dari *cloud computing* ini, yaitu:

1. *Public Cloud*

Public Cloud adalah layanan *Cloud Computing* yang disediakan untuk masyarakat umum. Pengguna bisa langsung mendaftar ataupun memakai layanan yang ada. Banyak layanan *Public Cloud* yang gratis, dan ada juga yang perlu membayar untuk bisa menikmati layanannya.

Keuntungan dari *Public Cloud* pengguna tidak perlu berinvestasi untuk merawat serta membangun infrastruktur, *platform*, ataupun aplikasi. Pengguna tinggal memakai secara gratis (untuk layanan yang gratis) atau membayar sebanyak pemakaian (*pay as you go*). Dengan pendekatan ini, kita bisa mengurangi dan merubah biaya Capex (*Capital Expenditure*) menjadi Opex (*Operational Expenditure*). Sedangkan kerugiannya sangat tergantung dengan kualitas layanan

internet (koneksi) yang kita pakai. Jika koneksi internet mati, maka tidak ada layanan yang dapat diakses. Untuk itu, perlu dipikirkan secara matang infrastruktur internetnya.

2. *Private Cloud*

Private Cloud adalah layanan *cloud computing* yang disediakan untuk memenuhi kebutuhan internal dari organisasi/perusahaan. Pada kasus ini umumnya bagian IT akan berperan sebagai *service provider* (penyedia layanan) dan bagian atau divisi lain menjadi *service consumer*. Bagian IT sebagai *service provider*, harus bertanggung jawab agar layanan bisa berjalan dengan baik sesuai dengan standar kualitas layanan yang telah ditentukan oleh perusahaan, baik infrastruktur, platform, maupun aplikasi yang ada.

Contoh layanan *Private Cloud* :

a. SaaS: *Web Application, Mail Server*, *Database Server* untuk keperluan internal.
b. PaaS: Sistem Operasi, *Web Server*, *Framework* serta *Database* untuk internal
c. IaaS: *Virtual machine* yang bisa di-*request* sesuai dengan kebutuhan internal

Keuntungan dari *Private Cloud* adalah menghemat *bandwidth* internet ketika layanan itu hanya diakses dari jaringan internal.Proses bisnis tidak tergantung dengan koneksi internet, akan tetapi tetap saja tergantung dengan koneksi jaringan lokal (intranet). Sedangkan kerugiannya adalah investasi besar, karena perusahaan yang

harus menyiapkan infrastrukturnya serta membutuhkan tenaga kerja untuk merawat dan menjamin layanan berjalan dengan baik

3. *Hybrid Cloud*

Hybrid Cloud adalah gabungan dari layanan *Public Cloud* dan *Private Cloud* yang diimplementasikan oleh suatu organisasi/perusahaan. Dalam *Hybrid Cloud* ini, kita bisa memilih proses bisnis mana yang bisa dipindahkan ke *Public Cloud* dan proses bisnis mana yang harus tetap berjalan di *Private Cloud*.

Keuntungan dari *Hybrid Cloud* adalah keamanan data terjamin karena data dapat dikelola sendiri dan lebih leluasa untuk memilih mana proses bisnis yang harus tetap berjalan di *private cloud* dan mana proses bisnis yang bisa dipindahkan ke *public cloud* dengan tetap menjamin integrasi dari keduanya. Sedangkan kerugiannya untuk aplikasi yang membutuhkan integrasi antara *public cloud* dan *private cloud*, investasi dan pengelolaan infrastruktur *cloud* harus dipikirkan secara matang.

4. *Community Cloud*

Community Cloud adalah layanan *Cloud Computing* yang dibangun eksklusif untuk komunitas tertentu, yang *consumer*-nya berasal dari organisasi yang mempunyai perhatian yang sama atas sesuatu/beberapa hal, misalnya saja standar keamanan, aturan, *compliance*, dsb. *Community Cloud* ini bisa dimiliki, dipelihara,

dan dioperasikan oleh satu atau lebih organisasi dari komunitas tersebut, pihak ketiga, ataupun kombinasi dari keduanya.

Keuntungan dari *Community Cloud* adalah bisa bekerja sama dengan organisasi lain dalam komunitas yang mempunyai kepentingan yang sama. Melakukan hal yang sama bersama-sama tentunya lebih ringan daripada melakukannya sendiri. Sedangkan kerugiannya adalah ketergantungan antar organisasi jika tiap-tiap organisasi tersebut saling berbagi sumber daya.

2.5.3 Keuntungan *Cloud Computing*

Ada beberapa keuntungan yang dapat dilihat dari perkembangan *Cloud Computing* menurut Stiawan (2012), seperti:

1. Lebih efisien karena menggunakan anggaran yang rendah untuk sumber daya.
2. Membuat lebih *agility*, dengan mudah dapat berorientasi pada profit dan perkembangan yang cepat.
3. Membuat operasional dan manajemen lebih mudah, dimungkinkan karena sistem pribadi atau perusahaan yang terkoneksi dalam satu *cloud* dapat dimonitor dan diatur dengan mudah.
4. Menjadikan kolaborasi yang terpecaya.
5. Membantu dalam menekan biaya operasi biaya modal pada saat kita meningkatkan *reliability* dan kritikal sistem informasi yang kita bangun.

2.6 Manufaktur

Manufacturing adalah satu rangkaian kegiatan yang meliputi: desain produk, pemilihan bahan, perencanaan, manufaktur (pembuatan), jaminan kualitas, manajemen, dan penjualan; yang dilakukan dalam satu perusahaan. CIRP (1983)

Manufaktur secara luas adalah proses merubah bahan baku menjadi produk yang meliputi perancangan produk, pemilihan material, tahap-tahap proses di mana produk tersebut dibuat. Manufaktur secara umum adalah suatu aktifitas yang kompleks yang melibatkan barbagai variasi sumberdaya dan aktifitas perancangan produk pembelian, pemasaran, mesin, dan perkakas *manufacturing*, penjualan, perancangan proses, *production control*, pengiriman material, *support service*, dan *customer service*.

Sistem Informasi Manufaktur adalah suatu sistem barbasis komputer yang bekerja dan hubungannya dengan sistem informasi fungsional lainnya untuk mendukung manajemen perusahaan dalam pemecahan masalah yang berhubungan dengan manufaktur produk perusahaan yang pada dasarnya tetap bertumpu pada *input*, proses dan *output*.

Manfaat dari sistem ini adalah mendukung fungsi produksi yang meliputi seluruh kegiatan yang terkait dengan perencanaan dan pengendalian proses untuk memproduksi barang atau jasa,manfaat lainnya yaitu :

1. Hasil produksi perusahaan lebih cepat dan tepat waktu.
2. Perusahaan lebih cepat memperoleh informasi yang akurat dan terpercaya.

3. Arsip lebih terstruktur karena menggunakan sistem *database*.
4. Sistem informasi manufaktur yang berupa fisik robotik,hasil produksi semakin cepat, tepat dan berkurangnya jumlah sisa bahan yang tidak terpakai.

Ruang lingkup sistem informasi manufaktur terdiri dari sistem perencanaan manufaktur, rencana produksi, rencana tenaga kerja, rencana kebutuhan bahan baku serta sistem pengendalian manufaktur.