PENGUKURAN RISIKO PADA PENERAPAN CLOUD COMPUTING UNTUK SISTEM INFORMASI (Studi Kasus Universitas Bina Darma)

Ria Andriyani, Edi Surya Negara, Maria Ulfa, Widya Cholil

Fakultas Ilmu Komputer
Universitas Bina Darma
Jl. A. Yani No. 12, Palembang 30624, Indonesia

Abstrak

Perguruan Tinggi merupakan sebuah organisasi akademis, institusi yang memiliki peran dan posisi strategis dalam pencapain tujuan pendidikan, yaitu mencerdaskan kehidupan bangsa untuk insan indonesia cerdas dan kompetitif. Untuk mencapai tujuan tersebut, perguruan tinggi juga membutuhkan dukungan Teknologi Informasi dalam menjalankan kegiatan kegiatannya. Namun permasalahan-permasalahan finansial yang melanda, pemotongan anggaran teknologi informasi kemungkinan besar terjadi dan berpengaruh pada bidang teknologi informasi di suatu universitas. Selain itu terjadi perubahan secara terus menerus terkait kebijakan mengenai perguruan tinggi. Oleh karena itu perguruan tinggi perlu mencari cara untuk mengotimalkan efektivitas dan efisiensi dari semua operasional. Maka untuk mencapai tujuan perguruan tinggi yang didukung oleh teknologi informasi, perlu ada manajemen risiko yang tepat untuk penerapan cloud computing guna meningkatkan performa perguruan tinggi. Oleh karena itu pada penelitian ini, akan dirancang suatu model manajemen risiko pada penerapan teknologi cloud computing untuk sistem informasi di perguruan tinggi dengan metode framework octave.

Kata kunci: *Cloud computing, teknologi informasi, model manajemen risiko,framework OCTAVE*

1 PENDAHULUAN

Perguruan Tinggi merupakan sebuah organisasi akademis, institusi yang memiliki peran dan posisi strategis dalam pencapain tujuan pendidikan, yaitu mencerdaskan kehidupan bangsa untuk insan indonesia cerdas dan kompetitif. Untuk mencapai tujuan tersebut, perguruan tinggi juga membutuhkan dukungan Teknologi Informasi dalam menjalankan kegiatan kegiatannya.

Perkembangan teknologi informasi menjadi solusi yang inovatif, dinamis, dan memiliki manfaat secara ekonomi, Teknologi tersebut yaitu cloud computing. Teknologi informasi ini mampu menjawab masalah dan tantangan di atas yang dihadapi oleh perguruan tinggi. Cloud Computing mengubah cara bagaimana layanan teknologi informasi disediakan dan disebarkan, sehingga institusi memiliki kesempatan untuk mengakses informasi informasi

pendidikan dan ilmu pengetahuan. Melalui teknologi informasi ini, diharapkan pendidikan di perguruan tinggi mendapat performa optimal, karena institusi dapat lebih fokus pada proses utama yang seharusnya dilakukan dibanding mengelola teknologi informasi secara ekstensif.

Disamping kebutuhan akan teknologi informasi, organisasi juga menghadapi beragam peluang dan risiko yang mungkin mempengaruhi secara positif ataupun negatif terhadap pencapaian tujuan mereka. Risiko juga muncul terutama ketika akan menerapkan suatu teknologi informasi baru kedalam suatu organisasi. Pernyataan ini diperkuat oleh Mirae dan Andreecu (2011) yang menyatakan bahwa pengambilan keputusan untuk menggunakan cloud computing perlu diperhitungkan risiko terkait implementasi solusi. Oleh karena itu agar dapat menangani risiko risiko ini secara memadai, merupakan suatu prasyarat untuk merancang dan menerapkan sistem manajemen risiko. Maka untuk mencapai tujuan perguruan tinggi yang didukung oleh teknologi informasi, perlu ada manajemen risiko yang tepat untuk penerapan cloud computing guna meningkatkan performa perguruan tinggi.

Risiko terkait TI merupakan suatu pengukuran kuantitatif dari kerugian atau kerusakan yang disebabkan oleh ancaman (threat), vulnerability, atau oleh suatu kejadian (event: malicious atau non malicious) yang berpengaruh pada kumpulan aset TI yang dimiliki oleh organisasi. Menurut HM Treasury, mengidentifikasi dan menilai risiko (risiko turunan atau yang melekat) serta merespon terhadap hal tersebut merupakan hal-hal yang termasuk dalam manajemen risiko. Sedangkan COSO mendefinisikan manajemen risiko sebagai suatu proses, yang dilakukan oleh entitas dewan direksi, manajemen, dan personil lainnya, diterapkan dalam pengaturan strategi dan di seluruh perusahaan, yang dirancang untuk mengidentifikasi peristiwa potensial yang dapat mempengaruhi entitas, dan mengelola risiko agar berada di dalam risk appetite, untuk menyediakan keyakinan memadai tentang pencapaian tujuan entitas.

Kouns dan Minoli mendefinisikan manajemen risiko TI (manajemen risiko keamanan informasi) sebagai proses untuk mengurangi risiko TI (proses adalah aktivitas yang berkelanjutan dan didefinisikan dengan baik). Manajemen risiko merupakan proses yang berkelanjutan, fundamental dan kompleks, sebagai bagian dari keamanan informasi. Kemudian National Institute of Standards and Technology (NIST) sendiri mendefinisikan manajemen risiko sebagai proses yang memperkenankan manajer TI untuk menyeimbangkan biaya operasional dan ekonomis untuk ukuran-ukuran protektif dan mencapai keuntungan pada kapabilitas misi dengan menjaga sistem TI dan data yang mendukung misi organisasi mereka. Dari semua pengertian yang ada, manajemen risiko merupakan suatu proses yang berkelanjutan dalam menilai, memitigasi, dan mengevaluasi risiko. Hal ini dilakukan untuk meningkatkan efektivitas biaya yang dikeluarkan guna memastikan keamanan dari sistem teknologi informasi yang digunakan pada organisasi. Sehingga semua aset TI yang dimiliki oleh organisasi aman dari segala gangguan maupun ancaman yang dapat mengenainya.

Berbagai definisi mengenai cloud computing banyak diungkapkan oleh para ahli dan peneliti, Perter Mell dan Tim Grance dari National Institute of Standards and Technology (NIST), Information Technology Laboratory mendefinisikan cloud computing sebagai suatu model yang mempermudah ketersediaan dan konfigurasi layanan baik berupa perangkat lunak, jaringan, server, media penyimpanan maupun aplikasi. Suatu layanan dapat dipasang dan dihilangkan dengan mudah. Model Cloud computing memiliki lima karakteristik utama yaitu On-demand self-service, Broad network access, Resource pooling, Rapid elasticity dan Measured Service. Ada tiga model layanan yang ditawarkan oleh cloud com-

puting, berdasarkan level abstraksi dari kemampuan yang disediakan dan model layanan dari penyedia seperti yang terlihat pada Gambar 2, yaitu:

1. Infrastructure as a Service (IaaS)

   IaaS menyediakan sumber daya virtualisasi (komputasi, penyimpanan, dan komunikasi) sesuai permintaan. Kemampuan yang diberikan kepada konsumen ialah penyediaan pemrosesan, penyimpanan, jaringan, dan sumber daya komputasi fundamental lainnya, sehingga konsumen dapat menyebarkan dan menjalankan perangkat lunak tertentu meliputi perangkat lunak dan aplikasi.

2. Platform as a Service (PaaS)

   Cloud platform menyediakan lingkungan agar pengembang bisa membuat dan menyebarkan aplikasi tanpa perlu mengetahui jumlah processor atau jumlah memori yang dibutuhkan oleh aplikasi tersebut [13].

3. Software as a Service (SaaS)

   Kemampuan yang diberikan kepada konsumen ialah menggunakan aplikasi penyedia yang berjalan di atas infrastruktur cloud. Aplikasi dapat diakses dari berbagai perangkat klien, baik melalui antarmuka thin client, seperti web browser, atau antarmuka program [14].

2 METODOLOGI PENELITIAN

Kerangka penelitian yang dituangkan dalam diagram alir dibawah ini menggambarkan proses penelitian yang akan ditempuh sekaligus menggambarkan penelitian secara keseluruhan. Diagram alir ini memperlihatkan tahapan-tahapan proses penulisan yang akan dilakukan dari tahap awal sampai akhir.

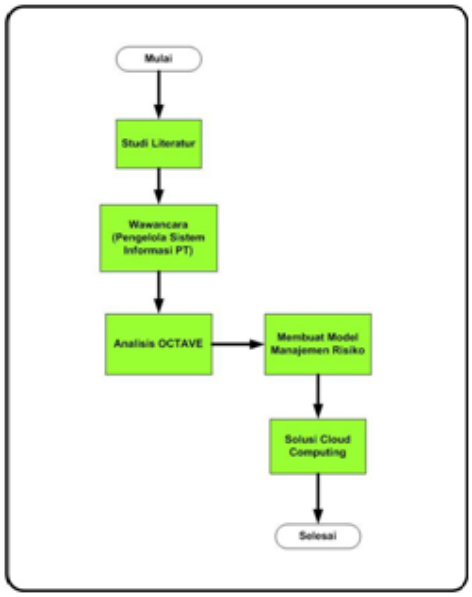
Motode yang digunakan dalam penelitian ini adalah OCTAVE Metodologi. Metode OCTAVE-S (The Operationally Critical Threat, Asset, and Vulnerability Evaluation for Small Organizations) merupakan bagian dari metode OCTAVE yang disusun dan dikembangkan sebagai metode analisis risiko untuk perusahaan kecil. Analisis risiko metode OCTAVE-S dilakukan dengan langkah langkah sebagai berikut.

1. Fase 1 : Membuat profil ancaman berbasis aset (Build Asset-Based Threat Profile).

   Fase ini merupakan evaluasi pada aspek keorganisasian. Pada fase ini tim analisis mengidentifikasi Impact Evaluation Criteria yang akan digunakan untuk mengevaluasi tingkat risiko. Pada fase ini juga dilakukan identifikasi aset aset penting perusahaan dan evaluasi tingkat keamanan saat ini diterapkan oleh perusahaan. Tim analisis memilih 3 (tiga) sampai (5) aset terpenting perusahaan yang akan dianalisis secara mendalam. Hasil fase ini adalah pendefenisian kebutuhan keamanan informasi dan profil ancaman untuk aset aset terpenting tersebut.

2. Fase 2 : Mengidentifikasi kelemahan infrastruktur (Identify Infrastructure Vulnerabilities).

   Pada fase ini high level riview terhadap infrastruktur computer perusahaan dan berfokus pada hal hal yang menjadi perhatian utama para pengelola infrastruktur. Tim menganalisis bagaimana penggunaan (konfigurasi, pengelolaan, dan lain-lain) infrastruktur terutama yang berhubungan dengan aset aset terpenting (critical aset).



Gambar 1: Kerangka Penelitian

3. Fase 3 : Membuat perancangan dan strategi keamanan (Develop Security Strategy and Plans).

   Pada fase ini dilakukan identifikasi risiko terhadap aset aset terpenting (critical assets) dan memutuskan langkah langkah apa yang harus dilakukan.

3 HASIL DAN PEMBAHASAN

3.1 Analisis Risiko Metode OCTAVE pada Sistem Informasi Universitas Bina Darma

Analisis yang dilakukan pada Sistem Informasi perguruan tinggi, kami telah megumpulkan dan mengolah data berdasarkan wawancara dan kuisioner bagikan kepada pengelola sistem informasi perguruan tinggi. Wawancara dan quisioner yang dibagikan digunakan untuk mengetahui kelemahan dari sistem informasi yang digunakan oleh perguruan tinggi serta mencara solusi atas risiko risiko yang mungkin terjadi. Kuisioner yang dibuat menggunakan metode OCTAVE terdiri dari tahap tahap berikut :

1. Membangun aset berbasis profile ancaman (Built asset-based Threat Profiles) yang terdiri dari 2 proses, 6 aktifitas dan 16 langkah dimana proses pertamannya yaitu mengidentifikasi informasi organisasi (Identify Orgazational Information) yang memiliki 3 aktifitas yaitu membangun kriteria evaluasi (Establish Impact Evaluation Criteria), mengidentifikasi aset organisasi (Identify Organizational Asset) dan mengevaluasi prakter keamanan organisasi (Evaluate Organizational Secrutity Practices) serta 4 langkah dan proses ke-duanya, membuat profile ancaman (Create Theart Profiles) yang memiliki 3 aktifitas yaitu memilih aset kritis (Select Critical Asset), identifikasi kebutuhan keamanan untuk aset kritis (Identify Security Requirements for Critical Asset)

dan identifikas ancaman pada aset kritis (Identify Threat of Critical Asset) serta 12 langkah.

2. Mengidentifikasi kerentanan infrastruktur (Identify Infrastructure Vurnerabilities) yang terdiri dari 1 proses, 2 aktifitas dan 5 langkah, prosesnya yaitu memeriksa perhitungan infrastruktur yang berhubungan dengan aset kritis (Exmine Computing Infrastructure in Relation to Critical Asset) dan memiliki 2 aktifitas yaitu memeriksa jalur akses (Examine Access Path) dan menganalisa proses terkait dengan teknologi (Analyze Technology-Related Proceses) serta 5 langkah.

3. Mengembangkan strategi keamanan dan perancangan (Develop Security Strategy and Plans) yang terdiri dari 2 proses, 8 aktifitas dan 9 langkah dimana proses pertamannya yaitu : identifikasi dan analisis risiko (Identify and Analyze Risk) yang terdiri dari 3 aktifitas yaitu mengevaluasi dampak ancaman (Evaluate Impact of Threat), membangun kemungkinan kriteria evaluasi (Establish Probability Evaluation Criteria), dan mengevaluasi kemungkinan ancaman (Evaluate Probability of Threat) serta 3 langkah. Proses keduannya yaitu mengembangkan strategi perlindungan dan rencanan mitigasi (Develop Protection Strategy and Mitigation) dan memiliki 5 aktifitas yaitu menggambarkan strategi perlindungan saat ini (Describe Current Protection Strategy), memilih pendekatan mitigasi (Select Mitigation Approuch), Mengembangakan rencanan mitigasi risiko (Develop Risk Mitigation Plans), Identifikasi perubahan untuk strategi perlindungan (Identify Change to Protection Strategy) dan identifikasi langkah selanjutnya (Identify Next Step) serta 6 langkah.

Dengan metode OCTAVE yang terdiri dari 3 fase, 5 Proses, 16 Aktifitas dan 30 langkah tersebut, diharapkan dapat membantu dalam penilaian dan pengukuran risiko pada penerapan cloud computing untuk sistem informasi di perguruan tinggi. Analisis dilakukan terhadap quisioner yang telah di isi oleh pengguna dan pengelola sistem informasi perguruan tinggi berdasarkan kriteria penilaian yang telah ditentukan pada framework OCTAVE, adapun kriteri tersebut adalah :

Penilaian :
Y (sudah ada / diimplementasikan) = 3
T (belum ada / tidak diimplementasikan) = 2
? tidak tahu/ragu-ragu = 1

Spotplight :
Green = Telah diimplementasikan dengan sangat baik sehingga belum memerlukan peningkatan.
Yellow = Telah diimplementasikan tetapi masih banyak yang harus ditingkatkan.
Red = Belum diimplementasikan.

3.2 Hasil Analisis OCTAVE pada Sistem Informasi di Unviersitas Bina Darma

Analsis OCTAVE telah dilakukan terhadap sepuluh assessment point. Hasil analsis tersebut antara lain :

1. **Security Policy** pada perguruan tinggi berada pada spotplight **YELLOW**, ini menunjukkan bahwa pada beberapa perguruan tinggi telah mengimplementasikan Security Policy, tetapi masih banyak yang harus ditingkatkan.

2. **Organizational Security** pada perguruan tinggi berada pada spotplight **YELLOW**, ini menunjukkan bahwa pada beberapa perguruan tinggi telah mengimplementasikan Organizational Security, tetapi masih banyak yang harus ditingkatkan.

3. **Asset Clasification & Control** pada perguruan tinggi berada pada spotplight **YELLOW**, ini menunjukkan bahwa pada beberapa perguruan tinggi telah mengimplementasikan Asset Clasification & Control, tetapi masih banyak yang harus ditingkatkan.

4. **Personnel Security** pada perguruan tinggi berada pada spotplight **YELLOW**, ini menunjukkan bahwa pada beberapa perguruan tinggi telah mengimplementasikan Personnel Security, tetapi masih banyak yang harus ditingkatkan.

5. **Fhysical Environmental Security** pada perguruan tinggi berada pada spotplight **YELLOW**, ini menunjukkan bahwa pada beberapa perguruan tinggi telah mengimplementasikan Fhysical Environmental Security, tetapi masih banyak yang harus ditingkatkan.

6. **Communication and Operations Management** pada perguruan tinggi berada pada spotplight **YELLOW**, ini menunjukkan bahwa pada beberapa perguruan tinggi telah mengimplementasikan Communication and Operations Management, tetapi masih banyak yang harus ditingkatkan.

7. **Access Control** pada perguruan tinggi berada pada spotplight **YELLOW**, ini menunjukkan bahwa pada beberapa perguruan tinggi telah mengimplementasikan Access Control, tetapi masih banyak yang harus ditingkatkan.

8. **System Development & Maintenance** pada perguruan tinggi berada pada spotplight **RED**, ini menunjukkan bahwa sebagaian beser perguruan tinggi belum mengimplementasikan System Development & Maintenance dengan baik.

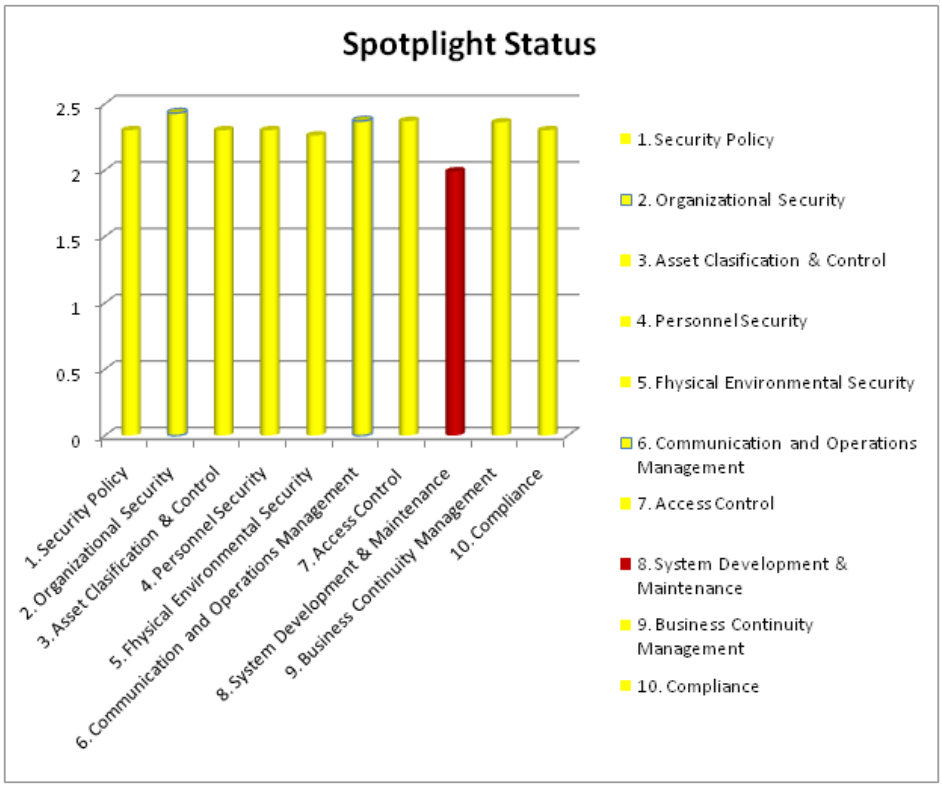
9. **Business Continuity Management**, pada perguruan tinggi berada pada spotplight **YELLOW**, ini menunjukkan bahwa pada beberapa perguruan tinggi telah mengimplementasikan Business Continuity Management, tetapi masih banyak yang harus ditingkatkan.

10. **Compliance** pada perguruan tinggi berada pada spotplight **YELLOW**, ini menunjukkan bahwa pada beberapa perguruan tinggi telah mengimplementasikan Compliance, tetapi masih banyak yang harus ditingkatkan.

Hasil Analsis OCTAVE dengan Spotplight Status Sistem Informasi di Universitas Bina Darma ditunjukkan pada Gambar 2.

4 KESIMPULAN

Berdasarkan hasil analisis yang telah dilakukan, maka dapat diambil beberapa kesimpulan sebagai berikut:



Gambar 2: Hasil Analsis OCTAVE Sistem Informasi Universitas Bina Darma

Spotplight Status Sistem Informasi pada Universitas Bina Darma berdara pada posisi **YELLOW**. Ini menunjukkan bahwa sistem informasi telah diimplementasikan tetapi masih banyak yang harus ditingkatkan.