JURNAL TEKNOLOGI TECHNOSCIENTIA ISSN: 1979-8415
Vol. 8 No. 2 Februari 2016

PENGUKURAN RISIKO PADA PENERAPAN CLOUD COMPUTING UNTUK SISTEM INFORMASI (STUDI KASUS UNIVERSITAS BINA DARMA)

Ria Andryani[1]

[1]Fakultas Ilmu Komputer, Universitas Bina Darma Palembang

Masuk: 15 Desember 2015, revisi masuk: 17 Januari 2016, diterima:30 Januari 2016

ABSTRACT

College is an academic organization, an institution which has a role and strategic position in the achievement of educational goals. To achieve The goal, the college needs the support of information technology in carrying out its activities. There are currently utilizing cloud computing technology be one solution to optimize operational effectiveness and efficiency information technology in higher education. However, the use of new technologies of potential risks in their operations that have an impact on performance organization. Therefore we need appropriate risk management for implementation cloud computing in order to improve the performance of colleges. Research It aims to measure the level of possible risks arising from the introduction cloud computing at the university to make use of the OCTAVE Framework on the application of cloud computing technology for information systems at universities high (Bina Darma University case study). This research resulted in the level of University information system readiness Bina Darma in applying technology cloud computing that are in a position YELLOW, namely the implementation of the information system has supported the adoption of cloud computing, but more needs to be improved.

Keywords*: Cloud computing, information technology, risk management Model Framework OCTAVE*

INTISARI

Perguruan Tinggi merupakan sebuah organisasi akademis, institusi yang memiliki peran dan posisi strategis dalam pencapain tujuan pendidikan. Untuk mencapai tujuan tersebut, perguruan tinggi membutuhkan dukungan teknologi informasi dalam menjalankan kegiatannya. Dewasa ini pemenfaat teknologi cloud computing menjadi salah satu solusi untuk mengotimalkan efektivitas dan efisiensi operasional teknologi informasi pada perguruan tinggi. Namun penggunaan teknolgi baru berpotensi menimbulkan resiko dalam operasionalnya yang berdampak terhadap kinerja organisasi. Oleh karena itu diperlukan manajemen risiko yang tepat untuk penerapan cloud computing guna meningkatkan performa perguruan tinggi. Penelitian ini bertujuan untuk mengukur tingkat kemungkinan risiko yang timbul dari penerapan cloud computing pada perguruan tinggi dengan menggunaka OCTAVE Framework pada penerapan teknologi cloud computing untuk sistem informasi di perguruan tinggi (studi kasus Universitas Bina Darma). Penelitian ini menghasilkan tingkat kesiapan sistem informasi Universitas Bina Darma dalam menerapkan teknologi cloud computing yang berada pada posisi YELLOW, yaitu implementasi sistem informasi telah mendukung penerapan cloud computing tetapi masih banyak yang harus ditingkatkan.

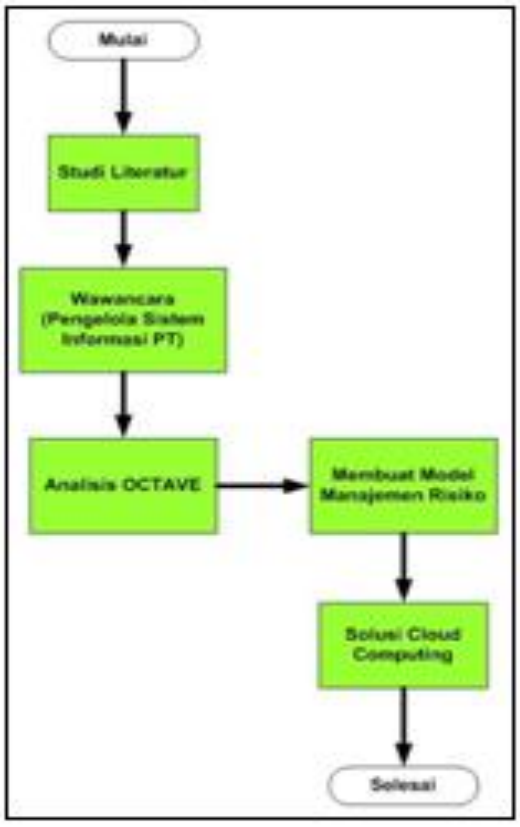
Kata kunci: Cloud computing, Teknologi informasi, Model manajemen risiko, Framework OCTAVE

PENDAHULUAN

Perguruan Tinggi merupakan sebuah organisasi akademis, institusi yang memiliki peran dan posisi strategis dalam pencapain tujuan pendidikan, yaitu

[1] ria.andryani@binadarma.ac.id

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 diatas 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.



Gambar 1: Kerangka Penelitian

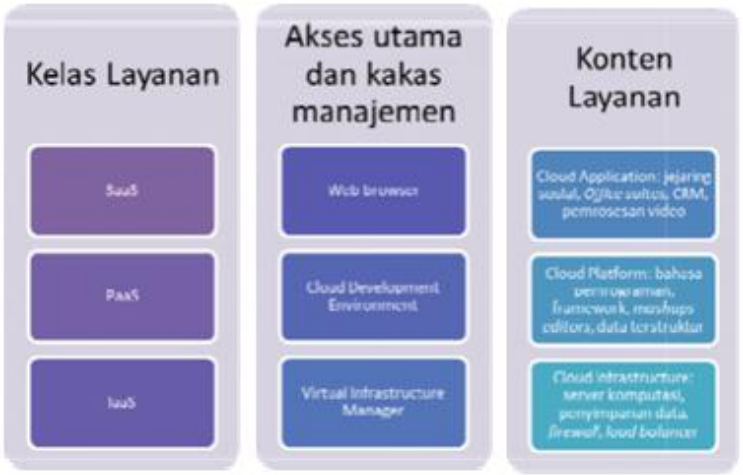
Disamping kebutuhan akan teknologi informasi, organisasi juga menghadapi beragam peluang dan risiko yang mungkin mempengaruhi secara positif ataupun negatif terhadap pencapaian tujuan mereka. Risiko juga muncul terutama ketika akan menerapkan suatu teknologi informasi baru kedalam suatu organisasi. Pernyataan ini diperkuat oleh Mircea, M. and Andreescu, A.I (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 (2004), mengidentifikasi dan menilai risiko (risiko turunan atau yang melekat) serta merespon terhadap hal tersebut merupakan hal-hal yang termasuk dalam manajemen risiko. Sedangkan COSO (2004) 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 didalam risk appetite, untuk menyediakan keyakinan memadai tentang pencapaian tujuan entitas.

Minoli, D. and Kouns, J (2010) 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.Mell, P. and Grance, T (2011) National Institute of Standards and Technology (NIST) 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, Mell, P. and Grance, T (2011) 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 Mell, P. and Grance, T., (2010). Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M., (2010) 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 computing, Rimal, B.P., Choi, E. and Lumb, I., (2009); Voorsluys, W., Broberg, J. and Buyya, R., (2011), 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. 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.



Gambar 2: Model Layanan Cloud Computing

METODE

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.

Metode 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, Alberts, C., Dorofee, A., Stevens, J. and Woody, C., (2003).

Analisis risiko metode OCTAVE-S dilakukan dengan langkah langkah sebagai berikut: 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 kea manan 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. Fase 2 yaitu Mengidentifikasi kelemahan infrastruktur (Identify Infrastructure Vulnerabilities). Pada fase ini high level riview terhadap infrastruktur komputer 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). 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.

PEMBAHASAN

Analisis Risiko Metode OCTAVE Pada Sistem Informasi Universitas Bina Darma

Analisis yang dilakukan pada Sistem Informasi perguruan tinggi, telah dikumpulkan 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 beberapa tahap.

Tahap pertama Membangun aset berbasis profile ancaman (Built asset-based Threat Profiles) yang terdiri dari 2 proses, 6 aktifitas dan 16 langkah dimana proses pertamanya 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 keduanya, 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.

Tahap kedua Mengidentifikasi kerentanan infrastruktur (Identify Infrastructure Vurnerabili ties) 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.

Tahap ketiga 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.

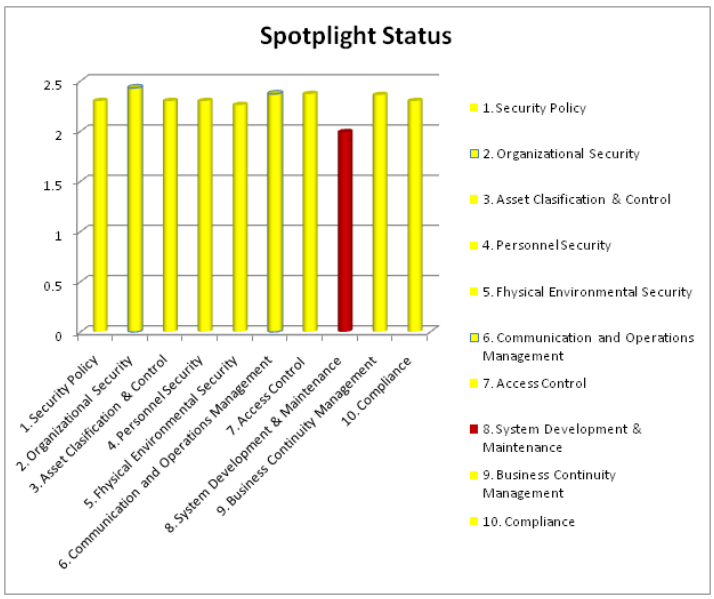
Dengan metode OCTAVE yang terdiri dari3 fase, 5 Proses, 16 Aktifitas dan 30 langkah tersebut, diharapkan dapat membantu dalam penilaian dan pengukuran risiko pada penerapan cloud computing untuk sistem informasi di perguruan tinggi. Analisis dilakukan terhadap quisioner yang telah di isi oleh pengguna 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.



Gambar 3: Hasil Analsis OCTAVE Sistem Informasi Universitas Bina Darma

Hasil Analisis OCTAVE Pada Sistem Informasi Di Universitas Bina Darma

Analisis OCTAVE yang 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. Physical Environmental Security pada perguruan tinggi berada pada spotplight YELLOW, ini menunjukkan bahwa pada beberapa perguruan tinggi telah mengimplementasikan Physical 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 yang 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 yang 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 yang belum mengimplementasikan model System Development & Maintenance dengan baik. 9. Business Continuity Management, pada perguruan tinggi berada pada spotplight YELLOW, ini

menunjukkan bahwa pada beberapa perguruan tinggi yang telah mengimplementasikan model 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 yang telah mengimplementasikan Compliance, tetapi masih banyak yang harus ditingkatkan.

Hasil Analsis OCTAVE dengan Spotplight Status Sistem Informasi di Universitas Bina Darma ditunjukkan pada Gambar 3.

KESIMPULAN

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

DAFTAR PUSTAKA

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M., 2010. A view of cloud computing. Communications of the ACM, 53(4), pp.50-58.

Alberts, C., Dorofee, A., Stevens, J. and Woody, C., 2003. Introduction to the OCTAVE Approach. Pittsburgh, PA, Carnegie Mellon University.

COSO, 2004, Jersey City: Committee of Sponsoring Organisations of the Treadway Commission (COSO). Jersey City: Committee of Sponsoring Organisations of the Treadway Commission (COSO).

Mircea, M. and Andreescu, A.I., 2011. Using cloud computing in higher education: A strategy to improve agility in the current financial crisis. Communications of the IBIMA.

Minoli, D. and Kouns, J., 2010. Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams. Wiley.

Mell, P. and Grance, T., 2011. The NIST definition of cloud computing.

Mell, P. and Grance, T., 2010. The NIST definition of cloud computing. Communications of the ACM, 53(6), p.50.

Rimal, B.P., Choi, E. and Lumb, I., 2009, August. A taxonomy and survey of cloud computing systems. In 2009 Fifth International Joint Conference on INC, IMS and IDC (pp. 44-51). Ieee.

Treasury, H.M., 2004, The Orange Book: Management of Risk–Principles and Concepts. Norwich, UK: HM Treasury on behalf of the Controller of Her Majesty Stationary Office.

Voorsluys, W., Broberg, J. and Buyya, R., 2011. Introduction to cloud computing. Cloud computing: Principles and paradigms, pp.1-44.