PENGUJIAN KEAMANAN TRANSAKSI *CLOUD COMPUTING* PADA LAYANAN *SOFTWARE AS A SERVICE (SaaS)* MENGGUNAKAN KERANGKA KERJA NIST SP800-53A (Studi Kasus pada PT. X di Bandung)

Nanang Sasongko
Jurusan Akuntansi, Fak. Ekonomi, Universitas Jenderal Achmad Yani (UNJANI)
Jl.Terusan Jend.Sudirman , PO Box 48 Cimahi, Bandung,40321 Tlp/ Fax 022-6610201
E-Mail : nanangs@bdg.centrin.net.id

ABSTRAK
Pada Cloud computing , jasa layanan yang dapat disampaikan yaitu Infrastruture as a service (IaaS), Platform as a service(PaaS) dan Software as a service (SaaS) dan jasa yang paling banyak digunakan adalah di Penggunaan Software as a service(SaaS) , bagi perusahaan pelanggan dapat menghemat pengeluaran biaya belanja TI. Namun, konsep software as a service juga memiliki sisi yang perlu diwaspadai yakni dalam hal keamanan data pelanggan. PT X berupaya untuk melakukan pengamanan terhadap data milik pelanggan dengan meningkatkan upaya pemasangan sistem kontrol keamanan transaksi pada sistem informasi yang dikelolanya.
Penerapan sistem kontrol keamanan yang telah dilakukan perlu diuji. Mekanisme pengujian sistem kontrol keamanan dapat menggunakan kerangka kerja NIST SP800-53A yang menyediakan standard pengujian terhadap tiga faktor, yaitu faktor manajemen, operasional dan teknikal. Mekanisme pengujian menggunakan kerangka kerja NIST SP800-53A menentukan status dari penerapan sistem pengamanan transaksi yang dilakukan terhadap suatu sistem informasi dengan 2 alternatif yaitu satisfied(S) atau other than satisfied (O) dalam menerapkan suatu sistem kontrol keamanan.
Dengan menggunakan metode penilaian pemeriksaan dan pengamatan langsung terhadap objek penilaian, wawancara (interview), dan Pengujian (test), proses menguji objek penilaian dalam kondisi tertentu untuk membandingkan kondisi aktual dengan perilaku yang diharapkan.
Berdasarkan hasil pengujian terhadap sistem informasi hotel dan restoran yang dibangun dan dikelola oleh PT.X memiliki status satisfied tetapi masih banyak parameter kontrol keamanan transaksi yang perlu diperbaiki atau ditingkatkan sehingga menghasilkan sistem informasi yang memiliki sistem pengamanan yang lebih baik.

Kata kunci : Cloud computing, Software as a service, NIST SP800-53A

1. PENDAHULUAN

Berdasarkan informasi yang diperoleh dari SDA ASIA dalam kurun waktu lima tahun ke depan, pasar analisa bisnis *software-as-a service* (*SaaS*), dan *cloud system* akan tumbuh tiga kali lipat hingga 2013. Menurut IDC, pasar *SaaS* di Asia Pasifik tahun ini meningkat cukup signifikan. Faktor pertumbuhan lainnya terkait dengan faktor kebijakan pengeluaran kapital dan pengetatan anggaran. Ketatnya biaya yang dapat dikeluarkan oleh perusahaan, membuat penawaran *software as a service* (*SaaS*) lebih menarik, sebab mereka dapat mengalihkan biaya operasional TI menjadi biaya berlangganan yang lebih hemat dan mudah. *SaaS* merupakan layanan terbanyak dari *cloud system* , selain *Infrastructure as a Service (IaaS)* dan *Platform as a Service(PaaS).*

Dengan adanya jasa ini transaksi dipermudah, fasulitas IT yang lebih murah, dan kontrol integritas data yang memadai.

Tujuan penelitin ini adalah menguji masalah keamanan data pelanggan, disebabkan karena adanya kekhawatiran gangguan *server* atau koneksi mengalami gangguan jaringan dan kemanan data, yang merupakan salah satu hal yang perlu menjadi perhatian dalam menerapkan bisnis berbasis konsep *software as a service(SaaS)* . Guna meminimalisasi masalah penyediaan dan keamanan data terhadap layanan berbasis *software as a service(SaaS)*.

PT X ,sebagai perusahaan penyedia layanan *SaaS* perlu dilakukan pengujian terhadap jaringan dan sistem pengamanan transaksi yang telah diterapkan oleh PT X terhadap sistem teknologi informasi yang telah dibangun dan disediakannnya, untuk mendukung layanan *SaaS.*
Dengan menyadari bahwa aplikasi terdistribusi seperti ini akan diterapkan dimana-mana dan juga visi bahwa tidak lama lagi semua hal yang berhubungan dengan data dan komputasi akan dapat dilakukan dengan tingkat independensi yang tinggi, mengantarkan penulis melakukan riset lebih lanjut mengenai perkembangan terbaru dari *distributed computing* ini.

2. LANDASAN TEORI

2.1. *Software as a Service (SaaS)*

Software as a Service (SaaS) merupakan salah satu jenis layanan *cloud computing* yang mengijinkan konsumen untuk dapat menggunakan aplikasi yang berjalan pada infrastruktur *cloud* yang disediakan oleh provider sehingga dapat diakses dari berbagai perangkat melalui *browser Web*. Konsumen tidak perlu mengelola atau mengendalikan infrastruktur, jaringan, *server,* sistem operasi, media penyimpanan. (Mell and Grance, 2009:2).

Dengan *software as a service*, pengguna tak perlu memusingkan kerumitan sistem tersebut dan hanya menggunakan sumber daya yang disediakan. Pertumbuhan lainnya didorong oleh *platform* baru dari perangkat lunak yang fungsinya cocok dengan pengiriman *software as a service*.

Pada konsep *software as a service* memiliki sisi yang perlu diwaspadai dan menjadi issu sentral yakni dalam hal keamanan transaksi data pelanggan, dan adanya kekhawatiran server mengalami *crash*. Guna meminimalisasi masalah keamanan data terhadap layanan berbasis *software as a service*, layanan yang disediakan oleh PT.X ini perlu dilakukan pengujian. Pengujian yang dilakukan terhadap sistem pengamanan yang diterapkan oleh PT X menggunakan kerangka kerja NIST (*National Institute of Standards and Technology*) secara khususnya menggunakan kerangka acuan SP 800-53A (*Special Publication* 800-53A).

2.2. Acuan NIST SP800-53A

NIST *(National Institute Standards Technology*) merupakan salah satu lembaga pemerintahan Amerikas Serikat yang bekerja sama dengan badan-badan federal lainnya untuk meningkatkan pemahaman terhadap pelaksanaan FISMA *(Federal Information Security Management Act)* dalam melindungi informasi dan sistem informasi serta menerbitkan standar dan pedoman yang memberikan dasar untuk program keamanan informasi yang kuat. NIST melakukan tanggung jawab hukum melalui Divisi Keamanan Komputer dari Laboratorium Teknologi Informasi (*Information Technology Laboratory* - ITL*)*. NIST mengembangkan standar, metrik, pengujian, dan program validasi untuk mempromosikan, mengukur, dan memvalidasi keamanan sistem informasi.

Laporan penelitian ITL *(Information Technology Laboratory)* berupa *Special Publication 800-series,* merupakan pedoman, dalam upaya memperoleh keamanan sistem informasi, dan laporan tersebut diperoleh dari kegiatan bersama dengan industri, pemerintah, dan organisasi akademis. NIST mengeluarkan dokumen SP800-53 untuk memberikan pedoman dalam pengelolaan kontrol keamanan terhadap sistem informasi federal maupun organisasi lainnya. Rekomendasi SP800-53 dibagi kedalam 3 kelas kontrol, 18 bagian *(family)* seperti yang terlihat pada tabel 1.

Tabel 1. Daftar kontrol NIST SP800-53

Class control	No	Family	Identifier
Technical	1	Access Control	AC
	2	Audit and Accountability	AU
	3	Identification and Authentication	IA
	4	System and Communications Protection	SC
Operational	5	Awareness and Training	AT
	6	Configuration Management	CM
	7	Contingency Planning	CP
	8	System and Information Integrity Operational	SI
	9	Incident Response	IR
	10	Maintenance	MA

	11	Media Protection	MP
	12	Physical and Environmental Protection	PE
	13	Personnel Security	PS
Management	14	Security Assessment and Authorization Management	CA
	15	Program Management	PM
	16	Planning Management	PL
	17	Risk Assessment Management	RA
	18	System and Services Acquisition Management	SA

Source :NIST SP800-53

2.3 Komputasi awan (*Cloud computing*)

Cloud computing atau komputasi awan merupakan tren baru di bidang komputasi ter distribusi dimana berbagai pihak dapat mengembangkan aplikasi dan layanan berbasis SOA (*Service Oriented Architecture*) di jaringan internet. misalanya: *Infrastucture as a Service (IaaS) , Platform as a Service (PaaS), dan Software as a Service (SaaS),* dan issu sentralnya adalah masalah keamanan transaksi

Komputasi awan ini sebenarnya juga bukanlah "barang baru", hanya mungkin karena lebih spesifik diarahkan ke jaringan internet dan karena berkembangnya konsep *web services* maka teknologi ini perlu memiliki suatu istilah yang segar dan tidak terjebak menjadi kata yang klise. Selain juga karena internet sering digambarkan sebagai awan di dalam diagram-diagram teknis jaringan

3. OBJEK PENELITIAN

Berdasarkan faktor-faktor yang telah diuraikan sebelumnya, PT X berupaya mengembangkan bisnisnya sebagai penyedia jasa yang berbasis pada *software as a service*. Dalam *software as a service*, seluruh bisnis proses dan data pelanggan ditempatkan di sebuah server *data centre* milik *service provider*. Semua proses dikelola oleh penyedia layanan, pelanggan dapat menggunakan dan membayar jasa sewanya setiap bulan sesuai dengan pemakaian. Sistem *software as a service* bagi perusahaan dapat menghemat pengeluaran biaya belanja TI.

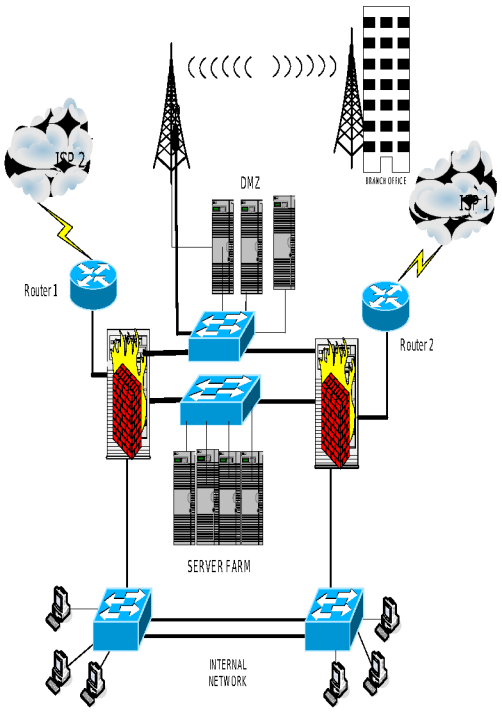
Saat ini PT X telah memiliki 2 produk *software* layanan SaaS *(software as a services)*, antara lain produk *SaaS* untuk sistem informasi perhotelan dan sistem informasi restoran. Aplikasi-aplikasi tersebut merupakan aplikasi yang berbasis web yang dipasangkan dalam *web server* yang terhubung dengan jalur internet sehingga dapat diakses oleh pelanggan dari manapun.

PT X memiliki jaringan di kantor pusat dan kantor cabang. *Server – server* utama tersimpan di kantor pusat dan untuk keperluan DRC *(Dissaster Recovery Center)* tersedia pula *server-server* cadangan di kantor cabang. Koneksi ke DRC dihubungkan dengan menggunakan media jaringan nirkabel. Sehingga replikasi data antara *server-server* di kantor pusat dapat dilakukan dengan *server-server* di kantor cabang.

Aplikasi *SaaS* yang disediakan oleh PT.X, dapat diakses melalui fasilitas jaringan VPN *(Virtual Private Network).* Hal ini disediakan untuk mengamanan transaksi data yang terjadi antara jaringan disisi pelanggan yang melewati jaringan publik untuk mengakses *server* aplikasi yang terdapat di PT X. Konfigurasi jaringan PT X dapat dilihat pada gambar 1. Segmentasi jaringan dilakukan pada jaringan PT X. *Firewall* yang dipasang di PT X membagi ke dalam empat segmen, yang terdiri dari segmen-segmen :

1. *Internal network*, merupakan jaringan internal dari PT X yang berisi komputer-komputer dari staf PT X.
2. *Eksternal network*, merupakan jaringan eksternal dari PT X yang terhubung dengan jaringan publik atau internet.
3. DMZ *(Demilitary Zone)*, merupakan jaringan yang berisi server-server yang disediakan agar pengguna jaringan publik dapat mengakses layanan yang disediakan oleh PT X. Salah satu layanan tersebut adalah berupa aplikasi perhotelan dan restoran yang merupakan aplikasi berbasis web dan dapat diakses oleh para pelanggan melalui internet.
4. *Server farm*, merupakan wilayah jaringan yang berisi server-server internal PT X, seperti mail server, database server. Server-server ini tidak dapat diakses secara langsung melalui wilayah eksternal.

ISSN: 1907-5022



Gambar 1. Topologi Jaringan PT X

4. METODOLOGI PENELITIAN

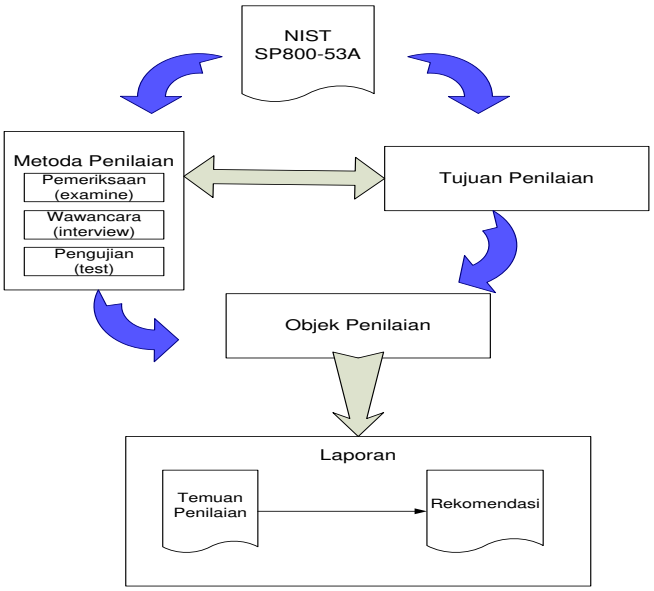
Dalam melakukan pengujian terhadap mekanisme sistem pengamanan yang diterapkan PT X, penulis menggunakan kerangka acuan NIST SP800-53A. Prosedur pengujian berdasarkan kerangka acuan NIST SP800-53A, terdiri dari beberapa tahapan sebagai berikut :

1. Persiapan untuk melakukan penilaian mekanisme pengamanan, dalam tahap ini ruang lingkup dirumuskan, mencakup karakteristik organisasi, lokasi, aset, dan teknologi yang dimiliki dan digunakan.
2. Membuat perencanaan terhadap kegiatan penilaian keamanan, dalam tahapan ini :
    a. Jenis penilaian kontrol keamanan ditentukan.
    Banyak pengendalian manajemen dan operasional diperlukan untuk melindungi sistem informasi dapat menjadi kandidat yang sangat baik untuk memiliki status *common security controls*. Tujuannya untuk mengurangi biaya pengelolaan keamanan dengan melakukan pemusatan dalam implementasi, dan penilaian keamanan. Kontrol keamanan yang tidak termasuk dalam *common security controls* dianggap sebagai *system specific controls*. Sistem *security plan* harus mengidentifikasi kontrol keamanan yang telah ditunjuk sebagai *common security controls* dan *system specific controls*.
    b. Menentukan kontrol keamanan / perangkat kontrol tambahan yang harus dimasukkan dalam penilaian berdasarkan *security plan* dan tujuan / lingkup penilaian.
    c. Memilih, menyesuaikan dan mengembangkan prosedur penilaian yang digunakan selama penilaian.
3. Melakukan penilaian terhadap sistem pengamanan, temuan yang diharapkan dalam tahap penilaian ini berupa status penilaian sebagai berikut :
    a. Puas *(Satisfied* (S)), yang mengindikasikan bahwa tujuan kontrol keamanan telah dipenuhi.
    b. Selain puas *(Other than satisfied* (O)), menunjukkan bahwa kontrol keamanan memiliki potensi anomali dalam operasional organisasi atau pelaksanaan kontrol perlu ditangani oleh organisasi. Temuan selain puas juga menunjukkan bahwa karena alasan-alasan tertentu dalam laporan penilaian, penilai tidak bisa memperoleh informasi yang cukup untuk membuat keputusan tertentu dalam laporan tersebut.
4. Mendokumentasikan hasil penilaian dalam bentuk laporan penilaian. Menetapkan jumlah status penilaian satisfied dan other than satisfied pada masing-masing kelas.
5. Melakukan analisa terhadap hasil laporan penilaian sistem pengamanan, berdasarkan indikator dari selain puas *other than satisfied)* dan puas *(satisfied)*, yang terdapat pada laporan penilaian kontrol keamanan untuk mengetahui kelemahan dan kekurangan pada sistem informasi dan memfasilitasi pendekatan yang terstruktur untuk melakukan mitigasi risiko sesuai dengan prioritas organisasi.

 ISSN: 1907-5022

Untuk mengetahui informasi dan data-data yang akurat untuk menunjang penulisan ini maka dilakukan proses pengumpulan data dengan menggunakan metode penilaian sebagai berikut :

1. Melakukan pemeriksaan dan pengamatan langsung terhadap objek penilaian, hal ini dilakukan untuk memperoleh gambaran dan data yang obyektif mengenai sistem informasi yang terdapat pada objek penelitian.
2. Proses wawancara *(interview)*, proses melakukan diskusi dengan pengelola layanan *SaaS* di PT X untuk memudahkan pemahaman, mencapai klarifikasi, atau mengarah ke lokasi bukti.
3. Pengujian *(test),* proses menguji beberapa objek penilaian dalam kondisi tertentu untuk membandingkan kondisi aktual dengan perilaku yang diharapkan.



Gambar 2. Kerangka Penelitian

proses penilaian dilakukan melalui tahapan-tahapan berikut :

1. Mengkategorisasi Sistem Informasi, pada tahap ini dilakukan langkah untuk mengkategorisasi sistem informasi dan informasi yang diproses, disimpan dan dikirimkan oleh sistem berdasarkan pada analisis dampak. Pengkategorian didasarkan pada tingkat pengaruh informasi atau sistem informasi terhadap organisasi dalam mencapai misi yang ditetapkan, melindungi aset, mempertahankan fungsinya sehari-hari dan melindungi individu ketika suatu peristiwa terjadi.
2. Menentukan baseline kontrol keamanan, berdasarkan hasil kategorisasi sistem informasi. Pemilihan *baseline* kontrol keamanan dilakukan berdasarkan pada dampak yang ditimbulkan akibat dari gangguan yang muncul terhadap sistem informasi hotel. Berdasarkan kategori keamanan sistem informasi yang dilakukan pada tahap sebelumnya dan standard *baseline* yang ditetapkan oleh *framework* NIST SP800-53.
3. Penerapan kontrol keamanan terhadap sistem informasi hotel diterapkan oleh PT.X pada komponen-komponen pendukung sistem informasi tersebut. Berdasarkan *security plan* yang diharapkan oleh pihak managemen PT X, kontrol keamanan yang diterapkan di PT X mengikuti standard kontrol kemananan SP800-53 .
4. Melakukan penilaian kontrol keamanan dengan menggunakan prosedur penilaian yang tepat untuk menentukan sejauh mana kontrol keamanan diterapkan secara benar, beroperasi sesuai dengan yang dimaksud dan menghasilkan *outcome* yang diharapkan dengan memenuhi persyaratan keamanan bagi sistem. Dalam tahapan ini kita menentukan kontrol-kontrol keamanan yang diterapkan untuk dinilai berdasarkan assesstment objektif yang ditelah ditetapakan berdasarkan framework NIST SP800-53A, hasilnya berupa status *satisfied* atau *other than satisfied.*

Prosedur penilaian terdiri dari serangkaian tujuan, metode dan objek penilaian. Tujuan penilaian meliputi serangkaian parameter terkait dengan kontrol keamanan tertentu. Penerapan prosedur penilaian terhadap pengendalian keamanan menghasilkan temuan penilaian. Temuan penilaian selanjutnya digunakan dalam membantu untuk menentukan efektifitas kontrol keamanan.

5. HASIL PENGUJIAN

Berdasarkan hasil pengujian yang dilakukan terhadap kontrol keamanan yang digunakan pada sistem informasi PT X, dapat dilihat pada tabel 2.

Tabel 2 Tabel hasil penilaian terhadap sistem pengamanan sistem informasi

Kelas Kontrol	Jumlah status *Satisfied*	Jumlah status *Other than Satisfied*
Operational controls	34	14
Management controls	9	11
Technical controls	40	38

Sumber : Hasil pengolahan data

Pada objek penelitian kelas operational controls, jumlah perolehan satisfy lebih banyak dari other satisfy,ini artinya opertion control sudah baik. Pada management controls, jumlah perolehan satisfy lebih sedikit dari other satisfy,ini artinya opertion control sudah belum baik. Dan pada technical controls jumlah perolehan satisfy hampir sama banyak dari other satisfy,ini artinya opertion control tidak terlalu baik.

Berdasarkan rekapitulasi hasil pengujian terhadap sistem informasi hotel yang dibangun dan dikelola oleh PT X memiliki status *satisfied* tetapi masih banyak parameter kontrol keamanan yang perlu diperbaiki atau ditingkatkan sehingga menghasilkan sistem informasi yang memiliki sistem pengamanan yang lebih baik.

6. SIMPULAN

Berdasarkan hasil pengujian yang telah dilakukan terhadap sistem informasi hotel yang dibangun dan dikelola oleh PT.X, diperoleh beberapa kesimpulan berikut :

1. Pengujian kontrol keamanan yang menggunakan *framework* NIST SP800-53A sangat mengutamakan pemeriksaan terhadap ketersediaan dokumentasi.
2. Secara keseluruhan sistem kontrol keamanan yang dibangun oleh PT. X sudah relatif *satisfied* tetapi masih terdapat banyak item kontrol keamanan yang perlu ditingkatkan.
3. Hasil pengujian yang dilakukan berdasarkan pada *framework* NIST SP800-53A terhadap aspek teknikal dan operasional sistem informasi hotel sudah memperoleh status *satisfied* tetapi masih terdapat beberapa hal yang perlu diperbaiki atau ditingkatkan. Pengujian terhadap aspek manajemen sistem informasi hotel memperoleh status *other than satisfied*, sehingga masih banyak hal yang perlu diperbaiki atau ditingkatkan sistem kontrol keamanannya.

DAFTAR PUSTAKA

Bowen Pauline. *A Guide to NIST Information Security Documents.* NIST U.S. Department of Commerce, 2009

Garfinkel Simson, Schwartz Alan & Spafford Gene. *Practical Unix & Internet Security*, 3rd Edition. O'Reilly & Associates, Inc. Sabastopol California. 2003

ISO/IEC FDIS 27001:2005(E). *Information technology – Security techniques - Information security management systems – Requirements.* ISO. Geneva, 2005

Mell Peter and Grance Tim, *The NIST Definition of Cloud Computing v15.* National Institute of Standards and Technology, Information Technology Laboratory, Gaithersburg , 2009.

Miller Michael. *Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online.* Que Publishing, Indianapolis.2009

Ross Ron, Johnson Arnold, Katzke Stu, Toth Patricia, Stoneburner and Rogers George. *NIST Special Publication 800-53A - Guide for Assessing the Security Controls in Federal Information Systems.* NIST U.S. Department of Commerce, Gaithersburg. 2008

Stoneburner Gary, Goguen Alice and Feringa Alexis. *NIST Special Publication 800-30 - Risk Management Guide for Information Technology Systems.* NIST U.S. Department of Commerce, Gaithersburg. 2002.

Whilsher Richard. *FISMA & ISMS alignment opportunities v1.0*. *Zygma* partnership LLC, 2006