

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari analisis dan evaluasi yang telah dilakukan penulis atas tata kelola TI PT Widautama Semarang menggunakan framework COBIT 5 domain Deliver, Support, and Service, dapat disimpulkan *capability level* untuk tiap sub – domain atau proses. Pada proses DSS01 *manage operation*, tata kelola dan manajemen TI perusahaan mencapai level 1 (*performed process*), karena perusahaan telah menjadwalkan aktivitas operasional TI yang dibutuhkan perusahaan dan mulai mengelolanya. Pada proses DSS02 *manage service request and incidents* tata kelola dan manajemen TI perusahaan berada pada level 2 (*managed process*), karena perusahaan telah memastikan bahwa insiden TI diselesaikan sesuai dengan perjanjian dengan vendor dan dengan waktu yang secepat mungkin, serta telah melaksanakan pengawasan atas layanan TI yang diterima, yaitu dengan melakukan konfirmasi dengan *user* untuk memastikan permasalahan telah selesai dan user dapat beraktivitas kembali sesuai semula. Pada proses berikutnya, yaitu DSS03 *manage problems*, *capability level* tata kelola dan manajemen TI perusahaan berada pada level 1 (*performed process*), yaitu karena perusahaan perusahaan

melakukan pengelolaan masalah TI agar masalah yang sama tidak terjadi kembali. Pada proses DSS04 *manage continuity*, tata kelola dan manajemen TI perusahaan berada pada level 0 (*incomplete process*). PT Widautama belum memiliki BCP secara jelas dan tertulis, serta belum memperhatikan kontinuitas TI perusahaan, hanya fokus pada aktivitas jual – beli perusahaan. Di proses DSS05 *manage security services*, berada pada level 1 (*performed process*). Perusahaan telah melakukan usaha – usaha untuk menjaga keamanan layanan TI, kontrol informasi, dan memberikan hak akses yang terbatas terhadap data dan informasi perusahaan sesuai dengan peran dan tanggungjawab. Pada proses yang terakhir, yaitu DSS06 *manage business process controls*, tata kelola dan manajemen TI perusahaan ada di level 1 (*performed process*), karena perusahaan telah melaksanakan pengelolaan proses bisnis, namun belum melakukan pengelolaan atas proses tersebut secara lebih lanjut.

Secara keseluruhan, pada domain DSS ini PT Widautama Semarang mencapai *capability level 1 (performed process)*. Level ini berdasarkan pengelolaan TI perusahaan yang masih minim dan dilaksanakan ketika diperlukan saja tanpa pengelolaan dan evaluasi secara berkala terhadap TI yang ada dan pengelolaan keamanannya.

Kelemahan tata kelola dan manajemen TI PT Widautama Semarang dari hasil wawancara dan observasi penulis berdasarkan COBIT 5 domain DSS, antara lain :

- 1) Perusahaan masih kurang memperhatikan letak perangkat keras TI yang dimiliki.
- 2) Perusahaan tidak melakukan peninjauan atas permasalahan TI secara berkala.
- 3) Ketika terjadi permasalahan TI yang memerlukan keputusan bersama, permasalahan TI ini dibicarakan dalam rapat, namun isi dan hasil pembicaraan selama rapat tidak didokumentasikan dengan baik.
- 4) Pelatihan yang diberikan kepada karyawan perusahaan belum menyeluruh, hanya pelatihan untuk penggunaan software SAP B1 saja, belum ada pelatihan untuk pemahaman mengenai software – software berbahaya, pentingnya menjaga perangkat keras, serta tindakan yang perlu dilakukan jika terjadi eror atau adanya serangan *virus* ke sistem komputer. Pelatihan yang terprogram dan terjadwal untuk keseluruhan aktivitas perusahaan belum direncanakan.
- 5) Perusahaan belum terlalu memperhatikan pengelolaan TI, hanya aktivitas jual beli saja.

- 6) Perusahaan tidak memiliki catatan atas insiden – insiden TI yang terjadi, gejala, progress, solusi, penerapan solusi, serta hasil akhir ketika insiden TI selesai.
- 7) Meskipun perusahaan memiliki log data dan informasi di software SAP B1, tetapi *log data* dan informasi ini masih jarang dicek oleh perusahaan.
- 8) Perusahaan belum mengarsip seluruh permintaan layanan yang dikirimkan ke *vendor* serta jawaban atau solusi dan tip dari *vendor* yang dikirim melalui *email*.
- 9) Perusahaan belum memiliki rencana yang perlu dilakukan ketika terjadi bencana yang dapat merusak perangkat TI dan hilangnya informasi perusahaan.
- 10) Perusahaan belum memperhatikan keamanan informasi perusahaan selain memberikan batas – batas hak akses berdasarkan peran, tanggungjawab, dan jabatan.
- 11) Perusahaan belum menyadari pentingnya memiliki business continuity plan untuk keberlangsungan dan kemajuan perusahaan.

5.2 Saran

Dari hasil evaluasi yang telah disebutkan diatas, maka peneliti memberikan beberapa saran untuk PT Widautama Semarang sebagai upaya memperbaiki dan meningkatkan tata kelola dan manajemen TI perusahaan, yaitu :

5.2.1 Saran berdasarkan DSS01 *Manage Operation* :

- 1) Perusahaan perlu lebih memperhatikan letak perangkat keras TI. Server diletakkan di ruang khusus yang terkunci dan bebas dari berbagai bencana, misalnya banjir, kebakaran, dan gempa bumi. Kunci ruang server diberikan kepada orang – orang tertentu agar akses terhadap server terbatas dan keamanan informasi serta data perusahaan lebih terlindungi.
- 2) Perusahaan perlu melakukan analisis perubahan lingkungan, agar jika ada perubahan lingkungan yang dapat menimbulkan resiko bagi perangkat keras TI, perangkat keras TI dapat dipindahkan ke lokasi yang lebih aman.
- 3) Perusahaan merekrut seorang ahli TI agar dapat menangani permasalahan TI yang terjadi dalam perusahaan dan jika terjadi suatu masalah TI di perusahaan, pihak perusahaan tidak

tergantung pada bantuan dari vendor dan dapat mengatasinya sendiri.

- 4) Memberikan pelatihan dan pengertian kepada seluruh karyawan perusahaan untuk penggunaan dan perawatan perangkat keras dan lunak milik perusahaan agar perangkat yang digunakan tidak mudah rusak dan tidak digunakan secara sembarangan. Pelatihan untuk memberikan pemahaman kepada seluruh karyawan mengenai tugas dan tanggungjawab masing – masing juga perlu diberikan secara terprogram dan terjadwal.
- 5) Membersihkan permukaan perangkat keras komputer dan server secara rutin dan lebih sering, misalnya seminggu sekali, karena perangkat keras ini terkena langsung debu dari udara luar dan produk – produk milik perusahaan sehingga cepat kotor. Untuk membersihkan bagian dalam dari perangkat keras TI, dapat ditambahkan frekuensinya dari 6 bulan sekali menjadi 4 bulan sekali.
- 6) Mencatat jadwal – jadwal penting terkait aktivitas TI agar tidak lupa untuk dilaksanakan.
- 7) Lebih sering melakukan pengecekan terhadap daya simpan server agar server tidak *overload* dan *down*.

5.2.2 Saran berdasarkan DSS02 *Manage Service Requests and Incidents*

- 1) Perusahaan perlu melakukan pengkomunikasian kepada seluruh *user* TI perusahaan atas solusi dan tip yang diterima dari konsultan, agar solusi tersebut dapat menjadi panduan perusahaan dalam meminimalisir kesalahan terutama kesalahan pencatatan dalam software SAP B1.
- 2) Perusahaan perlu melakukan pencatatan atas seluruh insiden TI yang terjadi agar kejadian yang sama dapat dicegah tidak terjadi kembali.
- 3) Perusahaan perlu melakukan klasifikasi layanan berdasarkan tipe dan kategori insiden TI diperlukan untuk mempermudah perusahaan dalam meminta layanan baik kepada *vendor* maupun teknisi *freelancer* dan mempersingkat waktu yang dibutuhkan untuk melakukan perbaikan atau penerapan solusi atas masalah TI yang terjadi.

5.2.3 Saran berdasarkan DSS03 *Manage Problems* :

- 1) Perusahaan perlu membuat manajemen untuk mengatasi masalah darurat TI.
- 2) Permasalahan terkait TI yang dibahas dalam rapat perlu dicatat dan diarsip.
- 3) Mencatat insiden TI yang terjadi lengkap beserta progres dan solusinya.

5.2.4 Saran berdasarkan DSS04 *Manage Continuity*

- 1) Membuat *Business Continuity Plan* berisi dengan tindakan – tindakan yang perlu dilakukan untuk menjaga kontinuitas bisnis dan TI perusahaan ketika terjadi bencana yang dapat menyebabkan hilangnya aset informasi perusahaan dan rencana untuk mengembangkan TI perusahaan, misalnya menambah server untuk beberapa tahun kedepan. Perbaikan atas BCP ini juga perlu untuk terus dilakukan.
- 2) Penilaian terhadap kemungkinan ancaman ini dapat membantu perusahaan untuk mengetahui ancaman – ancaman yang mungkin terjadi dan menentukan tindakan yang dapat meminimalisir terjadinya ancaman.

- 3) Pemberian tanggungjawab kepada seorang karyawan lain untuk menghubungi *vendor* maupun teknisi *freelancer*, namun karyawan ini hanya boleh menghubungi *vendor* maupun teknisi jika Manager Operasional dan Direktur Operasional tidak dapat dihubungi.

5.2.5 Saran berdasarkan DSS05 *Manage Security Services*

- 1) Manajemen perusahaan perlu memberikan pelatihan dan sosialisasi kepada seluruh karyawan untuk meningkatkan pemahaman seluruh karyawan terhadap keamanan TI dan *software* yang berbahaya agar tidak diakses oleh karyawan.
- 2) Melakukan peninjauan ancaman potensial secara berkala.
- 3) Mengalokasikan beberapa penanggungjawab pengelola keamanan untuk melakukan *scanning* sistem komputer secara berkala untuk memastikan bahwa sistem komputer telah aman.
- 4) Mengalokasikan sumberdaya yang diperlukan untuk pengelolaan keamanan ini misalnya, penanggungjawab pengelola keamanan dan jika dimungkinkan, perusahaan dapat membeli *anti – virus* agar memperoleh perlindungan maksimal

dari virus dan mengalokasikan tanggungjawab pengelolaan keamanan kepada beberapa karyawannya.

5.2.6 Saran berdasarkan DSS06 *Manage Business Process Controls*

- 1) Meninjau ulang *log data* dan akses informasi perusahaan untuk meminimalisir terjadinya kecurangan dan akses yang tidak sah terhadap informasi perusahaan.
- 2) Mengarsip secara teratur tindakan korektif dan solusi yang selama ini diterima dari vendor.

5.3 Kelemahan Penelitian

Kelemahan dalam penelitian ini yaitu dilakukan dengan wawancara dan observasi yang memiliki sifat subyektivitas. Untuk meminimalisir subyektivitas ini, peneliti melakukan *cross check* dengan pihak terkait dan wawancara dilakukan dengan lebih dari satu narasumber.