BAB 5. SIMPULAN DAN SARAN

5.1 Simpulan

Dari penilaian dilakukan pada Departemen TI Maranatha, maka diperoleh kesimpulan sebagai berikut:

1. Departemen TI Maranatha belum pernah melakukan evaluasi untuk menilai aset informasi yang sifatnya kritikal serta ancaman dan risiko yang mungkin terjadi.
2. Departemen TI Maranatha belum pernah membuat perencanaan pengurangan risiko untuk mengurangi risiko-risiko yang mungkin terjadi.
3. *OCTAVE Allegro* merupakan suatu evaluasi risiko keamanan informasi yang sifatnya *self-directed* yang memungkinkan perusahaan untuk membuat keputusan dalam perlindungan informasi berdasarkan risiko terhadap *confidentiality, integrity,* dan *availability* dari aset informasi kritikal.
4. Untuk membuat keputusan perlindungan informasi yang paling terbaik, sangat penting untuk mengidentifikasikan ancaman atas aset kritikal. Secara kolektif, semua sumber dari ancaman didokumentasikan dalam *threat profile*. *Threat profile* dapat digunakan untuk mengidentifikasikan serangkaian *threat* terhadap setiap *critical asset*. Jika perusahaan mengerti akan ancaman terhadap aset kritikal, maka langkah selanjutnya akan sangat mudah untuk mengerti risiko terhadap perusahaan dan melakukan langkah-langkah untuk pengurangan risiko terhadap aset informasi kritikal tersebut.
5. Hasil yang telah didapat dari serangkaian langkah yang telah dikerjakan pada penilaian risiko di Departemen TI Maranatha adalah:
   a. Pada Langkah 1 – Membangun Kriteria Pengukuran Risiko: Pertama tentukan terlebih dahulu *impact area* dari Departemen TI Maranatha. *Impact area* yang dipilih yaitu Reputasi dan kepercayaan pelanggan, Finansial, Produktivitas, Keamanan dan kesehatan, serta Denda dan penalti. Kemudian pada masing-masing *impact area* ini, diberikan

penilaian kondisi seperti apakah *impact area* tersebut dikategorikan *low, medium,* dan *high*. Selain itu, pada masing-masing *impact area* diberikan skala prioritas, Reputasi dan kepercayaan pelanggan terjaga atau meningkat, apabila terjadi peningkatan kepercayaan maka *customer* akan menyebarkannya dari mulut kemulut sehingga makin membuka peluang untuk lebih banyak lagi user/pelanggan yang akan melakukan pendaftaran sebagai pelanggan baru yang masuk sebagai pengguna layanan dari Departemen TI Maranatha.

b. Pada Langkah 2 – Mengembangkan *Information Asset Profile*: Langkah awal yang harus dilakukan terlebih dahulu yaitu menentukan aset informasi apa saja yang kritikal bagi Departemen TI Maranatha, *assessment* dilakukan dengan terfokus pada *core process* dari Departemen TI Maranatha itu sendiri. Tahap awal aset-aset penting didefinisikan bersama dengan pimpinan dari Departemen TI Maranatha atau staff yang memiliki wewenang terhadap aset informasi tersebut. Dari kumpulan aset penting tersebut, aset informasi kritikal yang berhasil teridentifikasi dalam laporan ini adalah; Profil user/pelanggan, profil data komplain user, aset *hardware*, dan aset *software*.
c. Pada Langkah 3 – Mengidentifikasi *Information Asset Containers*: *Information asset containers* dimana aset informasi kritikal Departemen TI Maranatha tersebut disimpan, dipindahkan, atau diproses. Setelah mengetahui lokasi dari aset informasi tersebut kemudian lakukan identifikasi dengan membagi *container* dalam kategori *technical, physical,* dan *people.*
d. Pada Langkah 4 – Mengidentifikasi *Area of concern*: Tahap awal *Area of concern* diidentifikasikan dengan melihat *container* yang telah diidentifikasi pada pembahasan dalam langkah sebelumnya.
e. Pada Langkah 5 – Mengidentifikasi *Threat Scenarios*: *Area of concern* diperluas menjadi *threat scenario* yeng lebih mendetail mengenai *property* dari *threat.*

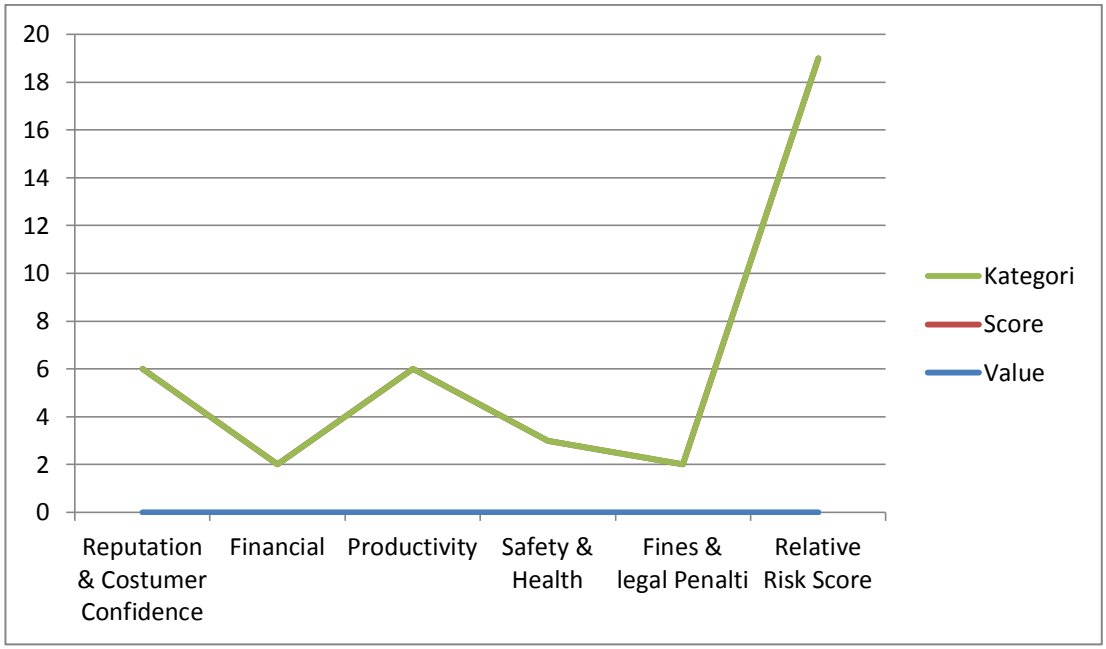
f. Pada Langkah 6 – Mengidentifikasikan Risiko: Pada tahap ini ditujukan untuk menentukan bagaimana *threat scenario* yang telah dicatat, apakah akan memberikan dampak bagi perusahaan?.
g. Pada Langkah 7 – Analisis Risiko: Pada tahap ini, perlunya pengukuran secara kualitatif dilakukan dengan menghitung *score* untuk setiap risiko pada *information asset* yang ada saat ini.
h. Pada Langkah 8 – Pemilihan *Mitigation Approach*: Pada tahap ini, perusahaan dituntut untuk menentukan tindakan-tindakan yang dapat dilakukan untuk memitigasikan setiap risiko.

5.2 Saran

Saran yang dapat diusulkan oleh Auditor dalam penelitian ini, yaitu:

1. perusahaan Departemen TI Maranatha dapat membuat peraturan tertulis mengenai semua tanggung jawab dalam menjaga keamanan informasi dan sanksi keras bagi siapapun yang melanggar serta melakukan sosialisasi terhadap peraturan tersebut secara bertahap semua karyawan Departemen TI Maranatha.
2. Departemen TI Maranatha dapat membuat simulasi secara visual untuk memudahkan karyawan untuk mengerti akan pentingnya aset informasi, siap untuk menghadapi ancaman dan risiko yang mungkin terjadi, serta konsekuensi yang harus mereka hadapi bila terjadi.
3. Departemen TI Maranatha dapat melakukan evaluasi kembali terhadap keamanan informasi dengan menggunakan metode *OCTAVEAllegro* yang mana telah dibahas secara detail dalam laporan ini. Terutama tahapan yang paling penting yang harus diperhatikan yaitu pada Langkah 7 – Analisis Risiko, jika pada Langkah 7 diperhatikan dan diantisipasi maka akan membantu perusahaan untuk memutuskan strategi terbaik dalam menghadapi Risiko yang akan muncul.

   Contohnya: Analisa Risiko – *Hardware* (hal 112), berikut ini merupakan simulasi diagram dari tabel 4.12-4:



Gambar 5.2.1 Grafik Analisis Risiko - *Hadware*

4. Penelitian berikutnya, diharapkan supaya ruang lingkup yang akan dibahas jangkauannya lebih diperluas, misalnya yang dibahas tentang keseluruhan aset-aset yang dimiliki Universitas Kristen .Maranatha, dan bagaimana cara untuk melindungi aset informasi yang ada agar tetap terjaga keamanannya.