BAB V
KESIMPULAN DAN SARAN

1.1 Kesimpulan

Setelah melakukan analisis manajemen risiko berdasarkan ISO 31000 yang dilakukan dengan tahapan komunikasi dan konsultasi, menentukan konteks, mengidentifikasi risiko, analisis risiko, evaluasi risiko, evaluasi risiko, penanganan risiko, serta riviu dan pemantauan dapat disimpulkan bahwa terdapat 60 kemungkinan risiko yang dapat terjadi di Unit Laboratorium Fakultas Ilmu Terapan Telkom University. Dari ke-60 kemungkinan risiko tersebut, 9 atau 15 % kemungkinan risiko memiliki level risiko *high*, 50 atau 83,33% kemungkinan risiko berlevel *medium*, dan 1 atau 1,67% kemungkinan risiko berlevel *low*.

9 kemungkinan risiko yang memiliki level *high* antara lain adalah pandemi, kesalahan dalam mempekerjakan staff, data tidak terintegrasi, penggunaan *flashdisk*, *network failure*, data tidak terenkripsi dengan baik, proses transmisi data yang lambat, kemungkinan *hardware* rusak karena serangan rayap, dan kemungkinan jaringan kabel putus karena serangan tikus.

Sedangkan 50 risiko dengan level *medium*, yaitu gempa bumi, banjir, petir, kebakaran, listrik padam, debu atau kotoran, pergantian staff, *human error*, pencurian perangkat, penyalahgunaan hak akses, kesalahan input data, kualitas SDM, kurangnya jumlah staff, tidak sesuai SOP, pembatasan akses, pembaruan kebijakan, kesalahan dalam melakukan penanganan insiden atau pemenuhan layanan TI, kurangnya pengetahuan mengenai pekerjaan yang ditempuh, manipulasi data, terlalu lambat dalam menangani risiko, staff tidak masuk atau sakit, kesalahan konfigurasi, migrasi data, tidak ada *maintenance, SQL Injection, virus ,worms, trojan*, pencurian data, *backup data failure*, sistem tidak berfungsi, *overheat, overload*, kehilangan data, *data corruption, malware, bug*, kurang berfungsinya secara maksimal fungsi dari *firewall, server down*, *maintenance* tidak terjadwal dengan baik, teknologi tidak ter*update, k*oneksi jaringan tidak stabil, kerusakan pada *software*, kerusakan pada *hardware*, serangan *cyber*, *user interface* sulit dipahami, Ddos, lisensi *software*, kesalahan instalasi, dan *memory*

penyimpanan terlalu kecil. Sisanya adalah 1 kemungkinan yang berlevel *low*, yaitu pembagian *bandwidth*.

1.2 Saran

Untuk meminimalisir kemungkinan risiko yang dapat terjadi pihak Unit Laboratorium harus segera menerapkan manajemen risiko agar aktivitas yang berjalan tidak mengalami hambatan atau gangguan, serta tidak banyak mengalami kerugian. Disarankan agar Unit Laboratorium membuat SOP atau *Standard Operational Procedure* yang berhubungan dengan manajemen risiko teknologi dan sistem informasi sebagai bentuk acuan untuk melakukan manajemen risiko. SOP dibuat dengan cara didokumentasikan, lalu disebar luaskan kepada pengguna Unit Laboratorium dengan dara melakukan sosialisai. Dengan mengimplementasikan solusi dan melanjutkannya ke tahap *monitoring* dan *review* diharapkan dapat membantu Unit Laboratiurium menghasilkan strategi penanganan risiko di kemudian hari.