BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan evaluasi pengukuran tingkat kapabilitas yang dilakukan pada DISKOMINFO Kabupaten Sampang, terdapat beberapa kesimpulan yang telah didapat. Pengukuran tingkat kapabilitas yang dilakukan dengan kerangka kerja COBIT 5 dan berfokus pada tiga proses, yaitu APO12 Mengelola Risiko, APO13 Mengelola Keamanan, dan DSS05 Mengelola Layanan Keamanan.

Proses APO12 – Mengelola Risiko mencapai tingkat kapabilitas level 1 (*Performed Process*) dengan nilai sebesar **40,34%** dan berada pada kategori **P** (***Partially Achieved***) Untuk proses APO13 – Mengelola Keamanan mencapai tingkat kapabilitas level 1 (Performed Process) dengan nilai sebesar **84,60%** dan berada pada kategori **L (*Largely Achieved).*** Kemudian untuk proses DSS05 – Mengelola Layanan Keamanan mencapai tingkat kapabilitas level 1 *(Performed Process*) dengan nilai sebesar **57,23%** dan berada pada kategori **L (*Largely Achieved).***

Dengan hasil demikian, diperoleh kesenjangan (*gap*) **2 tingkatan** dari hasil yang diharapkan (level 3) untuk masing-masing proses yang diteliti. Maka dari itu untuk mencapai level 3 (*Esthablised Process*) yang diharapkan, Dinas Komunikasi dan Informatika Kabupaten Sampang harus melakukan perbaikan atau melaksanakan saran rekomendasi yang telah disusun oleh penulis.

Berdasarkan temuan yang sering muncul dalam evaluasi keamanan informasi di DISKOMINFO Sampang menggunakan COBIT 5, terdapat beberapa rekomendasi penting untuk tiga domain utama. Pada domain APO12 (*Manage Risk*), disarankan agar organisasi menyusun SOP dan *template* dokumentasi risiko, melakukan evaluasi risiko secara berkala, menerapkan analisis *cost-benefit*, menyampaikan hasil evaluasi secara tertulis, serta menetapkan *Key Risk Indicators* (KRI). Untuk domain APO13 (*Manage Security*), rekomendasi utamanya adalah menyusun SOP dan jadwal implementasi keamanan informasi, membuat daftar kontrol keamanan secara formal, meningkatkan pelatihan dan audit internal,

menyusun *Risk Treatment Plan* secara detail, serta menetapkan indikator kinerja keamanan seperti jumlah insiden tertangani. Sedangkan pada domain DSS05 (*Manage Security Services*), perlu dilakukan pengelolaan antivirus secara terpusat, penetapan kebijakan keamanan jaringan dan enkripsi, penerapan enkripsi pada data yang disimpan maupun ditransmisikan, pengintegrasian audit *log* dan SOP insiden, serta penetapan aturan penggunaan perangkat pribadi untuk keamanan layanan TI. Rekomendasi ini diharapkan dapat meningkatkan kapabilitas keamanan informasi dan mendukung pencapaian tujuan bisnis organisasi.

5.2 Saran Pengembangan

Adapun saran yang dapat diberikan untuk penelitian selanjutnya sebagai berikut.

1. Penelitian selanjutnya diharapkan dapat menyusun produk kerja yang masih belum terpenuhi bahkan yang tidak ada untuk membantu pencapaian tingkat kapabilitas yang diharapkan oleh instansi.
2. Melakukan evaluasi dengan *stakeholder needs "is the information I am processing wells secured?"* sesuai dengan kerangka kerja COBIT 5 yang tidak hanya berfokus pada manajemen keamanan informasi, sehingga lebih banyak proses yang dapat diukur dengan fokus proses yang berbeda.
3. Penelitian selanjutnya dapat berupa pengembangan sistem informasi berbasis aplikasi untuk membantu proses *monitoring*, pencatatan insiden, dan audit keamanan informasi secara berkala dan otomatis.