

BAB V

PENUTUP

5.1 Kesimpulan

Penelitian ini bertujuan untuk mengevaluasi lalu mengimplementasikan domain APO12 (*Managed Risk*), APO13 (*Managed Security*), dan DSS05 (*Managed Security Services*) pada COBIT 2019, guna meningkatkan keamanan sistem informasi di LAZIS Sabilillah Malang. Berdasarkan hasil pengisian kuesioner dan wawancara terhadap empat narasumber, ditemukan bahwa sebagian besar proses yang berhubungan dengan *risk management* dan keamanan informasi masih berada di tingkat kapabilitas dan kematangan yang relatif rendah.

Dari hasil analisis capability level, hanya sub-domain DSS05 yang telah mencapai level 4, sementara APO12 dan APO13 berada pada level 2. Dalam hal maturity level, DSS05 berada pada level 3 (*Defined*), APO12 pada level 2 (*Managed*), dan APO13 masih pada level 1 (*Initial*). Hal ini menunjukkan bahwa pengelolaan keamanan informasi di LAZIS Sabilillah masih belum optimal dan perlu adanya peningkatan secara bertahap dan berkelanjutan.

Sebagai luaran dari penelitian ini, peneliti merumuskan serangkaian *Standard Operating Procedures* (SOP) yang ditujukan untuk mendukung perbaikan dan peningkatan keamanan sistem informasi. SOP disusun berdasarkan identifikasi aktivitas proses yang mendesak (*urgent*) dan memungkinkan (*possible*) untuk diterapkan segera. Implementasi SOP diharapkan dapat membantu organisasi dalam mengurangi gap antara kondisi aktual dengan kondisi ideal sesuai dengan standar COBIT 2019.

5.2 Saran

1. Implementasi Bertahap SOP: Disarankan agar LAZIS Sabilillah segera menerapkan SOP pada sub-domain yang bersifat *urgent*, seperti DSS05.04 dan DSS05.05, dengan memastikan kesiapan SDM dan infrastruktur.

2. Evaluasi Berkala *Maturity* dan *Capability Level*: Organisasi perlu melakukan evaluasi minimal setiap tahun terhadap proses APO12, APO13, dan DSS05 untuk memantau peningkatan *maturity* dan *capability level*.
3. Peningkatan Literasi Keamanan Informasi: Pelatihan internal secara rutin bagi seluruh staf sangat penting untuk menumbuhkan kesadaran dan pemahaman akan pentingnya keamanan informasi.
4. Penetapan Tim Keamanan Informasi: LAZIS Sabilillah disarankan membentuk tim khusus yang bertanggung jawab untuk merancang, menjalankan, dan mengevaluasi kebijakan serta prosedur keamanan TI.
5. Kolaborasi dengan Pihak Ketiga: Dalam beberapa aspek teknis seperti pemantauan infrastruktur atau audit eksternal, organisasi dapat menggandeng mitra profesional atau konsultan TI untuk memastikan objektivitas dan efisiensi pelaksanaan.

Dengan menerapkan saran-saran ini, diharapkan LAZIS Sabilillah dapat membangun sistem keamanan informasi yang andal, terukur, dan berkelanjutan, serta menjadi contoh praktik tata kelola keamanan TI yang baik di sektor filantropi.