BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian yang dilakukan untuk penilaian kapabilitas tata kelola keamanan IT di PT Omni Digitama Internusa (Ruparupa) dengan mengimplementasikan kerangka kerja COBIT 5, maka dapat diambil kesimpulan sebagai berikut:

1. Level kapabilitas (*capability level*) tata kelola keamanan IT di PT Omni Digitama Internusa (Ruparupa) saat ini berada di level 1 (*performed process*) untuk proses APO12 (*Manage Risk*), APO13 (*Manage Security*) dan DSS05 (*Manage Security Services*). PT Omni Digitama Internusa (Ruparupa) tidak mencapai target level yang diinginkan, yaitu di level 3 (*Establish Process*) dengan jumlah *gap* sebesar 2.
2. Hasil wawancara dan observasi menunjukkan bahwa PT Omni Digitama Internusa (Ruparupa) belum memiliki tim khusus dan terpisah untuk menangani masalah keamanan dan resiko IT perusahaan, sehingga untuk saat ini seluruh hal yang berkaitan dengan resiko dan IT perusahaan ditangani langsung oleh divisi *technology and system infrastructure*.
3. Rekomendasi yang diberikan kepada PT Omni Digitama Internusa (Ruparupa) sebagian besar berkaitan dengan dokumentasi dikarenakan perusahaan belum melakukan atau tidak memiliki

dokumentasi yang cukup *proper* dalam pengelolaan keamanan IT dan dokumen yang sudah ada sebelumnya belum dikumpulkan dalam sebuah wadah untuk mengumpulkan seluruh dokumentasi agar menjadi terpusat dan dapat diakses jika dibutuhkan.

5.2 Saran

Berdasarkan hasil penelitian yang dilakukan di PT Omni Digitama Internusa (Ruparupa), maka terdapat beberapa saran yang diberikan terkait dengan pengelolaan keamanan IT di perusahaan kedepannya, yaitu:

1. Melaksanakan rekomendasi-rekomendasi yang telah diberikan terkait pengelolaan keamanan IT perusahaan secara bertahap agar dapat mencapai target level yang diharapkan sesegera mungkin.
2. Membentuk sebuah tim terpisah yang secara khusus melaksanakan tugas-tugas yang berkaitan dengan masalah pengelolaan resiko dan keamanan IT di perusahaan.
3. Membuat dan melengkapi dokumen-dokumen yang diperlukan untuk penanganan resiko dan keamanan IT di perusahaan dan mengumpulkan semua dokumentasi tersebut kedalam sebuah *platform* yang terpusat.
4. Menentukan sebuah standar atau kerangka kerja baku untuk mengelola resiko dan keamanan IT di perusahaan, salah satunya COBIT 5 *framework* yang dapat dijadikan sebagai bahan pertimbangan.

5. Mengimplementasikan proses EDM01-*Ensure Governance Framework Setting* dan EDM03-*Ensure Risk Optimization* untuk proses *monitoring* tata Kelola resiko keamanan dan memastikan optimisasi pengendalian resiko dan keamanan di perusahaan di masa mendatang.

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA