BAB 4
SIMPULAN DAN SARAN

4.1 Simpulan

Setelah melakukan analisis dan perhitungan tingkat kematangan berdasarkan kontrol objektif ISO 27001:2013, maka dapat disimpulkan bahwa tingkat kematangan keamanan informasi divisi TIK Politeknik Pos Indonesia berada pada level sebagai berikut:

Tabel 4-1 Penilaian Tingkat Kematangan (Maturity Level)

No	Klausul	Nilai	Tingkat Kematangan
1	*A.5 Information Security Policies*	2	2 - AKTIF
2	*A.6 Organization of Information Security*	2	2 - AKTIF
3	*A.7 Human Resources Security*	2,67	2 - AKTIF
4	*A.8 Asset Management*	2,2	2 - AKTIF
5	*A.9 Access Control*	2,35	2 - AKTIF

Berdasarkan hasil penilaian diatas, diketahui bahwa tingkat kematangan divisi TIK Politeknik Pos Indonesia secara umum berada pada level 2 (AKTIF), terlihat dari hasil penilaian pada 5 klausul yang digunakan yaitu Annex 5, 6, 7, 8, dan 9. Dan hasil pengukuran kelengkapan dan kematangan keamanan informasi masih belum sesuai dengan standar yang ditetapkan oleh Diskominfo yaitu pada level 3 dengan status PRO-AKTIF. Penjelasan mengenai penilaian tersebut dipaparkan sebagai berikut:

1. Penilaian terkait dengan klausul Annex 5 – *Information Security Policies.*

   Sudah ada pengakuan atas kebutuhan terkait dengan sistem manajemen keamanan informasi. Berbagai kegiatan operasional yang dilakukan oleh divisi TIK Politeknik Pos Indonesia terkait dengan manajemen keamanan informasi belum terdokumentasi dengan baik dan belum memenuhi kebutuhan organisasi karena ditentukan melalui kebijakan internal (legalisasi kepala divisi) yang dihasilkan tanpa dukungan pihak manajemen level atas.

2. Penilaian terkait dengan klausul Annex 6 – *Organization of Information Security*.

   Untuk bagian pertama mengenai *internal organization*, tujuannya adalah untuk membangun kerangka kerja untuk memulai dan mengontrol pelaksanaan operasional keamanan informasi dalam organisasi. Berdasarkan hasil analisis yang dilakukan, pihak divisi TIK sudah cukup *aware* terhadap bagian tersebut. Sebagai contoh, sudah ada pembagian tanggung jawab kerja walaupun belum diimplementasikan dengan efektif.

   Bagian kedua, membahas mengenai *mobile devices and teleworking*. Divisi TIK sudah memiliki kesadaran akan kebutuhan kebijakan *mobile devices*, hal tersebut terlihat dari upaya penyusunan kebijakan terkait perangkat *mobile*. Sedangkan kebijakan *teleworking*, sama sekali belum ditentukan karena memang tidak pernah dilakukan aktivitas *teleworking* tersebut, karena dianggap cenderung berpotensi besar untuk menghasilkan risiko terkait keamanan informasi, misalnya pencurian data yang tersimpan di *cloud*.

3. Penilaian terkait dengan klausul Annex 7 – *Human Resource Security*

   Berdasarkan hasil analisis yang dilakukan penulis, divisi TIK dirasa sudah cukup baik terkait klausul Annex 7 ini. Hal ini terlihat dari penerapan kebijakan dan prosedur yang sudah ditentukan, diterapkan secara konsisten, didokumentasikan dengan baik, dan ditinjau secara berkala. Misalnya, kebijakan dan prosedur mulai dari tahap awal perekrutan pegawai, selama masa kerja dan juga aturan untuk *resign* sudah merujuk berdasarkan *risk analysis*. Yang menjadi masalah sehingga perlu mendapat perhatian adalah kontrol *disciplinary process*, tidak ada kebijakan yang ditetapkan terkait kontrol tersebut. Intensitas pelanggaran yang jarang terjadi serta jenis pelanggaran yang dianggap kecil, mengakibatkan kurangnya pengawasan pihak manajemen untuk mengantisipasi kemungkinan risiko yang mungkin terjadi atas suatu pelanggaran lainnya. Akibatnya hanya ada pengakuan kebutuhan tanpa ada tindak lanjut dari proses pendisiplinan pegawai yang mungkin melakukan pelanggaran.

4. Penilaian terkait dengan klausul Annex 8 – *Asset Management*.

   Kegiatan manajemen aset (pemeliharaan aset, penentuan pemilik aset serta penghancuran aset yang tidak digunakan) dilakukan dengan koordinasi antara divisi TIK dan divisi inventaris aset (bagian inventaris aset YPBPI), namun secara dominan tanggung jawab terhadap aset lebih dilimpahkan kepada divisi TIK. Berdasarkan hasil analisis yang dilakukan, manajemen aset terkait pengolahan informasi sudah diterapkan cukup baik walaupun belum optimal, sebagai contoh : manajemen penghancuran/pembuangan pirati yang sudah tidak terpakai, dan pengelolaan PC yang tidak terawat dengan baik *(dapat dilihat pada Lampiran B – Bukti Foto nomor 6-7)*. Untuk pemetaan tanggung jawab aset dan identifikasi pemilik aset sudah sesuai dengan kebutuhan organisasi *(dapat dilihat pada lampiran B – Bukti Foto nomor 3)*.

5. Penilaian terkait dengan klausul Annex 9 – *Access Control*.

   Pembatasan akses terhadap informasi internal sudah dikontrol dengan menggunakan SSO (Single Sign On). Hak akses juga sudah diklasifikasikan berdasarkan tanggung jawab kerja dan klasifikasi jenis informasi. Aturan penggantian *password* juga sudah dilakukan secara berkala, yaitu setiap 6 bulan sekali dengan kriteria *password* terdiri dari kombinasi *alphanumeric*. Namun belum ada kebijakan khusus untuk kontrol *access to network and netrok services*, misalnya pemblokiran terhadap situs-situs yang mengandung konten pornografi, karenanya nilai *maturity* bernilai 0. Begitupun untuk kontrol *review of user access rights, removal or adjustment of access right,* dan *use of provoleged utility programs* yang bernilai 1, harusnya dilengkapi dengan adanya prosedur yang jelas serta terdokumentasi serta diterapkan secara konsisten untuk meningkatkan keamanan informasi bukan sekedar pengakuan kebutuhan akan kebijakan terkait kontrol-kontrol tersebut.

4.2 Saran

Beberapa hal yang direkomendasikan oleh penulis untuk divisi TIK Politeknik Pos Indonesia, yaitu:

1. Lebih sering melaksanakan program-program seperti pelatihan, seminar, dan sosialisasi untuk meningkatkan *awareness* pimpinan dan fungsi kerja yang ada, tentang pentingnya keamanan informasi dalam bentuk aturan maupun penerapannya.
2. Menyusun dan mengembangkan *blueprint* yang dimiliki oleh divisi TIK Politeknik Pos Indonesia yang digunakan untuk pengembangan aplikasi dan infrastruktur secara terencana.
3. Melakukan enskripsi dengan metode tertentu terhadap informasi-informasi yang bersifat vital, agar tidak dapat dimengerti dan tidak dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab.
4. Diberlakukannya tindakan displiner atau sanksi terhadap pelanggaran kebijakan terkait keamanan informasi.
5. Membuat kebijakan untuk pembatasan hak akses terhadap situs yang mengandung pornografi serta melanggar tindakan hukum lainnya.
6. Membuat aturan untuk tidak mengunduh *software* yang melanggar ketentuan lisensi yang ditetapkan oleh divisi TIK Politeknik Pos Indonesia.

Beberapa hal yang disarankan untuk penilitian berikutnya, yaitu:

1. Melakukan analisis kelayakan kebijakan dan prosedur untuk setiap kegiatan operasional yang dilakukan.
2. Menggunakan standar ISO yang sesuai dengan kebutuhan, versi internasional atau adaptasi SNI.
3. Melakukan analisis terhadap seluruh kontol objektif yang tersedia.
4. Melakukan identifikasi risiko yang terjadi pada divisi Politeknik Pos Indonesia, secara khusus dengan melibatkan ISO 27005 - *Risk Management*.