# BAB 4. SIMPULAN DAN SARAN

## 4.1 Simpulan

Simpulan yang dapat diambil dari hasil analisis berdasarkan kontrol area yang diambil dari ISO 27001:2005 yaitu keamanan fisik dan lingkungan, manajemen komunikasi dan operasi dan pengendalian akses yang dibahas pada BAB 3 adalah sebagai berikut:

1. Analisis manajemen keamanan sistem informasi *remittance* di PT Pos Indonesia menggunakan metode ISO27001:2005 dan menggunakan 3 kontrol yaitu keamanan fisik dan lingkungan, manajemen komunikasi dan operasi serta pengendalian akses.
2. PT. Pos Indonesia sudah cukup memahami proses-proses dalam keamanan fisik dan lingkungan, hal tersebut dapat dilihat dari adanya dokumen-dokumen yang membahas keamanan fisik dan lingkungan dan dokumentasi keamanan fisik dan lingkungan sudah disetujui oleh manajemen yang bersangkutan, tapi dalam beberapa penerapannya belum sepenuhnya berjalan dengan baik di seluruh devisi. Dari hasil analisis dapat disimpulkan bahwa GAP kesesuaian antara proses di PT. Pos Indonesia dan proses ISO 27001:2005 mengenai kebijakan keamanan fisik dan lingkungan cukup besar.
3. PT. Pos Indonesia sudah memahami dan mengelola manajemen komunikasi dan operasi. Manajemen sudah mendukung dan sudah memberikan wewenang pada pihak yang bertanggung jawab sesuai dengan peran dan fungsi kerjanya masing-masing. Dokumentasi formal mengenai manajemen komunikasi dan operasi sudah ada di PT. Pos Indonesia namun ada beberapa dokumentasi dan kurangnya kesadaran para pegawai mengenai manajemen komunikasi dan operasi menjadikan kendala PT. Pos Indonesia untuk menjalankan manajemen komunikasi dan operasi dengan benar. Dengan hasil analisis di atas dapat disimpulkan

bahwa GAP kesesuain proses di PT. Pos Indonesia dengan proses ISO 27001:2005 mengenai kebijakan keamanan komunikasi dan operasi cukup kecil sehingga diperlukan perbaikan atau perubahan.

4. PT. Pos Indonesia sudah memahami dan menjalankan pengendalian akses terhadap akses pekerja atau akses pihak ketiga, hal tersebut dapat dilihat dari adanya dokumentasi mengenai pengendalian akses di PT. Pos Indonesia. Namun ada beberapa prosedur atau pengendalian yang belum dikendalikan seperti kerja jarak jauh, *mobile computing* dan komunikasi. Berdasarkan analisis diatas maka dapat disimpulkan bahwa GAP kesesuaian antara proses di PT. Pos Indonesia saat ini dengan proses ISO 27001:2005 masih cukup kecil maka diperlukan perbaikan mengenai kebijakan pengendalian akses.

## 4.2 Saran

Penerapan SMKI (Sistem Manajemen Keamanan Informasi) pada PT. Pos Indonesia dapat mengacu pada persyaratan standarisasi sesuai dengan ketentuan pada SMKI ISO 27001:2005 sebagai implementasinya. Untuk itu aspek keamanan harus memenuhi kriteria CIA (*confidentially, integrity, availability*). Untuk mencapai aspek tersebut maka perlu diperhatikan beberapa hal yang penting yaitu adanya kontrol, *monitoring*, *auditing*, dan pemahaman tentang dampak dan ancaman pada PT. Pos Indonesia. Kontrol pada pokok masalah yang diambil adalah keamanan fisik dan lingkungan, manajemen komunikasi dan operasi dan pengendalian akses. Berikut ini adalah saran dari hasil analisis yang dilakukan pada BAB 3. Referensi penulisan dokumen ISO 27001:2005 dapat dilihat pada lampiran P untuk *Policy*, lampiran U untuk *Procedure*, lampiran V untuk *Work Instruction*, dan lampiran W untuk *Record Schedule*.

1. Pembuatan dokumen SMKI ini bersifat strategis yang memuat komitmen yang dituangkan dalam bentuk kebijakan, standar,

sasaran dan rencana terkait pengembangan (*development*), penerapan (*implementation*), dan peningkatan (*improvement*) sistem manajemen keamanan informasi. Berikut ini adalah dokumen yang sesuai dengan kontrol yang diambil:

A. *Internet Acceptable Usage Policy* (Doc 7.2)
B. *Mallcious Code Policy (Doc 10.11)*
C. *Access Control Policy(Doc 11.1)*
D. *Network Access Policy(Doc 11.7)*

2. Pembuatan prosedur dan panduan ini dikembangkan secara internal oleh PT. Pos Indonesia sebagai penyelenggara publik dan memuat cara menerapkan kebijakan yang telah ditetapkan serta menjelaskan penanggung jawab kegiatan. Dokumen ini bersifat operasional. Berikut ini adalah dokumen yang sesuai dengan kontrol yang diambil :

   A. *External Parties (Doc 6.8)*
   B. *Rules for e-mailusage(doc 7.3)*
   C. *Information Security Classification(Doc 7.6)*
   D. *Telecommunications reqts(Doc 7.11)*
   E. *Physical Entry Controls(Doc 9.8)*
   F. *Equipment Sy(Doc 9.10)*
   G. *Disposals of info eqpt, devices and media(Doc.9.11)*
   H. *Loading and Unloading(Doc 9.9)*
   I. *Off-site Removals Authorisaltions(Doc 9.12)*
   J. *Documenting Operating Procedure(Doc 10.1)*
   K. *Change Control Procedure(Doc 10.7)*
   L. *Separation of operational, test and development environments(Doc 10.8)*
   M. *System Planning and Acceptance(Doc 10.10)*
   N. *Malicious Code Procedure(Doc 10.12)*
   O. *Back-Up(Doc 10.13)*
   P. *Network Management(Doc 10.14)*

Q. *Media Handling(Doc 10.15)*
R. *Business Information Systems(Doc 10.16)*
S. *Monitoring(Doc 10.18)*
T. *E-Commenrce(Doc 10.17)*
U. *User Acess Rights(Doc 11.2)*
V. *User Registration(Doc 11.3)*
W. *Teleworkers Procedure(Doc 11.12)*
X. *Mobile Computing(Doc 11.11)*
Y. *Access Control Procedure(Doc 11.8)*
Z. *Secure Log-On(Doc 11.9)*
AA. *System Utilities(Doc 11.10)*
BB. *Control Of Cryplograpic Keys(Doc 12.2)*

3. Pembuatan dokumen petunjuk teknis, instruksi kerja dan formulir yang digunakan untuk mendukung pelaksanaan prosedur tertentu sampai ke tingkatan teknis. Berikut dokumen yang seduai dengan kontrol yang di ambil :

A. *Fire Doors WI(Doc 9.1)*
B. *Fire Alarms Wi(Doc 9.2)*
C. *Burglar Alarms WI(Doc 9.3)*
D. *Fire Suppression eqpt WI(Doc 9.4)*
E. *Air conditioning WI(Doc 9.5)*
F. *Reception Management WI(Doc 9.6)*
G. *Physycal Perimeter Security Cheklist(Doc 9.7)*
H. *Notebook Configuration WI(Doc 9.13)*
I. *Anti Malware WI(Doc 10.2)*
J. *User Name Admin WI(Doc 10.3)*
K. *Website tems WI(Doc 10.5)*
L. *Privacy statements WI (Doc 10.4)*
M. *Administrator Logging (REC 10.6)*
N. *Audit Logging Schedule(REC 10.6)*
O. *Monitoring Schedule(REC 10.5)*
P. *Teleworks user Agreement(Doc 11.13)*

Q. *User Afreement(Doc 11.4)*

4. Dokumen *Record Schedule* berisi bukti objektif yang menunjukan seberapa baik kegiatan yang dilakukan atau apa hasil benar-benar tercapai. Berikut dokumen yang dapat menjadi acuan:
    *A. Off-Site Removals Request Log(REC 10.1)*
    *B. Disposal Log(REC 9.1)*
    *C. Change Request Log( REC 10.2)*
    *D. Change Request WI(REC 10.3)*
    *E. Teleworker Checklist(REC 11.3)*
    *F. Replacement Passwords(REC 11.1)*
    i. *Deletion Request WI(REC 11.2)*