Berdasarkan hasil penilaian diatas maka penulis merekomendasikan perbaikan pada setiap *activi* kesenjangan (gap) maka harus dilakukan hal – hal sebagai berikut :

1. *Activity* DSS5.1 Melindungi Terhadap *Malware*

a. Melakukan peningkatan keamanan terhadap *malware* yang dapat merusak sistem serta
b. Melakukan peningkatan dan memastikan bahwa semua informasi yang diproses disim

2. *Activity* DSS5.2 Mengelola Keamanan dan Konektivitas

a. Pastikan bahwa pengelolaan keamanan jaringan dan konektivitas sesuai standar yang telah di
b. Gunakan prosedur atau langkah – langkah terbaru untuk menjaga keaman sistem.

3. *Activity* DSS5.3 Mengelola Keamanan *End-Point* (Titik Akhir)

Tingkatkan keamanan titik akhir (*end point*) minimal pada tingkat yang sama atau leb
Selalu pastikan informasi yang diproses, disimpan dan dikirimkan telah disaring dan d

***4. Activity* DSS5.4 Mengelola Identitas dan Akses**

a. Pastikan bahwa semua pengguna sistem memiliki akses informasi sesuai dengan kebu
b. Lakukan filtering terhadap hak akses agar tidak ada *maleware* yang dapat merusak ata

5. *Activity* DSS5.5 Mengelola Akses Fisik Ke Aset TI

a. Tentukan dan terapkan prosedur untuk memberikan akses fisik dengan cara memberi,
b. Lakukan peningkatan pemantauan terhadap akses yang diberikan agar semua *user* yan

6. *Activity* DSS5.6 Mengelola Dokumen Sensitif dan Perangkat *Output* .

a. Lakukan peningkatan pengelolaan dan pemeliharaan dokumen yang bersifat sensitif (*I*
Data tersebut harus dikelola pada slah satu piak pengeloala yang benar – benar bisa m
b. Lakukan penukaran data transaksi sensitif pada jalur media yang benar – benar aman

7. *Activity* DSS5.7 Memantau Infrastruktur Yang Berhubungan dengan Keamanan

a. Lakukan pemantauan infrstruktur keamanan denagn cara menggunakan alat deteksi in
b. Integrasikan peristiwa yang terjadi dengan pemantauan kejadian dan pengelolaan seca

8. *Activity* APO13.1 Menetapkan dan Memelihara ISMS

a. Lakukan peningkatan dalam menetapkan dan memelihara sistem manajemen keamanan infor
mekan pendekatan yang sesuai standar, formal dan berkesinambungan
b. Sesuaikan kembali dan pastikan bahwa ISMS sesuai dengan proses teknologi dan pers
c. Lakukan secara berkala agar ISMS berjalan sesuai prosedur.

9. *Activity* APO13.2 Menentukan dan Mengelola Rencana Penanganan Resiko Keamanan Informa

a. Lakukan penjagaan terhadap rencana keamanan informasi dengan cara bagaimana me
dan disesuaikan dengan strategi perusahaan dan arsitekturnya.
b. Berikan rekomendasi untuk menetapkan keamanan didasarkan pasa kasus bisnis yang disetu

10. *Activity* APO13.3 Memantau dan Meninjau ISMS

a. Lakukan pemantauan dengan cara mengkomunikasikan kebutuhan akan dan manfaat,s
b. Kumpulkan data yang berkaitan dengan ISMS untuk melakukan perbaikan terhadap ISMS ya
dengan cara mempromoosikan budaya keamanan secara terus menerus.

ty untuk mencapai target yang diinginkan serta memperkecil jarak

a keamanan data
pan dan dikirim melalui perangkat yang terlindungi.

tentukan.

ıih besar dari persyaratan keamanan yang ditetapkan
lipastikan amanagar terlindungi dari *maleware*

tuhan
ıu memanipulasi data sistem

, membatasi dan mencabut akses terhadap aset fisik
ıg masuk kedalam sistem dapat teridentifikasi

Privasi).
enjaga kerahasiaan data.
agar keaslian konten data terjaga

struksi untuk hak akses yang tidak sah.
ra umum.

ımasi dengan cara

ʂyaratan bisnis. Lakukan secara berkala agar ISMS berjalan sesuai prosedur.

ısi.
njelaskan resiko keamanan informasi dikelola

ıjui dan diterapkan

ʂerta perbaikan secara terus menerus
ng belum terpenuhi