PEMBAHASAN SOAL UAS KJI 2019/2020

1. a. Menentukan apa yang harus dilindungi

Tujuan dari informasi keamanan/IA adalah untuk melindungi sistem dan data penting. contohnya melindungi informasi pembayaran pelanggan dan sejarah; melindungi riwayat dan preferensi pembelian pelanggan; melindungi pelanggan secara online, suara, Faks, dan hardcopy transaksi.

b. Mengidentifikasi system

Sistem merupakan koleksi komponen terorganisir untuk mencapai fungsi tertentu atau set fungsi. Sebuah sistem terdiri dari bagian yang lebih kecil yang bekerja sama untuk mencapai sesuatu.

c. Karakteristik system operasi

Sebuah karakterisasi operasi sistem mengambil dua bentuk yaitu mode operational atau negara dan profil operasional. Informasi ini berfungsi sebagai masukan terhadap analisis kerentanan dan ancaman.

d. Memastikan apa yang dilakukan seseorang dan tidak memiliki control lebih

Kegiatan akhir dalam mendefinisikan batas-batas sistem adalah untuk memastikan apa yang entitas sistem satu tidak dan tidak memiliki kontrol atas.

2. a. Kerentanan

- Jenis tindakan (type action) yang menyebabkan kerentanan untuk memanifestasikan dirinya: tindakan disengaja (atau tidak bertindak) atau tindakan jahat disengaja atau tidak bertindak.

- Metode Eksploitasi kerentanan : keterlibatan pelaku baik langsung atau tidak langsung pada bagian tertentu.

- Sifat dari kerentanan atau kelemahan (type kerentanan): keselamatan, keandalan, keamanan, atau beberapa kombinasi daripadanya

b. Ancaman

- Ancaman aktif merupakan suatu kejahatan yang terjadi pada komputer dan suatu kecurangan berupa pencurian data. Contohnya : Menimpa, memodifikasi, menyisipkan, menghapus, dan memblokir akses untuk

- Ancaman pasif merupakan kegagalam sistem itu sendiri atau kesalahan manusia dalam memproses sistem, atau karena adanya bencana alam yang terjadi yang mengakibatkan

ancaman bagi sistem itu sendiri. Contohnya : browsing, agregasi dan inferensi, memutar, kebocoran, menyalin dan mendistribusikan.

3. a. anticipate prevent : IA analysis technique, IA integrity level, IA design technique/features, Perception management

   b. Detect : IA design technique/ features, in service considerations, operational procedures

   c. Characterize : IA analysis technique, controllability, IA accident/incident investigation technique

   d. Respond, contain consequence : IA design technique/ features, operational procedures, contingency plans

   e. Recover : operational procedures, contingency plans

4. a. Kegiatan dilakukan ketika memverifikasi efektivitas tindakan pengendalian ancaman

   - Pastikan bahwa teknik/fitur desain IA yang sesuai dipilih.

   - Verifikasi bahwa IA desain teknik/fitur yang dilaksanakan dengan benar.

   - Verifikasi ketangguhan dan ketahanan dari tindakan pengendalian ancaman.

   - Pemilihan dan pelaksanaan teknik verifikasi IA

   - Penentuan eksposur risiko residual dan evaluasi penerimaan

   - Pemantauan kerentanan, ancaman dan survivability yang sedang berlangsung

   b. Pengukuran pengendalian ancaman terhadap Jaminan informasi

   - Apakah seperangkat teknik ini yang sesuai untuk menghilangkan atau mengurangi kerentanan /ancaman ini?

   - Apakah seperangkat teknik ini yang efektif terhadap semua mode operasional/keadaan dan profil di mana kerentanan/ancaman ini terjadi?

   - Apakah seperangkat teknik ini mencakup semua lapisan di mana kerentanan/ancaman terjadi?

   - Apakah seperangkat teknik ini mencakup semua tahapan pada kronologi kendali ancaman?

   - untuk setiap teknik/fitur: (a) adalah EAL sesuai? (b) adalah hasil analisis statis dan dinamis positif?

- Apakah tingkat integritas IA ditunjukkan dari seperangkat teknik yang konsisten dengan tingkat integritas IA yang diperlukan?

- Apakah ada mismatches atau kesenjangan dalam mengendalikan kerentanan ini/ancaman?