BAB 1

PENDAHULUAN

1.1. Latar Belakang

Otoritas Jasa Keuangan (OJK) adalah lembaga independen negara yang memiliki fungsi dan tugas untuk mengawasi, dan melindungi lembaga – lembaga keuangan yang telah terdaftar berserta konsumennya. Berdasarkan UU No 21 Tahun 2011 Otoritas Jasa Keuangan (OJK) adalah lembaga pengawas yang di bentuk Negara yang berfungsi menyelenggarakan sistem pengaturan dan pengawasan yang terintegrasi terhadap keseluruhan kegiatan di dalam sektor jasa keuangan baik di sektor perbankan, pasar modal, dan sektor keuangan non-bank seperti asuransi, dana pensiun, lembaga pembiayaan, dan lembaga jasa keuangan lainnya.

Sebelum ada OJK, pengawasan industri keuangan berjalan terpisah di bawah dua regulator yaitu Bank Indonesia yang mengawasi perbankan dan Bapepam-LK (Lembaga Keuangan) yang mengawasi pasar modal dan industri keuangan non-bank. Pasal 4 UU Nomor 21 Tahun 2011 tentang OJK menyebutkan bahwa OJK dibentuk dengan tujuan agar keseluruhan kegiatan di dalam sektor jasa keuangan terselenggara secara teratur, adil, transparan, akuntabel dan mampu mewujudkan sistem keuangan yang tumbuh secara berkelanjutan dan stabil, serta mampu melindungi kepentingan konsumen maupun masyarakat.

Ketika pengawasan perbankan masih diawasi oleh Bank Indonesia, sistem yang digunakan dalam meminta informasi debitur (i-Debt) bernama BI *Checking*. Kini, ketika pengawasan lembaga keuangan berpindah dari BI ke OJK sistem pun juga berubah menjadi SLIK atau Sistem Layanan Informasi Keuangan yang sama memiliki fungsi sebagai i-Debt, SLIK merupakan penjualan jasa dari OJK yang berupa layanan pemberian

informasi debitur, dengan kata lain, SLIK adalah sistem yang digunakan oleh kreditur untuk memeriksa apakah debitur yang mengajukan kredit ke bank tersebut memiliki riwayat kesehatan kredit yang baik atau tidak, sehingga bank tersebut dapat menganalisa kemampuan debitur dalam mengangsur cicilan.

Pengajuan data SLIK dapat dilakukan dengan dua cara yaitu dengan cara *offline* dan dengan cara *online*, tetapi pengajuan informasi secara *online* hanya dapat dilakukan oleh Lembaga Jasa Keuangan yang telah terdaftar (Bank, BPR, dll). Lembaga Jasa Keuangan yang telah terdaftar tersebut memiliki *ID username* dan *password* untuk mengambil data konsumen yang membutuhkan guna pengajuan kredit atau untuk dokumentasi pribadi, sedangkan konsumen perorangan pengajuan hanya dapat melalui pengajuan secara *offline*, yaitu dengan mendatangi langsung Kantor Regional maupun kantor cabang OJK, adapun secara *online* tetapi hanya diperuntukan konsumen wilayah kantor Regional 1 Jakarta, dan itu pun hanya sebatas pendaftaraan dimana hanya pemilihan hari, jam dan pengisian dokumen, selebihnya pendaftar tersebut harus melakukan secara manual dengan datang ke kantor OJK.

Oleh sebab itu, mudahnya akses oleh Lembaga Jasa Keuangan (LJK) dapat dimanfaatkan oleh oknum yang tidak bertanggung jawab. Salah satu contoh, baru - baru ini telah terjadi pengambilan data I-Debt oleh oknum internal LJK. I-Debt tersebut di perjual - belikan oleh pelaku kepada pihak yang tidak bertanggung jawab dengan harga Rp 75.000 – Rp 100.000 per data. Berdasarkan berita yang dimuat oleh CNN Indonesia pada hari Kamis 6 Februari 2020, korban dari kebocoran data tersebut adalah seorang wartawan senior, Bapak Ilham Bintang yang kehilangan tabungan ratusan juta rupiah hanya dalam waktu 3 jam.

Oleh dengan adanya korban dalam kebocoran data SLIK tersebut, sistem keamanan yang diterapkan OJK masih kurang dalam pengamanan hak akses dan dalam penampilan data debitur, sehingga dalam pengaksesan SLIK

masih mengakibatkan kebocoran. Berdasarkan temuan masalah yang terdapat pada latar belakang di atas, dapat disimpulkan bahwa sistem keamanan data pada SLIK OJK harus disempurnakan, maka dari itu Laporan Tugas Akhir ini mengangkat judul **"Analisis Keamanan Data Sistem Layanan Informasi Keuangan (SLIK) pada Otoritas Jasa Keuangan"**

1.2. Landasan Teori

1.2.1. Sistem, Sistem Informasi Akuntansi

Sistem (Romney dan Steinbart, 2014:2) adalah suatu kerangka prosedur-prosedur yang saling berhubungan yang disusun dengan suatu skema yang menyeluruh dan sistematis sehingga bagian-bagian pada prosedur tersebut saling berinteraksi yang dikoordinasikan untuk mencapai tujuan yang sama. Sistem adalah rangkaian dari dua atau lebih komponen - komponen yang saling berhubungan , yang berinteraksi untuk mencapai suatu tujuan**.**

Sedangkan, untuk Sistem informasi Akuntansi adalah rangkaian sistem yang terintegrasi antara *software* dan akuntansi yang dapat mengumpulkan, mengolah, mencatat, menganalisa, mengklasifikasikan sehingga dapat menjadi informasi bagi pihak internal maupun pihak eksternal dari perusahaan ."Sistem Informasi Akuntansi (Romney dan Steinbart ,2014 :37) merupakan proses identifikasi, pengumpulan, mencatat, penyimpanan serta pengembangan informasi dan memproses akuntansi dan data lainnya untuk menghasilkan informasi bagi pembuat keputusan."

1.2.2. Keamanan Data

Data adalah fakta yang dikumpulkan, direkam, disimpan, dan diproses oleh sistem informasi. Sedangkan Informasi (Romney

dan Steinbart ,2014:31) adalah data yang telah diorganisir dan diproses untuk memberikan makna dan meningkatkan proses pengambilan keputusan.

Layanan kerangka kerja terpercaya (Romney dan Steinbart, 2014:256) yang mengorganisir kendali terkait TI menjadi lima prinsip yang secara bersama-sama berkontribusi pada keamanan sistem :

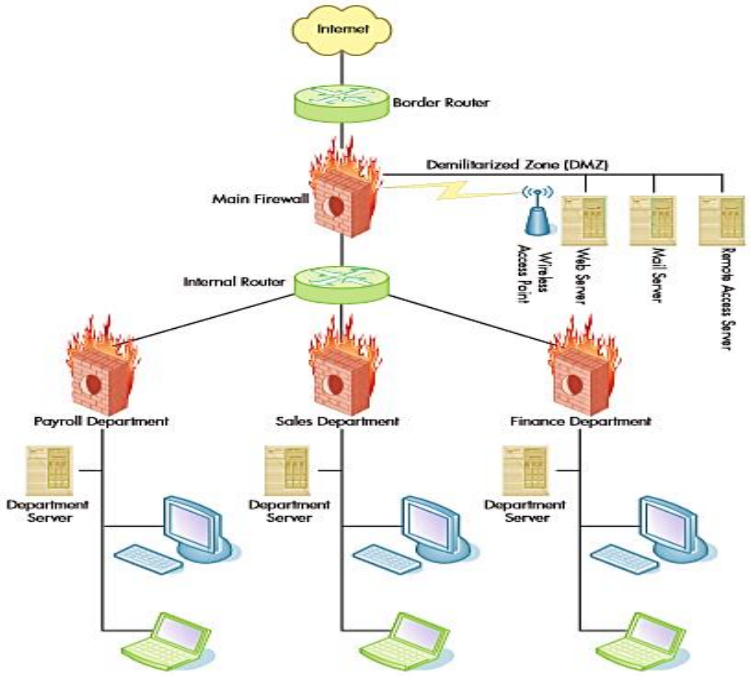
1. Keamanan — akses (baik fisik dan logis) ke sistem dan datanya dikendalikan dan dibatasi untuk pengguna yang sah.
2. Kerahasiaan — informasi organisasi yang sensitif (mis., Rencana pemasaran, rahasia dagang) dilindungi dari pengungkapan yang tidak sah.
3. Privasi — informasi pribadi tentang pelanggan, karyawan, pemasok, atau mitra bisnis dikumpulkan, digunakan, diungkapkan, dan dipelihara hanya sesuai dengan kebijakan internal dan persyaratan peraturan eksternal dan dilindungi dari pengungkapan yang tidak sah.
4. Memproses Integritas — data diproses secara akurat, lengkap, tepat waktu, dan hanya dengan otorisasi yang tepat.
5. Ketersediaan — sistem dan informasinya tersedia untuk memenuhi kewajiban operasional dan kontrak.

Gagasan pertahanan mendalam adalah untuk menggunakan beberapa lapis kontrol untuk menghindari satu titik kegagalan. Misalnya, banyak organisasi menggunakan tidak hanya *firewall* tetapi juga beberapa metode otentikasi (kata sandi, *token*, dan biometrik) untuk membatasi akses ke sistem informasi mereka. Penggunaan kontrol yang tumpang tindih, komplementer, dan berlebihan meningkatkan efektivitas secara keseluruhan karena

jika satu kontrol gagal atau dielakkan, yang lain dapat berfungsi sesuai rencana. Pertahanan mendalam biasanya melibatkan penggunaan kombinasi kontrol preventif, detektif, dan korektif.

1.2.2.1. Kontrol Akses

Perangkat yang disebut *router* perbatasan menghubungkan sistem informasi organisasi ke *Internet*. Di belakang *router* perbatasan adalah *firewall* utama, yang dapat berupa perangkat keras atau perangkat lunak tujuan khusus yang berjalan pada komputer serba guna, yang mengontrol komunikasi *inbound* dan *outbound* antara sistem di balik *firewall* dan jaringan lain. Zona demiliterisasi (DMZ) adalah jaringan terpisah yang terletak di luar sistem informasi internal organisasi yang memungkinkan akses terkontrol dari *Internet* ke sumber daya yang dipilih, seperti *server* web *e-commerce* organisasi. Bersama-sama, *router* perbatasan dan *firewall* bertindak sebagai filter untuk mengontrol informasi mana yang diizinkan masuk dan keluar dari sistem informasi organisasi.

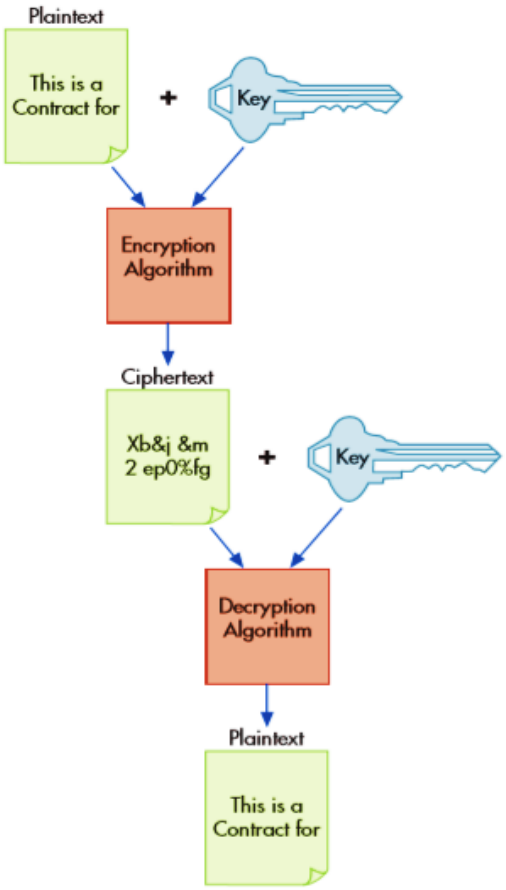


Gambar 1.1 Kontrol Akses

Sumber : Romney dan Steinbart 2014

1.2.2.2. Enkripsi

Enkripsi adalah kontrol preventif yang dapat digunakan untuk melindungi kerahasiaan dan privasi. Enkripsi (Romney dan Steinbart 2014:295-296) melindungi data saat sedang dalam perjalanan melalui *Internet* dan juga menyediakan satu penghalang terakhir yang harus diatasi oleh penyusup yang telah memperoleh akses tidak sah ke informasi yang disimpan. Enkripsi juga memperkuat prosedur otentikasi dan memainkan peran penting dalam memastikan dan memverifikasi validitas transaksi e-bisnis.



Gambar 1.2 Enkripsi

Sumber : Romney dan Steinbart 2014

1.2.3 Pengendalian Internal

Pengendalian internal adalah suatu proses karena merembes ke dalam aktivitas operasi organisasi dan merupakan bagian integral dari aktivitas manajemen. Kontrol internal (Romney dan Steinbart 2014:217)memberikan jaminan yang masuk akal — jaminan lengkap sulit dicapai dan mahal. Selain itu, sistem kontrol internal memiliki keterbatasan yang melekat, seperti kerentanan terhadap kesalahan dan kesalahan sederhana, penilaian dan pengambilan keputusan yang salah, penggantian manajemen, dan kolusi. Mengembangkan sistem kontrol internal membutuhkan pemahaman menyeluruh tentang kemampuan dan risiko teknologi

informasi (TI), serta cara menggunakan TI untuk mencapai tujuan kontrol organisasi.

Kontrol internal melakukan tiga fungsi penting: (Romney dan Steinbart 2014:217)

1. Kontrol pencegahan mencegah masalah sebelum timbul. Contoh: termasuk merekrut personil yang memenuhi syarat, memisahkan tugas karyawan, dan mengendalikan akses fisik ke aset dan informasi.
2. Kontrol detektif menemukan masalah yang tidak dapat dicegah. Contoh: termasuk pemeriksaan *history* aktivitas
3. Kontrol korektif mengidentifikasi dan memperbaiki masalah serta memperbaiki dan memulihkan dari kesalahan yang dihasilkan. Contoh: termasuk mempertahankan salinan cadangan file, memperbaiki kesalahan entri data, dan mengirimkan kembali transaksi untuk diproses selanjutnya.

Kontrol internal (Romney dan Steinbart ,2014:217-218) sering dipisahkan menjadi dua kategori:

1. Kontrol umum memastikan lingkungan kontrol organisasi stabil dan dikelola dengan baik, termasuk keamanan; Infrastruktur TI; dan akuisisi perangkat lunak, pengembangan, dan kontrol pemeliharaan.
2. Kontrol aplikasi mencegah, mendeteksi, dan memperbaiki kesalahan transaksi dan penipuan dalam program aplikasi. Mereka memperhatikan keakuratan, kelengkapan, validitas, dan otorisasi dari data yang ditangkap, dimasukkan, diproses, disimpan, dikirim ke sistem lain, dan dilaporkan.

1.3 Tujuan Praktik Kerja Lapangan

Kegiatan Praktik Kerja Lapangan bagi mahasiswa bertujuan :

1. Memahami secara langsung sistem informasi penjualan jasa yang terjadi di Otoritas Jasa Keuangan,
2. Mengetahui sistem informasi penjualan jasa yang terjadi,
3. Memperoleh data dan ilmu tentang sistem informasi yang diterapkan,
4. Menerapkan ilmu yang telah di peroleh selama masa perkuliahan, dan
5. Sebagai persyaratan kelulusan akademik D3 Akuntansi Universitas Airlangga.

1.4. Manfaat Pelaksanaan Praktik Kerja Lapangan

Manfaat yang di peroleh dalam Praktik Kerja Lapangan :

1. Bagi Penulis
   a. Menambah wawasan tentang Otoritas Jasa Keuangan,
   b. Menjadi sarana pembelajaran sistem keamanan data pada *Database* SLIK, dan
   c. Memiliki kesempatan menganalisis sesuai teori keamanan sistem yang dipelajari selama masa perkuliahan.

2. Bagi Fakultas
   a. Dapat menjalin kerjasama terkait program Praktik Kerja Lapangan
   b. Menjadi sarana promosi tentang mahasiswa Fakultas Vokasi

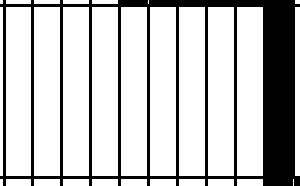
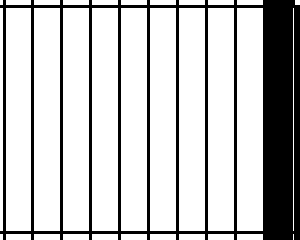
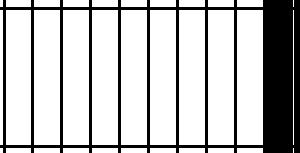
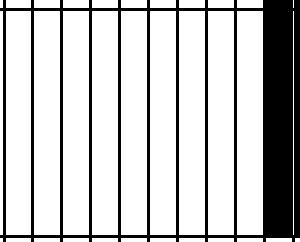
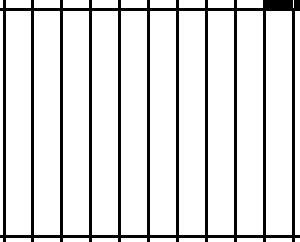
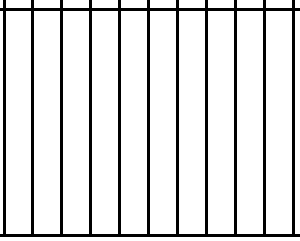
3. Bagi Otoritas Jasa Keuangan
   a. Mendapat gambaran kualitas mahasiswa Fakultas Vokasi Universitas Airlangga
   b. Mendapat usulan sistem keamanan atas *database* I-Debt sehingga dapat melayani pengguna dengan jaminan keamanan data bagi nasabah Lembaga Jasa Keuangannya

4. Bagi pembaca
    a. Menjadi sumber pengetahuan mengenai keamanan data yang ada di Otoritas Jasa Keuangan.
    b. Menjadi referensi pengamanan data pada sebuah sistem.

1.5. Rencana Kegiatan

Kegiatan Praktek Kerja Lapangan dilaksanakan selama 30 hari kerja yang dimulai pada hari Senin tanggal 6 Januari 2020 sampai dengan hari Jumat tanggal 14 Februari 2020, bertempat di Otoritas Jasa Keuangan Kantor Regional 4 Jawa Timur yang berlokasi di Gedung Bank Indonesia Lantai 4, Jalan Pahlawan No. 105 Surabaya, Jawa Timur. Pelaksanaan Praktik kerja Lapangan menyesuaikan jadwal masuk pegawai, setiap hari Senin – Jumat selama kurang lebih 9 jam, dari Pukul 07.30 WIB sampai Pukul 17.00 WIB.

No.	Kegiatan	2019				2020																							
		Des				Jan				Feb				Mar				Apr				Mei				Jun			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Pengajuan Lokasi PKL																												
2	Penyusunan Proposal PKL																												
3	Pengajuan Proposal ke Instansi																												
4	Pelaksanaan																												

	PKL	
5	Penentuan Dosen Pembimbing	
6	Penentuan Topik Tugas Akhir	
7	Pengambilan Data	
8	Penyusunan Laporan PKL dan TA	
9	Penyerahan Laporan PKL dan Tugas Akhir	
10	Presentasi Laporan Tugas Akhir	

Tabel 1.1 Rencana Kegiatan