BAB IV

HASIL DAN PEMBAHASAN

Pada bab ini diuraikan tentang analisa hasil dan pembahasan dari tahap perencanaan audit, tahap persiapan audit, tahap pelaksanaan audit kontrol akses sistem informasi, serta tahap pelaporan akhir audit kontrol akses sistem informasi. Temuan-temuan yang belum sesuai dengan standar implementasi yang digunakan diberikan rekomendasi.

4.1 Hasil Perencanaan dan Persiapan Audit Sistem Informasi

Tahap perencanaan dan persiapan ini adalah tahap awal yang dilakukan pada proses audit. Langkah ini dilakukan untuk memastikan bahwa pihak perusahaan yang diaudit telah memberikan kewenangan dan mempersiapkan segala sesuatu demi kelancaran pelaksanaan audit yang akan dilakukan.

4.1.1 Hasil Identifikasi Proses Bisnis dan TI

Dari hasil identifikasi yang telah dilakukan maka diperoleh gambaran umum perusahaan mulai dari profil perusahaan, visi dan misi perusahaan, struktur organisasi, serta gambaran umum lingkungan TI yang ada.

1) Profil Perusahaan

Audit dilakukan di PT Karya Karang Asem Indonesia merupakan induk perusahaan dalam bidang usaha daur ulang. Sampai saat ini PT Karya Karang Asem Indonesia mempunyai beberapa anak cabang perusahaan sejenis di beberapa daerah Jawa dan sekitarnya. PT Karya Karang Asem Indonesia

khususnya pada daerah Sedati, Sidoarjo merupakan pusat dari seluruh cabang yang memproduksi biji plastik dalam berbagai jenis dan tipe, perusahaan ini memproduksi antara lain PP YRC hijau, PP YRC merah, PP YRC hitam, PP YRC biru dan sebagainya.

PT. Kuyang Putra Perkasa secara resmi mendirikan unit usaha sampingannya yaitu PT. Karya Karang Asem Indonesia pada tahun 1992. KKAI bertugas menghancurkan sampah, menjadikannya biji plastik dan menjadi perusahaan yang berdiri sendiri yaitu PT. Karya Karang Asem Indonesia pada tahun 1993. Kemudian, pada tahun 1994 PT. Karya Karang Asem Indonesia menyerahkan pengelolaan sampah jenis kusus untuk dikelola oleh PT. Karya Agung. Pada tahun 2001 PT. Karya Karang Asem Indonesia mengembangkan berbagai jenis baru biji plastik di beberapa kota dipulau Jawa.

Seiring dengan pertumbuhan ekonomi yang cukup tinggi dan pesatnya perkembangan sektor industri plastik, khususnya perabotan rumah tangga dan barang-barang elektronik dari plastik, PT Karya Karang Asem Indonesia ikut berpartisipasi melalui usaha penyediaan bahan dasar perusahaan-perusahaan tersebut seperti PP YRC hijau, PP YRC merah, PP YRC hitam, PP YRC biru dan sebagainya.

Dengan didukung staf karyawan yang berpengalaman di bidang daur ulang sampah plastik, peralatan-peralatan daur ulang yang tepat serta fasilitas perusahaan yang senantiasa mengutamakan kepuasan dan kepercayaan pelanggan, dengan menjamin bahwa produk yang dihasilkan dapat memenuhi mutu yang diinginkan, penyerahan produk yang konsisten dalam segala kondisi serta harga yang bersaing dibanding pemasok lain.

2) Visi, Misi, dan Prinsip Manajemen PT. Karya Karang Asem Indonesia

Dengan didukung staf karyawan yang berpengalaman di bidang daur ulang, peralatan-peralatan yang tepat guna serta fasilitas perusahaan yang memadai dan senantiasa mengutamakan kepuasan dan kepercayaan pelanggan, dengan menjamin bahwa produk yang dihasilkan dapat memenuhi mutu yang diinginkan, penyerahan produk yang konsisten dalam segala kondisi serta harga yang bersaing dibanding supplier lain maka ditetapkan visi, misi dan *principle & management* perusahaan sebagai berikut:

VISI

Menerapkan standart manajemen mutu untuk tetap menjaga kepuasan konsumen atas produk yang dihasilkan.

MISI

Menjadi salah satu perusahaan terbesar yang turut serta menjaga dan melestarikan lingkungan dengan cara mengolah berbagai jenis plastik menjadi end product yang berguna bagi masyarakat secara globalisasi.

PRINSIP MANAJEMEN

Penerapan manajement PT. Karya Karang Asem Indonesia didasarkan pada kepercayaan pada para karyawannya bahwa setiap karyawan wajib mempunyai komitmen untuk bekerja sebaik dan semaksimal mungkin bagi nama baik perusahaan yang menaungi mereka. Hal ini merupakan keyakinan dari filosofis perusahaan, bahwa apabila PT. Karya Karang Asem Indonesia berhasil memberikan produk bahan baku yang tepat guna bagi masyarakat, berarti para karyawannya telah melakukan hal yang positif bagi nama baik perusahaannya. Hal ini merupakan gengsi tersendiri bagi para karyawan PT KKAI. Sehingga

dapat di simpulkan bahwa semua karyawan ikut berperan dalam pencapaian sukses perusahaan.

Struktur perusahaan sangat sederhana dan sehingga mudah melakukan koordinasi bagi semua karyawan perusahaan. Sehingga bisa bertemu langsung dengan kepala bagian di setiap divisi sehingga berakibat dapat merespon lebih cepat.

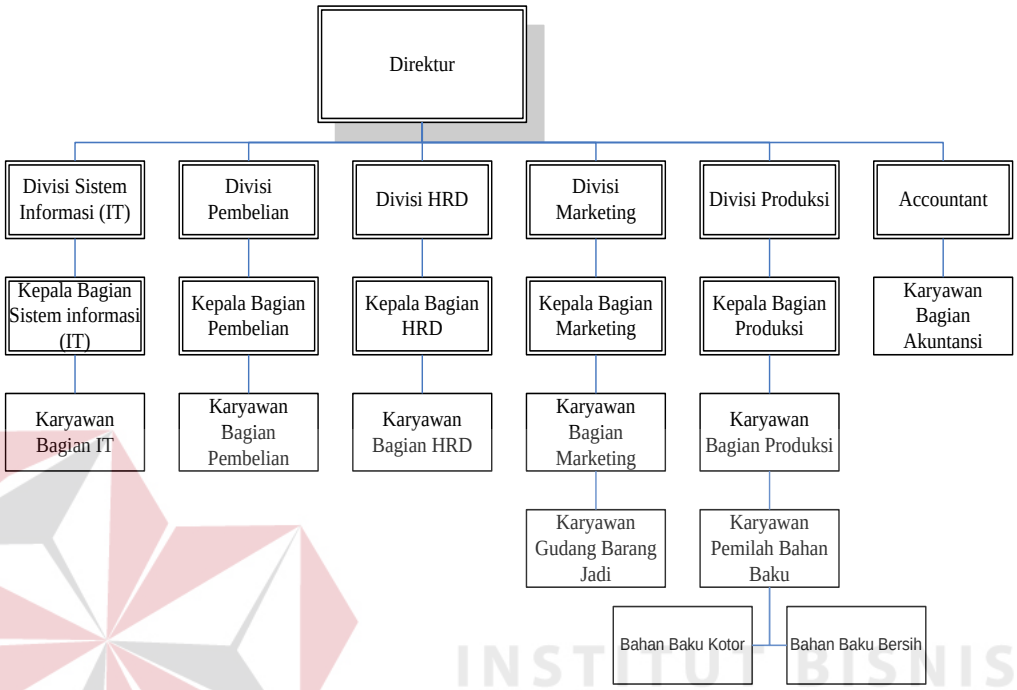
3) Struktur Organisasi

PT. Karya Karang Asem Indonesia merupakan anak usaha dari PT. Kuyang Putra Perkasa. Sampai saat ini PT. Karya Karang Asem Indonesia mempunyai cabang di beberapa daerah di pulau Jawa. Secara fungsional maka struktur organisasi PT. Karya Karang Asem Indonesia dapat dilihat pada Gambar 4.1 di halaman 69.

4) Gambaran PT. Karya Karang Asem Indonesia

PT. Karya Karang Asem Indonesia memiliki kantor pusat di Jl. Raya Pabean No.77, Sedati – Sidoarjo. Sebagai kantor pusat, PT. Karya Karang Asem Indonesia sangat berperan penting dalam memanajemen keamanan informasi, karena *plant* di seluruh Indonesia akan mengirimkan dan mengakses data-data kepada pusat dengan rentang waktu tertentu. Aplikasi SDCI yang dimiliki oleh PT. Karya Karang Asem Indonesia sudah beroperasi secara online dengan menggunakan server yang berada di kantor pusat. PT Karya Karang Asem Indonesia memiliki *server* utama, yang di letakkan di lantai 2 perusahaan tersebut. Dengan demikian, sebagai kantor pusat yang memiliki seluruh informasi

perusahaan yang ada harus memiliki *backup* dan *recovery* yang berjalan dengan baik.



Gambar 4.1 Struktur Organisasi PT. Karya Karang Asem Indonesia

4.1.2 Hasil Menentukan Ruang Lingkup dan Tujuan Audit

Setelah dilakukan observasi maka hasil yang diperoleh adalah penetapan ruang lingkup audit yaitu sistem informasi standar yang digunakan adalah ISO 27002. Dari tahap identifikasi ini dihasilkan juga pemetaan klausul, objektif kontrol, dan kontrol keamanan yang telah disepakati oleh PT. KKAI. Klausul yang digunakan adalah Klausul 11 tentang Kontrol Akses kecuali bagian kontrol akses jaringan dan *teleworking*. Detail struktur dokumen keamanan ISO/IEC 27002 dapat dilihat pada Lampiran 1. Klausul, objektif kontrol, dan kontrol keamanan yang telah ditetapkan dapat dilihat pada Tabel 4.1 di halaman 70.

Tabel 4.1 Klausul, Objektif Kontrol dan Kontrol Keamanan ISO 27002 yang Telah Dipetakan

Klausul	Objektif Kontrol	Kontrol Keamanan
11 Kontrol akses	11.1 Persyaratan bisnis untuk kontrol akses	11.1.1 Kebijakan kontrol akses
	11.2 Manajemen akses *user*	11.2.1 Registrasi pengguna
		11.2.2 Manajemen hak istimewa atau khusus
		11.2.3 Manajemen *password*
		11.2.4 Tinjauan terhadap hak akses *user*
	11.3 Tanggung jawab pengguna	11.3.1 Penggunaan *password*
		11.3.2 Peralatan pengguna yang tidak dijaga
		11.3.3 Kebijakan *clear desk* dan *clear screen*
	11.5 Kontrol akses sistem operasi	11.5.1 Prosedur *log-on* yang aman
		11.5.2 Identifikasi dan otentifikasi *user*
		11.5.3 Manajemen *password*
		11.5.4 Penggunaan *utilities* sistem
		11.5.5 Sesi *time-out*
		11.5.6 Batasan waktu koneksi
	11.6 Kontrol akses informasi dan aplikasi	11.6.1 Pembatasan akses informasi
		11.6.2 Isolasi sistem yang sensitif

4.1.3 Hasil Menentukan Metode dan Pembuatan Proposal ke Perusahaan

Pada audit kontrol akses sistem informasi di PT. KKAI ini menggunakan metode audit kepatutan dengan acuan ISO 27002 sebagai pedomannya serta melakukan wawancara, observasi, dan pemeriksaan sebagai teknik pelaksanaan audit. Setelah menentukan metode dan merancang perencanaan audit, selanjutnya membuat proposal yang berisi kesepakatan antara auditor dengan pihak perusahaan dan mengajukan permintaan kebutuhan data. Lampiran proposal yang telah disetujui oleh PT. KKAI dapat dilihat pada Lampiran 2. Hasil dari tahap ini adalah pemetaan klausul, objektif kontrol dan kontrol keamanan.

4.1.4 Hasil Penentuan *Auditee*

Sebelum audit kontrol akses sistem informasi dilakukan terlebih dahulu menentukan bagian mana di perusahaan yang akan diaudit atau yang disebut *auditee*. Tabel 4.2 menunjukkan bagian yang akan diwawancara berdasarkan klausul yang telah ditentukan.

Tabel 4.2 Hasil Penentuan *Auditee*

Klausul	Deskripsi	*Auditee*	Keterangan
11	Kontrol Akses	Bagian pengembang aplikasi	*Responsible*
		Project manager	*Accountable*
		programmer	*Consulted*

4.1.5 Hasil Penentuan Jadwal Audit (Rencana Kerja Audit)

Hasil dari proses penyusunan rencana kerja audit berupa tabel yang berisi tentang aktifitas yang dilakukan selama audit berlangsung. Pelaksanaan audit

kontrol akses sistem informasi dilakukan secara bertahap sesuai dengan jadwal yang dapat dilihat pada Tabel 4.3.

Tabel 4.3 Jadwal Kegiatan Audit (*Audit Working Plan*)

No	Kegiatan	Bulan													
		April				Mei				Juni				Juli	
		1	2	3	4	1	2	3	4	1	2	3	4	1	2
1	Studi Literatur														
2	Penentuan ruang lingkup														
3	Pengumpulan Bukti: • Peninjauan Struktur Organisasi • Peninjauan kebijakan dan prosedur yang terkait dengan TI • Peninjauan standar yang terkait dengan TI														
	• Peninjauan dokumentasi pengelolaan SI/TI • Wawancara														
	• Pengobservasian proses dan kinerja karyawan														
4	Pelaksanaan uji kepatutan														
5	Penentuan tingkat kematangan														
6	Penentuan hasil audit														
7	Penyusunan laporan audit														

4.1.6 Hasil Pembuatan Pernyataan

Hasil dari proses membuat pernyataan berapa tabel yang berisi rincian pernyataan yang telah disesuaikan dengan standar ISO 27002. Pernyataan yang telah dibuat dapat dilihat pada Tabel 4.4.

Tabel 4.4 Hasil Pernyataan pada Kontrol Kebijakan Kontrol Akses

Klausul 11 Kontrol Akses	
Kategori Keamanan Utama: 11.1 Persyaratan bisnis untuk akses kontrol	
Kontrol Keamanan: 11.1.1 Kebijakan Kontrol Akses	
No	Pernyataan
1	Terdapat persyaratan bisnis kontrol akses yang telah ditetapkan dan didokumentasikan.
2	Terdapat peraturan dan hak kontrol akses untuk setiap pengguna yang telah dinyatakan dengan jelas dalam suatu pernyataan kebijakan tentang akses.
3	Pengguna dan penyedia layanan telah diberi satu pernyataan persyaratan bisnis yang jelas yang harus dipenuhi untuk pengontrolan akses.
4	Terdapat persyaratan keamanan dari aplikasi bisnis perorangan.
5	Terdapat identifikasi dari seluruh informasi yang berhubungan dengan aplikasi bisnis.
6	Terdapat kebijakan diseminasi dan otorisasi informasi. misalnya kebuuhan untuk mengetahui prinsip dan tingkat keamanan serta klasifikasi informasi.
7	Terdapat peraturan yang relevan terkait dengan perlindungan akses ke data atau layanan.
8	Terdapat kewajiban kontrak yang terkait dengan perlindungan akses ke data atau layanan.
9	Terdapat profil standar akses pengguna untuk kategori pekerjaan yang umum.
10	Terdapat manajemen hak akses dilingkungan yang terdistribusi dan terjaring yang mengatur semua jenis koneksi yang tersedia.

Hasil pernyataan pada klausul 11 kontrol keamanan yang terdiri dari 11.2.1 sampai dengan 11.6.2 dapat dilihat pada Lampiran 3.

4.1.7 Hasil Pembuatan Pertanyaan

Hasil dari proses pembuatan pertanyaan ini adalah tabel yang berisi pertanyaan sesuai dengan pernyataan yang telah dibuat pada proses sebelumnya. Pertanyaan yang telah dibuat akan diperlukan untuk mendukung saat wawancara. Pertanyaan yang telah dibuat dapat dilihat pada Tabel 4.5.

Tabel 4.5 Hasil Pertanyaan pada Kontrol Kebijakan Kontrol Akses

Klausul 11 Kontrol Akses		
Kategori Keamanan Utama: 11.1 Persyaratan bisnis untuk akses kontrol		
Kontrol Keamanan: 11.1.1 Kebijakan Kontrol Akses		
No	Pernyataan	Pertanyaan
1	Terdapat persyaratan bisnis kontrol akses yang telah ditetapkan dan didokumentasikan.	Apakah terdapat persyaratan bisnis kontrol akses yang telah ditetapkan dan didokumentasikan?
2	Terdapat peraturan dan hak kontrol akses untuk setiap pengguna yang telah dinyatakan dengan jelas dalam suatu pernyataan kebijakan tentang akses.	Apakah terdapat peraturan dan hak kontrol akses untuk setiap pengguna yang telah dinyatakan dengan jelas dalam suatu pernyataan kebijakan tentang akses?
3	Pengguna dan penyedia layanan telah diberi satu pernyataan persyaratan bisnis yang jelas yang harus dipenuhi untuk pengontrolan akses.	Apakah pengguna dan penyedia layanan telah diberi satu pernyataan persyaratan bisnis yang jelas yang harus dipenuhi untuk pengontrolan akses?
4	Terdapat persyaratan keamanan dari aplikasi bisnis perorangan.	Apakah terdapat persyaratan keamanan dari aplikasi bisnis perorangan?
5	Terdapat identifikasi dari seluruh informasi yang berhubungan dengan aplikasi bisnis.	Apakah terdapat identifikasi dari seluruh informasi yang berhubungan dengan aplikasi bisnis?
6	Terdapat kebijakan diseminasi dan otorisasi informasi. misalnya kebuuhan untuk mengetahui prinsip dan tingkat keamanan serta klasifikasi informasi.	Apakah terdapat kebijakan diseminasi dan otorisasi informasi. misalnya kebuuhan untuk mengetahui prinsip dan tingkat keamanan serta klasifikasi informasi?

Tabel 4.5 (Lanjutan)

Klausul 11 Kontrol Akses		
Kategori Keamanan Utama: 11.1 Persyaratan bisnis untuk akses kontrol		
Kontrol Keamanan: 11.1.1 Kebijakan Kontrol Akses		
No	Pernyataan	Pertanyaan
7	Terdapat peraturan yang relevan terkait dengan perlindungan akses ke data atau layanan.	Apakah terdapat peraturan yang relevan terkait dengan perlindungan akses ke data atau layanan ?
8	Terdapat kewajiban kontrak yang terkait dengan perlindungan akses ke data atau layanan.	Apakah terdapat kewajiban kontrak yang terkait dengan perlindungan akses ke data atau layanan.
9	Terdapat profil standar akses pengguna untuk kategori pekerjaan yang umum.	Apakah terdapat profil standar akses pengguna untuk kategori pekerjaan yang umum?
10	Terdapat manajemen hak akses dilingkungan yang terdistribusi dan terjaring yang mengatur semua jenis koneksi yang tersedia.	Apakah terdapat manajemen hak akses dilingkungan yang terdistribusi dan terjaring yang mengatur semua jenis koneksi yang tersedia?

Hasil pernyataan pada klausul 11 kontrol keamanan yang terdiri dari 11.2.1 sampai dengan 11.6.2 dapat dilihat pada Lampiran 3.

4.2 Hasil Pelaksanaan Audit Kontrol Akses Sistem Informasi

4.2.1 Hasil Wawancara

Setelah dilakukan proses wawancara maka hasil yang diperoleh adalah dokumen wawancara yang telah di tanda tangani oleh direksi PT KKAI. Dokumen wawancara merupakan tabel yang berisi pernyataan, pertanyaan, dan jawaban *auditee*. Untuk hasil wawancara yang telah dilakukan dapat dilihat pada Tabel 4.6 di halaman 76.

Tabel 4.6 Dokumen Wawancara pada Kontrol Kebijakan Kontrol Akses

Klausul 11 Kontrol Akses			
Kategori Keamanan Utama: 11.1 Persyaratan bisnis untuk akses kontrol			
Kontrol Keamanan: 11.1.1 Kebijakan Kontrol Akses			
No	Pernyataan	Pertanyaan	Jawaban
1	Terdapat persyaratan bisnis kontrol akses yang telah ditetapkan dan didokumentasikan.	Apakah terdapat persyaratan bisnis kontrol akses yang telah ditetapkan dan didokumentasikan?	Persyaratan bisnis control akses telah ditetapkan di dalam peraturan perusahaan dan didokumentasikan.
2	Terdapat peraturan dan hak kontrol akses untuk setiap pengguna yang telah dinyatakan dengan jelas dalam suatu pernyataan kebijakan tentang akses.	Apakah terdapat peraturan dan hak kontrol akses untuk setiap pengguna yang telah dinyatakan dengan jelas dalam suatu pernyataan kebijakan tentang akses?	Persyaratan bisnis control akses telah ditetapkan di dalam peraturan perusahaan dan didokumentasikan.
3	Pengguna dan penyedia layanan telah diberi satu pernyataan persyaratan bisnis yang jelas yang harus dipenuhi untuk pengontrolan akses.	Apakah pengguna dan penyedia layanan telah diberi satu pernyataan persyaratan bisnis yang jelas yang harus dipenuhi untuk pengontrolan akses?	Persyaratan bisnis control akses telah ditetapkan di dalam peraturan perusahaan dan didokumentasikan.
4	Terdapat persyaratan keamanan dari aplikasi bisnis perorangan.	Apakah terdapat persyaratan keamanan dari aplikasi bisnis perorangan?	Terdapat persyaratan keamanan, namun belum terdokumentasikan.
5	Terdapat identifikasi dari seluruh informasi yang berhubungan dengan aplikasi bisnis.	Apakah terdapat identifikasi dari seluruh informasi yang berhubungan dengan aplikasi bisnis?	Tentu saja, semua aplikasi bisnis didokumentasikan.
6	Terdapat kebijakan diseminasi dan otorisasi informasi. misalnya kebuuhan untuk mengetahui prinsip dan tingkat keamanan serta klasifikasi informasi.	Apakah terdapat kebijakan diseminasi dan otorisasi informasi. misalnya kebuuhan untuk mengetahui prinsip dan tingkat keamanan serta klasifikasi informasi?	Belum ada

Tabel 4.6 (Lanjutan)

Klausul 11 Kontrol Akses			
Kategori Keamanan Utama: 11.1 Persyaratan bisnis untuk akses kontrol			
Kontrol Keamanan: 11.1.1 Kebijakan Kontrol Akses			
No	Pernyataan	Pertanyaan	Jawaban
7	Terdapat peraturan yang relevan terkait dengan perlindungan akses ke data atau layanan.	Apakah terdapat peraturan yang relevan terkait dengan perlindungan akses ke data atau layanan ?	Terdapat peraturan yang relevan terkait dengan perlindungan akses ke data, peraturan tersebut tertulis pada peraturan perusahaan.
8	Terdapat kewajiban kontrak yang terkait dengan perlindungan akses ke data atau layanan.	Apakah terdapat kewajiban kontrak yang terkait dengan perlindungan akses ke data atau layanan.	Kewajiban kontrak telah tertulis pada perjanjian kontrak kerja sama.
9	Terdapat profil standar akses pengguna untuk kategori pekerjaan yang umum.	Apakah terdapat profil standar akses pengguna untuk kategori pekerjaan yang umum?	Terdapat pengaturan hak akses.
10	Terdapat manajemen hak akses dilingkungan yang terdistribusi dan terjaring yang mengatur semua jenis koneksi yang tersedia.	Apakah terdapat manajemen hak akses dilingkungan yang terdistribusi dan terjaring yang mengatur semua jenis koneksi yang tersedia?	Tentu saja, terdapat manajemen hak akses yang telah diatur oleh direksi dan bagian sistem informasi.

Hasil pernyataan pada klausul 11 kontrol keamanan yang terdiri dari 11.2.1 sampai dengan 11.6.2 dapat dilihat pada Lampiran 3.

4.2.2 Hasil Pemeriksaan

Setelah proses wawancara selesai maka dilakukan pemeriksaan baik melalui observasi maupun pengujian untuk mengetahui dan memastikan secara langsung kebenaran proses yang ada. Hasil dari proses pemeriksaan adalah temuan beserta bukti yang dapat dilihat pada Tabel 4.7 di halaman 78.

Tabel 4.7 Hasil Pemeriksaan Pernyataan Pada Kontrol Kebijakan Kontrol Akses

Kontrol Keamanan: 11.1.1 Pembatas keamanan fisik			
No	Pernyataan	Hasil Pemeriksaan	Bobot
1	Terdapat persyaratan bisnis kontrol akses yang telah ditetapkan dan didokumentasikan.	Persyaratan bisnis kontrol akses terdokumentasi dengan baik. Terdapat persyaratan bisnis kontrol akses didalam peraturan perusahaan dan telah terdefinisi.	1
2	Terdapat peraturan dan hak kontrol akses untuk setiap pengguna yang telah dinyatakan dengan jelas dalam suatu pernyataan kebijakan tentang akses.	Persyaratan bisnis kontrol akses terdokumentasi dengan baik. Terdapat persyaratan bisnis kontrol akses didalam peraturan perusahaan dan telah terdefinisi.	1
3	Pengguna dan penyedia layanan telah diberi satu pernyataan persyaratan bisnis yang jelas yang harus dipenuhi untuk pengontrolan akses.	Persyaratan bisnis kontrol akses terdokumentasi dengan baik. Terdapat persyaratan bisnis kontrol akses didalam peraturan perusahaan dan telah terdefinisi.	1
4	Terdapat persyaratan keamanan dari aplikasi bisnis perorangan.	Persyaratan keamanan telah tertuang pada prosedur operasi dan telah terdefinisi. Persyaratan keamanan tersebut sebagai contoh adalah: terdapat pengaturan hak akses, backup data dan lain sebagainya.	1
5	Terdapat identifikasi dari seluruh informasi yang berhubungan dengan aplikasi bisnis.	Identifikasi dari seluruh informasi yang berhubungan dengan bisnis telah terdokumentasi. Bukti: Terdapat daftar software.	1
6	Terdapat kebijakan diseminasi dan otorisasi informasi. misalnya kebutuhan untuk mengetahui prinsip dan tingkat keamanan serta klasifikasi informasi.	Terdapat kebijakan dan otorisasi terhadap sistem informasi namun masih dilakukan secara informal.	0,6

Tabel 4.7 (Lanjutan)

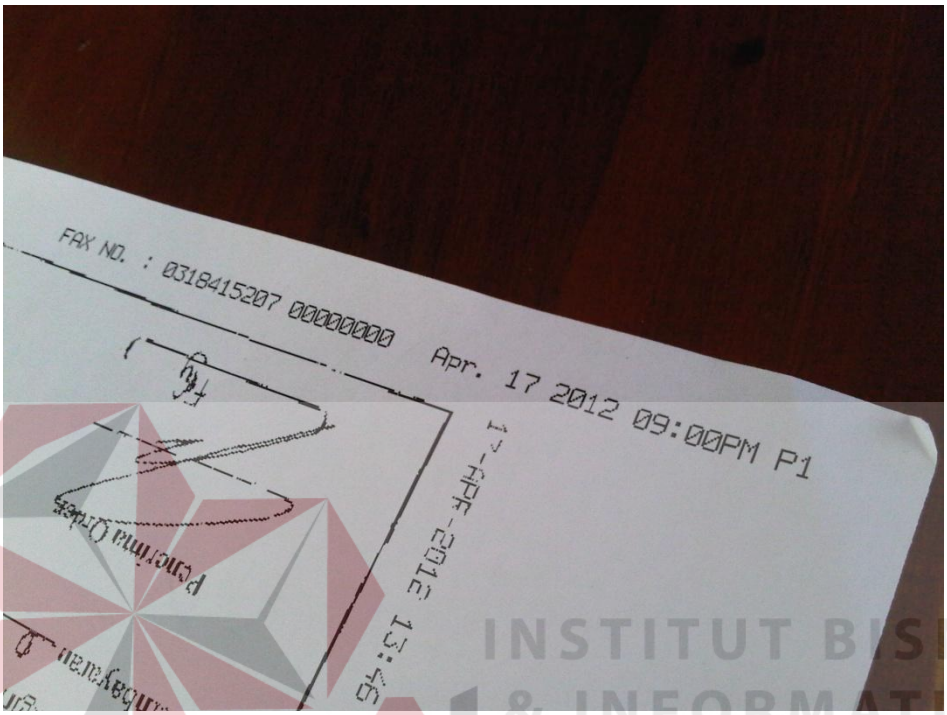
Kontrol Keamanan: 11.1.1 Pembatas keamanan fisik			
No	Pernyataan	Hasil Pemeriksaan	Bobot
7	Terdapat peraturan yang relevan terkait dengan perlindungan akses ke data atau layanan.	Terdapat peraturan yang relevan terkait dengan perlindungan akses ke data, peraturan tersebut tertulis pada peraturan perusahaan dan telah terdefinisi.	1
8	Terdapat kewajiban kontrak yang terkait dengan perlindungan akses ke data atau layanan.	Kewajiban kontrak telah sesuai dengan peraturan perusahaan. Kewajiban kontrak telah tertulis pada perjanjian kontrak kerja sama dan telah terdefinisi. Bukti: Terdapat pada peraturan perusahaan.	1
9	Terdapat profil standar akses pengguna untuk kategori pekerjaan yang umum.	Profil standar akses pengguna telah sesuai dengan kebijakan perusahaan. Terdapat perngaturan hak akses yang didokumentasikan dan didefinisikan.	1
10	Terdapat manajemen hak akses dilingkungan yang terdistribusi dan terjaring yang mengatur semua jenis koneksi yang tersedia.	Manajemen hak akses telah diatur sesuai dengan kebijakan perusahaan. Bandwith untuk server diatur ke stabilannya tetapi untuk akses data tergantung pada jabatan atau posisi dan tingkat kepentingannya.	1

Hasil pernyataan pada klausul 11 kontrol keamanan yang terdiri dari 11.2.1 sampai dengan 11.6.2 dapat dilihat pada Lampiran 4.

4.2.3 Hasil Dokumentasi (Data dan Bukti)

Hasil dokumentasi berisi data maupun bukti yang ada mengenai temuan-temuan yang ditemukan saat pelaksanaan audit. Bukti-bukti tersebut dapat berupa foto, rekaman, suara atau video. Hasil dokumentasi dapat dilihat pada Tabel 4.7 dan selengkapnya dapat dilihat pada Lampiran 4, sedangkan bukti audit yang

berupa dokumentasi foto dapat dilihat pada Gambar 4.2 dan selengkapnya dapat dilihat pada Lampiran 5.



Gambar 4.2 History Pengaksesan Data

4.2.4 Hasil Pelaksanaan Uji Kematangan

Berdasarkan analisa dari pengumpulan bukti dan wawancara dengan *auditee,* maka diperoleh hasil uji kepatutan dari tingkat kematangan untuk masing-masing kontrol. Adapun tingkat kematangan tersebut diperoleh dari masing-masing analisa yang dapat dilihat pada kerangka kerja pada Lampiran 4. Hasil perhitungan tingkat kematangan hasil audit kontrol akses informasi adalah sebagai berikut.

a. Hasil *Maturity Level* pada klausul 11 Kontrol Akses

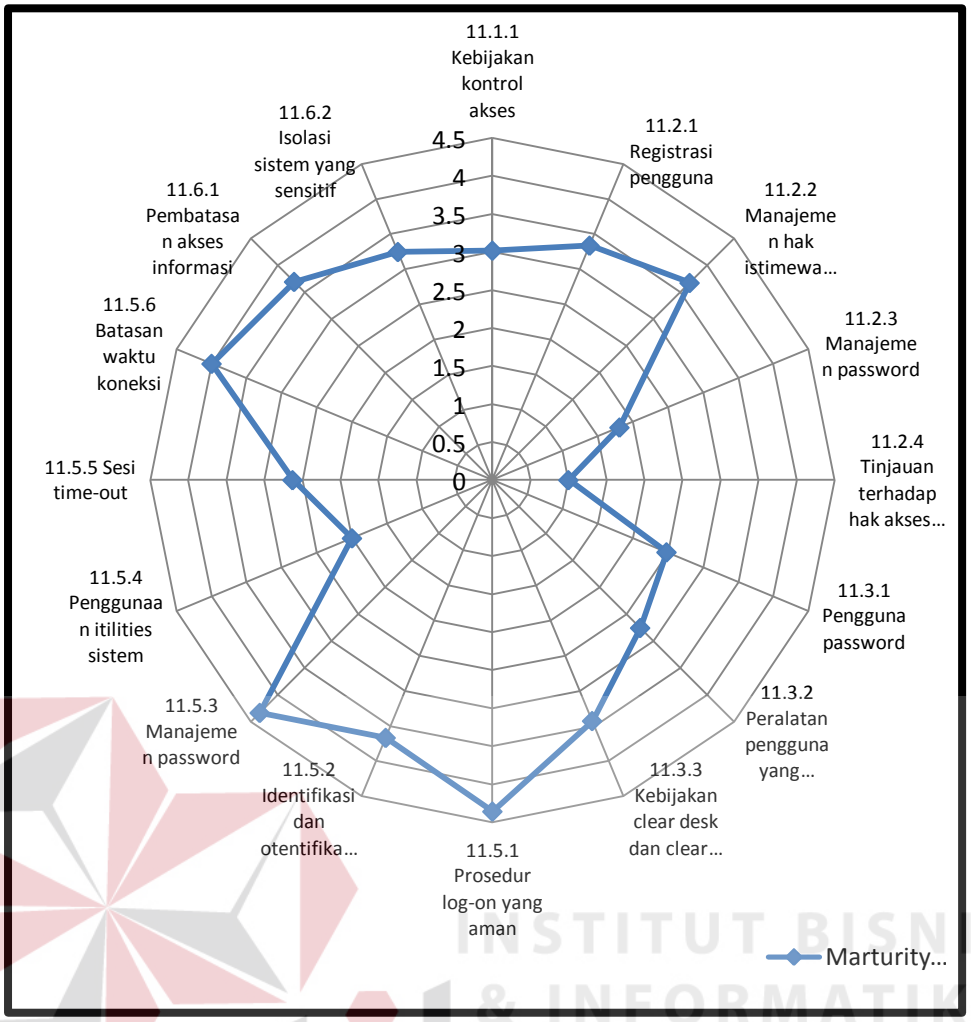
Hasil dari proses perhitungan *maturity level* pada klausul 11 kontrol akses adalah 3.13, hasil tersebut munjukkan bahwa proses pada manajemen komunikasi dan operasi dilakukan sesuai standar prosedur dan dilakukan secara rutin, hal tersebut dapat dilihat dengan adanya dokumentasi tingkat otorisasi sebagai contoh adanya pernyataan yang ditandatangani untuk menjaga *password*, adanya tinjauan terhadap hak akses *user*, terdapat kebijakan dan otorisasi terhadap keamanan informasi, persyaratan bisnis kontrol akses, persyaratan keamanan dan fasilitas sistem. Hasil perhitungan tersebut dapat dilihat pada Tabel 4.8. Hasil perhitungan *maturity level* pada klausul 11 kontrol akses dapat direpresentasikan dalam bentuk grafik. Hasil representasi perhitungan *maturity level* klausul 11 kontrol akses dapat dilihat pada Gambar 4.3 di halaman 83. Setelah dilakukan penilaian *maturity level* telah ditemukan fakta yang tidak sesuai dengan standar ISO 27002

Tabel 4.8 Hasil *Maturity Level* Klausul 11 Kontrol Akses

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
11 Kontrol akses	11.1 Persyaratan bisnis untuk kontrol akses	11.1.1 Kebijakan kontrol akses	3.02	3.02
	11.2 Manajemen akses *user*	11.2.1 Registrasi pengguna	3.34	2.46
		11.2.2 Manajemen hak istimewa atau khusus	3.67	
		11.2.3 Manajemen *password*	1.81	

Tabel 4.8 (Lanjutan)

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
11 Kontrol akses	11.2 Manajemen akses *user*	11.2.4 Tinjauan terhadap hak akses *user*	1	2.46
	11.3 Tanggung jawab pengguna	11.3.1 Pengguna *password*	2.48	2.89
		11.3.2 Peralatan pengguna yang tidak dijaga	2.75	
		11.3.3 Kebijakan *clear desk* dan *clear screen*	3.43	
	11.5 Kontrol akses sistem operasi	11.5.1 Prosedur log-on yang aman	4.36	3.59
		11.5.2 Identifikasi dan otentifikasi *user*	3.67	
		11.5.3 Manajemen *password*	4.33	
		11.5.4 Penggunaan utilities sistem	2	
		11.5.5 Sesi time-out	2.63	3.32
		11.5.6 Batasan waktu koneksi	4	
	11.6 Kontrol akses informasi dan aplikasi	11.6.1 Pembatasan akses informasi	3.69	3.47
		11.6.2 Isolasi sistem yang sensitif	3.25	3.47
	Marturity level Klausul 11			3.13



Gambar 4.3 Representasi Nilai *Maturity Level* Klausul 11 Kontrol Akses

b. Hasil Pembahasan Audit Kontrol Akses Sistem Informasi PT. KKAI

Hasil dari proses perhitungan *maturity level* pada seluruh klausul 11 adalah 3.13 yaitu *defined*. Hasil tersebut menunjukkan bahwa sebagian besar proses kontrol akses sistem informasi manajemen aset yang ada pada PT. Karya Karang Asem Indonesia telah dilakukan secara rutin dan sesuai dengan standar prosedur yang ada, kebocoran informasi yang terjadi merupakan akibat dari adanya penyalahgunaan *password* yang terjadi. Berdasarkan temuan-temuan hasil audit penyalahgunaan *password* yang terjadi disebabkan karena peraturan perusahaan yang kurang tegas dan kurang spesifik untuk

kerahasiaan *password*, belum jelasnya perjanjian atau pernyataan tertulis yang ditandatangani karyawan untuk benar-benar menjaga kerahasiaan dan keamanan *password* masing-masing, penerapan manajemen *password* yang tidak sesuai standar, dan kurangnya kesadaran serta pengetahuan karyawan terhadap pentingnya merahasiakan *password*. Hal tersebut dapat dilihat pada hasil *maturity level* kontrol keamanan 11.2.3 manajemen *password user* yang hanya memiliki nilai 1.81, kontrol keamanan 11.2.4 tinjauan terhadap akses *user* yang bernilai 1, dan kontrol keamanan 11.3.1 penggunaan *password* yang hanya memiliki nilai 2.48.

Gangguan pada sistem yang kadang terjadi merupakan akibat dari serangan virus yang mengacau keberlangsungan operasional perusahaan. Berdasarkan temuan-temuan hasil audit permasalahan virus yang terjadi disebabkan oleh tidak ada pelatihan penggunaan perlindungan virus, tidak dilakukan penyelidikan secara formal tentang keberadaan kelompok data tanpa persetujuan, tidak dilakukan penyelidikan secara formal tentang perubahan tanpa otorisasi, dan kurangnya pengetahuan karyawan tentang virus.

Penggantian-penggantian peralatan sistem informasi sebelum waktunya yang terjadi dan sistem yang sering *erorr*, hardware berdebu merupakan salah satu akibat dari kurangnya pemeliharaan yang dilakukan oleh perusahaaan, kurangnya manajemen kapasitas yang dilakukan, dan pemindahan peralatan yang kurang dimanajemen.

Tabel 4.9 Hasil *Maturity Level* Klausul 11

Klausul	**Deskripsi**	***Marturity Level***
11	Kontrol Akses	3.13
Nilai rata-rata m*arturity level*		3.13

4.2.5 Hasil Penyusunan Daftar Temuan dan Rekomendasi

Penyusunan temuan dan rekomendasi sebagai hasil evaluasi dari pelaksanaan audit sistem informasi ini muncul setelah dilakukan pembandingan antara apa yang seharusnya dilakukan dengan proses yang sedang berlangsung pada perusahaan. Dari hasil temuan tersebut kemudian dilaksanakan rekomendasi yang merupakan rincian temuan serta rekomendasi yang diberikan guna untuk perbaikan proses sistem informasi ke depannya. Salah satu contoh hasil temuan dan rekomendasi pada klausul 11 kontrol akses dengan kontrol keamanan 11.1.1 kontrol masuk fisik dapat dilihat pada Tabel 4.10.

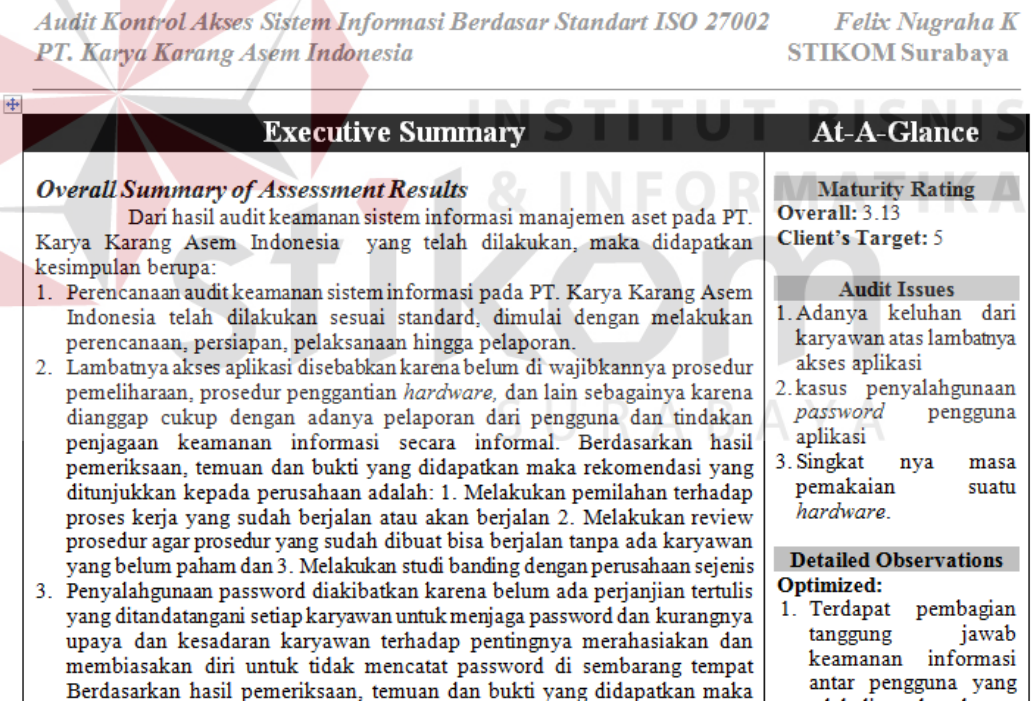
Tabel 4.10 Hasil Temuan Dan Rekomendasi

No	Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
10	11 Kontrol akses	11.1 Persyaratan bisnis untuk kontrol akses.	11.1.1 Kebijakan kontrol akses.	- Terdapat kebijakan dan otorisasi terhadap keamanan informasi namun masih dilakukan secara informal.	- Melakukan *review* dan pemetaan terhadap kondisi di lapangan mengenai kebijakan dan otorisasi keamanan informasi - Mendesain kebijakan dan otorisasi terhadap keamanan informasi - Mendokumentasikan kebijakan dan otorisasi mengenai keamanan informasi.

Hasil pernyataan pada klausul 11 kontrol keamanan yang terdiri dari 11.2.1 sampai dengan 11.6.2 dapat dilihat pada Lampiran 6.

4.3 Tahap Pelaporan Audit Sistem Informasi

Tahap pelaporan yaitu: memberikan laporan audit (*audit report*) sebagai pertanggung jawaban atas penugasan proses audit SI yang dilaksanakan. Laporan audit ditunjukkan kepada pihak yang berhak saja karena laporan audit SI merupakan dokumen yang bersifat rahasia. Hasil laporan audit dapat dilihat Gambar 4.4 dan selengkapnya pada Lampiran 7.



Audit Kontrol Akses Sistem Informasi Berdasar Standart ISO 27002 — *Felix Nugraha K*
PT. Karya Karang Asem Indonesia — STIKOM Surabaya

Executive Summary

Overall Summary of Assessment Results

Dari hasil audit keamanan sistem informasi manajemen aset pada PT. Karya Karang Asem Indonesia yang telah dilakukan, maka didapatkan kesimpulan berupa:

1. Perencanaan audit keamanan sistem informasi pada PT. Karya Karang Asem Indonesia telah dilakukan sesuai standard, dimulai dengan melakukan perencanaan, persiapan, pelaksanaan hingga pelaporan.
2. Lambatnya akses aplikasi disebabkan karena belum di wajibkannya prosedur pemeliharaan, prosedur penggantian *hardware*, dan lain sebagainya karena dianggap cukup dengan adanya pelaporan dari pengguna dan tindakan penjagaan keamanan informasi secara informal. Berdasarkan hasil pemeriksaan, temuan dan bukti yang didapatkan maka rekomendasi yang ditunjukkan kepada perusahaan adalah: 1. Melakukan pemilahan terhadap proses kerja yang sudah berjalan atau akan berjalan 2. Melakukan review prosedur agar prosedur yang sudah dibuat bisa berjalan tanpa ada karyawan yang belum paham dan 3. Melakukan studi banding dengan perusahaan sejenis
3. Penyalahgunaan password diakibatkan karena belum ada perjanjian tertulis yang ditandatangani setiap karyawan untuk menjaga password dan kurangnya upaya dan kesadaran karyawan terhadap pentingnya merahasiakan dan membiasakan diri untuk tidak mencatat password di sembarang tempat Berdasarkan hasil pemeriksaan, temuan dan bukti yang didapatkan maka

At-A-Glance

Maturity Rating
Overall: 3.13
Client's Target: 5

Audit Issues
1. Adanya keluhan dari karyawan atas lambatnya akses aplikasi
2. kasus penyalahgunaan *password* pengguna aplikasi
3. Singkat nya masa pemakaian suatu *hardware*.

Detailed Observations
Optimized:
1. Terdapat pembagian tanggung jawab keamanan informasi antar pengguna yang

Gambar 4.4 Laporan Audit Sistem Informasi