Audit Sistem Keamanan Informasi Departemen *Customer Relation* Pada PT Astra Honda Motor (AHM)

Kukuh Dwi Prasetyo [1], Endang Retnoningsih [1,*], Herlawati [1], Solikin [1]

[1] Sistem Informasi; STMIK Bina Insani; Jl. Siliwangi No.6 Rawa Panjang Bekasi Bekasi Timur 17114 Indonesia, Telp. (021) 824 36 886 / (021) 824 36 996. Fax. (021) 824 009 24; e-mail: kukuh_dwi92@yahoo.com, endang.retnoningsih@binainsani.ac.id, solikin2004@gmail.com , herlawati@binainsani.ac.id

* Korespondensi: e-mail: endang.retnoningsih@binainsani.ac.id

Diterima: 05 Januari 2018; Review: 15 Januari 2018; Disetujui: 2 Februari 2018

Cara sitasi: Prasetyo KD, Retnoningsih E, Herlawati, Solikin. 2018. Audit Sistem Keamanan Data Departemen Customer Relation Pada PT Astra Honda Motor (AHM). Jurnal Mahasiswa Bina Insani. 2 (2): 126 – 135

Abstrak: Setiap perusahaan memerlukan sistem informasi yang cepat, akurat serta tepat pada sasaran, sehingga perusahaan menjadi lebih unggul dalam persaiangan yang ada. Suatu sistem informasi perusahaan mungkin mengandung error. Oleh karena itu, penting ntuk melakukan audit terhadap keamanan informasi untuk menghindari kesalahan. Pelaksanaan audit dilakukan dengan interview, pemeriksaan data, dan uji data. Tujuan penelitian ini adalah untuk mengetahui sistem keamanan data dari PT Astra Honda Motor (AHM) yang berfokus pada Departemen Customer Relations, untuk mengetahui dampak dari resiko apabila terjadi kebocoran data perusahaan dan menilai keamanan data dalam mengakses beberapa data pada PT Astra Honda Motor (AHM). Berdasarkan kegiatan Audit sistem keamanan informasi yang telah dilakukan Ditemukannya kelemahan pada sistem keamanan informasi pada beberapa komputer user di ruangan Departemen *Customer Relation* yang rentan terhadap ancaman keamanan informasi. Hal tersebut menyebabkan timbulnya resiko-resiko seperti penyalahgunaan informasi, kekacauan pada internal perusahaan, dan hilangnya data perusahaan yang akan merugikan PT Astra Honda Motor (AHM).

Kata kunci: audit, kebocoran data, keamanan informasi

Abstract: *Every company needs a fast, accurate and precise information system to the target, so that the company becomes more superior in the existing competition. A company's information system may contain errors. Therefore, it is important to conduct an audit of information security to avoid mistakes. The implementation of the audit is done by interviewing, examining the data, and testing the data. The purpose of this research is to know the data security system from PT Astra Honda Motor (AHM)focusing on Customer Relations Department, to know the impact of risk in case of leakage of company data and to assess data security in accessing some data at PT Astra Honda Motor (AHM). Based on the activity of the audit of the information security system that has been done The discovery of weaknesses in the information security system on some user computers in the Department of Customer Relations room is vulnerable to information security threats. This leads to risks such as misuse of information, internal corporate confusion, and loss of corporate data that would harm PT Astra Honda Motor (AHM).*
Keywords*: audit, data penetration, information security*

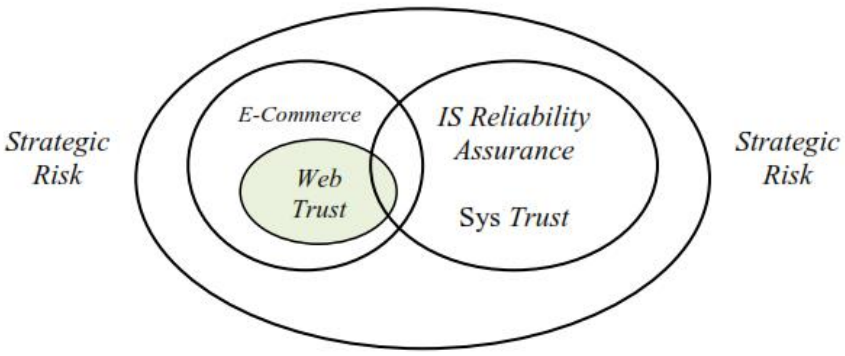
1. Pendahuluan

Setiap perusahaan memerlukan sistem informasi yang cepat, akurat serta tepat pada sasaran. Untuk itu diperlukan sistem informasi yang baik sehingga perusahaan menjadi lebih unggul dalam persaingan yang ada. Suatu sistem informasi perusahaan mungkin mengandung error karena kesalahan atau penyalahgunaan. Salah satu manfaat

 ISSN: 2528-6919 (Online); 126 – 135

komputer dapat mengolah data secara cepat, cermat, akurat, konsisten dan dapat dilakukan secara terus menerus dalam waktu yang relatif tidak terbatas. Namun, penerapan sistem informasi berbasis komputer kadang kala tidak berjalan dengan lancar yang sering kali menimbulkan masalah akibat dari sistem yang tidak terkendali dengan baik. Penting bagi perusahaan untuk melakukan audit terhadap sistem informasi yang mencakup *Security Control, Information Control dan Contunity Control* untuk menghindari kesalahan yang terjadi, sehingga informasi yang dihasilkan dapat mendukung tercapainya tujuan perusahaan. Kesalahan informasi adalah merupakan *information risks* yang dapat mengakibatkan kesalahan dalam perencanaan dan keputusan [Gondodityoto, 2007]. Oleh karena itu, suatu sistem yang baik seharusnya dilengkapi dengan mekanisme kontrol internal *(system of internal control)*. Pada awalnya kontrol internal sangat penting dari sisi manajemen perusahaan, yaitu sebagai sistem yang dapat menjamin dipatuhinya kebijakan perusahaan oleh para pegawai, melindungi aset perusahaan, dan menghindari terjadinya kesalahan dan penyalahgunaan.

Auditing adalah suatu proses yang sistematis untuk memperoleh dan menilai bukti-bukti secara objektif dan mengkomunikasikan hasilnya kepada pighak-pihak yang berkepentingan [Mayangsari and Wandanarum, 2013]. Proses audit secara umum dilakukan oleh ahli yang disebut auditor melalui proses terpadu dalam pengumpulan dan penilaian terhadap informasi sebagai satu kesatuan organisasi. Pelaksanaan program audit dilakukan dengan interview, pemeriksaan data, dan uji data [Hanindito, 2017]. Dalam proses auditing salahsatu dampaknya adalah perubahan cara pandang dari audit tradisional yang berbasis tugas menuju audit Teknologi Informasi berbasis risiko. Tantangan yang dihadapi auditor bagaimana dapat melakukan proses audit dengan efektif dan tepat. Oleh karena itu seorang auditor perlu menyusun strategi sehubungan dengan audit sesuai perkembangan Teknologi Informasi. Secara teknis Teknologi Informasi akan membantu dalam penilaian risiko serta penjaminan yang dilakukan seorang auditor. Peran Teknologi Informasi dalam membantu jasa penjaminan oleh seorang auditor sudah tidak diragukan lagi karena kegiatan bisnis saat ini cenderung menuju ke arah penggunaan Teknologi Informasi [Nugroho, 2011]. Hubungan Teknologi Informasi dengan penjaminan oleh auditor sebagaimana tergambar pada Gambar 1.



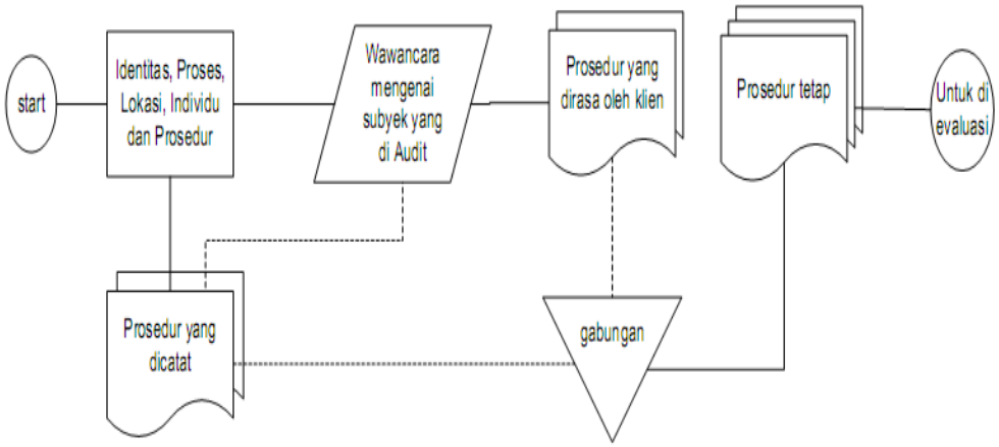
Sumber : Nugroho (2011)

Gambar 1. Hubungan Teknologi Informasi Dengan Penjaminan Auditor

Prioritas utama kebutuhan keamanan informasi perlu dilakukan untuk menjaga keamanan mencakup beberapa prosedur, seperti pengelolaan SDM, pengamanan fisik,

ISSN: 2528-6919 (Online); 126 – 135

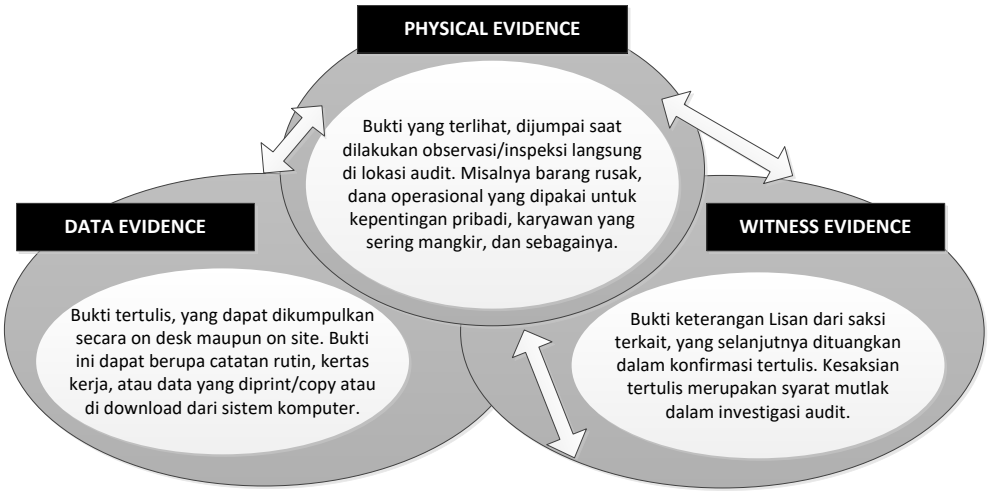
pengamanan operasional teknologi informasi [Kusumajaya et al., 2017]. Maka audit terhadap keamanan data perusahaan juga perlu dilakukan untuk mengetahui pengamanan asset dan menjamin integritas data yang memadai. Penelitian dimaksudkan untuk mengungkap seberapa besar resiko keamanan data pada perusahaan dimana berdampak tidak baik apabila kecurian data sewaktu waktu dapat terjadi dan menyebabkan resiko kerugian terhadap kebocoran data yang keluar dari perusahaan. Tanuwijaya (2010) Agar audit keamanan informasi dapat berjalan dengan baik diperlukan suatu standar untuk melakukan audit tersebut [Afandi and Darmawan, 2015]. Proses pelaksanaan audit sebuah perusahaan umumnya awali dengan mengetahui kondisi perusahaan pada saat ini sesuai pada Gambar 2 [Juliandarini and Handayaningsih, 2013].



Sumber : Juliandarini and Handayaningsih (2013)

Gambar 2. Langkah audit untuk mengetahui kondisi perusahaan

Untuk memenuhi tujuan audit, auditor harus memperoleh bukti dengan kualitas dan jumlah yang mencukupi. Bukti merupakan informasi yang oleh auditor digunakan untuk menentukan apakah informasi yang diaudit sesuai dengan kriteria. Bukti memiliki banyak bentuk antara lain kesaksian lisan dari klien, komunikasi dengan pihak luar, observasi oleh auditor dan data elektronik [Elder et al., 2011]. Keterkaitan antar bukti seperti terlihat pada gambar 3 berikut [Kumaat, 2011]:



Sumber : Kumaat VG (2011)

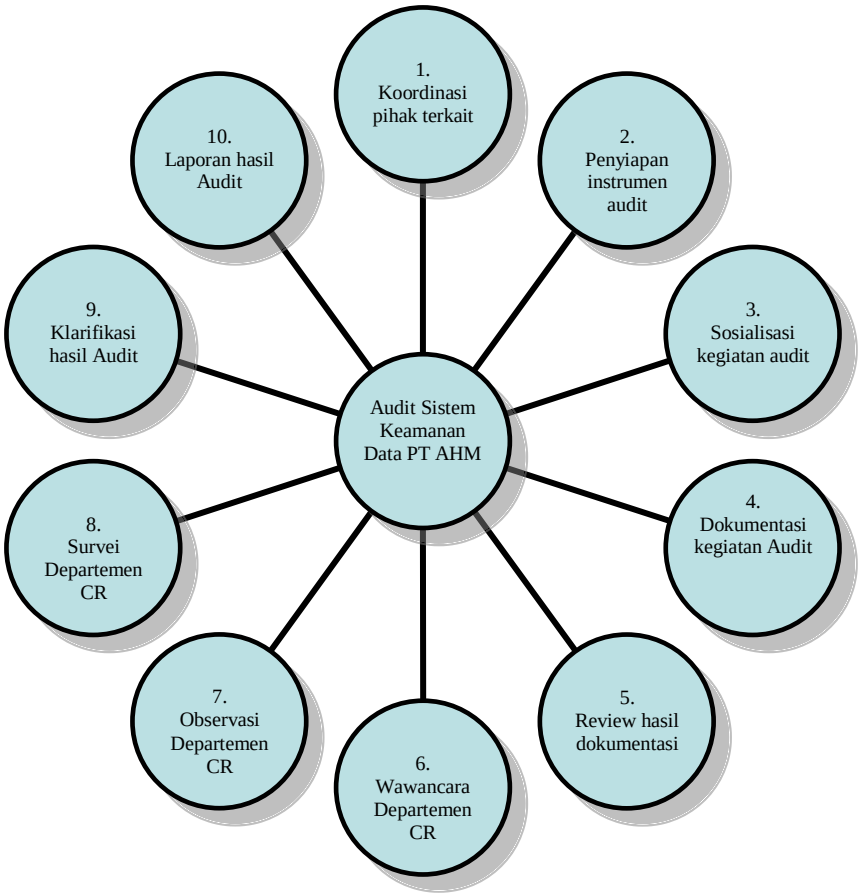
Gambar 3. Hubungan Antara Alat Bukti : Fisik, Data, dan Saksi

 ISSN: 2528-6919 (Online); 126 – 135

Tujuan penelitian ini adalah (1) Untuk mengetahui sistem keamanan informasi dari PT Astra Honda Motor yang berfokus pada Departemen Customer Relations. (2) Untuk mengetahui dampak dari resiko apabila terjadi kebocoran data perusahaan. (3) Untuk memberi masukan kepada pihak perusahaan, agar keamanan data lebih aman dan sesuai dengan SOP yang ada. (4) Menilai keamanan data dalam mengakses beberapa data pada PT Astra Honda Motor.

2. Metode Penelitian

Data yang digunakan dalam penelitian diperoleh dari PT Astra Honda Motor yang beralamat di Jl.Tipar Inspeksi Cakung Drain, Cakung RT.001/RW.009, Cakung Barat Jakarta Timur. Audit sistem informasi dilakukan pada Departemen Customer Relations. Pelaksanaan penelitian dilaksanakan pada bulan 21 Agustus 2017 sampai dengan 18 Oktober 2018, tahapan pelaksanaan audit dapat digambarkan pada alur Gambar 4 berikut:



Sumber : Hasil Penelitian (2017)

Gambar 4. Tahap Pelaksanaan Audit Sistem Keamanan Informasi

Berdasarkan pada Gambar 4 tahapan pelaksanaan audit sistem keamanan data pada Departemen Relation PT PT Astra Honda Motor (AHM) adalah **Pertama,** melakukan Koordinasi dengan Pihak terkait membahas rencana audit yang akan dilakukan yang di lakukan pada tanggal 21 agustus 2017. **Kedua**, menyiapkan instrumen dokumentasi yang berkaitan dengan audit (Lembar kerja, Survei, Wawancara) yang dilakukan pada tanggal 23 agustus 2017. **Ketiga**, melakukan

ISSN: 2528-6919 (Online); 126 – 135

Sosialisasi dengan pihak terkait untuk kegiatan Audit yang akan dilakukan pada tanggal 30 Agustus 2017. **Keempat**,mengumpulkan Dokumentasi berkaitan dengan Audit berupa rencana strategis (Rensa), Rencana kerja (Renja), struktur organisasi dan tata kerja (STOK) dan Standar Operasioanl Prosedur (SOP) yang akan dilakukan pada tanggal 04 September 2017. **Kelima**, Melakukan review terhadap dokumentasi yang berkaitan pada tanggal 11 September 2017. **Keenam**, melakukan Wawancara (interview) dengan pihak IT dilakukan pada tanggal 26 September 2017. **Ketujuh**, melakukan observasi langsung Ke Departemen Customer Relations (CR) pada tanggal 27 September 2017. **Kedelapan**, mengumpulkan data melalui survei yang dibuat untuk diisi oleh IT & Staff Departemen Customer Relations pada tanggal 2 Oktober 2017. **Kesembilan**, melakukan Klarifikasi hasil Audit pada tanggal 10 Oktober 2017. **Kesepuluh**, membuat Laporan hasil audit pada tanggal 18 Oktober 2017.

3. Hasil dan Pembahasan

PT Astra Honda Motor (AHM) sebagai pionir industri sepeda motor di Indonesia. Berdiri sejak 11 Juni 1971 dengan nama PT Federal Motor. Jumlah produksi pada tahun pertama selama satu tahun adalah 1500 unit, kemudian menjadi 30 ribuan dan terus berkembang. Tahun 2001 PT Astra Honda Motor (AHM) berubah nama dari PT Federal Motor dan kepemilikan sahamnya juga digabungkan menjadi satu dari beberapa anak perusahannya. Sekarang PT AHM memiliki 4 pabrik perakitan yaitu Sunter,Kelapa Gading, kawasan MM 2100 Cikarang Barat dan karawang. Prestasi puncak PT AHM antara lain pencapaian produksi 50 juta pada 2015. PT AHM mampu menjawab kebutuhan pelanggan dengan teknologi yang irit BBM dan mesin yang bandel, sehingga menjadi kendaraan roda dua ekonomis.

Berikut pelaksanaan Audit sistem keamanan informasi Departemen Customer Relation Pada PT AHM dilaksanakan sesuai jadwal yang telah di tetapkan.

1. **Koordinasi Pihak Terkait**
   Dalam pelaksanaan audit sistem keamanan informasi, kegiatan pertama melakukan Koordinasi dengan pihak terkait untuk membahas rencana audit yang akan dilakukan mulai tanggal 21 agustus 2017. Agar proses audit menjadi satu bagian yang dapat dipahami, penentuan objek audit sangat diperlukan. Objek Audit pada penelitian adalah Departemen Customer Relation PT AHM, Audit lebih ditekankan pada usaha untuk memperoleh informasi latar belakang tentang objek audit. Setiap aktivitas diselenggarakan setiap departemen harus selaras dengan tujuan perusahaan secara keseluruhan. Pada pelaksanaan Audit beberapa pihak yang akan di audit diantaranya **(1)** Staff Officer **(2)** IT Help Desk **(3)** Manager IT.
2. **Penyiapan Instrumen Audit**
   Instrumen Audit yang digunakan pada penelitian antara lain lembar kerja, survei menggunakan kuesioner dan melakukan wawancara untuk memperoleh informasi yang diperlukan.
3. **Sosialisasi Kegiatan Audit**
   Sosialisai kegiatan Audit dilakukan agar pelaksanaanya tidaak mengganggu proses bisnis sistem yang sedang berjalan pada objek audit. Sosialisasi antara lain dilakukan melalui penetapan jadwal pelaksanaan selama proses Audit berlangsung. Tabel 1 merupakan jadwal rencana pelaksanaan Audit keamanan informasi Departemen Customer Relations PT AHM.

 ISSN: 2528-6919 (Online); 126 – 135

Tabel 1. Jadwal Kegiatan Audit

No	Tanggal	Kegiatan
1	21 Agustus 2017	Melakukan Koordinasi dengan Pihak terkait membahas rencana audit yangakan dilakukan.
2	23 Agustus 2017	Menyiapkan dokumentasi yang berkaitan dengan audit (Lembar kerja, Survei, Wawancara).
3	30 Agustus 2017	Melakukan Sosialisasi dengan pihak terkait untuk kegiatan Audit yang akan dilakukan.
4	04 September 2017	Mengumpulkan Dokumentasi berkaitan dengan Audit yang akan dilakukan diantaranya: Rencana Strategis (Renstra),Rencana Kerja (Renja),Struktur Organisasi dan Tata Kerja (SOTK), Standar Operasional Prosedur (SOP), Pengadaan Aplikasi, Manual Pengguna Aplikasi.
5	11 September 2017	Melakukan review terhadap dokumentasi yang berkaitan.
6	13 September 2017	Melakukan Wawancara (interview) dengan pihak IT.
7	15 September 2017	Melakukan observasi langsung Ke Departemen Customer Relations.
8	19 September 2017	Mengumpulkan data melalui survei yang dibuat untuk diisi oleh IT & Staff Departemen Customer Relations.
9	22 September 2017	Melakukan penilaian tingkat kedewasaan (maturity level) untuk layanan aplikasi yang digunakan.
10	25 September 2017	Melakukan Klarifikasi hasil Audit
11	02 Oktober 2017	Membuat laporan yang berisi: Perencanaan dan persiapan Audit SI/TI yang mencakup ruang lingkup dan tujuan audit (scope dan objective), Kondisi sistem informasi/Aplikasi, Program Audit SI/TI yg dilakukan, Langkah Audit SI/TI yang dilakukan dan bukti (evidence) Audit SI/TI yang dikumpulkan. Temuan audit (findings) dan tingkat maturity Proses TI, Kesimpulan dari hasil temuan, Laporan-laporan lain terkait sebagai hasil dari pekerjaan Audit SI/TI, dan Rekomendasi untuk perbaikan berkelanjutan.

Sumber : Hasil Penelitian (2017)

4. Dokumentasi Kegiatan Audit

Dokumentasi kegiatan Audit pada penelitian dengan mengumpulkan dokumentasi berupa Rencana strategis (Rensa), Rencana kerja (Renja), struktur organisasi dan tata kerja (STOK) dan *Standar Operating Procedure (SOP).* Rensa dan Renja PT AHM sebagaimana tercermin dalam visi dan misi pada PT Astra Honda Motor yaitu PT Astra Honda Motor, perusahaan yang menjalankan fungsi produksi, penjualan dan pelayanan purna jual yang lengkap untuk kepuasan pelanggan. PT AHM berkontribusi kepada masyarakat dengan mampu mewujudkan impian konsumen serta menciptakan kegembiraan konsumen. *Standard Operating Procedure (SOP)* pada PT Astra Honda Motor diharapkan agar data perusahaan yang terdapat pada komputer hanya bisa di akses oleh user yang sudah terdaftar sebagai administrator yaitu TOP manager dan IT. Hal tersebut dikarenakan untuk menjaga keamanan data agar tidak terjadinya kehilangan data secara permanen.

5. Review Hasil Dokumentasi

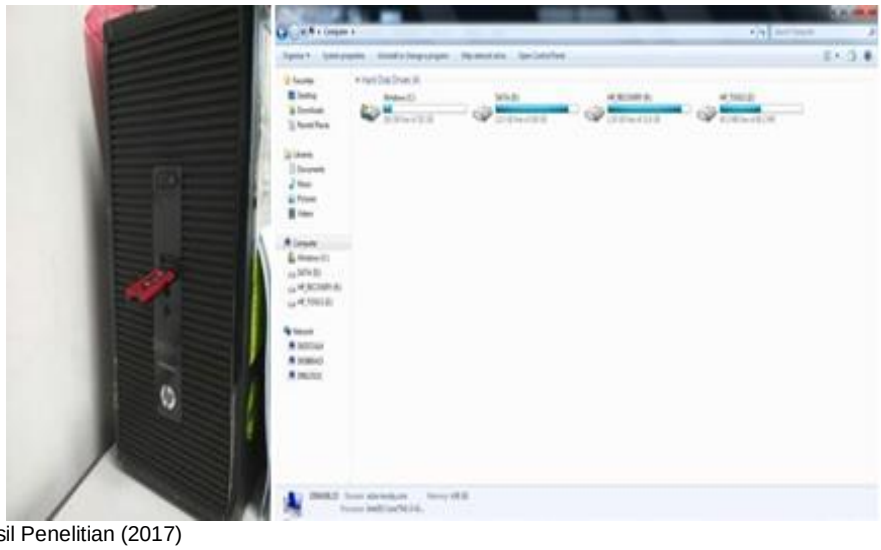
Review hasil dokumentasi merupakan alat pembantu peneliti dalam mengumpulkan data atau informasi dengan cara memperoleh hasil data tersebut dengan melakukan survei langsung ke pihak yang akan diaudit untuk mendapatkan bukti yang benar-benar valid. Berikut adalah data hasil dari review dokumentasi pada ruangan customer relation di PT Astra Honda Motor sebagaimana digambarkan pada Tabel 2.

ISSN: 2528-6919 (Online); 126 – 135

Tabel 2. Hasil Review Dokumentasi

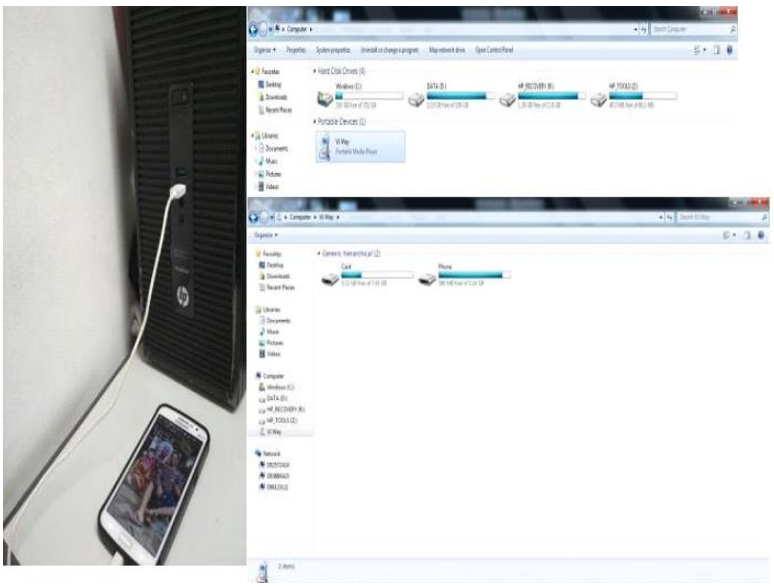
No	Kegiatan	Hasil Temuan
1	Flashdisk dihubungkan ke port USB	Pada tindakan ini tidak ditemukan kelemahan sistem pengamanan data. Karna flashdisk tidak dapat terkoneksi dengan komputer pada ruangan Customer Relation, seperti ditunjukkan pada Gambar 5.
2	Kabel data yang dihubungkan ke handphone dimasukkan ke port USB	Pada tindakan ini ditemukan kelemahan sistem pengamanan data pada komputer. Karna kabel data sebagai penghubung antara handphone dan komputer dapat terkoneksi dengan komputer pada ruangan Customer Relation. Hal ini user dapat melakukan pembackupan data perusahaan melalui komputer, seperti ditunjukkan pada Gambar 6.

Sumber : Hasil Penelitian (2017)



Sumber : Hasil Penelitian (2017)

Gambar 5. Flashdisk dihubungkan ke port USB



Sumber : Hasil Penelitian (2017)

Gambar 6. Flashdisk dihubungkan ke port USB

6. Wawancara Departemen *Customer Relation*

Adapun proses interview yang dilakukan pada Departemen *Customer Relation* terkait dengan pengamanan data adalah sebagai berikut: **(a)** Pada tanggal 12 September 2017 melakukan wawancara secara tidak formal terhadap IT Helpdesk. Hasil dari perbicaraan tersebut bahwa beberapa pertanyaan mengenai sistem yang terdapat pada server IT Helpdesk tidak bisa menjawab dikarenakan bukan wewenangnya. Karena divisi IT terbagi 3 yaitu, IT Server, IT Helpdesk dan IT Second Level yang masing- masing bagian tersebut mempunyai wewenang dan hak aksesnya sendiri. **(b)** Pada tangal 13 September 2017 melakukan pencarian kontak IT Server melalui Call Helpdesk dan mendapatkan nama karywanan IT Server yaitu Bapak Fajar untuk dicari melalui aplikasi chating pada PT AHM. **(c)** Pada tanggal 22 September 2017 tidak dapat berkomunikasi melalui aplikasi chating AHM, sehingga menelpon kembali Call Helpdesk untuk meminta nomer ext. Bapak Fajar IT Server tersebut dan langsung menelponya. **(d)** Pada tanggal 25 September 2017 dapat menghubungi Bapak Fajar melalui telpon ext. dan beliau tidak dapat memberikan info tersebut dikarenakan privaci perusahaan. **(e)** Pada tanggal 26 September 2017 pertanyaan wawancara diubah karena kendala informasi yang tidak bisa didapatkan dan langsung dikonfirmasi kepada Bapak Ridwan selaku IT Helpdesk untuk melakukan wawancara di tanggal 26 September 2017.

7. Observasi Departemen *Customer Relation*

Adapun observasi yang dilakukan secara langsung ke Departemen Customer Relation adalah **(a)** Melakukan pengecekan terhadap 4 komputer sebagai sample. **(b)** Melakukan tindakan pengecekan melalui jalur port USB dengan Flashdisk dan Kabel Data yang di hubungkan ke Handphone. **(c)** Flashdisk dihubungkan ke port USB mendapat notifikasi bahwa flashdisk tidak dapat terkoneksi dengan empat komputer yang diuji coba. **(d)** Kabel data yang dihubungkan ke handphone dimasukkan ke port USB lalu penyimpahan data internal dan eksternal pada handphone dapat terkoneksi dan terbaca pada empat komputer yang diuji coba. Berdasarkan kegiatan yang dilakukan ini diperoleh temuan adanya kelemahan pada empat komputer yang diuji coba tersebut bahwa pada kabel data yang dihubungkan ke handphone dapat mem*backup* data perusahaan yang di akses melalui empat komputer tersebut.

8. Survei Departemen *Customer Relation*

Berikut data hasil survei yang diperoleh dari Departemen Customer Relations seperti pada Tabel 3.

Tabel 3. Hasil Survei Audit

No	Pertanyaan	Jawaban
1	Siapa saja yang mempunyai hak akses untuk masuk ke dalam ruangan server?	IT Server dan Top Manager
2	Adakah informasi dan data yang informasinya sampai keluar perusahaan?	Tidak ada, karena kami menutup akses pada port USByang berfungsi untuk transfer data pada komputer danhak akses internet hanya kepada supervisor dan TOPmanager yang sebelumnya sudah metandatanganiperaturan atau prosedur dan kesepakatan penggunaan internet.
3	Siapa saja yang bertanggung jawab atas data yang tersimpan di server?	IT Server
4	Jika ada trouble pada komputer user siapa	IT Helpdesk dan IT Second Level

ISSN: 2528-6919 (Online); 126 – 135

No	Pertanyaan	Jawaban
	yang berwenang untuk memperbaikinya?	
5	Menurut bapak, apa kelamahan dari keamanan data diperusahaan ini?	Tidak ada
6	Jika server mengalami down, semua akses data akan tertampung dimana?	Server Backup
7	Bisakah komputer user terkoneksi dengan Flashdisk atau Hardisk eksternal?	Tidak Bisa, karna kami menutup akses pada port USB yang berfungsi untuk transfer data pada komputer.
8	Jika terjadi kebocoran data tindakan apa yang bapak lalukan?	Kami akan menelusuri faktor terjadinya kebocoran dataserta langsung menutup akses tersebutdan menindak lanjuti user yang melakukan tindakanpencurian data perusahaan kepada pihak HRD dan kepolisisan.

Sumber : Hasil Penelitian (2017)

9. Klarifikasi Hasil Audit

Temuan audit merupakan bagian dari suatu proses audit kinerja dimana bagian ini memuat pesan pokok yang ingin disampaikan auditor ke pembaca laporan, dan merupakan alasan utama dibuatnya laporan. Hasil dari temuan audit yang telah kami lakukan di PT AHM tepatnya pada bagian Customer Relation adalah Handphone bisa terkoneksi pada komputer hanya dengan menggunakan kabel data sehingga data yang terdapat pada komputer bisa dengan mudah di ambil ataupun di copy. Tujuan dari klarifikasi hasil temuan audit adalah agar PT AHM segera mengambil tindakan yaitu dengan memasang kunci berupa software atau lainnya pada semua komputer yang ada pada departemen Customer Relation di PT AHM.

10. Laporan Hasil Audit

Situasi yang terjadi pada Departemen Customer Relation di PT AHM terkait dari hasil temuan audit tersebut sangatlah membahayakan dimana data yang terdapat pada komputer bisa diambil atau dicopy dengan menggunakan Handphone yang disambungkan ke komputer dengan menggunakan kabel data. Untuk mengetahui penting tidaknya temuan yang diungkapkan, auditor perlu menentukan "akibat" atau kemungkinan akibat yang timbul. Jenis temuan yang ada pada kegiatan audit antara lain: **(a)** Hasil temuan tidak signifikan yaitu tidak disembunyikan atau tidak dilewatkan. **(b)** Hasil temuan kecil yaitu perlu dilaporkan dalam bentuk surat kepada manajemen. **(c)** Hasil temuan besar yaitu dapat menghalangi tujuan utama organisasi. Untuk jenis temuan yang terjadi pada Departemen Customer Relation di PT AHM adalah temuan besar karena dengan kebocoran data yang sudah menyebar ke berbagai media bisa menimbulkan kerugian yang besar baik itu berupa profit maupun nama baik dari perusahaan itu sendiri. Solusi yang diberikan terhadap temuan hasil Audit adalah dengan memasang software pada semua komputer agar pada saat Handphone dihubungkan dengan kabel data tidak dapat terbaca.

4. Kesimpulan

Berdasarkan kegiatan Audit sistem keamanan informasi yang telah dilakukan berikut kesimpulan yang diperoleh yaitu **(a)** Hasil wawancara kepada pihak IT PT Astra Honda Motor terhadap keamanan data tidak sesuai dengan hasil survey audit yang

 ISSN: 2528-6919 (Online); 126 – 135

dilakukan pada ruangan Departemen Customer relation. **(b)** Kurangnya ketelitian pada pihak IT terhadap Standart Operating procedure keamanan sistem yang diterapkan oleh perusahaan. **(c)** Ditemukannya kelemahan pada sistem keamanan informasi pada beberapa komputer user di ruangan Departemen *Customer Relation* yang rentan terhadap ancaman keamanan informasi. Hal tersebut menyebabkan timbulnya resiko-resiko seperti penyalahgunaan informasi, kekacauan pada internal perusahaan, dan hilangnya data perusahaan yang akan merugikan PT Astra Honda Motor (AHM).

Referensi

Afandi H, Darmawan A. 2015. Audit Kemanan Informasi Menggunakan ISO 27002 Pada Data Center PT.Gigipatra Multimedia. Jurnal TIM Darmajaya 01: 175–191.

Elder RJ, Beasley MS, Arens AA, Jusuf AA. 2011. Jasa Audit dan Assurance: Pendekatan Terpadu (Adaptasi Indonesia), Buku 1. Jakarta: Salemba Empat. 5 p.

Gondodityoto S. 2007. Audit Sistem Informasi + Pendekatan CobIT. Jakarta: Mitra Wacana Media.

Hanindito GA. 2017. Analisis dan Audit Sistem Manajemen Keamanan Informasi (SMKI) pada Instansi Perpustakaan dan Arsip Daerah Kota Salatiga. Jurnal Teknologi dan Sistem Informasi. 3: 279–284.

Juliandarini, Handayaningsih S. 2013. Audit Sistem Informasi Pada Digilib Universitas XYZ Menggunakan Kerangka Kerja Cobit 4.0. Jurnal Sarjana Teknik Informatika. 1: 276–286.

Kumaat VG. 2011. Internal Audit. Jakarta: Erlangga. 86 p.

Kusumajaya RA, Sembiring I, Purnomo H. 2017. Audit Internal Keamanan Sistem Informasi Keuangan STEKOM Menggunakan Acunetix Tools Dengan Standart SMKI. Jurnal Teknologi Informasi dan Komunikasi. 8: 39–44.

Mayangsari S, Wandanarum P. 2013. Auditing Pendekatan Sektor Publik dan Privat. Jakarta: Media bangsa. 6 p.

Nugroho MA. 2011. Audit Lingkungan TI: Perspektif Dan Dampak Pada Proses Auditing Secara Komprehensif. J. Pendidik. Akunt. Indones. 9: 24–42.