Audit Keamanan Sistem Informasi Pada Bagian Desktop Management Berdasarkan Standar ISO 27002:2005 di PT. Telkom Divre V Jatim

Dian Ayu Permata[1] **Teguh Sutanto**[2] **Erwin Sutomo**[3]
Program Studi/Jurusan Sistem Informasi
STMIK STIKOM Surabaya
Jl. Raya Kedung Baruk 98 Surabaya, 60298
Email : 1)ayudian00@gmail.com, 2)teguh@stikom.edu, 3)sutomo@stikom.edu

Abstract: Desktop management section PT Telkom Regional Division V East Java has an important role in meeting the needs of employees working facilities . If the process isn't going well , it can hamper the company's business processes . The section hasn't been audited , therefore it is necessary to audit.
Audit conducted by Telkom policy document with numbers: KD.57 / HK-290 / ITS-30/2006 which have been adapted to ISO 27002: 2005. Audit carried out through four stages: planning, preparation, execution, and reporting. Clause used are clauses 8, 9, and 11.
of the audit results, obtained findings on clause 8 are poor employees of company policy, clause 9 namely there emergency exit used to review out access goods and in clause 11 that the co-worker who entrust each password. Recommendations to the findings of clause 8 is added the consequences of the policy document the company in accordance offense, to clause 9 immediately give special procedures so that the emergency exit is used for emergencies only and to clause 11, immediately repair mechanisms to control access to information by making ladder level password security on the application used.

Keywords: Audit, ISO 27002:2005, Information Systems Security, Desktop Management

Perseroan Terbatas Telekomunikasi (PT Telkom) merupakan suatu Badan Usaha Milik Negara (BUMN) yang bergerak dalam bidang jasa telekomunikasi dan telah berdiri sejak tahun 1882. Sebagai hasil restrukturisasi, sejak 1 Juli 1995 organisasi PT Telkom terdiri dari 7 (tujuh) Divisi Regional dan 1 (satu) Divisi Network yang keduanya mengelola bidang usaha utama, profil tersebut menggunakan referensi dari laporan kerja praktek Dian Firda (2011:5). PT Telkom DIVRE V JATIM merupakan salah satu dari 7 (tujuh) Divisi Regional yang terletak di JL. Ketintang no.156 Surabaya. Salah satu aset PT Telkom DIVRE V JATIM adalah *Computer&Network Equipment Management System*(CNEMAS) merupakan aset piranti lunak yang dimiliki oleh bagian *desktop management* di Divisi *Information System Service Support Management* (ISSSM) sejak 5 tahun lalu. Bagian *desktop management* memiliki tugas mendukung kebutuhan di bidang *desktop* dan fasilitas kerja pegawai seluruh Indonesia.

Pada bagian *desktop management* ini belum pernah dilakukan audit sebelumnya dan berdasarkan rekomendasi pihak perusahaan untuk dilakukan audit pada bagian *desktop management*. Apabila proses kerja pada bagian *desktop management* mengalami suatu kendala dikhawatirkan akan berdampak pada proses bisnis perusahaan, karena bagian *desktop* berperan penting dalam mendukung fasilitas kerja pegawai dan pemenuhan kebutuhan di bidang desktop untuk pegawai Telkom di seluruh Indonesia. Apabila terdapat kendala dalam pemenuhan kebutuhan fasilitas kerja para karyawan maka jelas akan menghambat kinerja pegawai Telkom dan merugikan perusahaan dalam hal waktu, dimana seharusnya waktu yang dapat digunakan untuk bekerja tetapi karyawan tersebut tidak dapat bekerja karena mengalami kendala yaitu belum terpenuhi fasilitas kerjanya seperti laptop dan perangkat desktop lainnya. Maka bagian *desktop management* perlu diaudit dan diperkuat oleh dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006 tentang Kebijakan Sekuriti Sistem Informasi untuk menjamin keberlangsungan keamanan sistem informasi. Oleh karena itu bagian *desktop management* membutuhkan evaluasi dan pemeriksaan tentang proses manajemen resiko.

Audit dilakukan dengan menggunakan standar keamanan dari perusahaan yaitu dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor KD. 57/HK-290/ITS-30/2006 tentang Kebijakan Sekuriti Sistem Informasi dan juga menggunakan standar ISO 27002:2005 sebagai standar yang paling baru diterapkan menggantikan standar lama ISO 17799:2005. ISO 27002 menyediakan rekomendasi *best practice* terhadap manajemen keamanan informasi untuk digunakan oleh mereka yang bertanggung jawab untuk proses implementasi, dan pemeliharaan *Information Security Management Systems* (ISMS) pada suatu organisasi.

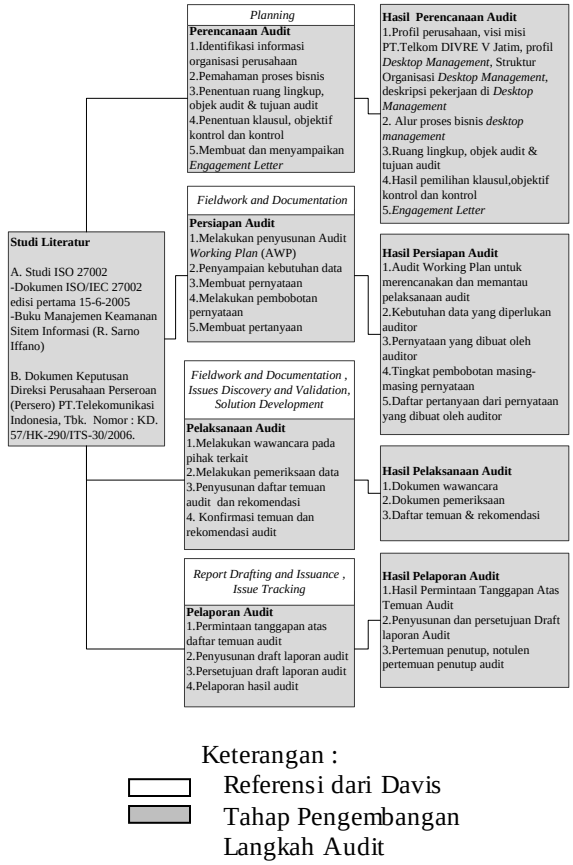
Klausul yang digunakan sebagai acuan untuk melakukan audit keamanan sistem informasi yaitu : Keamanan Sumber Daya Manusia (Klausul 8), Keamanan Fisik dan Lingkungan (Klausul 9), Kontrol Akses (Klausul 11).

METODE PENELITIAN

Tahapan audit keamanan sistem informasi dalam metode penelitian ini dibuat dengan menggunakan gambaran proses audit berdasarkan referensi dari Davis dengan memperhatikan juga referensi dari (Windriya, 2013:35) audit dari Davis dkk (2011:42) dan dikembangkan menjadi beberapa tahap audit seperti pada gambar 1.

Beberapa tahapan tersebut adalah:

1. Tahap Perencanaan Audit Keamanan Sistem Informasi
   a. Pemahaman proses bisnis
   b. Penentuan ruang lingkup, objek audit dan tujuan audit
   c. Penentuan klausul, objektif kontrol dan kontrol
   d. Membuat dan menyampaikan *engagement letter*
2. Tahap Persiapan Audit Keamanan Sistem Informasi
   a. Melakukan penyusunan *audit working plan* (awp)
   b. Penyampaian kebutuhan data
   c. Membuat pernyataan
   d. Melakukan pembobotan pernyataan
   e. Membuat pertanyaan
3. Pelaksanaan Audit Keamanan Sistem Informasi
   a. Melakukan wawancara pada pihak terkait
   b. Melakukan pemeriksaan data
   c. Penyusunan daftar temuan audit dan rekomendasi
   d. Konfirmasi temuan dan rekomendasi audit
4. Pelaporan Audit Keamanan Sitem Informasi
   a. Permintaan tanggapan atas daftar temuan audit
   b. Penyusunan draft laporan audit
   c. Persetujuan draft laporan audit
   Pelaporan hasil audit



Gambar 1. Tahapan – Tahapan dalam Audit Keamanan Sistem Informasi

HASIL DAN PEMBAHASAN

Hasil Identifikasi Informasi Organisasi Perusahaan

Pada perencanaan audit, identifikasi informasi organisasi perusahaan merupakan hal pertama yang harus dilakukan oleh seorang auditor untuk mengetahui seluk beluk

perusahaan sebelum dilakukan audit dengan cara memahami dokumen perusahaan, yaitu profil perusahaan, visi dan misi PT.Telkom DIVRE V Jatim, profil *Desktop Management* PT. Telkom DIVRE V Jatim, struktur organisasi fungsional *Desktop Management* PT. Telkom DIVRE V Jatim dan *Job description* pegawai *Desktop Management* PT. Telkom DIVRE V Jatim,

Hasil pemahaman proses bisnis

Setelah mengidentifikasi informasi organisasi perusahaan maka langkah selanjutnya adalah memahami proses bisnis pada *Desktop Management* dengan mempelajari alur proses bisnis pada bagian tersebut.

Ruang lingkup, objek audit dan tujuan audit

Menentukan ruang lingkup, objek audit dan tujuan audit ditentukan dengan cara melakukan observasi, wawancara dan review pada *Desktop Management*. Adapun hasil dari penentuan ruang lingkup objek audit dan tujuan audit yaitu ruang lingkup yang akan diaudit membahas keadaan fisik dan lingkungan yang terdapat di *Desktop Management*, kepatuhan karyawan terhadap kebijakan yang terdapat di bagian *Desktop Management* dan kontrol akses informasi di *Desktop Management*. Objek auditnya yaitu pada bagian *Desktop Management* di PT. Telkom DIVRE V Jatim. Pemetaan permasalahan dan ruang lingkup audit dapat dilihat pada Tabel 1.

Menentukan Klausul, Objektif Kontrol dan Kontrol

Untuk melakukan audit keamanan sistem informasi, digunakan standar ISO 27002:2005 dan beberapa klausul sebagai acuan dalam pelaksanaan audit.

Berdasarkan beberapa permasalahan dan penetapan ruang lingkup, maka langkah selanjutnya adalah menentukan klausul, objektif kontrol dan kontrol. Adapun dalam menetapkan klausul, objektif kontrol dan kontrol berdasarkan beberapa permasalahan dan ruang lingkup yang telah ditetapkan dan disesuaikan berdasarkan kesepakatan bersama kedua belah pihak. Sehingga hasil yang didapatkan adalah klausul 8 (Keamanan Sumber Daya Manusia), Klausul 9 (Keamanan Fisik dan Lingkungan) dan Klausul 11 (Kontrol Akses). Penentuan ruang lingkup dilakukan dengan cara melakukan observasi, wawancara dan review pada *Desktop Management*. Pemetaan klausul yang digunakan dapat dilihat pada Tabel 2.

Tabel 1. Pemetaan Permasalahan dan Ruang Lingkup Audit Keamanan Sistem Informasi

No.	Indikasi Permasalahan	Ruang Lingkup	Penjelasan
1.	Dicurigai bahwa karyawan mengabaikan kebijakan penggunaan aplikasi dan tidak menjaga akses informasi desktop sebagai mana mestinya	Kepatuhan karyawan terhadap kebijakan perusahaan khususnya untuk penggunaan aplikasi dan kontrol akses terhadap informasi desktop	Berdasarkan indikasi permasalahan ketidak patuhan karyawan tersebut maka ruang lingkup yang harus diaudit adalah keamanan sumber daya manusia yang terdapat di klausul 8. Dan untuk permasalahan menjaga keamanan akses informasi desktop maka ruang lingkup yang harus diaudit adalah kontrol akses yang terdapat di klausul 11.
2.	Dicurigai bahwa lingkungan fisik pada *desktop management* kurang terlindungi dengan optimal	Keadaan Fisik dan Lingkungan yang Terdapat di *Desktop Management*	Berdasarkan indikasi permasalahan kurangnya perlindungan pada lingkungan fisik tersebut maka ruang lingkup yang harus diaudit adalah keamanan fisik dan lingkungan yang terdapat di klausul 9.

Tabel 2. Pemetaan Klausul yang Digunakan

Klausul	Keterangan
8	Keamanan Sumber Daya Manusia
9	Keamanan Fisik dan Lingkungan
11	Kontrol Akses

Membuat *Engagement Letter*

Engagement Letter merupakan surat perjanjian kedua belah pihak antara auditor dengan client sebagai bentuk kesepakatan, definisi tersebut menggunakan referensi dari laporan tugas akhir Yaner (2013:26). Adapun surat perjanjian atau *Engagement Letter* ada pada lampiran 1 dan berisi peran auditor, tujuan auditor, tugas dan tanggung jawab auditor, kewenangan dan kode etik auditor, ruang lingkup auditor, bentuk laporan, akses auditor, pengesahan dan waktu pelaksanaan.

Hasil Pembuatan Pernyataan

Beberapa hasil pernyataan tersebut menggunakan referensi dari Sarno (2009a:310), dan juga standar ISO 27002 yang dikembangkan dan menjadi kalimat pernyataan seperti pada Tabel 3.

Tabel 3. Contoh Pernyataan Pada Klausul 11

PERNYATAAN KLAUSUL 11 (KONTROL AKSES)	
Klausul 11.3 Tanggung Jawab Pengguna (*User Responsibilities*)	
11.3.1 Penggunaan Password (*Password Use*)	
Kontrol : Pengguna seharusnya mengikuti praktek keamanan yang baik dalam pemilihan dan penggunaan password.	
No.	PERNYATAAN
1	Terdapat larangan untuk tidak membagi satu password kepada pengguna lain
2	Terdapat pemilihan password secara berkualitas yang mudah diingat

Dari hasil pembuatan pernyataan yang sesuai standar ISO 27002 tersebut, akan memudahkan untuk membuat pertanyaan saat akan melakukan wawancara audit yang dilakukan oleh auditor.

Hasil Pembobotan Pernyataan

Pembobotan pernyataan digunakan untuk memilih pernyataan yang memiliki peranan cukup penting dan sangat penting dalam proses audit keamanan sistem informasi. Nilai hasil pembobotan didapatkan dari penyebaran angket dan dinilai sendiri oleh pihak auditee seperti yang ada dalam Tabel 4.

Hasil Pembuatan Pertanyaan

Hasil pertanyaan didapatkan dari pernyataan yang sebelumnya telah dibuat berdasarkan standar ISO 27002, dimana beberapa perntanyaan bisa mewakili satu pernyataan untuk pelaksanaan wawancara audit.

Hasil Wawancara Audit

Setelah memilih pernyataan dan membuat beberapa pertanyaan, maka dilakukan proses wawancara audit dengan pihak auditee seperti yang ada pada Tabel 5.

Hasil Pemeriksaan Data

Setiap langkah pemeriksaan yang ada dalam program audit dilaksanakan oleh auditor TI dengan menggunakan satu atau lebih teknik audit yang sesuai dan disertai data /bukti pendukung yang memadai / mencukupi. Wawancara dan observasi dilakukan untuk mendapatkan bukti atau temuan mengenai fakta terkait dengan masalah yang ada. Bukti-bukti tersebut berupa foto, dokumen, rekaman dan data. Contoh dokumen pemeriksaan audit dapat dilihat pada Tabel 6.

Tabel 4. Contoh Pembobotan Pernyataan

HASIL PEMBOBOTAN PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 11 (KONTROL AKSES)		Auditor: Dian Ayu P Auditee: Bpk Setiyobudi (Bagian Off 1Administrasi&Monitoring) Tanggal: 6-7 Mei 2015		
Klausul 11.3 Tanggung Jawab Pengguna (*user*)				
11.3.1 Penggunaan *password* (*Password Use*)				
Kontrol : Pengguna seharusnya mengikuti praktek keamanan yang baik dalam pemilihan dan penggunaan password.				
No	Pernyataan	Bobot		
		Rendah (0,1-0,39)	Cukup (0,4-0,69)	Tinggi (0,7-1,0)
1.	Terdapat larangan untuk tidak membagi satu *password* kepada pengguna lain			1

Tabel 5. Contoh Hasil Wawancara Audit

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 11 (KONTROL AKSES)		Auditor : Dian Ayu Auditee : Bpk Setyobudi Tanggal : 2 Maret – 31 Juli 2015
Klausul 11.3 Tanggung Jawab Pengguna (*user*)		
111.3.1 Penggunaan *password* (*Password Use*)		
1	Terdapat larangan untuk tidak membagi satu password kepada pengguna lain	
	P: Apakah ada larangan agar tidak membagi satu password kepada pengguna lain? J: Iya ada P: Apakah karyawan pernah melakukan penyebaran password individu kepada karyawan lain atau orang lain? J: Pernah, yaitu saling menitipkan password P: Berdasarkan kuesioner terdahulu, apabila sudah ada yang mengatur bahwa tidak diperbolehkan membagi password, lantas mengapa masih ada saja yang melanggar prosedur tersebut pak? J: Kalau sadar akan pentingnya password sudah menyadari namun tingkat kedisiplinan para karyawan yang masih kurang akan hal tersebut	

Tabel 6 Contoh Pemeriksaan Data Audit

PROGRAM PEMERIKSAAN AUDIT KEAMANAN SISTEM INFORMASI ASPEK : KLAUSUL 11 (KONTROL AKSES)			Pemeriksa: Bpk Erwin Sutomo/Bpk Teguh Sutanto Auditor : Dian Ayu P Auditee : Bpk Setyobudi Tanggal : 1 Juni – 30 Juli 2015
Klausul 11.3 Tanggung Jawab Pengguna (*User Respon Sibilities*)			
ISO 27002 11.3.1 Penggunaan *Password*			
No	Pemeriksaan	Catatan Pemeriksa	Catatan Review
1.	Identifikasi mengenai larangan untuk tidak membagi satu password kepada pengguna lain Dengan cara 1. Wawancara 2. Survey	Telah diperiksa bahwa terdapat larangan untuk tidak membagi satu password kepada pengguna lain namun karena tingkat kedisiplinan yang kurang, ada saja karyawan yang melanggar aturan	Tingkat kedisiplinan karyawan untuk menjaga password yang dimiliki masih kurang. Konsekuensi pada karyawan hanya berupa teguran lisan.

PROGRAM PEMERIKSAAN AUDIT KEAMANAN SISTEM INFORMASI ASPEK : KLAUSUL 11 (KONTROL AKSES)			Pemeriksa: Bpk Erwin Sutomo/Bpk Teguh Sutanto Auditor : Dian Ayu P Auditee : Bpk Setyobudi Tanggal : 1 Juni – 30 Juli 2015
Klausul 11.3 Tanggung Jawab Pengguna (*User Respon Sibilities*)			
ISO 27002 11.3.1 Penggunaan *Password*			
No	Pemeriksaan	Catatan Pemeriksa	Catatan Review
		tersebut, yaitu dengan cara saling menitipkan password ke sesama rekan kerja. Sampai saat ini konsekuensinya hanyalah berupa teguran lisan belum ada konsekuensi yang lebih khusus.	

Temuan dan Rekomendasi

Penyusunan temuan dan rekomendasi sebagai hasil evaluasi dari pelaksanaan audit keamanan sistem informasi ini muncul setelah dilakukan pembandingan antara apa yang seharusnya dilakukan dengan proses yang sedang berlangsung pada perusahaan.Contoh temuan dan rekomendasi pada klausul 11 (sebelas) Kontrol Akses dengan kontrol 11.3.1 (penggunaan password) dapat dilihat pada Tabel 7.

Pada klausul 11 (sebelas) Kontrol Akses dengan kontrol 11.3.1 (penggunaan *password*) dalam pernyataan terdapat larangan untuk tidak membagi satu password kepada pengguna lain, terdapat temuan yaitu masih ada karyawan kurang disiplin dalam menjaga passwordnya agar tidak dititipkan ke sesama rekan kerja .

Untuk rekomendasi klausul 11 dengan kontrol 11.3.1 yaitu pihak perusahaan segera memberi konsekuensi khusus untuk karyawan yang salling menitipkan *password* tersebut, dan dibuatkan jenjang level keamanan password pada aplikasi yang digunakan, rekomendasi tersebut menggunakan referensi dari IBISA (2011:45).

Tabel 7. Contoh Temuan dan Rekomendasi

TEMUAN AUDIT KEAMANAN SISTEM INFORMASI			Auditor : Dian Ayu P Auditee : Bpk Setiyobudi (Bagian Off 1 Administrasi & Monitoring)		
ASPEK : KLAUSUL 11 (KONTROL AKSES)			Tanggal : 30 Juni -30 Juli 2015		
No	Pernyataan	Hasil Analisa Wawancara	Temuan	Referensi, Penyebab Risiko dan Rekomendasi	Tanggapan dan Komitmen Penyelesaian
1.	Terdapat larangan untuk tidak membagi satu password kepada pengguna lain	Telah diperiksa bahwa karyawan di larang untuk tidak membagi *password* kepada pengguna lain namun karena tingkat kedisiplinan yang kurang, ada saja karyawan yang melanggar aturan tersebut, yaitu saling menitipkan *password* ke sesama rekan kerja. Sampai saat ini konsekuensinya hanyalah berupa teguran lisan belum ada konsekuensi yang lebih khusus.	Terdapat temuan bahwa tingkat kedisiplinan karyawan untuk menjaga password yang dimiliki masih kurang karena saling menitipkan *password*. Konsekuensi pada karyawan hanya berupa teguran lisan.	Ref Temuan : - Wawancara klausul 11 dengan objektif kontrol 11.3.1 pertanyaan dan jawaban no.4 yang terdapat detailnya di lampiran 7 (Wawancara Audit) Ref Rekomendasi : - ISO 27002 11.3.1 Penggunaan Password - Dokumen Keputusan Direksi Perusahaan Perseroan PT Telekomunikasi Indonesia dengan nomor : KD.57/HK-290/ITS-30/2006 Bab VIII (Kontrol Akses) - (IBISA, 2011:45). IBISA. 2011. *Keamanan Sistem Informasi*. Yogyakarta : Andi. Resiko : Informasi yang seharusnya tidak diketahui oleh yang bukan haknya bisa diketahui dengan mudah dengan adanya saling menitipkan password. Pihak manajemen bisa memberikan sanksi kepada pemilik user-ID dan resiko yang paling fatal ialah pemutusan hubungan kerja dan dituntut secara hukum. Rekomendasi : - Segera merencanakan konsekuensi khusus bagi karyawan yang belum sadar akan pentingnya untuk tidak menyebarkan password dan perusahaan harus konsisten dengan peraturan yang dibuat karena tidak ada gunanya	Tanggapan : Meskipun sudah ada peraturan atau kebijakan mengenai larangan untuk tidak menyebarkan password namun tingkat kedisiplinan dari beberapa karyawan masih ada yang kurang akan hal tersebut Komitmen Penyelesaian : Kami pihak *desktop management* akan mempertimbangkan terlebih dahulu untuk menambahkan konsekuensi di dalam dokumen KD 57 Bab VIII Pasal 34 ayat 4d yang mengatur tentang larangan menyebarluaskan password, karena urusannya langsung kepada yang membuat dokumen kebijakan yaitu pihak Direksi perusahaan.

TEMUAN AUDIT KEAMANAN SISTEM INFORMASI			Auditor : Dian Ayu P Auditee : Bpk Setiyobudi (Bagian Off 1 Administrasi & Monitoring)		
ASPEK : KLAUSUL 11 (KONTROL AKSES)			Tanggal : 30 Juni -30 Juli 2015		
No	Pernyataan	Hasil Analisa Wawancara	Temuan	Referensi, Penyebab Risiko dan Rekomendasi	Tanggapan dan Komitmen Penyelesaian
				peraturan dibuat namun implementasinya masih kurang	Begitu pula dengan penambahan level keamanan passwordnya nanti kami akan mencoba mengusulkan nya ke pihak Unit Pengelola Teknologi Informasi.

SIMPULAN

Berdasarkan hasil audit keamanan sistem informasi yang telah dilakukan maka didapat kesimpulan berupa:

1. Audit keamanan sistem informasi pada bagian *desktop management* di PT Telkom DIVRE V Jatim telah berhasil dilakukan dan didokumentasikan sesuai dengan Audit Working Plan (AWP) berdasarkan standar ISO 27002:2005 dan dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006 tentang Kebijakan Sekuriti Sistem Informasi yang dilakukan dengan menggunakan beberapa klausul yang telah disepakati bersama yaitu Keamanan Sumber Daya Manusia, Keamanan Fisik dan Lingkungan, dan Kontrol Akses
2. Berdasarkan hasil evaluasi keamanan sistem informasi pada bagian *desktop management* terdapat beberapa temuan yaitu adanya ketidak patuhan karyawan terhadap kebijakan perusahaan, penempatan lingkungan fisik yang kurang terlindungi secara optimal seperti adanya pintu darurat yang digunakan untuk akses keluar masuk barang sehingga terkadang pintu darurat tersebut rusak serta adanya rekan kerja yang menitipkan *password* kepada rekan kerja yang memiliki akses informasi yang berbeda
3. Rekomendasi untuk beberapa temuan audit yang tidak sesuai dengan kebijakan perusahaan tersebut yaitu dengan menambahkan konsekuensi yang jelas pada dokumen kebijakan perusahaan bagi karyawan yang tidak patuh, sesuai dengan pelanggaran yang dilakukan. Untuk penempatan lingkungan fisik segera dilakukan perlindungan yang optimal seperti memberi prosedur khusus agar pintu darurat hanya digunakan untuk kondisi darurat saja dan tidak boleh digunakan untuk akses keluar masuk barang agar tidak cepat rusak. Untuk akses informasi yang kurang terlindungi dan kurangnya tingkat kedisiplinan karyawan dalam menjaga *password*, sebaiknya pihak perusahaan segera memperbaiki mekanisme pengendalian akses informasi dengan cara membuat jenjang level keamanan *password* pada aplikasi yang digunakan.

RUJUKAN

Davis, Chris.2007. *IT Auditing Using Controls to Protect Information Assets*. United States of America : The McGraw-Hill Companies.

Dian Firda. 2011. *Analisa Sistem Informasi Penilaian Kinerja Karyawan Pada PT. Telkom, Tbk Sidoarjo*. Stikom Surabaya. Laporan Kerja Praktek.

Direksi Perusahaan Perseroan (Persero) PT. Telekomunikasi Indonesia, Tbk . 2006. *Kebijakan Sekuriti Sistem Informasi*.

Surabaya : PT. Telekomunikasi Indonesia, Tbk

IBISA. 2011. *Keamanan Sistem Informasi*. Yogyakarta : Andi

ISO/IEC 27002. 2005. *Information technology — Security techniques — Code of practice for information security management International*.ISO.

Sarno, R. dan Iffano, I. 2009a. *Sistem Manajemen Keamanan Informasi*. Surabaya: ITS Press.

Windriya, Danastri Rasmona. 2013. *Audit Keamanan Sistem Informasi Pada Instalasi Sistem Informasi Manajemen RSUD Bangil Berdasarkan ISO 27002*. STIKOM Surabaya. Laporan Tugas Akhir STIKOM Surabaya.

Yaner, Annisa Destiara. 2013. *Audit Keamanan Sistem Informasi Pada Instalasi Sistem Informasi Management (SIM-RS) Berdasarkan ISO 27002:2005 (Pada Rumah Sakit Haji Surabaya)*. STIKOM Surabaya. Laporan Tugas Akhir STIKOM Surabaya.