AUDIT KEAMANAN SISTEM INFORMASI PADA BAGIAN SIMDA BERDASARKAN STANDART ISO 27002:2005 DI DINAS PENDAPATAN DAN PENGELOLAAN KEUANGAN DAERAH KABUPATEN LOMBOK BARAT

Riyadi Atmajaya[1)] **Haryanto Tanuwijaya**[2)] **Erwin Sutomo**[3)]
Email : 1)anggagorgo@gmail.com, 2)haryanto@stikom.edu, 3)sutomo@stikom.edu

Abstract: *The revenue and regional financial management (dppkd) one intansi implementing information technology as distributor information in released a report will generate by the revenue and financial management districts of West Lombok. The revenue and regional financial management (dppkd) one intansi implementing information technology as distributor information in released a report will generate by the revenue and financial management districts Of Wes Lombok, One framework used to that the audit it uses iso 27002: 2005 to know the security system information ongoing and methods used to stage the security system audit reference this is cisa , clause and scope used is clause 8 , 9, and 11 . The result of the security audit information system , obtained a list of the findings and recommendations to reduce security risk information from evidence and findings that is to improve security the the information system to the revenue and regional financial management Of West Lombok.*

Keywords: Audit, ISO 27002: 2005, Security of Information Systems, The revenue and regional financial management

Dinas pendapatan dan pengelolaan keuangan daerah (DPPKD) Salah satu intansi yang menerapkan teknologi informasi sebagai penyalur informasi di dalam menerbitkan laporan-laporan yang akan di hasilkan oleh dinas pendapatan dan pengelolaan keuangan daerah kabupaten Lombok Barat. Instansi ini berusaha memberikan pelayanan yang terbaik dengan memanfaatkan teknologi untuk mendukung proses pengelolaan informasi agar cepat dan tepat, khususnya untuk memajukan instansi dalam memahami perkembangan teknologi informasi serta memberikan informasi mengenai terbitnya APBD. Salah satu penunjang pada instansi pemerintah ini adalah sistem informasi keuangan daerah (SIMDA) yang mempunyai program untuk menyediakan data-data mengenai kondisi di daerah yang terpadu

baik dari aspek keuangan, informasi tentang kegiatan – kegiatan yang di laksanakan oleh PEMDA selama satu tahun anggaran dari januari – desember, serta kondisi dari aset daerah, kepegawaian/ aparatur daerah maupun pelayanan publik yang dapat digunakan untuk penilaian kinerja instansi pemerintah daerah, menghasilkan informasi yang komprehensif, tepat dan akurat kepada manajemen pemerintah daerah. Informasi ini dapat digunakan sebagai bahan untuk mengambil keputusan, mempersiapkan aparat daerah untuk mencapai tingkat penguasaan dan pendayagunaan teknologi informasi yang lebih baik dan memperkuat basis pemerintah daerah dalam melaksanakan otonomi daerah. Mengingat pentingnya informasi dalam SIMDA, yang berupa informasi penting mengenai terbitnya atau tersusunnya APBD, pembuatan SPP (surat permintaan pembayaran) dan pencarian dana. Maka kebijakan tentang keamanan informasi harus mencakup hal tentang prosedur pengendalian Hak akses dan dokumen terkait kebijakan keamanan, prosedur pengendalian rekaman, prosedur tindakan perbaikan dan pencegahan terjadianya kerusakan pada lingkungan fisik dan prosedur pemantauan penggunaan fasilitas teknologi informasi.

Adapun kondisi permasalahan yang terjadi di bagian SIMDA khususnya dalam mengakses suatu data yang seharusnya terlindungi, dapat dilihat oleh pegawai lain di bagian yang sama namun sebenarnya pegawai tersebut tidak memiliki akses untuk melihat informasi khusus yang bukan haknya yang akan berdampak pada hilangnya data atau pencurian data yang sangat merugikan DPPKD. Adapun ancaman lain seperti pegawai belum atau tidak memahami aturan dan tanggung jawab keamanan sistem informasi seperti menyalah gunakan *password* yang bisa berdampak kepada kerahasiaan data di DPPKD. Tidak hanya itu dikhawatirkan dapat juga memicu pada terjadinya penyalahgunaan fasilitas informasi yang merugikan DPPKD.

Kurangnya pemeliharaan terhadap fasilitas seperti pemeliharaan terhadap perangkat keras yang ada serta kurangannya pengamanan di lingkungan ruang server dan pemrosesan informasi yang terganggu oleh virus dapat mengganggu sistem yang desadang berjalan seperti halnya komputer sering hang, jaringan akses internet down hal itu dapat menghambat kinerja instansi. DPPKD juga belum memiliki kebijakan atau prosedur mengenai ancaman virus. Ancaman virus itu dapat mengakibatkan gangguan kinerja sistem informasi bahkan dapat menghambat terbitnya informasi penerbitan surat permintaan pembayaran dan pencairan dana. Ancaman seperti ini akan berdampak buruk bagi instansi DPPKD, maka untuk itu diperlukan audit keamanan sistem informasi pada DPPKD agar mampu menjaga asetnya untuk kelangsungan proses bisnisnya, data dan informasi merupakan aset yang penting bagi DPPKD dan butuh penanganan khusus agar terjaga keamanannya. Berdasarkan permasalahan yang ada di DPPKD khususnya bagian SIMDA, maka didapatkan klausul yang digunakan dalam melakukan audit di DPPKD, Klausul yang pertama mengenai keamanan fisik dan lingkungan, Keamanan sumber daya manusia, kontrol akses. Penyusunan tugas akhir ini menggunakan referensi dari standar ISO 27002:2005 sebagai standar internasional dalam melakukan audit keamanan sistem informasi. ISO 27002:2005 ini menyediakan rekomendasi best practice terhadap manajemen keamanan. Dengan menggunakan standart ISO 27002:2005, DPPKD bertujuan untuk mengedintifikasi manajemen resiko terhadap keamanan informasi serta meminimalkan potensi terjadi resiko pada keamanan informasi, penerapan manajemen keamanan informasi pada DPPKD dilakukan untuk mendapatkan temuan yang berpotensi menjadi resiko terhadap keamanan. Dengan adanya penelitian tentang audit keamanan sistem informasi pada DPPKD, maka di harapkan dapat memberikan rekomendasi pebaikan dan kelemahan keamanan informasi yang ada di Dinas Pendapatan Dan Pengelolaan Keuangan Daerah Lombok Barat.

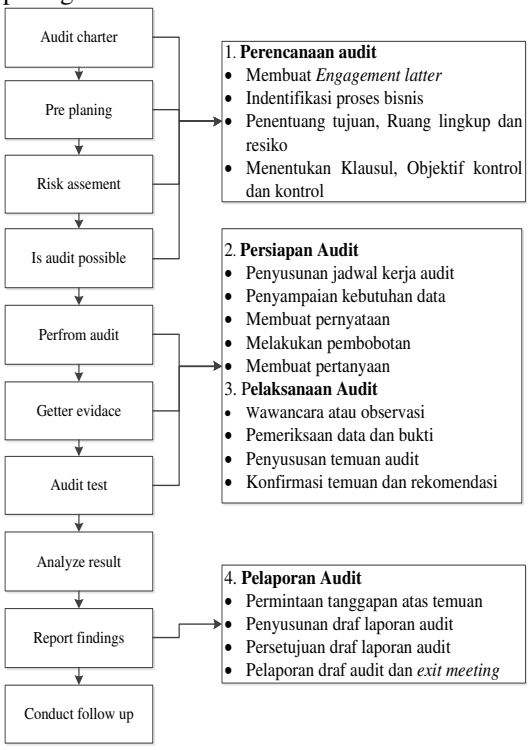
METODE

Metode pelelitian yang saya gunakan dalam audit keamanan sistem informasi ini menggunakan metode (CISA, 2011), dimana terdapat sepuluh (10) tahap yang dilakukan dalam proses audit, yaitu: 1. Membuat dan Mendapatkan Persetujuan Surat Kerjasama, 2. Perencanaan Audit, 3. Analisi Risiko. 4. Kemungkinan Audit, 5. Pelaksanaan Audit, 6. Pemeriksaan Data dan Bukti, 7. Tes Audit, 8. Pemeriksaan Hasil Audet,9. Pelaporan Audit, 10. Penutup/ *Exit Meting*. Dari beberapa tahapan yang terdapat di CISA saya mengelompokan menjadi 4 tahapan.

Tahap pertama, Perencanaan dimana dalam tahapan ini akan membuat *engagement letter*, Identifikasi proses bisnis., Penentuan tujuan ruang lingkup dan resiko., Penentuan klausul., objektif kontrol dan control.

Tahap kedua, Persiapan audit dimana dalam tahapan ini akan menyusun kegiatan yang nantinya dilakukan saat mengaudit seperti., Membuat jadwal kerja Audit,. Menyampaian kebutuhan data, Membuat pernyataan, memberi bobot pada pernyataan, Membuat pertanyaan. Tahap ketiga Pelasanaan audit, Tahapan ini berisi kegiatan- kegiatan seperti, melakukan wawancara serta observasii,. Melakukan pemeriksaan data, menyusun daftar temuan audit dan rekomeandasi, Dan konfirmasi temuan dan rekomendasi audit. Tahapan terakhir adalah tahap pelaporan audit, Dimana tahapan ni berisi: Permintaan tanggapan atas daftar temuan audit., Menyusunan draft laporan audit, Persetujuan draft laporan audit, Melaporan hasil audit.

Hasil gambaran Metode penelitian dapat dlihat pada gambar 1



Gambar 1. Metode Penelitian Audit Keamanan Sistem Informasi

HASIL DAN PEMBAHASAN

Pada proses pembahasan hasil audit ini sebelumnya diperlukan pemahaman proses "bisnis yang sedang berjalan di DPPKD. Hal pertama yang harus dikerjakan seorang auditor agar mengetahui segala hal yang ada di dinas pendapatan dan pengelolalan keuangan lombok barat, sebelum dilakukannya audit hatuslah memahami dokumen instansi.

Keluaran yang di hasilkan pada tahap ini adalah:

a. Profile perusahaan,.
b. Visi, misi, dan prinsip & menejemen,
c. Struktur organisasi,

Setelah itu auditor harus mengetahui dan mempelajari dokumen yang berdada di DPPKD.

Membuat *Engagement Letter*

Engagement Letter merupakan surat perjanjian antara kedua belah pihak auditor dengan klien sebagai bentuk kesepakatan. Definisi ini menggunakan refsensi dari laporan tugas akhir Yaner (2013:26). Adapun surat perjanjian atau *Engagement Letter* berisi peran auditor, tujuan auditor, tugas dan tanggung jawab sebagai auditor, kewenangan dan kode etik auditor, ruang lingkup auditor, bentuk laporan, akses auditor, pengesahan dan waktu pelaksanaan keluaran pada pembuatan surat perjanjian ini atau *enggagement letter* adalah:

1. Pendahuluan
2. Peran Auditor
3. Tujuan
4. Tugas dan Tanggung jawab auditor (*responsiibility*)
5. Kewenangan dan Kode etik
6. Ruang Lingkup
7. Pengesahan dan Waktu Pelaksanaan Audit

Ruang lingkup, objek audit dan tujuan audit

Penentuan ruang lingkup dilakukan dengan cara melakukan observasi, wawancara dan kuesioner pada dinas dppkd. Hasil yang didapat dari penentuan ruang lingkup melalui wawancara dengan pihak dppkd didapatkan hasil dimana masih kurangnya keamanan pada akses aplikasi. Adapun hasil dari penentuan ruang lingkup, yaitu ruang lingkup yang akan diaudit membahas kepatuhan pegawai terhadap kebijakan yang terdapat di DPPKD (klausul 8), keamanan fisik dan lingkungan yang terdapat di bagian DPPKD (klausul 9) dan kontrol akses informasi di DPPKD (klausul 11). Objek auditnya yaitu pada bagian DPPKD Lombok Barat. Keluaran yang dihasilkan pada tahap ini adalah hasil ruang lingkup,.objek audit dan tujuan audit.

Menentukan Klausul, Objektif Kontrol dan Kontrol

Pada proses ini penentuan klausul, haruslah sesuai dengan permasalahan yang ada di dppkd. Berdasarkan beberapa permasalahan yang ada di dinas dppk maka di dapatkan penetapan Klausul, obyektif kontrol dan kontrol yang ditentukan harus berdasarkan kesepakatan antara auditor dengan *auditee*, Keluaran yang dihasilkan pada tahap ini adalah hasil dari pemilihan klausul bisa dilihat pada tabel 1 penentuan klausul.

Tabel 1. Pemilihan Klausul yang Digunakan auditor

Klausul	Deskripsi
8	Keamanan Sumber Daya Manusia
9	Keamanan Fisik dan Lingkungan

11	Kontrol Akses

Membuat Pernyataan

Proses selanjutnya pada tahapan persiapan audit ini dilakukan dengan membuat pernyataan berdasarkan kontrol keamanan yang terdapat pada setiap klausul yang telah ditetapkan berdasarkan standar ISO 27002,. Serta menggunakan refsrensi dari Sarno (2009: 310) keluaran yang dihasilkan pada tahap ini adalah contoh pernyataan pada klausul 8 (delapan) Keamanan Sumber Daya Manusia dengan obyek kontrol 8.1.1 (Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*).

Pernyataan yang berdasarkan standar ISO 270002 digunakan untuk memudahkan auditor sebagai panduan membuat pertanyaan untuk wawancara audit keamanan sistem informasi.

Contoh Pernyataan dapat dilihat pada Tabel 2.

Tabel 2. Pernyataan klausul 8.1.1

PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)	
Klausul 8.1 Keamanan Sumber Daya Manusia Sebelum Menjadi Pegawai (*Prior to Employement*)	
ISO 27002 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)	
Kontrol : Aturan-aturan dan tanggung jawab keamanan dari pegawai, kontraktor dan pengguna pihak ketiga harus didefinisikan, didokumentasikan sesuai dengan kebijakan keamanan informasi organisasi.	
No.	PERNYATAAN
1	Terdapat peraturan pada proses penerimaan pegawai
2	Terdapat dokumentasi kebijakan organisasi aturan dan tanggung jawab penerapan keamanan asset
3	Terdapat dokumentasi kebijakan organisasi aturan dan tanggung jawab pemeliharaan keamanan asset
4	Terdapat prosedur kebijakan tanggung jawab pegawai terhadap perlindungan asset

Setelah membuat pernyataan, tahap selanjutnya adalah melakukan pembobotan pada setiap pernyataan yang telah dibuat. Pada setiap pernyataan yang telah dibuat ini harus ditentukan Nilai bobotnya masing-masing, karena setiap pernyataan tersebut tidak bernilai sama dalam penerapannya untuk kontrol keamanan yang telah ditentukan.Metode ini menggunakan bobot pada penilaian resiko metode kualitatif, karena menurut Sarno dan Iffano (2009: 89) resiko memiliki hubungan dengan keamanan informasi dan resiko merupakan dampak yang ditimbulkan atas terjadinya sesuatu yang mengancam keamanan informasi,. Hasil dari pembobotan pertanyaan dapat dilihat pada Table 3.

Tabel 3. Pembobotan Pernyataan

HASIL PEMBOBOTAN PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 11 (KONTROL AKSES)	Auditor : Riyadi atmajaya
	Auditee: Normansyah, SE
	NIP. 19810921 200501 1 006
	Tanggal: 27 juli 2015
Klausul 11.1 Persyaratan Bisnis Untuk Akses Kontrol	
ISO 27002 11.1.1 Kebijakan kontrol akses	
Kontrol : Suatu kebijakan kontrol akses harus dibuat, didokumentasikan dan dikaji ulang berdasarkan kebutuhan bisnisdan keamanan untuk akses.	

No.	PERNYATAAN	Bobot		
		Rendah (0,1-0,39)	Cukup (0,4-0,69)	Tinggi (0,7-1,0)
1.	Terdapat kebijakan dalam menyebarkan informasi dan otorisasi informasi			0,9

Pertanyaan

Tahap selanjutnya adalah membuat pertanyaaan., Pertanyaan yang dibuat mengacu pada pernyataan- pernyataan yang ada., Dimana satu pernyataan bisa memiliki lebih dari satu pertanyaan,. Hal ini dikarenakan setiap pertanyaan harus mewakili pernyataan pada saat melakukan wawancara untuk mendapatkan pertanyaan yang baik dan mudah dimengerti dibutuhkan pemahaman dari setiap pernyataan.

Wawancara

proses selanjutnya adalah cara atau langkah- langkah yang dilakukan dalam melakukan wawancara. Untuk melakukan wawancara ini auditor harus memahami pernyataan dari klausul yang ada, karena saat wawancara mungkin saja auditee tidak mengerti dari pernyataan yang anda jabarkan serta pertanyaan dari pernyataan yang anda buat. Contoh hasil wawancara dengan *auditee* dapat dilihat pada Tabel 4.

Tabel 4 Hasil Wawancara Audit

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 11 (KONTROL AKSES)	Auditor : Riyadi Atmajaya
	Auditee : Auditee: Normansyah, SE / NIP. 19810921 200501 1 006
	Tanggal : 2 Maret – 31 Juli 2015
	Tanda Tangan :
Klausul 11.5 Kontrol Akses Sistem Operasi (*Operating system access control*)	
ISO 27002 11.5.3 Sistem Manajemen *Password*	
1	Terdapat manajemen password dengan cara memastikan pengguna password individu untuk menjaga tingkat kebenarannya
	P: Apakah manahemen password memastikan pengguna password individu sudah terjaga tingkat kebenarannya? J: Pada umumnya sudah P: Apakah terdapat dokumentasi khusus mengenai manajemen password sehingga dapat menjaga tingkat kebenarannya? J: Tidak terdapat dokumentasi mengenai manajemen password P: Bagaimana mensosialisasikan pentingnya manajemen password individu kepada pengguna sehingga dapat menjaga tingkat kebenarannya? J: Hanya sebatas pemberitahuan lisan

Hasil Pemeriksaan Data

Pada tahap ini 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 mencukupi. Seperti melakukan wawancara dan observasi yang dilakukan untuk mendapatkan bukti,. Dokumen atau temuan mengenai fakta terkait dengan masalah yang ada di dinas pendapatan dan pengelolaan keuangan daerah lombok barat. Bukti-bukti yang didapat berupa foto,dokumen, rekaman dan data. Contoh dokumen pemeriksaan audit dapat dilihat pada Tabel 5.

Table 5 dokumen pemeriksaan audit

PROGRAM PEMERIKSAAN AUDIT KEAMANAN SISTEM INFORMASI ASPEK : KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)	Pemeriksa : Bpk Haryanto Tanuwijaya/Bpk Erwin Sutomo
	Auditor : Riyadi Atmajaya
	Auditee : Dra Sri Muryaningsih
	Tanggal : 29 juli – 21agustus 2015
	Tanda Tangan :
Klausul 8.1 Sebelum Menjadi Pegawai (*Prior to Employment*)	

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 instansi. Dari hasil temuan tersebut kemudian dilaksanakan rekomendasi yang merupakan rincian temuan serta rekomendasi yang diberikan untuk perbaikan proses keamanan sistem informasi ke depannya. Hasil temuan dan rekomendasi dapat dilihat pada tabel 6.

Tabel 6 Temuan dan Rekomendasi

TEMUAN AUDIT KEAMANAN SISTEM INFORMASI				Auditor : Riyadi Atmajaya Auditee : Ikhwania safitri, SE NIP. 19790723 200501 2 017
ASPEK : KLAUSUL 9 (KEAMANAN FISIK DAN LINGKUNGAN)				Tanggal : 27 juli 2015 Tanda Tangan :
No	Pernyataan	Temuan	Referensi, Penyebab Risiko dan Rekomendasi	Tanggapan dan Komitmen Penyelesaian
1.	Akses menuju tempat kerja harus dibatasi hanya untuk pesonil dengan otorisasi.	Tidak terdapat dokumen yang mengatur untuk akses menuju tempat kerja ataupun cctv di ruang kerja/ pemrosesan informasi di DPPKD	Ref : ISO 27002 9.1.1 Pembatas keamanan fisik Resiko : Apabila tidak terdapat cctv di ruang kerja/pemrosesan informasi pada dinas DPPKD, maka kegiatan memonitoring tidak dapat dilakukan untuk para pegawai saat sedang bekerja atau bukan pegawai yang memasuki lingkungan kantor dari dinas pendapatan dan pengelolaan keuangan daerah Lombok barat. Rekomendasi : - Segera merencanakan untuk memasang cctv yang sesuai standar pada umumnya khususnya di ruangan kerja/ arah menuju tempat pemrosesan informasi di DPPKD	Tanggapan : Memang tidak terdapat Cctv di semua ruangan baik diruangan server, jalan menuju ruang server ,ruang pemprosesan informasi serta di tempat menaik turunkan barang tangga menuju gudang Komitmen Penyelesaian : Kami akan mengusulkan untuk segera mengadakan dan memasang cctv di ruangan kerja/pemrosesan informasi yang ada di DPPKD.

SIMPULAN

Audit keamanan sistem informasi pada bagian Simda di DPPKD telah berhasil dilakukan sesuai dengan jadwal kerja audit berdasarkan standar ISO 27002:2005, dan dokumen- dokumen dari pihak instansi dppkd maupun dokumen penunjang lainnya tentang. Tupoksi pegawai yang dilakukan dengan menggunakan beberapa klausul yang telah disepakati oleh pihak auditor dan audiite yaitu klausul 8,9,11. Masih terdapat beberapa ketidaksesuaian dengan kebijakan keamanan informasi yang berlangsung di DPPKD contohnya seperti pengaman di ruang server masih kurang dimana harus terdapat camera pengawas pada ruang server/ pemprosesan informasi dan ada pula informasi yang berada di SIMDA yang seharusnya terlindungi, namuin

dapat dilihat oleh pegawai lain di bagian yang sama yang sebenarnya pegawai tersebut tidak memiliki akses untuk melihat informasi khusus yang bukan haknya. serta Penyalahgunaan *password* disebabkan belum adanya dokumen maupun pernyataan tertulis untuk membuat manajemen *password*, belum terdapat pemberian sanksi bagi pengguna yang melanggar *password* dan masih banyaknya pengguna *password* yang belum memiliki kesadaran untuk menjaga keamanan *password*. Telah disusun hasil audit keamanan sistem informasi pada DPPKD, Harus segera menerapkan kebijakan dan prosedur dalam mengatasi kelemahan yang terdapat pada sisi keamanan sistem informasi yang ada.

SARAN

Beberapa saran yang dapat diberikan untuk pengembangan audit lebih lanjut adalah sebagai berikut:

-Bagian Simda yang berada di DPPKD lombok barat harus melakukan audit keamanan sistem informasi secara berkala agar mengurangi Ancaman dari keamanan informasi setidaknya 1 (satu) tahun sekali.

-Audit keamanan sistem informasi pada bagian Simda ini yang berada Pada dinas pendapatan dan pengelolaan keuangan daerah dapat dikembangkan dengan beberapa keamanan kontrol yang lain pada standar ISO 27002:2005.

DAFTAR PUSTAKA

Gondodiyoto, Sanyoto. 2007. *Audit Sistem Informasi +Pendekatan Cobit.*. Jakarta : Mitra Wacana Media.

ISACA. 2010. *Guide to the Audit of IT Application*. Switzerland : Felice Lutz.

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

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

Sarno, Riyanarto. 2009. *Audit Sistem & Teknologi Informasi*. Surabaya: ITS Press.

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