EVALUASI KEAMANAN INFORMASI BERBASIS ISO 27001 PADA DINAS PENGELOLAAN PENDAPATAN KEUANGAN DAN ASET DAERAH KABUPATEN KARAWANG

Nina Sulistiyowati
Fakultas Ilmu Komputer Universitas Singaperbangsa Karawang
Jl. H.S. Ronggowaluyo Telukjambe Timur Karawang
e-mail: nina.sulistio@unsika.ac.id

Abstrak

Penelitian ini bertujuan untuk mengidentifikasi dan menilai resiko keamanan informasi di DPPKAD, serta memberikan rekomendasi mengenai keamanan informasi yang harus diterapkan. Data yang digunakan dalam penelitian adalah data primer dan sekunder. Metode penelitian dilakukan dengan observasi dan wawancara untuk mengevaluasi dan menganalisa resiko menggunakan ISO 27001. Teknik analisis yang digunakan adalah (1)identifikasi aset (2) identifikasi ancaman dan kelemahan (3) identifikasi kemungkinan terjadi, dan (4) analisa resiko. Hasil analisa resiko menggunakan ISO 27001 menunjukan tingkat resiko yang harus dimitigasi adalah (1) Klausa 8: keamanan sumber daya manusia, (2) Klausa 9: Keamanan fisik dan lingkungan, (3) Klausa 11: kontrol akses, dan (4) Klausa 12: Akuisisi sistem informasi pembangunan dan pemeliharaan. Hasil evaluasi menunjukan bahwa masih banyak aktivitas yang sebaiknya diperbaiki dan diterapkan untuk meningkatkan keamanan informasi di DPPKAD.

Kata kunci: DPPKAD, Keamanan informasi, risk assesment, ISO 27001

PENDAHULUAN

Keamanan teknologi informasi dan komunikasi adalah aset yang sangat penting dan sangat berharga bagi kelangsungan hidup suatu organisasi, bisnis, pertahanan keamanan, keutuhan Negara, Kepercayaan publik atau konsumen, termasuk juga kualitas layanan untuk masyarakat. Suatu kenyataan yang dihadapi pada era globalisasi ini adalah lembaga organisasi dihadapkan pada sejumlah ancaman keamanan informasi dari berbagai sumber.

Salah satu lembaga pemerintah yang menggunakan teknologi sistem informasi adalah Dinas Pengelolaan Pendapatan Keuangan dan Aset Daerah (DPPKAD). Pada dinas ini dukungan informasi sangat penting karena menyangkut kegiatan teknis operasional di bidang pendapatan, pengelolaan keuangan, bagi pembangunan daerah. DPPKAD telah membangun aplikasi yang mendukung pengelolaan keuangan, serta infrastruktur TI yang menjadi hal penting dalam operasional lembaga. Adapun aplikasi yang telah digunakan adalah aplikasi sistem informasi daerah (SIMDA), dan aplikasi Pajak (SISMIOP).

Kontrol keamanan informasi di DPPKAD masih bersifat manual atau asas kepercayaan dengan memberikan hak akses penggunaan aplikasi kepada orang-orang yang diberikan wewenang untuk mengerjakan input data tanpa ada penilaian resiko terlebih dahulu, dan pemilihan strategi untuk meredakan resiko, sehingga kontrol keamanan informasi tidak sepenuhnya berfungsi. Aspek organisasi dan personil belum menjadi perhatian khusus dalam keamanan informasi di DPPKAD sehingga dalam penerapan keamanan informasi belum didukung oleh kebijakan dan prosedur yang jelas. Selain itu, belum adanya rancangan maupun dokumentasi keamanan informasi berdasarkan penilaian resiko keamanan informasi di DPPKAD sehingga kemungkinan dapat meningkatkan ancaman resiko.

Pada penelitian ini akan dilakukan evaluasi keamanan resiko dan menyusun rancangan keamanan informasi berdasarkan penaksiran resiko keamanan informasi dalam pengelolaan resiko. Akan dilakukan evaluasi sejauh mana pengamanan tersebut telah sesuai dengan standar Keamanan informasi ISO 27001 , dan bagaimana hasil evaluasi keadaan keamanan informasi berdasarkan penilaian resiko di DPPKAD.

Maksud yang ingin dicapai dari penelitian ini adalah melakukan evaluasi (*risk evaluation*) untuk mengetahui apakah keamanan yang diterapkan saat ini sudah sesuai dengan standar keamanan ISO/IEC 27001dan memberikan usulan atau rekomendasi mengenai keamanan informasi yang diperlukan untuk menerapkan keamanan sistem informasi. Evaluasi penilaian resiko keamanan difokuskan pada bagian yang menggunakan sistem informasi SIMDA dan SISMIOP yaitu bagian anggaran, bagian aset, bagian akuntansi, dan bagian pajak. Proses analisa resiko dan evaluasi keamanan menggunakan ISO/IEC 27001

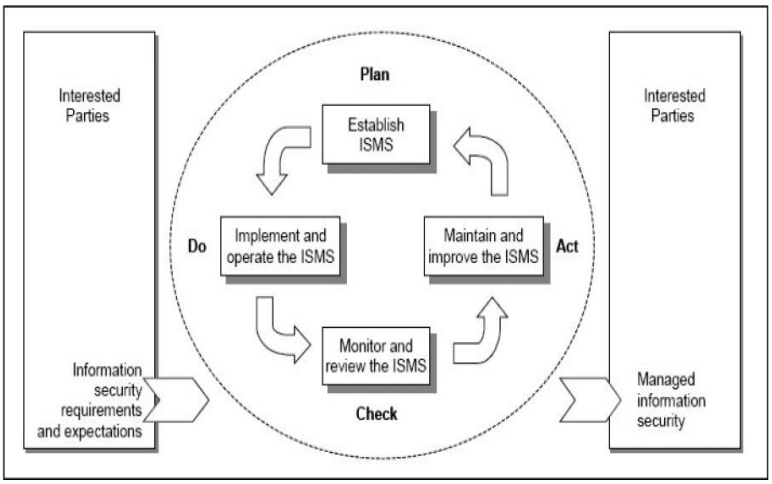
dan Evaluasi keamanan informasi dilakukan berdasarkan kondisi sistem informasi DPPKAD pada tahun 2015.

METODOLOGI PENELITIAN

Metode yang digunakan dalam penelitian ini adalah metode kuantitatif dengan mengkaji bagaimana keadaan keamanan informasi saat ini di DPPKAD apakah sudah sesuai dengan standar ISO 27001 dengan menganalisa resiko keamanan informasi dan dampak resiko keamanan informasi dengan menerapkan model PDCA *(Plan-Do-Check-Act)*.

Dari hasil analisa resiko akan didapatkan hasil kelompok kebutuhan kontrol keamanan yang harus diutamakan. Dari kajian hasil kontrol keamanan tersebut akan didapatkan usulan dan rekomendasi bagaimana sebaiknya kebijakan keamanan informasi yang sebaiknya diterapkan di DPPKAD berdasarkan analisa resiko (*risk analysis), e*valuasi risiko *(risk evaluation),* dan pengurangan resiko *(risk mitigation).*

Pendekatan proses yang didefinisikan dalam ISO/IEC 27001 mengadopsi siklus PDCA (*Plan-Do-Check-Act)*.



Gambar 1 Model PDCA

Secara ringkas model PDCA bisa dijelaskan sebagai berikut :

Plan (Menetapkan ISMS) : Membangun kebijakan, objektif, proses, dan prosedur ISMS yang berhubungan dengan pengelolaan resiko dan peningkatan keamanan informasi untuk memberikan hasil-hasil yang sesuai dengan kebijakan dan objektif yang menyeluruh dari suatu organisasi.

Do(Menerapkan dan mengoperasikan ISMS): Menerapkan dan mengoperasikan kebijakan, kontrol, proses, dan prosedur ISMS.

Check(Memantau dan melakukan tinjau ulang ISMS): Menilai dan, jika dapat dilakukan, mengukur performa proses terhadap kebijakan, objektif, dan pengalaman praktis ISMS dan melaporkan hasilnya ke manajemen sebagai tinjauan.

Act (Memelihara dan meningkatkan ISMS): Mengambil tindakan perbaikan dan pencegahan, berdasarkan hasil audit ISMS internal dan tinjauan manajemen atau informasi lain yang relevan, untuk mencapai peningkatan yang berkesinambungan dari ISMS.

HASIL DAN PEMBAHASAN

Nilai informasi yang dimiliki oleh organisasi dihitung dalam nilai aset dengan menjumlahkan kriteria *Confidentiality*, *Integrity,* dan nilai *Availability* berdasarkan hasil perhitungan kuesio*ne*r. Berikut adalah hasil penilaian aset di DPPKAD.

Perhitungan nilai aset didapatkan dari acuan tabel tabel 2 dengan menghitung nilai *Confidentiality, Integrity, Availability,* dengan menggunakan rumus sebagai berikut :

Nilai Aset (NA) = NC + NI + NV

Dimana : NC = Nilai *Confidentiality*

NI = Nilai *Integrity*

NV = Nilai *Availability*

Tabel 2 Hasil Penilaian Aset di DPPKAD

No	Nama Aset	Lokasi Aset	Penanggung Jawab	C	I	A	Nilai Aset
1	Database Keuangan	Bagian Keuangan	Administrator	3	2	4	9
2	Database Barang	Bagian Aset	Administrator	3	2	2	7
3	Database Gaji	Bagian Anggaran	Administrator	3	2	4	9
4	Database Pajak	Bagian Pajak	Administrator	3	2	4	9
5	Unit Komputer	Seluruh Bagian	Operator	1	3	3	7
6	*Server*	di masing-masing bagian	Operator	3	3	3	9
7	Acess Point	di masing-masing bagian	Operator	1	2	2	5
8	Switch	di masing-masing bagian	Operator	1	2	2	5
9	Router	di masing-masing bagian	Operator	1	2	2	5
10	Printer	di masing-masing bagian	Operator	1	2	2	5
11	*Scanner*	di masing-masing bagian	Operator	1	2	2	5
12	OS	di masing-masing bagian	Operator	2	2	3	7
13	Acess *Control*	Administrator	Administrator	3	3	3	9
14	Air Conditioner	di masing-masing bagian	Operator	0	2	2	4
15	UPS	*Server*	Operator	2	2	2	6
16	Administrator	di masing-masing bagian	Administrator	3	3	3	9
17	Kasubag Keuangan	Bagian Keuangan	Kepala Dinas	2	2	4	8
18	Kasi Pajak	Bagian Pajak	Kepala Dinas	2	2	4	8
19	Kabid Anggaran	Bagian Anggaran	Kepala Dinas	2	2	4	8
20	Kabid Aset	Bagian Aset	Kepala Dinas	2	2	4	8

Tabel 3 Acuan Penilaian Aset

Kriteria	Keterangan	Nilai
Confidentiality	Publik	0
	Pengguna dari dalam	1
	Pribadi	2
	Rahasia	3
	Sangat Rahasia	4
Integrity	Tdk ada dampak	0
	Gangguan kecil	1
	Gangguan umum	2
	Gangguan Besar	3
	Kerusakan yg tdk dpt diterima	4
Availability	Tdk tersedia	0
	Tersedia waktu tertentu	1
	Tersedia	2
	Sangat tersedia	3
	Selalu tersedia	4

Perhitungan nilai aset didapatkan dari acuan tabel tabel 2 dengan menghitung nilai *Confidentiality, Integrity, Availability,* dengan menggunakan rumus sebagai berikut :

Nilai Aset (NA) = NC + NI + NV

Dimana : NC = Nilai *Confidentiality*

NI = Nilai *Integrity*

NV = Nilai *Availability*

Hasil Analisis Resiko

(Identifikasi Ancaman, Kelemahan, Kemungkinan terjadi, dan dampaknya) Analisis risiko dilakukan berdasarkan hasil dari identifikasi kelemahan, ancaman, besar kemungkinan kejadian, dan tingkat dampak yang ditimbulkan. Identifikasi dilakukan berdasarkan hasil temuan-temuan yang telah terjadi di lapangan maupun hasil analisis kemungkinan ancaman yang terjadi. Dari hasil analisis risiko dapat dilihat mana saja risiko yang diterima, dimitigasi, dihindari atau dialihkan. Risiko-risiko yang dimitigasi kemudian akan digunakan sebagai acuan dalam pemilihan kontrol keamanan, berikutnya menghitung nilai dampak yang mungkin terjadi. Hasil analisis risiko, bobot untuk penilaian probabilitas kejadian, dan acuan penilaian dampak dapat dilihat dalam tabel 4 dan 5.

Tabel 4 Bobot Penilaian Probabilitas

Bobot Nilai	Kriteria Probabilitas	Deskripsi
0	Tidak Pernah terjadi	Tidak terjadi selama kurun waktu tiga tahun
1	Terjadi Sesekali	Terjadi sekali dalam kurun waktu tiga tahun
2	Kejadian Berkala	Terjadi sekali dalam kurun waktu tiga bulan
3	Kejadian Reguler	Terjadi sekali dalam kurun waktu dua minggu
4	Kejadian sering	Terjadi sekali dalam kurun waktu seminggu

Tabel 5 Penilaian Skala Impact Analysis

Batas Toleransi Gangguan	Keterangan	Nilai
< dari 1 minggu	*Not Critical*	0 – 20
1 hr s/d 2 hr	*Minor Critical*	21 – 40
< 1 hari	*Mayor Critical*	41 – 60
< 12 jam	*High Critical*	61 – 80
< 1 jam	*Very High Critical*	81 - >=100

Selanjutnya menentukan nilai resiko dengan acuan sebagai berikut :

Tabel 6 Kriteria Penerimaan Resiko

Batas Bawah	Batas Atas	Status
0	30	Risk Acceptance
31	80	Risk Reduction
81	132	Risk Avoidance
133	192	Risk Transfer

Menentukan Nilai Resiko (*Risk Value)* adalah dengan mengalikan nilai aset dengan nilai dampak dan nilai probabilitas.

Risk Value = NA x IA x NP

Dimana :NA = Nilai Aset

IA = *Impact* Analysis (Nilai Dampak)

NP = Nilai Probabilitas

Berikut adalah contoh hasil analisa resiko yang telah disimpulkan dari perhitungan hasil analisa resiko sebelumnya secara rinci. Dapat ditarik kesimpulan resiko yang akan dimitigasi adalah resiko yang memiliki status *risk reduction* dan *risk avoidance*

No	Nama Aset	Ancaman	Kelemahan	Nilai Dampak	Status Dampak
1	SIMDAKeuangan	pencarian ulang dari media didaur ulang/dibuang	Kekurangan pemahaman pada perangkat lunak.	36	Minor Critical
		pemberitahuan rahasia	Tidak 'logout' ketika meninggalkan komputer.	54	Mayor Critical
		Gangguan perangkat lunak	Pembuangan/reuse media penyimpanan tanpa penghapusan yg tpt.	72	High Critical
2	SIMDA Barang	pencarian ulang dari media didaur ulang/dibuang	Kekurangan pemahaman pada perangkat lunak.	56	Mayor Critical
		pemberitahuan rahasia	Tidak 'logout' ketika meninggalkan komputer.	42	Mayor Critical
		Gangguan perangkat lunak	Pembuangan/reuse media penyimpanan tanpa penghapusan yg tpt.	28	Minor Critical
		pencarian ulang dari media didaur ulang/dibuang	Tidak 'logout' ketika meninggalkan komputer.	72	High Critical
		pemberitahuan rahasia	Pembuangan atau pemakaian ulang media	72	High Critical
3	SISMIOP	pencarian ulang dari media didaur ulang/dibuang	Kekurangan pemahaman pada perangkat lunak.	36	Minor Critical
		pemberitahuan rahasia	Pembuangan/reuse media penyimpanan tanpa penghapusan yg tpt.	72	High Critical
		Gangguan perangkat lunak	Kesalahan penempatan hak akses.	36	Minor Critical
4	Unit Komputer	hilangnya pasokan listrik	Kurangnya pemeliharaan / kesalahan instalasi perangkat keras.	21	Minor Critical
6	Administrator	Penyusupan	Ketidakhadiran personel.	72	High Critical
		pencurian media atau dokumen	Prosedur rekrutmen yang tidak memadai.	54	Mayor Critical
		pencurian peralatan	Pelatihan keamanan yang tidak cukup.	54	Mayor Critical
		pencarian ulang dari media didaur ulang/dibuang	Kesalahan penggunaan atas perangkat lunak dan perangkat keras.	27	Minor Critical
		pemberitahuan rahasia	Kurangnya kesadaran akan keamanan.	54	Mayor Critical
		Data dari sumber yang tidak dapat dipercaya	Kurangnya mekanisme pemantauan.	54	Mayor Critical
7	K.Keuangan	pencarian ulang dari media didaur ulang/dibuang	Ketidakhadiran personel.	32	Minor Critical
		pemberitahuan rahasia	Pelatihan keamanan yang tidak cukup.	72	High Critical
		Penyalahgunaan hak	Kurangnya kesadaran akan keamanan.	72	High Critical
			Pelatihan keamanan yang tidak cukup.	72	High Critical
		pencarian ulang dari media didaur ulang/dibuang	Kurangnya kesadaran akan keamanan.	48	Mayor Critical
		pemberitahuan rahasia	Kurangnya mekanisme pemantauan.	32	Minor Critical
		pencarian ulang dari media didaur ulang/dibuang	Pelatihan keamanan yang tidak cukup.	72	High Critical
		pemberitahuan rahasia	Kurangnya kesadaran akan keamanan.	48	Mayor Critical
		Penyalahgunaan hak	Kurangnya mekanisme pemantauan.	32	Minor Critical
8	K.Pajak	pencarian ulang dari media didaur ulang/dibuang	Pelatihan keamanan yang tidak cukup.	48	Mayor Critical
		pemberitahuan rahasia	Kurangnya kesadaran akan keamanan.	32	Minor Critical

Hasil Identifikasi Tingkat Kesiapan

Daftar resiko yang akan dimitigasi menjadi acuan dalam penentuan kontrol keamanan. Resiko yang dimitigasi adalah resiko yang berhubungan dengan teknikal berjalannya sistem informasi sehingga kontrol yang dipilih adalah berdasarkan klausa yang berhubungan dengan teknikal yaitu sebagai berikut :

1. Klausa 8 : Keamanan sumber daya manusia
2. Klausa 9 : Keamanan fisik dan lingkungan
3. Klausa11: Kontrol Akses
4. Klausa12:Akuisisi sistem informasi, pembangunan, dan pemeliharaan

Dari setiap klausa terdiri dari kontrol keamanan dimana setiap kontrol keamanan terdiri dari kontrol yang harus diimplemetasikan oleh DPPKAD. Hasil identifikasi tingkat kesiapan diperoleh berdasarkan hasil kuesi*oner* tingkat kesiapan pada saat pengumpulan data. Dari hasil kuesi*oner* tingkat kesiapan, dapat diketahui nilai tingkat kesiapan dari setiap kontrol keamanan yang harus diimplementasikaan dimana nilai setiap kontrol keamanan ditentukan melalui perkalian jumlah pertanyaan yang bernilai Y atau Dan dengan lima (nilai tingkat kesiapan maksimal) dan kemudian dibagi dengan banyaknya pertanyaan pada kontrol keamanan tersebut. Untuk setiap kontrol keamanan akan dijelaskan kriteria dari nilai yang didapat dari setiap kontrol keamanan. Dari nilai-nilai kontrol keamanan tersebut kemudian dapat ditentukan rata-rata objektif kontrolnya dan nilai rata-rata objektif kontrol kemudian dipakai untuk menentukan nilai tingkat kesiapan klausa tersebut. Hasil identifikasi tingkat kesiapan dan nilai-nilai tersebut dapat dipakai untuk mengetahui apakah pengamanan sistem informasi di DPPKAD sudah sesuai dengan standar ISO/IEC 27001. Dalam penelitian ini tahapan kontrol keamanan tidak dilakukan seperti yang sudah dijelaskan pada bab batasan masalah. Hasil evaluasi analisa resiko digunakan sebagai acuan untuk penyebaran kuesi*oner* pada bagian mana saja *assesment* keamanan informasi akan dilakukan.

KESIMPULAN

Berdasarkan tahapan penelitian yang telah dilakukan dalam evaluasi keamanan menggunakan ISO 27001 di DPPKAD Kabupaten Karawang, maka dapat disimpulkan bahwa penerapan keamanan informasi di Dinas Pendapatan Pengelolaan Keuangan dan Aset Daerah, belum didukung oleh kebijakan dan prosedur yang jelas. Selain itu, belum adanya bagian khusus dalam struktur organisasi yang mengelola masalah keamanan informasi. Selain itu, tidak adanya rancangan maupun dokumentasi keamanan informasi menyebabkan kurangnya kesadaran dan kedisiplinan para pegawai di DPPKAD terhadap masalah keamanan informasi. Selain itu, hasil evaluasi keamanan informasi di Dinas Pendapatan Pengelolaan Keuangan dan Aset Daerah menunjukan bahwa sejauh ini aktivitas-aktivitas yang mendukung terciptanya keamanan informasi sudah dijalankan meskipun masih dalam upaya minimal.

DAFTAR PUSTAKA

Afifa, L. N. (2011, Juni 14-15). ”Usulan Panduan Pelaksanaan Manajemen Resiko Tata Kelola TIK Nasional". Konferensi Teknologi Informasi & Komunikasi untuk Indonesia.

ANSIL. (2007, May 23). 2700x, Roadmap ISO/IEC. *ISMS*. Dipetik Maret 23, 2014, dari http://www.ansil.eu/files/pres-eurosec2007-23052007.pdf

Ariyus, D. (2005). *"Computer Security"*. (R. W. Rosari, Penyunt.) Yogyakarta, Jawa Tengah, Indonesia: ANDI. doi:DDC'21:658.478

Azwar Saifuddin, M. (2003). *"Reliabilitas dan Validitas"* (3rd ed.). Yogyakarta, Jawa Tengah, Indonesia: Pustaka Pelajar.CSI. (2009). *"14th Annual CSI Computer Crime and Security Survey"*.

Darmawi, H. (2006). *"Manajemen Risiko."*. Jakarta: Bumi Aksara.

Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika RI. (2011, September). *"Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik"*. Depkominfo. Jakarta: Direktorat Keamanan Informasi. Dipetik Maret 23, 2014, dari http://publikasi.kominfo.go.id/handle/54323613/119

ESCAP. (2009). "Module 3: Cyber Crime and Security". *Akademi Esensi Teknologi Informasi dan Komunikasi untuk Pimpinan Pemerintahan, III*. Dipetik Maret 23, 2014, dari http://www.unescap.org/icstd/POLICY/publications/internet-use-for-business-development/module3-sources.asp

IBISA. (2011). *"Keamanan Sistem Informasi"* (1 ed.). (T. A. Prabawati, Penyunt.) Yogyakarta, Jawa Tengah, Indonesia: ANDI. doi:DDC'21:658.4

Iffano, R. S. (2009). "Sistem Manajemen Keamanan Informasi". Dalam A. Herdiyanti (Penyunt.), *Sistem Manajemen Keamanan Informasi* (hal. 26). Surabaya: ITS Press. Dipetik 03 2014

ISO 27001:2005. (2014, May 09). *http://www.iso.org/iso/home/standards/management-standards/iso27001.htm*. Diambil kembali dari http://www.iso.org: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

ITGI. (2007). *"Framework Control Objectives Management Guidelines Maturity Models"*. Diambil kembali dari http://www.itgi.org/.

Notoatmodjo. (2002). *"Metodologi Penelitian Kesehatan"*. Jakarta, Jawa Barat, Indonesia: Rineka Cipta.Peltier, T. R. (2005). *"Information Security and Risk Analyse Second Edition"*. Boca Raton: Taylor and Francis Group.

Rahardjo, B. (2005). *"Keamanan Sistem Informasi Berbasis Internet"*. Bandung: PT. Insan Indonesia.

Syafrizal, M. (2010). *" Information Security Managemen System" Sistem Manajemen Keamanan Informasi*.

Tim Direktorat Keamanan Informasi. (2011). *"Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Pelayanan Publik" Sistem Keamanan Sistem Informasi*. Jakarta: Depkominfo.

BIODATA PENULIS

Nina Sulistiyowati, Dosen Tetap di Fakultas Ilmu Komputer Universitas Singaperbangsa Karawang. Mengajar mata kuliah *Computer Security*, Manajemen Proyek, Audit IT. Menyelesaikan pendidikan Strata 1 (S1) Fakultas Teknik Jurusan Teknik Informatika di Universitas Nurtanio Bandung. Menyelesaikan pendidikan Strata 2 (S2) Program Pascasarjana Magister Komputer jurusan Sistem Informasi Bisnis di Sekolah Tinggi Ilmu Komputer LIKMI Bandung.