AUDIT SISTEM INFORMASIDAN PROSEDUR NYA Studi Kasus Audit Teknologi Informasi Kejahatan Di Dunia Perbankan

Yeni susanti

165100114

Fakultas Komputer

yenisusanti.student@umitra.ac.id

Abstract

Audit laporan keuangan (general audit on financial statement audit) ini dilakukan untuk mengetahui tingkat kewajaran laporan keuangan yang disajikan oleh perusahaan (sesuai dengan standar akuntansi keuangan dan tidak ada salah saji materialistis). Audit ini termasuk general audit. Apabila sistem akuntansi perusahaan merupakan sistem berbasis komputer/teknologi informasi, maka perlu dilakukan audit terhadap sistem aplikasi (komputerisasi) akuntansi tersebut atau komponen teknologi informasi (hardware, software, netware, infrastructures, dan bahkan dataware atau data yang ada di database dari sistem informasi akuntansi tersebut.

Kata Kunci : laporan audit keuangan .

A. PENDAHULUAN

Udit Sistem Informasi dan Prosedur

Istilah EDP-Audit (electronic data processing audit), atau computer audit, kini lebih sering disebut dengan audit sistem informasi (information

systems audit). Pada awalnya EDP audit dilakukan hanya dalam rangka audit laporan keuangan.

Dalam perkembangannya kemudian, karena pentingnya dan makin besarnya investasi dalam TI. Organisasi perusahaan makin merasakan perlunya audit operasional terhadap fungsi TI-nya. Maka

secara umum audit sistem informasi dimaksudkan untuk mengevaluasi tingkat kesesuaian antara sistem informasi dengan prosedur bisnis (bisnis processes) perusahaan (atau kebutuhan pengguna, user needs), untuk mengetahui apakah suatu sistem informasi telah didesain dan diimplementasikan secara efektif, efisien, dan ekonomis, memiliki mekanisme pengamanan aset, serta menjamin integritas data yang memadai. Audit SI berbasis teknologi informasi dapat digolongkan dalam tipe atau jenis-jenis pemeriksaan:

- a) Audit laporan keuangan (general audit on financial) Dalam hal ini audit terhadap aspek-aspek teknologi informasi pada suatu sistem informasi. akuntansi berbasis teknologi informasi adalah dilaksanakan dalam rangka audit keuangan.
- b) Audit sistem informasi (SI) sebagai kegiatan tersendiri, terpisah dari pada keuangan. Sebetulnya audit SI pada hakekatnya salah satu dari bentuk audit operasional, tetapi kini lebih dikenal sebagai satu satuan jenis audit tersendiri yang tujuan utamanya lebih untuk meningkatkan IT governance.

Makin Perlunya Audit TI

Audit TI sangat diperlukan karena akuntan yang melakukan audit laporan keuangan harus memahami dan

menguji sistem dan pengendalian internnya, dan dalam rangka memeriksa data akuntansi (substantive test). Selain alasan tersebut, audit TI makin diperlukan sehubungan dengan resiko yang semakin tinggi di bidang sistem berbasis teknologi informasi, yaitu antara lain:

- Resiko penggunaan teknologi secara tidak layak (tidak tepat)
- Kesalahan berantai atau pengulangan kesalahan secara cepat konsisten pada sistem berbasis komputer
- Logika pengolahan salah (dapat menyebabkan kesalahan-kesalahan serius).
- Ketidakmampuan menterjemahkan kebutuhan (sistem tidak sesuai).
- Konsentrasi tanggungjawab, antara lain konsentrasi data pada satu lokasi atau orang-orang TI (khususnya database administrator).
- Kerusakan sistem komunikasi yang dapat berakibat pada proses atau data.
Data input atau informasi bisa saja tidak akurat, kurang mutakhir, palsu.
Ketidakmampuan mengendalikan teknologi.
Praktek pengamanan sistem informasi yang tidak efektif, kurang memadai atau bahkan mungkin tidak direncanakan dengan baik. Penyalahgunaan atau kesalahan pengoperasian atau penggunaan data.
Akses sistem yang tidak terkendali.

Audit Laporan Keuangan

Audit laporan keuangan (general audit on financial statement audit) ini dilakukan untuk mengetahui tingkat kewajaran laporan keuangan yang disajikan oleh perusahaan (sesuai dengan standar akuntansi keuangan dan tidak ada salah saji materialistis). Audit ini termasuk general audit. Apabila sistem akuntansi perusahaan merupakan sistem berbasis komputer/teknologi informasi, maka perlu dilakukan audit terhadap sistem aplikasi (komputerisasi) akuntansi tersebut atau komponen teknologi informasi (hardware, software, netware, infrastructures, dan bahkan dataware atau data yang ada di database dari sistem informasi akuntansi tersebut).

Pemeriksaan TI khususnya untuk memahami/menguji struktur pengendalian intern klien (sebagaimana diwajibkan dalam standar pemeriksaan akuntan publik) dan dalam rangka pengujian substantif (atas transaksi serta terhadap saldo akun).

Pemeriksaan/audit laporan keuangan terdiri dari dua tahap, yaitu (a) audit pengendalian (test of controls), yaitu memeriksa apakah proses dan program komputer sudah betul, memeriksa apakah pengendalian sistem memadai, dan apakah pengendalian aplikasi sudah cukup baik. Sedangkan pemeriksaan tahap

berikutnya (b) adalah audit terhadap data substantif untuk mengakses data akuntansi yang ada di dalam file/media komputer, misalnya yaitu penjualan, nilai piutang, dan sebagainya.

Audit Around the Computer

Dalam pendekatan audit di sekitar komputer, auditor (dalam hal ini harus akuntan yang registered, dan bersertifikasi akuntan publik) dapat mengambil kesimpulan dan merumuskan opini dengan hanya menelaah struktur pengendalian dan melaksanakan pengujian transaksi dan prosedur verifikasi saldo perkiraan dengan cara sama seperti pada sistem akuntansi manual. Kunci pendekatan audit ini ialah pada penelusuran transaksi terpilih mulai dari dokumen sumber sampai ke bagan-perkiraan (akun) dan laporannya. Keunggulan metode audit di sekitar komputer adalah:

- Pelaksanaan audit lebih sederhana.
- Auditor yang memiliki pengetahuan minimal di bidang komputer dapat dilatih dengan mudah untuk melaksanakan audit.
- Kelemahannya adalah jika kondisi (user requirements) berubah, mungkin sistem itupun perlu diredesain dan perlu penyesuaian (update) program-program, bahkan

mungkin struktur data/file, sehingga auditor perlu menilai/menelaah ulang apakah sistem masih berjalan dengan baik.

Audit Through the Computer

Dalam pendekatan audit ke sistem komputer (audit through the computer) auditor melakukan pemeriksaan langsung terhadap program-program dan file-file komputer pada audit SI berbasis TI. Auditor menggunakan komputer (software) atau dengan cek logika atau listing program (desk test on logic or programs source code) untuk menguji logika program dalam rangka pengujian pengendalian yang ada pada komputer. Selain itu auditor juga dapat meminta penjelasan dari para teknisi komputer mengenai spesifikasi sistem dan/atau program yang diaudit. Keunggulan pendekatan audit dengan pemeriksaan sistem komputerisasi, ialah:

- (a) Auditor memperoleh kemampuan yang besar dan efektif dalam melakukan pengujian terhadap sistem komputer.
- (b) Auditor akan merasa lebih yakin terhadap kebenaran hasil kerjanya.
- (c) Auditor dapat menilai kemampuan sistem komputer tersebut untuk menghadapi perubahan lingkungan. Sebetulnya mungkin tidak dapat dikatakan sebagai suatu kelemahan dalam pendekatan

audit ini, namun jelas bahwa audit through the computer memerlukan tenaga ahli auditor yang terampil dalam pengetahuan teknologi informasi dan mungkin perlu biaya yang besar pula.

Audit with the Computer

Audit dengan komputer untuk kegiatan pendukung dan administrasi paling sering digunakan, bahkan meskipun sistem klien yang diaudit telah berbasis komputer. Selain untuk kegiatan administratif, penyusunan program audit dan kuesioner serta pencatatan-pencatatan dan pelaporan hasil audit, komputer biasanya juga digunakan oleh auditor atau pegawai perusahaan klien untuk melakukan analisis atau pengiktisaran, pembuatan grafik dan tabel-tabel tentang hasil audit, sertapemaparan atau presentasi hasil audit (misalnya dengan Microsoft Word, PowerPoint, dan Excel).

Prosedur Audit Keuangan (TI)

- a) Perencanaan audit (Audit Planning)
Langkah pertama dalam perencanaan audit adalah untuk menetapkan ruang lingkup dan tujuan pemeriksaan. Pada audit laporan keuangan, pemeriksaan dilakukan oleh editor (akuntan) ekstern dan independen terhadap laporan keuangan perusahaan, ditujukan kepada para pemegang saham pihak lain terkait. Tujuan audit untuk

menilai kelayakan atau kewajaran (fairness) laporan keuangan yang disajikan oleh perusahaan.

b) Pemahaman sistem dan struktur pengendalian internnya
Pada tahap ini yang dilakukan adalah pemahaman terhadap sasaran yang akan diaudit, pengumpulan informasi awal, dan identifikasi resiko, antara lain:

- Pemahaman sistem informasi untuk pelaksanaan transaksi
- Penentuan kemungkinan salah saji dalam tiap tahap pelaksanaan transaksi
- Penentuan aktivitas pengendalian untuk deteksi salah saji.
- Penentuan prosedur audit untuk deteksi efektivitas aktivitas pengendalian
Penyusunan program audit pengendalian

c) Pengumpulan bukti audit
Bukti audit dikumpulkan dengan sejumlah instrumen audit, pengujian, dan prosedur yang bermacam-macam

d) Evaluasi bukti pemeriksaan
Setelah bukti-bukti audit dikumpulkan, auditor mengevaluasi bukti audit tersebut sesuai dengan tujuan dari audit dan kemudian:

- Dilakukan tests of controls yang bertujuan untuk mengetahui apakah pengendalian yang ada telah

dilakukan dengan prosedur yang telah ditetapkan.

- Dilakukan substantive test, yang terdiri dari:
 - a. Tests of transactions yang bertujuan untuk mengevaluasi apakah terdapat kekeliruan atau kesalahan
 - b. Tests of balances or overall results yang bertujuan untuk menjamin laporan keuangan yang dihasilkan adalah benar dan akurat
 - e) Komunikasi hasil pemeriksaan
Segera setelah pekerjaan pemeriksaan diselesaikan dan diperoleh kesimpulan pendapat auditor, perlu disiapkan laporan hasil audit mengenai temuan-temuan dan rekomendasi-rekomendasinya. Dalam penyelesaian audit (completion of the audit) dibuat kesimpulan dan rekomendasi untuk dikomunikasikan pada manajemen.

Tujuan Audit SI

- a) Pengamanan aset
Aset informasi suatu perusahaan seperti perangkat keras (hardware), perangkat lunak (software), sumber daya manusia, dan data harus dijaga dengan sistem pengendalian intern yang baik agar tidak ada penyalahgunaan aset perusahaan.
- b) Efektifitas sistem
Efektifitas sistem informasi perusahaan memiliki peranan penting dalam proses pengambilan keputusan. Suatu sistem informasi dapat

dikatakan efektif bila sistem informasi tersebut sudah dirancang dengan benar (doing the right thing), telah sesuai dengan kebutuhan user. Informasi yang dibutuhkan oleh para manajer dapat dipenuhi dengan baik.

c) Efisiensi sistem

Efisiensi menjadi sangat penting ketika sumber daya kapasitasnya terbatas. Jika cara kerja dari sistem aplikasi komputer menurun maka pihak manajemen harus mengevaluasi apakah efisiensi sistem masih memadai atau harus menambah sumber daya, karena suatu sistem dapat dikatakan efisien jika sistem informasi dapat memenuhi kebutuhan user dengan sumber daya informasi yang minimal. Cara kerja sistem benar (doing thing right).

d) Ketersediaan (Availability)

Berhubungan dengan ketersediaan dukungan/layanan teknologi informasi (TI). TI hendaknya dapat mendukung secara kontinyu terhadap proses bisnis kegiatan perusahaan. Makin sering terjadi gangguan (system down) maka berarti tingkat ketersediaan sistem rendah.

e) Kerahasiaan (Confidentiality)

Fokusnya ialah pada proteksi terhadap informasi dan supaya terlindungi dari akses dari pihak yang tidak berwenang.

f) Keandalan (Reliability)

Berhubungan dengan kesesuaian dan keakuratan bagi manajemen dalam pengolahan organisasi, pelaporan dan pertanggungjawaban.

g) Menjaga integritas data
Integritas data (data integrity) adalah salah satu konsep dasar sistem informasi. Data memiliki atribut-atribut seperti kelengkapan kebenaran dan keakuratan.

Perlunya kontrol dan audit

Faktor-faktor yang mendorong pentingnya kontrol dan audit SI adalah antara lain untuk:

a) Mendeteksi agar komputer tidak dikelola secara kurang terarah

b) Mendeteksi resiko pengambilan keputusan yang salah akibat informasi hasil proses sistem komputerisasi salah/lambat/tidak lengkap

c) Menjaga aset perusahaan karena nilai hardware, software dan dan personil lazimnya tinggi

d) Mendeteksi resiko error komputer

e) Mendeteksi resiko penyalahgunaan komputer (fraud)

f) Menjaga kerahasiaan

g) Meningkatkan pengendalian evolusi penggunaan komputer

Tahapan Audit

a) Subjek Audit

Tentukan/identifikasi unit/lokasi yang diaudit

b) Sasaran audit

Tentukan sistem secara spesifik, fungsi atau unit organisasi yang akan diperiksa

c) Jangkauan audit

Identifikasi sistem secara spesifik, fungsi atau unit organisasi untuk dimasukkan lingkup pemeriksaan.

d) Rencana pre-audit

1. Identifikasi kebutuhan keahlian teknik dan sumber daya yang diperlukan untuk audit

2. Identifikasi sumber bukti untuk tes atau review seperti fungsi flowchart, kebijakan, standard prosedur dan kertas kerja audit sebelumnya.

e) Prosedur audit dan langkah-langkah pengumpulan bukti audit

1. Identifikasi dan pilih pendekatan audit untuk memeriksa dan menguji pengendalian intern

2. Identifikasi daftar individu untuk interview

3. Identifikasi dan menghasilkan kebijakan yang berhubungan dengan bagian, standar dan pedoman untuk interview

4. Mengembangkan instrumen audit dan metodologi pengujian dan pemeriksaan kontrol internal

f) Prosedur untuk evaluasi

1. Organisasi sesuai kondisi dan situasi

2. Identifikasi prosedur evaluasi atas tes efektifitas dan efisiensi sistem, evaluasi kekuatan dari dokumen, kebijakan dan prosedur yang diaudit

g) Laporan hasil audit
Siapkan laporan yang objektif, konstruktif (bersifat membangun) dan menampung penjelasan audit.

Pendekatan Audit Berbasis Resiko

a) Mengumpulkan rencana dan informasi

Pemahaman proses bisnis, pengendalian resiko, hasil audit tahun sebelumnya, penaksiran resiko bawaan, dan informasi terakhir

b) Mendapatkan pengertian internal control

Pahami lingkungan pengendalian, penaksiran resiko, kontrol internal yang sudah ada, penaksiran resiko deteksi

c) Melakukan tes ketaatan
Pengujian pelaksanaan kebijakan dan prosedur, pemisahan tugas dan fungsi, dan sebagainya

d) Melakukan test substantif
Prosedur analitis, kebijakan audit substantif lainnya, pengujian atas keandalan dan keseimbangan laporan unit operasional (departemen)

e) Menyelesaikan audit
Menyusun temuan/rekomendasi, menyampaikan laporan hasil audit.

Teknik Penaksiran Resiko

Ada beberapa metode untuk melakukan penilaian resiko, yaitu:

a) Pendekatan penaksiran dengan sistem scoring sistem

- Pendekatan ini digunakan dengan mengutamakan audit berdasarkan pada evaluasi faktor-faktor resiko
- b) Penilaian resiko secara judgemental
Yaitu keputusan dibuat berdasarkan pengetahuan bisnis, instruksi manajemen eksekutif, sejarah kehilangan, tujuan bisnis dan faktor-faktor lingkungan.
- c) Teknik kombinasi.

B. PEMBAHASAN / STUDI KASUS

Studi Kasus Audit Teknologi Informasi Kejahatan Di Dunia Perbankan

JAKARTA – Masyarakat resah melihat kasus pembobolan dana nasabah di bank yang intensitasnya meningkat sejak awal 2011. Kasus-kasus yang terjadi dalam rentang waktu berdekatan ini pun berdampak pada makin kurangnya kepercayaan publik terhadap perbankan.

Dengan begitu, pengamat perbankan Mirza Adityaswara mengatakan, masyarakat akan lebih berhati-hati menggunakan layanan perbankan setelah mencuatnya kasus-kasus yang terjadi. “Masyarakat yang semula kurang awas, akan lebih waspada,” katanya, Ahad (2/5).

Mirza berpendapat sistem perbankan yang ada saat ini memang belum sempurna. Ini, jelas dia, bukan hanya terlihat dari sisi pegawai bank, melainkan juga nasabah. “Jangan tergoda melakukan penyelewengan,” katanya.

Tony Prasetyantono, pengamat perbankan, mengatakan berkurangnya kepercayaan publik pasti akan terjadi menyusul berbagai kasus tersebut. Namun, nasabah belum sampai pada satu tindakan menarik uangnya besar-besaran. Karena, jelas Tony, nasabah tidak memiliki pilihan lain yang lebih baik untuk menempatkan uangnya.

Sejauh ini, ujar Tony, bank masih dinilai sebagai tempat terbaik menyimpan aset. “Apalagi yang bersifat likuid, seperti rekening giro dan tabungan,” katanya. “Namun, nasabah akan lebih selektif memilih bank.”

Nasabah, lanjut dia, juga akan lebih memantau rekeningnya agar luput dari pembobolan. Tony menilai, kejahatan perbankan yang terjadi belakangan lebih mengarah pada kesalahan kolektif. Penyebabnya, ia menjelaskan, muncul dari sisi perbankan, nasabah, Bank Indonesia, maupun aturan hukumnya.

Tony mencontohkan, bank kerap menyembunyikan penyimpangan karena takut reputasinya rusak, sedangkan nasabah tidak aktif memantau rekening miliknya. Sementara, BI memiliki keterbatasan dalam memantau banyaknya perbankan yang ada di Tanah Air. “Hukuman terhadap pelaku fraud juga kurang maksimal sehingga kurang menimbulkan efek jera,” jelasnya.

Saat ini, Direktorat Kriminal Khusus (Ditkrimsus) Polda Metro Jaya sedang menangani sembilan kasus perbankan sejak Januari 2011. Bulan lalu, dana deposito milik PT Elnusa Rp 111

miliar di Bank Mega dicairkan tanpa seizin manajemen perusahaan tersebut dengan pelaku melibatkan orang dalam bank. Sebelumnya, simpanan nasabah prioritas Citibank dibobol oleh karyawan bank asing tersebut yang bernama Inong Malinda alias Malinda Dee.

Kepala Bidang Humas Polda Metro Jaya Kombes Baharudin Djafar mengatakan, kasus pembobolan bank tak ha-nya terjadi di bank swasta. Menurutnya, akhir pekan lalu, bank milik negara pun tak luput dari jaran oknum pegawainya yang nakal. Dari sembilan kasus perbankan itu, polisi berhasil menangkap 30 tersangkanya.

Kasat Fiskal, Moneter, dan Devisa Ditkrimsus Polda Metro Jaya AKBP Arismunandar menambahkan, kasus pembobolan dana perbankan biasanya melibatkan orang dalam bank. Sementara itu, Corporate Secretary BSB, Evi Yulia Kurniawati, mengatakan pihaknya menjalankan tata tertib sesuai standar dan memperketat kontrol internal agar terhindar dari kejahatan perbankan.

C. ID SECURITY

QWTD4452377-ASP-5244107

D. KESIMPULAN

Istilah EDP-Audit (electronic data processing audit), atau computer audit, kini lebih sering disebut dengan audit sistem informasi (information systems audit). Pada awalnya EDP audit dilakukan hanya dalam rangka audit laporan keuangan. Perencanaan audit (Audit Planning)

Langkah pertama dalam perencanaan audit adalah untuk menetapkan ruang lingkup dan tujuan pemeriksaan. Pada audit laoran keuangan, pemeriksaan dilakukan oleh editor (akuntan) ekstern dan independen terhadap laporan keuangan perusahaan, ditujukan kepada para pemegang saham pihak lain terkait. Tujuan audit untuk menilai kelayakan atau kewajaran (fairness) laporan keuangan yang disajikan oleh perusahaan.

Pemahaman sistem dan struktur pengendalian internnya Pada tahap ini yang dilakukan adalah pemahaman terhadap sasaran yang akan ddiaudit, pengumpulan informasi awal, dan identifikasi resiko

E. DISKUSI

Saya bersama teman saya bernama Alkha mendiskusikan tentang prosedur audit sistem informasi keuangan adalah ada babarapaperencanaan audit keungan yaitu:

a) Perencanaan audit (Audit Planning)

Langkah pertama dalam perencanaan audit adalah untuk menetapkan ruang lingkup dan tujuan pemeriksaan. Pada audit laoran keuangan, pemeriksaan dilakukan oleh editor (akuntan) ekstern dan independen terhadap laporan keuangan perusahaan, ditujukan kepada para pemegang saham pihak lain terkait. Tujuan audit untuk menilai kelayakan atau kewajaran (fairness) laporan keuangan yang disajikan oleh perusahaan.

b) Pemahaman sistem dan struktur pengendalian internnya
Pada tahap ini yang dilakukan adalah pemahaman terhadap sasaran yang akan diaudit, pengumpulan informasi awal, dan identifikasi resiko, antara lain:

- ✚ Pemahaman sistem informasi untuk pelaksanaan transaksi
 - ✚ Penentuan kemungkinan salah saji dalam tiap tahap pelaksanaan transaksi
 - ✚ Penentuan aktivitas pengendalian untuk deteksi salah saji.
 - ✚ Penentuan prosedur audit untuk deteksi efektivitas aktivitas pengendalian
- Penyusunan program audit pengendalian

c) Pengumpulan bukti audit
Bukti audit dikumpulkan dengan sejumlah instrumen audit, pengujian, dan prosedur yang bermacam-macam

d) Evaluasi bukti pemeriksaan
Setelah bukti-bukti audit dikumpulkan, auditor mengevaluasi bukti audit tersebut sesuai dengan tujuan dari audit dan kemudian:
Dilakukan tests of controls yang bertujuan untuk mengetahui apakah pengendalian yang ada telah dilakukan dengan prosedur yang telah ditetapkan.
Dilakukan substantive test, yang terdiri dari:

a. Tests of transactions yang bertujuan untuk mengevaluasi

apakah terdapat kekeliruan atau kesalahan

b. Tests of balances or overall results yang bertujuan untuk menjamin laporan keuangan yang dihasilkan adalah benar dan akurat

e) Komunikasi hasil pemeriksaan
Segera setelah pekerjaan pemeriksaan diselesaikan dan diperoleh kesimpulan pendapat auditor, perlu disiapkan laporan hasil audit mengenai temuan-temuan dan rekomendasi-rekomendasinya. Dalam penyelesaian audit (completion of the audit) dibuat kesimpulan dan rekomendasi untuk dikomunikasikan pada manajemen.

F. REFERENCE

- [1] O. M. Febriani and A. S. Putra, "Sistem Informasi Monitoring Inventori Barang Pada Balai Riset Standardisasi Industri Bandar Lampung," *J. Inform.*, vol. 13, no. 1, pp. 90–98, 2014.
- [2] A. S. Putra, "Paperplain: Execution Fundamental Create Application With Borland Delphi 7.0 University Of Mitra Indonesia," 2018.
- [3] A. S. Putra, "2018 Artikel Struktur Data, Audit Dan Jaringan Komputer," 2018.
- [4] A. S. Putra, "ALIAS MANAGER USED IN DATABASE DESKTOP STUDI CASE DB DEMOS."
- [5] A. S. Putra, "COMPREHENSIVE SET OF PROFESSIONAL FOR DISTRIBUTE COMPUTING."
- [6] A. S. Putra, "DATA ORIENTED RECOGNITION IN BORLAND DELPHI 7.0."
- [7] A. S. Putra, "EMBARCADERO DELPHI XE 2 IN GPU-POWERED FIREMONKEY APPLICATION."
- [8] A. S. Putra, "HAK ATAS KEKAYAAN INTELEKTUAL DALAM DUNIA TEKNOLOGY BERBASIS REVOLUSI INDUSTRI 4.0."
- [9] A. S. Putra, "IMPLEMENTASI PERATURAN PERUNDANGAN UU. NO 31 TAHUN 2000 TENTANG DESAIN INDUSTRI BERBASIS INFORMATION TECHNOLOGY."
- [10] A. S. Putra, "IMPLEMENTATION OF PARADOX DBASE."
- [11] A. S. Putra, "IMPLEMENTATION OF TRADE SECRET CASE STUDY SAMSUNG MOBILE PHONE."
- [12] A. S. Putra, "IMPLEMENTATION PATENT FOR APPLICATION WEB BASED CASE STUDI WWW. PUBLIKLAMPUNG.COM."
- [13] A. S. Putra, "IMPLEMENTATION SYSTEM FIRST TO INVENT IN DIGITALLY INDUSTRY."
- [14] A. S. Putra, "MANUAL REPORT & INTEGRATED DEVELOPMENT ENVIRONMENT BORLAND DELPHI 7.0."
- [15] A. S. Putra, "PATENT AS RELEVAN SUPPORT RESEARCH."
- [16] A. S. Putra, "PATENT FOR RESEARCH STUDY CASE OF APPLE. Inc."
- [17] A. S. Putra, "PATENT PROTECTION FOR

- APPLICATION INVENT.”
- [18] A. S. Putra, “QUICK REPORT IN PROPERTY PROGRAMMING.”
- [19] A. S. Putra, “REVIEW CIRCUIT LAYOUT COMPONENT REQUIREMENT ON ASUS NOTEBOOK.”
- [20] A. S. Putra, “REVIEW TRADEMARK PATENT FOR INDUSTRIAL TECHNOLOGY BASED 4.0.”
- [21] A. S. Putra, “TOOLBAR COMPONENT PALLETTE IN OBJECT ORIENTED PROGRAMMING.”
- [22] A. S. Putra, “WORKING DIRECTORY SET FOR PARADOX 7.”
- [23] A. S. Putra, “ZQUERY CONNECTION IMPLEMENTED PROGRAMMING STUDI CASE PT. BANK BCA Tbk.”
- [24] A. S. Putra, D. R. Aryanti, and I. Hartati, “Metode SAW (Simple Additive Weighting) sebagai Sistem Pendukung Keputusan Guru Berprestasi (Studi Kasus: SMK Global Surya),” in *Prosiding Seminar Nasional Darmajaya*, 2018, vol. 1, no. 1, pp. 85–97.
- [25] A. S. Putra and O. M. Febriani, “Knowledge Management Online Application in PDAM Lampung Province,” in *Prosiding International conference on Information Technology and Business (ICITB)*, 2018, pp. 181–187.
- [26] A. S. Putra, O. M. Febriani, and B. Bachry, “Implementasi Genetic Fuzzy System Untuk Mengidentifikasi Hasil Curian Kendaraan Bermotor Di Polda Lampung,” *SIMADA (Jurnal Sist. Inf. dan Manaj. Basis Data)*, vol. 1, no. 1, pp. 21–30, 2018.
- [27] A. S. Putra, H. Sukri, and K. Zuhri, “Sistem Monitoring Realtime Jaringan Irigasi Desa (JIDES) Dengan Konsep Jaringan Sensor Nirkabel,” *IJEIS (Indonesian J. Electron. Instrum. Syst.)*, vol. 8, no. 2, pp. 221–232.
- [28] D. P. Sari, O. M. Febriani, and A. S. Putra, “Perancangan Sistem Informasi SDM Berprestasi pada SD Global Surya,” in *Prosiding Seminar Nasional Darmajaya*, 2018, vol. 1, no. 1, pp. 289–294.