

SURAT TUGAS

Nomor: 290-R/UNTAR/Pengabdian/II/2024

Rektor Universitas Tarumanagara, dengan ini menugaskan kepada saudara:

F.X. KURNIAWAN TJAKRAWALA, S.E., M.Si., Ak., CA.

Untuk melaksanakan kegiatan pengabdian kepada masyarakat dengan data sebagai berikut:

Judul : PENYULUHAN TENTANG PEMERIKSAAN SISTEM INFORMASI BERBASIS KOMPUTER GUNA MENILAI KEEFEKTIFAN PENGENDALIAN INTERNAL DENGAN PENDEKATAN BERBASIS RESIKO BAGI PELAKU UMKM SEKTOR PERDAGANGAN ECERAN
Mitra : PT SUMBER BUDI SAKTI
Periode : 2 - 3 FEBRUARI 2024
URL Repository : -

Demikian Surat Tugas ini dibuat, untuk dilaksanakan dengan sebaik-baiknya dan melaporkan hasil penugasan tersebut kepada Rektor Universitas Tarumanagara

21 Februari 2024

Rektor



Prof. Dr. Ir. AGUSTINUS PURNA IRAWAN

Print Security : eff5eb8d5ebbfdb326616df9cf4b76f9

Disclaimer: Surat ini dicetak dari Sistem Layanan Informasi Terpadu Universitas Tarumanagara dan dinyatakan sah secara hukum.

Lembaga

- Pembelajaran
- Kemahasiswaan dan Alumni
- Penelitian & Pengabdian Kepada Masyarakat
- Penjaminan Mutu dan Sumber Daya
- Sistem Informasi dan Database

Fakultas

- Ekonomi dan Bisnis
- Hukum
- Teknik
- Kedokteran
- Psikologi
- Teknologi Informasi
- Seni Rupa dan Desain
- Ilmu Komunikasi
- Program Pascasarjana



PT. SUMBER BUDI SAKTI

INDUSTRIAL ELECTRICAL SUPPLIER STOCKIST & DISTRIBUTOR

Jln. Daan Mogot II Komplek Golden Ville No. 88 CM Phone : 62-21-5672489, 56980772

Fax. : 62-21 5672503, Jakarta 11510

INDONESIA

Nomor: 037/SBS/R/I/2024

Kepada Yth.

Bpk. Kurniawan Tjakrawala, S.E, M.Si, Ak, CA.

Dosen Fakultas Ekonomi dan Bisnis, Universitas Tarumanagara – Jakarta

Perihal : UNDANGAN

Dengan hormat,


Bersama ini kami mengundang Bapak yang merupakan Dosen pada Fakultas Ekonomi dan Bisnis Universitas Tarumanagara untuk memberikan pelatihan/penyuluhan singkat sebagai berikut:

Topik : Penyuluhan tentang Pemeriksaan Sistem Informasi Terkomputerisasi untuk Menilai Keefektifan Pengendalian Internal dengan Pendekatan Berbasis Resiko
Hari / Tanggal : Jum'at & Sabtu / 2 & 3 Februari 2024
Tempat Lokasi : Jl. Daan Mogot II Kompleks Golden Ville No. 88 CM, Jakarta Barat, Jakarta—11510
Peserta : Pimpinan dan karyawan bagian keuangan & akuntansi
Waktu : 09.00 s/d 11.00 WIB

Kami mohon Bapak berkenan menerima undangan ini dan bersedia memberikan pelatihan/penyuluhan singkat bagi karyawan kami.

Atas perhatian dan kerjasamanya, kami mengucapkan terima kasih.

Jakarta, 22 Jan-2024


PT. SUMBER BUDI SAKTI
JAKARTA - INDONESIA
(Sofyan Effendi)
Managing Director

**LAPORAN ABDIMAS (MANDIRI / NON-REGULER)
(Periode Pelaporan Kegiatan: 1-Sep-2023 s/d 29-Feb-2024)**

**PENYULUHAN TENTANG PEMERIKSAAN SISTEM INFORMASI BERBASIS
KOMPUTER GUNA MENILAI KEEFEKTIFAN PENGENDALIAN INTERNAL
DENGAN PENDEKATAN BERBASIS RESIKO BAGI PELAKU UMKM
SEKTOR PERDAGANGAN ECERAN**

PENDAHULUAN

Kegiatan abdimas semester gasal 2023/2024 berlangsung secara mandiri (non-reguler/tidak menggunakan dana hibah dari LPPM UNTAR) bersama dengan mitra abdimas yaitu pihak UMKM yang dikelola oleh bapak Sofyan Effendi yang bergerak di sektor perdagangan eceran khususnya peralatan Listrik dengan nama “PT Sumber Budi Sakti” (PT SBS). Perusahaan ini berdiri pada tahun 1998 dengan bentuk sebagai Usaha Dagang (PD) yang berlokasi di kawasan pertokoan Glodok Jaya Jakarta Barat. Perusahaan bergerak dibidang penjualan peralatan listrik yang menyediakan barang-barang elektrik (komponen panel listrik), lampu, dan kabel dengan berbagai macam merek untuk kebutuhan pabrik; gedung maupun perumahan. PD Sumber Budi Sakti berubah status hukum menjadi PT SBS pada tahun 2006. Pelanggan dari produk perusahaan terbagi menjadi pelanggan pabrikan dan pelanggan rumahtangga. Pelanggan pabrikan adalah industri tambak udang yang tersebar di Aceh, Sumatra Utara, Banyuasin, Lampung, Jawa Barat, Bima, Dompu, Gorontalo, Donggala, Wajo, Pinrang, Kolaka, Polewali. Sedangkan pelanggan rumahtangga tersebar di Jabodetabek. PT SBS menjalankan usahanya di dua lokasi yaitu area pertokoan Glodok Jaya untuk pemasaran semua jenis produk perusahaan dan area Daan Mogot II untuk produksi box panel dan perakitan komponen listrik. Pada awalnya usaha ini merupakan usaha keluarga dengan karyawan yang juga merupakan anggota keluarga. Namun setelah tahun 2006 dimana perusahaan telah beralih menjadi perseroan Terbatas, perusahaan mulai merekrut orang di luar keluarga sebagai bagian dari SDM perusahaan, khususnya di bagian marketing, pabrikasi box panel, dan bagian pembukuan. Saat ini karyawan perusahaan berjumlah sekitar 15 orang yang mencakup 7 orang di pertokoan wilayah Glodok dan 8 orang di area gudang dan workshop box panel di Daan Mogot II, Ruko Golden Ville No. 88, Kelurahan Duri Kepa. Karyawan perusahaan level manajerial mencakup manajer penjualan dan supervisor workshop. Bapak Sofyan selaku pemilik sekaligus menjadi managing director PT SBS. Beliau sering terlibat langsung bersama dengan karyawan bagian produksi dalam pembuatan box panel listrik tambak udang.

Tim abdimas pada semester gasal 2023/2024 beranggotakan dua personil, yaitu satu orang dosen tetap prodi PPAK (Kurniawan Tjakrawala) dan satu orang mahasiswa dari prodi PPAK yaitu Harli Hamdardi Yustia yang dilibatkan guna membantu dalam pengetikan materi (MS word dan powerpoint) maupun pengadaan copy materi penyuluhan bagi pihak mitra yaitu lima personil dari PT SBS. Tim Abdimas mendapatkan sejumlah fakta yang menjadi masalah bagi PT SBS yaitu: 1) bahwa pemilik perusahaan yang sekaligus merupakan managing partnernya yaitu bpk. Sofyan mengakui sering menemukan sejumlah ketidakcocokan antara catatan stok dengan fisik barang dagang perusahaan; 2) bahwa staf akuntansi dan keuangan sering melakukan input data transaksi hanya berdasarkan keterangan lisan tanpa bukti tertulis; 3) bahwa sering dijumpai kondisi dimana bukti transaksi tidak tersip dengan memadai; 4) bahwa terdapat kondisi dimana aplikasi Odoo ERP mengalami gagal operasi (hang) sehingga relatif mengganggu kelancaran input data transaksi penjualan dan juga pembelian. Oleh karena itu, sesuai dengan kepakaran yang dimiliki, maka tim abdimas pada semester gasal 2023/2024 memberikan solusi kepada PT SBS dengan berfokus pemeriksaan sistem informasi

terkomputerisasi guna menilai keefektifan pengendalian internal dengan pendekatan berbasis resiko.

METODE PELAKSANAAN

Kegiatan abdimas bersifat insidental yang diselenggarakan menggunakan metode ceramah dan tanya-jawab. Pelaksanaan abdimas mandiri semester gasal 2023/2024 berlangsung pada hari Jumat dan Sabtu/2 & 3 Februari 2024 yang dimulai pada pukul 9.00 s/d 11.00, sesuai dengan undangan yang disampaikan kepada kami. Materi hari Jumat (2-Feb-2024) berkenaan dengan penyuluhan mengenai konsep pemeriksaan sistem informasi terkomputerisasi dengan pendekatan berbasis resiko. Adapun materi pada hari Sabtu (3-Feb-2024) berhubungan dengan penyuluhan mengenai pemeriksaan dengan pendekatan berbasis resiko atas keefektifan pengendalian internal pada sistem Odoo ERP yang telah diterapkan oleh PT Sumber Budi Sakti.

HASIL ABDIMAS

Tim abdimas telah menyusun materi penyuluhan mengenai pemeriksaan sistem informasi berbasis komputer yang mana dalam hal ini adalah aplikasi Odoo ERP yang digunakan dalam PT Sumber Budi Sakti. Pemeriksaan atas sistem informasi terkomputerisasi bertujuan untuk memastikan terpenuhinya enam tujuan sebagai berikut: (1) **keamanan secara keseluruhan** demi melindungi peralatan komputer, program, komunikasi dan data dari akses yang tidak sah; modifikasi yang tidak sah; maupun kerusakan; (2) **pengembangan dan akuisisi program** demi memastikan bahwa seluruh pengembangan dan akuisisi program telah dilakukan sesuai dengan otorisasi manajemen umum maupun khusus; (3) **modifikasi program** demi memastikan bahwa seluruh modifikast program yang dilakukan telah mendapatkan persetujuan dan otorisasi dari manajemen; (4) **pemrosesan komputer** demi memastikan agar seluruh pemrosesan transaksi, arsip-arsip, laporan, dan catatan komputer lainnya akurat dan lengkap; (5) **data sumber** demi memastikan agar sumber data yang tidak akurat atau otorisasi yang tidak tepat dapat teridentifikasi dan tertangani sesuai dengan dengan kebijakan manajemen; (6) **arsip data** demi memastikan agar arsip-arsip data komputer telah akurat, lengkap dan rahasia.

Berdasarkan **Gambar 1** diketahui bahwa pada proses order penjualan akan dicantumkan ke dalam **form penerimaan pesanan penjualan** berupa jenis jenis pesanan yang dipesan oleh pelanggan dalam hal jenis produk; jumlah kuantitas yang dipesan; jenis pembayaran oleh pelanggan (pembayaran tunai atau pembayaran dengan berjangka waktu; serta beberapa hal lainnya seperti lokasi pengiriman jika berbeda dengan lokasi toko pelanggan dan jadwal pengiriman. Dalam hal ini sebelum proses diteruskan ke bagian gudang, maka akan dilakukan pengecekan terhadap beberapa hal umum seperti : (a) apakah pelanggan telah tercatat dalam sistem data pelanggan perusahaan. Jika belum tercatat maka dilakukan proses registrasi terhadap pelanggan baru; (b) bilamana sudah tercatat sebagai pelanggan, maka akan akan divalidasi dalam hal kualitas pembayaran pelanggan. Setelah lolos dari validasi data, melengkapi **form pengiriman barang kepada pelanggan**, bilamana barang tersedia maka dilakukan proses pengiriman oleh bagian logistik dan pergudangan. Selanjutnya setelah barang dikirim oleh bagian logistik diserahkan kembali dokumen penerimaan barang oleh pelanggan yang kemudian di validasi dan direkap untuk dikirimkan kepada bagian keuangan untuk kemudian dilakukan kegiatan invoicing. Sejumlah potensi resiko pada siklus pendapatan yaitu: terjadinya salah input dari sisi harga, potongan diskon dan juga jenis produk yang dipesan oleh outlet; terjadinya data pelanggan yang salah (contoh: tidak sesuai penyesuaian kredit limit; approval perubahan kredit limit tidak sesuai; modifikasi tidak sah); proses jumlah barang yang diinput di sistem dan keluar dari gudang tidak sesuai dengan pesanan; terjadinya salah input

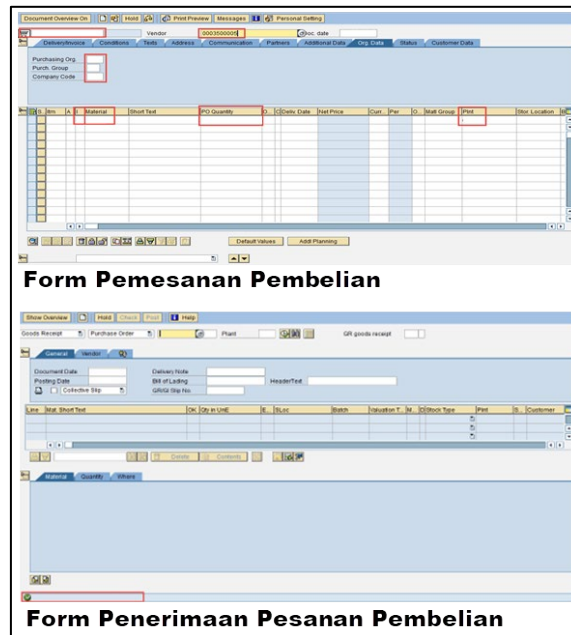
dalam pembuatan invoice ke dalam sistem invoicing. Prosedur kegiatan pemeriksaan untuk menguji keefektifan pengendalian sistem informasi di siklus penjualan yaitu: melakukan kegiatan wawancara untuk mengukur tingkat kesulitan yang dialami dalam menggunakan sistem informasi; verifikasi keandalan sistem informasi dalam melakukan transfer data antar departemen sehingga antara sales order hingga kegiatan pelunasan dapat berjalan dengan lancar; melakukan verifikasi atas keandalan kemampuan perangkat keras dalam mendukung kegiatan aktifitas dalam sistem informasi tersebut; melakukan pemeriksaan secara berkala atas data data yang disajikan dalam proses yang berjalan; melakukan pengujian terhadap perubahan user-id dan password secara berkala.

The image shows two screenshots of the Odoo ERP interface. The top screenshot is titled "Form Penerimaan Pesanan Penjualan" (Sales Order Receipt Form). It features a header with "Orders" and various input fields for "Net value", "Reference date", and "PO Number". Below this are tabs for "Item overview", "Item detail", "Ordering path", "Procurement", "Shipping", and "Reason for rejection". The main area contains a table with columns for "Item", "Material", "Order Quantity", "Unit", "Description", "Customer Material Name", "MCA", "COGP", "In. em", "First Date", and "Print". The bottom screenshot is titled "Form Pengiriman Barang kepada Pelanggan" (Goods Shipment to Customer Form). It has a header with "Post Goods Issue" and fields for "Outbound date" and "Document Date". Below are tabs for "Item Overview", "Picking", "Loading", "Transport", "Status Overview", and "Goods Movement Date". The main area contains a table with columns for "Item", "Material", "Deliv. Qty.", "Unit", "Description", "The", "Picking", "Lot Type", "Open Qty.", and "Ship Date".

Gambar 1. Tampilan Form untuk Siklus Pendapatan dari Aplikasi Odoo ERP

Gambar 2 menunjukkan bahwa pada proses order pembelian maka: departemen demand dan supply melakukan koordinasi dengan tim cabang untuk melakukan proyeksi yang dilakukan manual menggunakan spread sheet untuk menentukan jumlah pembelian barang persediaan menggunakan **form pesanan pembelian**: hasil estimasi jumlah pembelian yang dilakukan dimasukkan ke dalam sistem Odoo ERP berdasarkan nama partner dan juga jenis produk, volume yang dipesan dan cabang yang melakukan pemesanan; setelah melakukan pemesanan, maka dilakukan pengkajian oleh manajer demand supply planning untuk melakukan evaluasi dan menyetujui order pembelian yang telah dilakukan input tersebut; dalam melakukan pembelian ini, tim demand supply juga melakukan koordinasi dengan tim cabang untuk menentukan tanggal penerimaan barang di cabang, juga demi menyesuaikan waktu bongkar muat serta juga penyesuaian atas kapasitas gudang; pemesanan pembelian ini kemudian di create dan dikirimkan kepada pihak partner yang berkerjasama dengan perusahaan dan dituangkan ke dalam material resources planning perusahaan yang dilakukan melalui email; untuk pembelian yang telah dilakukan, lalu diterima oleh partner dan mengirimkan barang sesuai dengan jumlah barang yang dipesan; barang yang dibeli kemudian di terima di gudang menggunakan **form penerimaan pesanan pembelian** dan diperiksa oleh bagian gudang terlebih dahulu dan memasukkan jumlah barang di gudang serta menandatangani surat dokumen penerimaan barang. Sejumlah potensi resiko pada siklus pembelian yaitu: terjadinya ketidak sesuaian antara harga sebenarnya dengan harga yang tercantum di sistem; terjadinya

kelebihan pembayaran atas pembelian barang dagang; terjadinya pembayaran tidak sesuai dengan jatuh temponya; kesalahan dalam komputasi dalam perhitungan pembayaran. Adapun prosedur pemeriksaan untuk menguji keefektifan pengendalian sistem informasi di siklus pembelian yaitu: melakukan kegiatan wawancara untuk memahami tingkat pengetahuan pengguna dalam proses pembayaran barang dagang; melakukan verifikasi atas tingkat persetujuan yang dilakukan dalam melakukan pembayaran; melakukan pengujian terhadap perubahan user-id dan password secara berkala sesuai tingkatan wewenang dalam melakukan persetujuan pembayaran.



Gambar 2. Tampilan Form untuk Siklus Pengeluaran dari Aplikasi Odoo ERP

Sesi tanya-jawab berlangsung dengan antusias dari peserta penyuluhan. Keingintahuan peserta terkait dengan resiko yang potensial terjadi pada sistem informasi terkomputerisasi menjadikan sesi tanya-jawab berlangsung dinamis. Background pendidikan yang non akuntansi menjadikan peserta mendapatkan wawasan baru tentang pengendalian internal. Penyuluhan ini juga meneguhkan semangat dari bapak Sofyan selaku managing director PT Sumber Budi Sakti yang selalu ingin memastikan bahwa sistem informasi terkomputerisasi dari aktivitas akuntansi dan keuangan akan menghasilkan output yang dapat diandalkan dengan meminimalkan potensi resikonya sehingga pengendalian internal berlangsung secara efektif.

KESIMPULAN

Pelaksanaan abdimas mandiri pada semester gasal 2023/2024 ini memenuhi undangan dari bpk. Sofyan Effendi pemilik UMKM di bidang perdagangan eceran peralatan panel listrik dengan nama PT Sumber Budi Sakti guna memberikan penyuluhan tentang pemeriksaan keefektifan sistem informasi terkomputerisasi yang telah berlangsung di Perusahaan tersebut. Penyuluhan tersebut memberikan manfaat bagi pihak perusahaan berupa pemahaman yang semakin baik mengenai aktivitas pengendalian internal yang semestinya berlangsung dalam perusahaan yang telah menerapkan sistem informasi terkomputerisasi. Pihak mitra menjadi semakin aware mengenai resiko yang semakin tinggi pada aktivitas paperless. Penyuluhan ini juga membuka wawasan dari pihak mitra bahwa digitalisasi dari aktivitas akuntansi dan keuangan dalam siklus pendapatan dan pengeluaran selain memudahkan sistem informasi juga memuat resiko yang terkait dengan keamanan dan kegagalan sistem informasi memberikan luaran yang andal.

REFERENSI MATERI

- Ayodya, W. 2020. *UMKM 4.0: strategi umkm memasuki era digital*. Jakarta: Elex Media Komputindo.
- Ikatan Akuntan Indonesia. 2015. *Modul chartered accountant: sistem informasi & pengendalian internal*. Jakarta: IAI.
- Romney, M.B., Steinbart, P.J., Summers, S.L., & Wood, D.A. 2021. *Accounting information systems*, 15th edition, (Global Edition), Pearson.
- Turban, E., Pollard, C., & Wood, G. 2018. *Information technology for management on-demand strategies for performance, growth and sustainability* 11th edition. John Wiley & Sons.

PENYULUHAN TENTANG PEMERIKSAAN SISTEM INFORMASI BERBASIS KOMPUTER GUNA MENILAI KEEFEKTIFAN PENGENDALIAN INTERNAL DENGAN PENDEKATAN BERBASIS RESIKO BAGI PELAKU UMKM SEKTOR PERDAGANGAN ECERAN

PENYAJI MATERI:

**Kurniawan Tjakrawala & Harli H. Yustia
(FEB Universitas Tarumanagara–Jakarta)**

www.untar.ac.id [f](#) Untar Jakarta [t](#) @UntarJakarta [i](#) @untarjakarta

Audit atas sistem informasi

- Auditing merupakan Proses memperoleh dan mengevaluasi bukti mengenai asersi tentang tindakan dan peristiwa ekonomi untuk menentukan seberapa baik kesesuaiannya dengan kriteria yang telah ditetapkan.
- Audit sistem informasi adalah proses pengumpulan dan penilaian bukti-bukti untuk menentukan apakah sistem komputer dapat mengamankan aset, memelihara integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumberdaya secara efisien.

Memahami Tujuan Audit Sistem Informasi

- Tujuan dari audit sistem informasi adalah untuk meriviu dan mengevaluasi pengendalian internal yang melindungi sistem tersebut. Seperti :

- Mengamankan Asset
- Menjaga Integritas Data
- Menjaga Efektivitas Sistem
- Mencapai Efisiensi

JENIS PENDEKATAN AUDIT SYSTEM INFORMASI

- Pendekatan temuan (Exposures Approach),
 - › fokus utama ditekankan pada jenis kesalahan (losses) yang terjadi dalam suatu sistem informasi. Setelah itu ditentukan kendali (controls) yang dapat digunakan untuk mengurangi kesalahan tersebut sampai pada batas yang dapat diterima (acceptable levels).
- Pendekatan kendali (Control Approach),
 - › fokus utamanya adalah kendali-kendali di dalam suatu sistem informasi yang dapat digunakan untuk mengurangi kesalahan sampai pada level yang dapat diterima (acceptable levels).

3



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Tujuan Audit Sistem Informasi dan Pendekatan yang Digunakan

1. Keamanan secara Keseluruhan

Tindakan pengamanan secara keseluruhan bertujuan untuk melindungi peralatan computer, program, komunikasi dan data dari akses yang tidak sah, modifikasi yang tidak sah maupun perusakan.

2. Pengembangan dan Akuisisi Program

Memastikan bahwa seluruh pengembangan dan akuisisi program telah dilakukan sesuai dengan otorisasi manajemen umum maupun khusus.

3. Modifikasi Program

Memastikan bahwa seluruh modifikasi program yang telah dilakukan telah mendapatkan persetujuan dan otorisasi dari manajemen

4. Pemrosesan Komputer

Memastikan agar seluruh pemrosesan transaksi, arsip-arsip, laporan dan catatan computer lainnya akurat dan lengkap

5. Data Sumber

Memastikan agar sumber data yang tidak akurat atau otorisasi yang tidak tepat dapat teridentifikasi dan tertangani sesuai dengan kebijakan manajemen

6. Arsip Data

Memastikan agar arsip –arsip data computer telah akurat, lengkap, dan rahasia

4



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Langkah – Langkah dalam pendekatan audit berbasis - risiko

Memahami ancaman (kecurangan dan kesalahan) yang dihadapi oleh perusahaan.

Mengidentifikasi prosedur pengendalian untuk mencegah, mendeteksi atau mengoreksi ancaman tersebut.

Evaluasi atas prosedur pengendalian

Mengevaluasi kelemahan pengendalian untuk menentukan dampaknya terhadap sifat, waktu atau keluasan prosedur audit

5



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Merancang Suatu Rencana untuk Mengevaluasi Pengendalian Internal dalam Sistem Informasi

Kerangka audit untuk mengevaluasi pengendalian internal dalam sistem informasi

Keamanan secara Keseluruhan

Pengembangan dan Akuisisi Program

Modifikasi Program

Pemrosesan Komputer

Sumber Data

Arsip Data

6



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Keamanan secara Keseluruhan

5 Kerangka audit berbasis-risiko untuk memenuhi tujuan audit keamanan secara keseluruhan:

1. Jenis kesalahan (*errors*) dan kecurangan (*fraud*) yang mungkin terjadi dalam mengevaluasi tujuan audit:
 - Pencurian piranti keras atau kerusakan piranti keras yang disengaja maupun tidak disengaja;
 - Kehilangan, pencurian, atau akses yang tidak sah terhadap program, data dan sumber-sumber sistem lainnya.
 - Kehilangan, pencurian atau pengungkapan yang tidak sah atas data yang sifatnya rahasia;
 - Modifikasi yang tidak sah atau penggunaan program dan arsip data secara tidak sah;
 - Gangguan atas aktivitas-aktivitas bisnis yang utama.

7



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Keamanan secara Keseluruhan

2. Prosedur pengendalian yang seharusnya diterapkan/ada :
 - Rencana perlindungan atau pengamanan informasi;
 - Pembatasan akses fisik terhadap peralatan komputer;
 - Pembatasan akses logis terhadap sistem dengan menggunakan pengendalian otentikasi dan otorisasi;
 - Pengendalian atas penyimpanan data dan transmisi data;
 - Prosedur perlindungan terhadap serangan virus;
 - Prosedur pencadangan data dan pemulihan data;
 - Rancangan sistem toleransi-kegagalan;
 - Rencana untuk mengatasi kerusakan sistem;
 - Pemeliharaan pencegahan;
 - Firewall*;
 - Asuransi atas kerusakan besar dan gangguan aktivitas bisnis yang utama.

8



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Keamanan secara Keseluruhan

3. Prosedur audit untuk mereviu sistem:

- Inspeksi di lokasi tempat penyimpanan peralatan komputer;
- Reviu kewanan/perlindungan informasi dan rencana untuk mengatasi kerusakan sistem;
- Wawancara dengan personil sistem informasi mengenai prosedur kewanan;
- Reviu atas kebijakan dan prosedur akses fisik dan akses logis;
- Reviu kebijakan dan prosedur pencadangan dan pemulihan arsip;
- Reviu kebijakan dan prosedur penyimpanan dan transmisi data;
- Reviu kebijakan dan prosedur untuk meminimalisir kegagalan sistem;
- Reviu kontrak pemeliharaan dengan vendor;
- Memeriksa log/catatan akses sistem;
- Memeriksa kebijakan asuransi untuk menangani kerusakan besar dan gangguan aktivitas bisnis

9



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Keamanan secara Keseluruhan

4. Prosedur audit untuk menguji pengendalian:

- Mengamati dan menguji prosedur akses ke lokasi tempat penyimpanan peralatan komputer;
- Mengamati penyiapan penyimpanan dan pencadangan data *on-site* maupun *off-site*;
- Menguji prosedur pemberian dan modifikasi atas *user ID* dan kata kunci;
- Menyelidiki bagaimana cara untuk mengatasi akses-akses yang tidak sah;
- Memverifikasi keluasan dan efektivitas enkripsi data;
- Memverifikasi keefektifan pengendalian transmisi data;
- Memverifikasi keefektifan penggunaan firewall dan prosedur perlindungan atas virus;
- Memverifikasi penggunaan pemeliharaan pencegahan dan penggunaan tenaga listrik cadangan/UPS (*uninterruptable power supply*);
- Memverifikasi jumlah dan keterbatasan cakupan asuransi;
- Memeriksa hasil dari simulasi rencana pemulihan kerusakan data.

10



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Keamanan secara Keseluruhan

5. Pengendalian pengguna yang mungkin ada
 - Kebijakan personil yang mendukung termasuk pemisahan tugas
 - Pengendalian pengguna yang efektif

11



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Pengembangan dan Akuisisi Program

5 Kerangka audit berbasis-risiko untuk mengevaluasi tujuan audit atas pengembangan dan akuisisi program:

1. Jenis kesalahan (*errors*) dan kecurangan (*fraud*) yang mungkin terjadi dalam mengevaluasi tujuan audit:
 - Kesalahan dalam pemrograman yang tidak disengaja atau kode program yang tidak sah.
2. Prosedur pengendalian yang seharusnya diterapkan/ada:
 - Mereviu persetujuan lisensi piranti lunak;
 - Pengelolaan otorisasi pengembangan program dan perolehan piranti lunak;
 - Pengelolaan dan persetujuan pengguna atas spesifikasi pemrograman;
 - Pengujian secara menyeluruh atas program-program baru, termasuk melakukan *user-acceptance test*;
 - Dokumentasi sistem yang lengkap, termasuk persetujuannya.

12



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Pengembangan dan Akuisisi Program

3. Prosedur audit untuk mereviu sistem:

- Reviu independen atas proses pengembangan sistem;
- Reviu kebijakan dan prosedur pengembangan/perolehan sistem;
- Reviu kebijakan dan prosedur otorisasi sistem dan persetujuan;
- Reviu standar evaluasi pemrograman;
- Reviu standar program dan dokumentasi sistem;
- Reviu atas uji spesifikasi, uji data dan hasil pengujiannya;
- Reviu atas kebijakan dan prosedur uji persetujuan;
- Reviu atas kebijakan dan prosedur perolehan persetujuan lisensi piranti lunak;
- Diskusi dengan manajemen, para pengguna, dan personil sistem informasi terkait dengan prosedur pengembangan.

13



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Pengembangan dan Akuisisi Program

4. Prosedur audit untuk menguji pengendalian:

- Wawancara dengan pengguna atas keterlibatan mereka dalam perolehan/pengembangan system dan implementasinya;
- Reviu notulensi rapat tim pengembangan untuk membuktikan keterlibatannya dalam pengembangan/perolehan sistem;
- Verifikasi pengelolaan dan persetujuan *sign-off* pengguna pada setiap tahap-tahap pengembangan;
- Reviu atas pengujian spesifikasi, pengujian data, hasil pengujiannya;
- Reviu atas persetujuan lisensi piranti lunak.

5. Pengendalian pengganti yang mungkin ada:

- Pengendalian pemrosesan yang kuat;
- Pemrosesan independen atas pengujian data oleh auditor.

14



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Modifikasi Program

5 Kerangka audit berbasis-risiko untuk mengevaluasi tujuan audit atas modifikasi program terdiri dari:

1. Jenis kesalahan (*errors*) dan kecurangan (*fraud*) yang mungkin terjadi dalam mengevaluasi tujuan audit:
 - Kesalahan dalam pemrograman yang tidak disengaja atau kode program yang tidak sah.

2. Prosedur pengendalian yang seharusnya diterapkan/ada:

- Daftar komponen program yang akan dimodifikasi;
- Manajemen otorisasi dan persetujuan atas modifikasi program;
- Persetujuan pengguna atas spesifikasi perubahan program;
- Tes menyeluruh atas perubahan program, termasuk melakukan *user acceptance test*;
- Dokumentasi lengkap atas perubahan program, termasuk persetujuannya;
- Pemisahan pengembangan pengujian dan hasil dari setiap versi program
- Perubahan yang diterapkan oleh personel yang independen dari pengguna dan pemrogram;
- Pengendalian atas akses logis.

15



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Modifikasi Program

3. Prosedur audit untuk mereviu sistem:

- Reviu kebijakan, prosedur dan standar modifikasi program;
- Reviu standar dokumentasi untuk modifikasi program;
- Reviu dokumentasi akhir dari modifikasi program;
- Reviu pengujian modifikasi program dan prosedur pengujian persetujuan;
- Reviu uji spesifikasi, uji data dan hasil pengujiannya;
- Reviu kebijakan dan prosedur uji persetujuan;
- Reviu standar evaluasi pemrograman;
- Diskusi kebijakan dan prosedur modifikasi dengan manajemen, para pengguna dan personel sistem;
- Reviu kebijakan dan prosedur pengendalian atas akses logis.

16



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Modifikasi Program

4. Prosedur audit untuk menguji pengendalian:

- Verifikasi pengguna dan manajemen atas persetujuan *sign-off* untuk perubahan program;
- Verifikasi bahwa komponen program yang akan dimodifikasi telah diidentifikasi dan ada dalam daftar;
- Verifikasi bahwa prosedur uji perubahan program dan dokumentasinya sudah sesuai dengan standar;
- Verifikasi bahwa pengendalian akses logis sudah diterapkan atas perubahan dalam program;
- Mengamati implementasi perubahan program;
- Verifikasi bahwa pemisahan pengembangan, pengujian dan hasil dari setiap versi program telah dilakukan;
- Verifikasi bahwa perubahan tidak dilakukan oleh pengguna atau personil pemrograman;
- Pengujian atas perubahan program yang tidak sah atau kesalahan dalam perubahan program dengan menggunakan kode sumber dari program pembanding lainnya, pemrosesan ulang ataudari simulasi paralel.

17



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Modifikasi Program

5. Pengendalian pengganti yang mungkin ada:

- Pengendalian pemrosesan yang kuat;
- Pengujian independen atas perubahan program yang tidak sah atau kesalahan dalam perubahan program.

18



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Pemrosesan Komputer

5 Kerangka audit berbasis-risiko untuk mengevaluasi tujuan audit atas pemrosesan komputer:

1. Jenis kesalahan (*errors*) dan kecurangan (*fraud*) yang mungkin terjadi dalam mengevaluasi tujuan audit:
 - o Kegagalan untuk mendeteksi input data yang salah, tidak lengkap atau tidak sah;
 - o Kegagalan untuk memperbaiki kesalahan yang ditandai dengan adanya prosedur pengeditan data;
 - o Adanya kesalahan ke dalam arsip atau database selama proses pemutakhiran;
 - o Distribusi atau pengungkapan *output* komputer yang tidak tepat;
 - o Ketidakakuratan dalam pelaporan secara disengaja maupun tidak disengaja.

19



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Pemrosesan Komputer

2. Prosedur pengendalian yang seharusnya diterapkan/ada:
 - o Melakukan pengeditan data secara berkala;
 - o Penggunaan label yang tepat untuk setiap arsip internal dan eksternal;
 - o Rekonsiliasi atas *batch* total;
 - o Prosedur koreksi kesalahan yang efektif;
 - o Pelaksanaan dokumentasi yang dapat dipahami dan menjalankan manualnya;
 - o Supervisi yang kompeten atas pengoperasian komputer;
 - o Penanganan *input* dan *output* data yang efektif oleh personel pengendalian data;
 - o Penyusunan daftar perubahan arsip dan ikhtisarnya untuk direviu oleh departemen pengguna;
 - o Pemeliharaan atas kondisi lingkungan yang tepat dalam fasilitas komputer.

20



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Pemrosesan Komputer

3. Prosedur audit untuk mereviu sistem:
 - Reviu dokumentasi administratif untuk standar pengendalian pemrosesan;
 - Reviu dokumentasi sistem untuk pengeditan data dan pengendalian pemrosesan lainnya;
 - Reviu pelaksanaan dokumentasi untuk kelengkapan dan kejelasan;
 - Reviu salinan daftar kesalahan, laporan *batch* total dan daftar perubahan arsip;
 - Mengamati pengoperasian komputer dan fungsi pengendali data;
 - Membahas pengendalian pemrosesan dan output dengan operator dan supervisor sistem informasi.

21



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Pemrosesan Komputer

4. Prosedur audit untuk menguji pengendalian:
 - Evaluasi kecukupan standar dan prosedur pengendalian pemrosesan;
 - Evaluasi kecukupan dan kelengkapan pengendalian pengeditan data;
 - Verifikasi ketepatan prosedur pengendalian pemrosesan dengan mengamati pengoperasian komputer dan pengendalian data;
 - Verifikasi bahwa *output* dari sistem aplikasi telah didistribusikan dengan benar;
 - Rekonsiliasi sampel *batch* total dan tindak lanjut atas setiap perbedaan yang ada;
 - Menelusuri kesalahan dalam sampel pengeditan data untuk memastikan adanya penanganan yang tepat;

22



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Pemrosesan Komputer

4. Prosedur audit untuk mennguji pengendalian (lanjutan):
 - o Verifikasi akurasi pemrosesan transaksi yang sensitif;
 - o Verifikasi akurasi transaksi yang dihasilkan oleh komputer;
 - o Mencari kode-kode yang salah atau tidak sah dengan melakukan analisis logika program;
 - o Mengecek akurasi dan kelengkapan pengendalian pemrosesan dengan menggunakan pengujian data;
 - o Memonitor sistem pemrosesan online dengan menggunakan teknik audit yang terkini;
 - o Menghasilkan kembali laporan-laporan tertentu untuk menguji akurasi dan kelengkapan.

5. Pengendalian pengganti yang mungkin ada):
 - o Pengendalian pengguna yang kuat dan pengendalian sumber data yang efektif.

23



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Sumber Data

5 Kerangka audit berbasis-risiko untuk mengevaluasi tujuan audit atas pengendalian sumber data:

1. Jenis kesalahan (*errors*) dan kecurangan (*fraud*) yang mungkin terjadi dalam mengevaluasi tujuan audit:
 - Sumber data yang tidak akurat atau tidak sah.

2. Prosedur pengendalian yang seharusnya diterapkan/ada:
 - Penanganan input sumber data oleh personil pengendalian secara efektif;
 - Otorisasi pengguna atas sumber data *input*;
 - Penyusunan dan rekonsiliasi *total batch control*;
 - Mencatat setiap penerimaan, pergerakan dan disposisi semua sumber data input;
 - Verifikasi digit cek;
 - Verifikasi kunci;
 - Penggunaan dokumen pengembalian;
 - Pengeditan data secara rutin;
 - Reviu departemen pengguna atas daftar perubahan arsip dan ikhtisarnya;
 - Prosedur yang efektif untuk mengoreksi dan memasukkan ulang data yang salah.

24



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Sumber Data

3. Prosedur audit untuk mereviu sistem:

- Reviu dokumentasi mengenai tanggung jawab fungsi pengendalian data;
- Reviu administratif dokumentasi untuk standar pengendalian sumber data;
- Reviu metode otorisasi dan memeriksa tanda tangan otorisasi;
- Reviu dokumentasi untuk mengidentifikasi langkah-langkah pemrosesan serta pengendalian dan isi sumber data;
- Dokumentasi pengendalian sumber data dengan menggunakan matriks input pengendalian;
- Mendiskusikan pengendalian atas sumber data dengan personil pengendalian, para pengguna sistem dan para manajer.

25



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Sumber Data

4. Prosedur audit untuk mennguji pengendalian:

- Memantau dan mengevaluasi operasi departemen pengendalian dan prosedur pengendaliannya;
- Verifikasi pemeliharaan yang tepat dan penggunaan catatan (*log*) pengendalian data;
- Mengevaluasi bagaimana cara menangani kesalahan-kesalahan yang tercatat (*error log items*);
- Memeriksa sumber data untuk melihat apakah otorisasinya sudah tepat;
- Rekonsiliasi batch total dan tindak lanjut atas penyimpangan yang terjadi;
- Menelusuri disposisi atas kesalahan yang ditandai oleh adanya pengeditan data.

5. Pengendalian pengganti yang mungkin ada:

- Pengendalian pengguna yang kuat dan pengendalian pemrosesan yang efektif.

26



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Arsip Data

5 Kerangka audit berbasis-risiko untuk mengevaluasi tujuan audit pengendalian atas arsip data terdiri dari::

1. Jenis kesalahan (*errors*) dan kecurangan (*fraud*) yang mungkin terjadi dalam mengevaluasi tujuan audit:
 - Perusakan data yang tersimpan karena eror, piranti keras dan piranti lunak yang malfungsi, dan tindakan sabotase dan vandalisme yang disengaja;
 - Modifikasi atau pengungkapan atas data yang tersimpan secara tidak sah.

2. Prosedur pengendalian yang seharusnya diterapkan/ada:

- Penyimpanan data dalam arsip dokumen yang aman dan pembatasan akses fisik terhadap arsip-arsip data;
- Pengendalian atas akses logis dan matriks pengendalian akses;
- Penggunaan label arsip dan mekanisme perlindungan penulisan yang tepat;
- Pengendalian pemutakhiran yang berkelanjutan;
- Enkripsi data untuk data yang sifatnya rahasia;
- Piranti lunak untuk perlindungan terhadap virus;
- Cadangan seluruh arsip data secara *off-site*;
- Prosedur titik-titik pengecekan dan prosedur pengembalian data (*rollback*) untuk memfasilitasi pemulihan sistem.

27



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Arsip Data

3. Prosedur audit untuk mereviu sistem:

- Reviu dokumentasi untuk operasi perpustakaan arsip;
- Reviu kebijakan dan prosedur akses logis;
- Reviu standar untuk perlindungan atas virus, penyimpanan data *off-site*, dan prosedur pemulihan sistem;
- Reviu pengendalian untuk pemutakhiran berkelanjutan, enkripsi data, konversi arsip dan rekonsiliasi total arsip utama dengan total pengendalian independen;
- Memeriksa rencana pemulihan kerusakan sistem;
- Mendiskusikan prosedur pengendalian arsip dengan para manajer dan operator.

28



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

Arsip Data

4. Prosedur audit untuk menguji pengendalian:

- Memantau dan mengevaluasi operasi perpustakaan arsip;
- Mereviu catatan pemberian *password* dan modifikasinya;
- Memantau dan mengevaluasi prosedur penanganan arsip oleh personil operasi;
- Memantau persiapan dan penyimpanan cadangan arsip *off-site*;
- Verifikasi efektivitas penggunaan prosedur perlindungan atas virus;
- Verifikasi pengendalian pemutakhiran berkelanjutan dan enkripsi data;
- Verifikasi kelengkapan, keberlakuan, dan pengujian rencana pemulihan kerusakan;
- Rekonsiliasi total di arsip utama dengan total pengendalian yang dilakukan secara terpisah;
- Memantau prosedur yang digunakan untuk mengendalikan konversi arsip.

5. Pengendalian pengganti yang mungkin ada:

- Pengendalian pengguna dan pemrosesan data yang kuat;
- Pengendalian keamanan komputer yang efektif.

UNTAR
Universitas Tarumanagara



Teknik Audit Digunakan untuk Menguji Program

1. Integrated Test Facility (ITC)

Menggunakan data transaksi palsu yang dimasukkan ke dalam sistem untuk memastikan keakuratan dan ketepatan sistem.

2. Snapshot Technique

Merekam dan menganalisis kondisi sistem pada waktu tertentu dengan mengambil "snapshot" dari konfigurasi sistem, data transaksi, dan aktivitas pengguna pada saat tertentu untuk menguji keamanan dan keandalan sistem serta untuk memeriksa kepatuhan sistem terhadap kebijakan dan prosedur yang telah ditetapkan.

3. System Control Audit Review File (SCARF)

Membuat file SCARF yang mencatat aktivitas pengguna pada program, seperti waktu masuk dan keluar, hak akses, dan jenis aksi yang dilakukan oleh pengguna untuk memeriksa pengendalian akses dan pemakaian data pada program.

4. Audit Hooks

Menambahkan kode khusus ke dalam sistem yang disebut sebagai "hooks". Kode ini akan memantau aktivitas sistem dan merekam informasi seperti tindakan pengguna, data yang dimasukkan atau diubah, dan waktu akses. Teknik ini digunakan untuk memeriksa kepatuhan sistem terhadap kebijakan dan prosedur yang telah ditetapkan.

5. Continuous and Intermittent Simulation

Continuous Simulation adalah teknik audit yang menggunakan program yang didesain khusus untuk memantau dan merekam aktivitas sistem secara terus-menerus, sedangkan Intermittent Simulation adalah teknik audit yang menggunakan program yang dijalankan pada interval waktu tertentu untuk memantau dan merekam aktivitas sistem. Teknik ini menghasilkan output yang memberikan informasi tentang kinerja sistem pada waktu tertentu dan dapat digunakan untuk mengidentifikasi kelemahan dan masalah dalam penggunaan sistem.



UNTAR
Universitas Tarumanagara



Alat Perangkat Lunak Digunakan untuk Menguji Logika Program

1. Automated Flowcharting Program

Memungkinkan pengguna untuk menggambar diagram alur dengan mudah dan cepat dengan menggunakan simbol-simbol yang telah ditentukan, seperti kotak, panah, dan diamond.

2. Automated Decision Table Program

Program ini memungkinkan pengguna untuk memasukkan kriteria atau kondisi yang harus dipenuhi dalam tabel dan menentukan tindakan yang harus diambil berdasarkan kombinasi kondisi tersebut.

3. Scanning Routines

Digunakan untuk mengidentifikasi kerentanan dan ancaman yang mungkin terjadi pada sistem informasi, seperti serangan hacker, virus komputer, atau kesalahan pengguna.

4. Mapping Programs

Digunakan untuk memetakan data dari satu format ke format lainnya. Program ini dapat mengubah data dari berbagai jenis file, seperti file teks, spreadsheet, atau database, ke format lainnya yang sesuai dengan kebutuhan pengguna.

5. Program Tracing

Digunakan untuk memeriksa aliran data dan mengidentifikasi masalah pada program seperti kesalahan logika, operasi yang tidak diinginkan, atau adanya bug dalam program. Program tracing dapat dilakukan dengan menggunakan perangkat lunak yang disebut dengan debugger, untuk memperoleh informasi yang terkait dengan variabel, memori, stack, dan fungsi program

31



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA

End of Slides

32



UNTAR
Universitas Tarumanagara



UNTAR untuk INDONESIA



PT. SUMBER BUDI SAKTI

INDUSTRIAL ELECTRICAL SUPPLIER STOCKIST & DISTRIBUTOR

Jln. Daan Mogot II Komplek Golden Ville No. 88 CM Phone : 62-21-5672489, 56980772

Fax. : 62-21 5672503, Jakarta 11510

INDONESIA

SURAT KETERANGAN

No. 153/SBS/E/SK/II/2024

Kami yang bertandatangan di bawah ini menyatakan bahwa:

Nama : KURNIAWAN TJAKRAWALA, S.E, M.Si, Ak, CA.
Pekerjaan : Dosen
Asal Instansi : Universitas Tarumanagara - Jakarta
Alamat Instansi : Jl. Tanjung Duren Utara No.1, Jakarta Barat

memang benar telah melakukan kegiatan penyuluhan tentang pemeriksaan sistem informasi terkomputerisasi untuk menilai keefektifan pengendalian internal dengan pendekatan berbasis resiko selama dua hari (Jum'at dan Sabtu) tanggal 2 & 3 Februari 2024 pada jam 09.00 s/d 11.00 WIB dengan peserta yang terdiri dari pemilik, manajemen, serta karyawan bagian keuangan dan akuntansi PT Sumber Budi Sakti.

Demikian surat keterangan ini dibuat agar dapat digunakan sebagaimana mestinya oleh pihak-pihak yang berkepentingan.

Jakarta, 16 Feb-2024



PT. SUMBER BUDI SAKTI

JAKARTA - INDONESIA

(Sofyan Effendi)

Managing Director