Jurnal KomtekInfo , Vol.8 No.1 Tahun 2021
e-ISSN : 2502-8758 || p-ISSN : 2356-0010
DOI : 10.35134/komtekinfo.v7i4
Page : 49-56

Audit Infrastruktur IT Dalam Memenuhi Kebutuhan Bisnis
(Studi Kasus : Perusahaan Yang Begerak Pada Bidang Jasa)

Deval Gusrion
Universitas Putra Indonesia"YPTK" Padang, Indonesia
devalgusrion@gmail.com

Abstract

The audit of the Information Technology infrastructure in this journal uses the ISO 27001 standard which is carried out at a company engaged in the service sector in West Sumatra Province. As a company that is quite developed and already has an adequate IT infrastructure in running its business, it is felt necessary to carry out an IT audit to ensure whether the IT devices they have already have adequate internal controls and at the same time as preventive measures for business risks such as: operational, reputation , legal, compliance and strategic. Given that IT is an important asset in operations that can increase the added value and competitiveness of a company while its implementation contains various risks, companies need to implement IT Governance.

Keyword : Audit, Information Technologi, ISO 27001, *IT Governance*

Abstrak

*A*udit terhadap infrastruktur Teknologi Informasi dalam jurnal ini mengunakan standar ISO 27001 yang dilakukan di salah satu perusahaan yang bergerak di bidang jasa yang berada di Provinsi Sumatera Barat. Sebagai perusahaan yang cukup berkembang dan sudah memiliki infrastruktur IT yang cukup memadai dalam menjalankan bisnisnya dirasakan perlu dilakukan audit IT untuk memastikan apakah perangkat IT yang mereka memiliki sudah memiliki pengendalian internal yang memadai dan sekaligus sebagai langkah-langkah pencegahan atas risiko bisnis seperti : operasional, reputasi, legal, kepatuhan dan strategis. Mengingat bahwa TI merupakan aset penting dalam operasional yang dapat meningkatkan nilai tambah dan daya saing perusahaan sementara dalam penyelenggaraannya mengandung berbagai risiko, maka perusahaan perlu menerapkan *IT Governance.*

Kata kunci : Audit, Teknologi Informasi, ISO 27001, *IT Governance*

1. Pendahuluan

Transformasi digital secara drastis mengubah cara bisnis beroperasi dan melayani pelanggan di berbagai perusahaan, banyak perusahaaan di tuntut untuk mengembangkan strategi bisnis dengan memanfaatkan kemajuan teknologi informasi. Pengembangan strategi tersebut selanjutnya mendorong investasi baru terhadap infrastruktur TI yang digunakan dalam pemrosesan transaksi dan informasi. Infrastruktur TI tersebut merupakan sebuah aset jangka panjang, nilai jangka panjang dari *shareholder* dan merepresentasikan pilihan jangka panjang dari suatu organisasi [1].

Penggunaan TI selain meningkatkan kecepatan dan keakuratan transaksi serta pelayanan kepada pelanggan, juga meningkatkan risiko misalnya : risiko operasional, reputasi, legal, kepatuhan dan strategis. Untuk itu diharapkan perusahaan memiliki manajemen risiko yang terpadu untuk melakukan identifikasi, pengukuran, pemantauan dan pengendalian risiko.

Teknologi Informasi harus dikelola secara efektif guna memaksimalkan efektifitas penggunaannya dan agar risiko terkait dari

Jurnal KomtekInfo , Vol.8 No.1 Tahun 2021
e-ISSN : 2502-8758 || p-ISSN : 2356-0010
DOI : 10.35134/komtekinfo.v7i4
Page : 49-54

teknologi yang diimplementasikan dapat dimitigasi, mengingat bahwa TI merupakan aset penting dalam operasional yang dapat meningkatkan nilai tambah dan daya saing perusahaan sementara dalam penyelenggaraannya mengandung berbagai risiko, maka perusahaan perlu menerapkan *IT Governance*. Teknologi informasi yang dikelola dengan baik akan menghasilkan keselarasan antara bisnis dan teknologi informasi [2].

Maka dari itu, **audit** terhadap TI haruslah dilakukan untuk menjaga kehandalan, keamanan dan untuk meningkatkan keefektifan serta efisiensi pengunaan Teknologi Informasi yang merupakan asset perusahaan dengan nilai investasi yang cukup tinggi. Audit TI tersebut dilakukan melalui proses pengumpulan dan penilaian bahan bukti tentang informasi untuk menentukan dan melaporkan kesesuaian informasi dengan kriteria-kriteria yang telah ditetapkan [3].

Audit terhadap infrastruktur IT dalam jurnal ini mengunakan standar ISO 27001 yang dilakukan di salah satu perusahaan yang bergerak di bidang jasa yang memiliki beberapa kantor di Provinsi Sumatera Barat, sebagai perusahaan yang cukup berkembang dan sudah memiliki infrastruktur IT yang cukup memadai untuk menjalankan bisnisnya dirasakan perlu dilakukan audit IT untuk memastikan apakah perangkat IT yang mereka memiliki sudah memiliki pengendalian internal yang memadai dan sekaligus sebagai langkah-langkah pencegahan atas risiko bisnis.

2. Tinjauan Literatur

Dalam penulisan jurnal ini, beberapa hal-hal atau teori yang dikemukakan yang berkaitan dengan permasalahan dan ruang lingkup sebagai landasan dalam permbuat jurnal seperti : standar dari ISO 27001 serta tujuan dan ruang lingkup (ketentuan).

2.1. Standar ISO 27001

ISO 27001 merupakan suatu standar Internasional dalam menerapkan sistem manajemen kemanan informasi atau lebih dikenal dengan *Information Security Management Systems* (ISMS). Menerapkan standar ISO 27001 akan membantu organisasi atau perusahaan Anda dalam membangun dan memelihara sistem manajemen keamanan informasi (ISMS). ISMS merupakan seperangkat unsur yang saling terkait dengan organisasi atau perusahaan yang digunakan untuk mengelola dan mengendalikan risiko keamanan informasi dan untuk melindungi serta menjaga kerahasiaan *(confidentiality)*, integritas *(integrity)* dan ketersediaan *(availability)* informasi [4].

1. Kerahasiaan (*confidentiality*): adalah memastikan bahwa informasi yang ada di dalam perusahaan kita, dapat termonitor dan hanya dapat diakses oleh pihak yang memiliki wewenang terhadap informasi tersebut. Misalnya, Pembuatan regulasi terkait klasifikasi data, apakah rahasia, sangat rahasia, atau umum / biasa saja.
2. Integritas (*integrity*): adalah memastikan bahwa informasi yang ada di dalam perusahaan kita, bersifat akurat, lengkap, dan aman dari modifikasi oleh pihak yang tidak bertanggungjawab. Misalnya, Yang hanya bisa melakukan akses ke data center, adalah karyawan dengan ID Khusus.
3. Ketersediaan (*availability*): adalah memastikan bahwa informasi yang ada di dalam perusahaan kita, selalu tersedia dan mudah untuk diakses sesuai dengan kebutuhan. Misalnya, lokasi penyimpanan data yang aman dari gangguan berupa pencurian, bencana alam atau *cyber-attack*.

Jurnal KomtekInfo , Vol.8 No.1 Tahun 2021
e-ISSN : 2502-8758 || p-ISSN : 2356-0010
DOI : 10.35134/komtekinfo.v7i4
Page : 49-54

Gambar 1 : ISO 27001 memiliki 11 Domain

2.2. Versi ISO 27001: 2013

SO 27001: 2013 diperkenalkan pada September - Oktober 2013 oleh Lembaga yang sama yaitu International Organization for Standardization (ISO). Diperkenalkannya ISO 27001: 2013 secara resmi menggantikan penggunaan ISO 27001:2005. Standar ini dikembangkan agar menjadi lebih selaras dengan standar versi lainnya (misal ISO 9001, 20000, 31000) dan menampilkan 114 kendali (control) dalam 14 kelompok domain, dibandingkan standar sebelumnya yang terdiri dari 133 kendali dalam 11 kelompok domain. Perubahan pada persyaratan revisi 2013 ini merefleksikan perubahan teknologi yang banyak berdampak pada kelangsungan bisnis saat ini, misalnya perkembangan teknologi komputasi awan (cloud computing) serta perubahan susunan kendali keamanan pada lampiran Annex A [5].

3. Metodologi Penelitian

Metodologi penelitian mengunakan referensi ISO 27001 serta langkah-langkah pelaksanaan audit yang meliputi : mengidentifikasi proses bisnis dan IT, mengumpulkan data, melaksanakan audit kepatutan, menentukan hasil audit, menyusun laporan dari hasil audit insfrastruktur IT. Dalam menentukan ruang lingkup dan tujuan audit mengacu kepada aspek sebagai berikut :

1. *Backup* dan *Restore* Data
   Setiap aset TI termasuk didalamnya informasi dan sistem aplikasi memiliki resiko dari aspek ketersediaannyaDalam hal terjadinya kehilangan (*loss event*) atas informasi maupun sistem aplikasi, maka dibutuhkan adanya backup atas informasi dan sistem aplikasi tersebut yang dapat dipulihkan kembali ke dalam sistem utama.

2. Keamanan Informasi
   Dalam menjalankan pengamanan informasi, manajemen perusahaan harus menetapkan kebijakan dan memiliki komitmen yang tinggi terhadap keamanan informasi. Kebijakan tersebut harus dikomunikasikan secara berkala kepada seluruh karyawan dan pihak eksternal yang terkait.

3. *IT Security Awareness*
   Arsitektur keamanan informasi terdiri dari 3 komponen yaitu people, proses dan *technologi[6]*. Tanpa salah satunya, infrastrutur sekuriti lemah karena tidak dapat mencapai misinya yaitu melindungi asset perusahaan. People merupakan komponen terlemah dalam keamanan informasi, oleh karena itu diperlukan suatu pelatian/tingkat pemahaman akan kesadaran keamanan (*security awareness*).

4. Manajemen Antivirus
   Serangan virus dapat mempengaruhi keamanan sistem dan jaringan, untuk mencegah dampak kerugian yang lebih besar, perlu dilakukan tindakan pengamanan pada perangkat TI dengan mengunakan perangkat antivirus terkini dan dipercaya serta melakukan pengkinian patch sesuai kebutuhan.

5. Penanganan Informasi
   Informasi adalah asset yang sangat penting bagi perusahaan, baik informasi yang terkait dengan pelangan, keuangan, laporan maupun informasi lainnya [7]. Kebocoran, kerusakan, ketidakakuratan, ketidakteserdiaan atau

Jurnal KomtekInfo , Vol.8 No.1 Tahun 2021
e-ISSN : 2502-8758 || p-ISSN : 2356-0010
DOI : 10.35134/komtekinfo.v7i4
Page : 49-54

ganguan lain terhadap informasi tersebut dapat menimbukan dampak yang merugikan baik secara finasial maupun non-finansial, mengingat pentingnya informasi, maka informasi harus di lindungi ato diamanan kan oleh seluruh karyawan.

6. Pengendalian Akses Jaringan
   Peran jaringan komunikasi sangat penting didalam mendukung sistem informasi, maka perlu dilakukan pengelolaan yang memadai atas jaringan tersebut utuk mencegah tergangunya operasional perusahaan yang sedang berjalan karyawan, untuk itu perangkat jaringan perlu dipelihara dan dipantau serta dibutuhkan adanya batasan-batasan dalam pengunaannya.

7. Pengunaan Enkripsi
   Teknologi Informasi digunakan untuk berbagai macam kepentimgan termasuk di antaranya untuk pembuatan, penyimpanan da transmisi data elektronis. Namun demikian, pengunaan teknologi informasi untuk kepentingan tersebut diatas juga mengadung resiko di antarannya data di dalam sistem dapat terbaca oleh pihak yang tidak berwenang. Oleh karena itu perlu dilakukan tindakan pengamanan diantaranya pengunaan enkripsi untuk mengamankan data di dalamnya.

8. Registrasi Aset Teknologi
   Pengamanan informasi di suatu peruhaan sangat tergantung pada pengamanan terhadap semua aspek dan komponen IT terkait, termasuk di dalamnya aset TI. Pengamanan yang memadai terhadap aset TI harus dilakukan mengingat informasi yang mungkin terkandung didalamnya. Ketentuan ini bertujuan untuk pengaturan registrasi aset TI mencangkup identifikasi aset, penentuan pemilik/penangung jawab aset dan pecatatan aset TI yang dimiliki perusahaan.

9. Tata Kelola Password
   Password merupakan aspek yang penting dalam pengamanan TI. Password yang lemah atau tida disimpan dengan baik dapat mengakibatkan akses yang tidak sah ke dalam sistem perusahaan, setiap karyawan harus berperan sertaa dalam rangka mengamankan aset TI dengan mengamankan password yang menjadi kewengangan masing-masing.

10. Tata Kelola User Accout
    Sistem yang ada di perusahaan harus dapat menjamin kerahasiaan maupun integritas sistem dan datanya dapat dilakukan dengan mengendalikan akses ke dalam sistem dan tidak semua penguna harus memiliki hak akses yang sama.

4. Hasil

Pada bagian ini akan dibahas dan ditampilkan hasil audit yang telah dilakukan pada perusahaan berdasarkan data-data yang telah dikumpulkan melalui observasi, wawancara dan pengisihan form checklist. Data-data yang yang telah diolah dan dianalisis selanjutnya di lakukan tahap mengidentifikasi antara lain : menemukan akar masalah dari proses TI, mencegah munculnya risiko yang mungkin akan terjadi serta memberikan rekomendasi berdasarkan masalah yang ditemukan. Beberapa temuan audit yang didapatkan dapat di lihat pada tebel dibawah ini :

Tabel 1 : Temuan dalam Audit

No	Risk Issue	Jenis Risiko	Analisa
1.	Kegagalan infrastruktur IT dalam memenuhi kebutuhan bisnis (PMS, LAN, Storage, PC, Server)	Risiko Operasional	Tidak terpenuhinya Infrastruktur system informasi (PMS, LAN, Storage, PC, server) sesuai dengan standar yang

Jurnal KomtekInfo , Vol.8 No.1 Tahun 2021
e-ISSN : 2502-8758 || p-ISSN : 2356-0010
DOI : 10.35134/komtekinfo.v7i4
Page : 49-54

			berlaku. Akibatnya : jaringan menjadi lambat dan menimbulkan risiko operasioan, hal yang terjadi : 1. Netral-Ground tinggi dimana seharusnya grounding <1. 2. Penutup samping, dan belakang rak server tidak ditutup rapat dan berdebu. 3. Kondisi kabel yang menjalar dan belum dilindungi oleh duct/pipa pada ruang server 4. Belum ada labeling pada sistem kabel power Distribution
2	Kegagalan dalam proses *backup & restore* di *server local* di Unit Kerja Operasional.	Risiko Operasional	• Tidak dilaksanakanya setiap tahapan proses back-up data sesuai ketentuan yang berlaku, • Tidak sesuainya jenis media back-up sesuai ketentuan, • Tidak adanya kecukupan jumlah media backup sesuai ketentuan yang berlaku Periode back-up dilakukan tidak tertib. Akibatnya: perusahaan tidak memiliki back-up data yang kuat sehingga sulit melakukan investigasi bila terjadi bencana atau fraud, dapat menimbulkan kerugian financial dan risiko Operasional. Hal yang terjadi di : 1. Tidak melakukan Back-up data server local harian secara

Jurnal KomtekInfo , Vol.8 No.1 Tahun 2021
e-ISSN : 2502-8758 || p-ISSN : 2356-0010
DOI : 10.35134/komtekinfo.v7i4
Page : 49-54

			tertib . 2. Back-up data server local harian, mid, bulanan disimpan dalam 1 (satu) media back-up. 3. Tidak adanya labeling pada media bak-Up 4. Penyimpanan Bak-Up harian disimpan bersama back-Up bulanan pada 1 hardisk dipegang oleh Petugas IT.
3	Kegagalan infrastruktur penunjang/ non IT dalam memenuhi kebutuhan Unit Kerja	Risiko Operasional	1. Fasilitas pendingin (cooling) didalam ruangan server/distribusi sudah rusak 2. Fasilitas pengaman terhadap insiden (APAR) didalam ruang server tidak ada 3. Ruangan server kotor dan berdebu 4. Tidak terdapatnya termometer pada ruangan server serta kondisi ruangan server tidak memenuhi standar 5. Terdapat barang-barang yang tidak seharusnya berada diruangan server 6. Pintu ruangan server tidak tertutup dan terbuat dari kayu sehingga dapat diakses oleh pihak lain Kondisi ini mengakibatkan kerusakan pada perangkat, terganggunya operasional dan dapat menyebabkan terjadinya konslet pada jaringan listrik sehingga beresiko terjadinya kebakaran yang selanjutnya akan menimbulkan risiko operasional.

Jurnal KomtekInfo , Vol.8 No.1 Tahun 2021
e-ISSN : 2502-8758 || p-ISSN : 2356-0010
DOI : 10.35134/komtekinfo.v7i4
Page : 49-54

Dari hasil temuan diatas dapat diberikan beberapa rekomendasi sebagai berikut :

1. Petugas IT agar melakukan pemeliharaan atas infrastruktur IT terkait instalasi PMS-LAN antara lain memasang labelling pada setiap infrastruktur yang berhubungan dengan instalasi PMS–LAN, memberikan duck pada setiap kabel yang keluar dan berantakan, mengikat kabel LAN dengan kabel ties, serta melakukan koordinasi kepada PLN terkait perbaikan grounding terkait perbaikan panel listrik diruang server.
2. Supervisor untuk membuat laporan monitoring back-up data server local setiap bulanya untuk memastikan back-up data server local yang dilakukan petugas IT telah dilakukan sesuai ketentuan.
3. Pimpinan memberikan pembinaan dan arahan langsung kepada petugas terkait untuk menjaga kebersihan ruang server beserta perangkatnya.
4. Petugas IT agar segera meng-*install patching* operation sistem terbaru.
5. Petugas IT dan SPO agar mengamankan PC dengan men-disable shared folder yang tidak penting, memberikan password yang komplek pada shared folder yang penting, dan mengubah IP address sesuai dengan ketentuan.
6. Melakukan proses hardening pada PC yang bertugas dalam melayani konsumen untuk menghindari pengunaan software yang tidak berlisensi.

Tabel 2 : Kelemahan Pengedalian Intern Pada Perusahaan

No	Risk Issue	Jenis Risiko	Kelemahan Pengendalian Intern
1.	Kegagalan dalam proses backup & restore di Server	Risiko Operasional	• Tidak dilakukan pengujian atas hasil Back-up data server lokal. • Tidak adanya management inventori media back-up (onsite maupun offsite) yang memadai. • Tidak dilakukan monitoring dan tindak lanjut oleh petugas yang berwenang
2	Output aplikasi dapat diakses oleh pihak yang tidak berwenang	Pengamanan dan Security IT	• Tidak terdapat proses tata kelola output aplikasi dengan baik • Tidak terdapat penggunaan mekanisme enkripsi untuk distribusi data elektronik yang sensitif
3	Kegagalan Infrastruktur IT dalam memenuhi kebutuhan bisnis (Power Management System,	Risiko Operasional	• ketidak tahuan terkait instalasi PMS-LAN • kurang mengetahui pedoman Instalasi

	LAN, Storage, PC, Server)		PMS-LAN.
4	Perangkat IT menjadi rentan terhadap serangan program jahat	Risiko Operasional	• Tidak dilakukanya patching operation sistem

5. Kesimpulan

Kesimpulan yang dapat dikemukakan berdasarkan hasil analisis data dan pengujian dari studi kasus audit infrastruktur IT pada perusahaan yang bergerak di bidang jasa yang berada di Provinsi Sumatera Barat adalah sebagai berikut :

a. Perlunya pengendalian intern untuk membantu manajemen perusahaan agar pengunaan perangkat IT lebih efisien dan efektif sehingga melancarkan aktifitas bisnis di perusahaan.
b. Dengan adanya pemetaan analisis resiko pada masing-masing temuan audit terhadap perangkat IT dapat menjadi salah satu acuan untuk perbaikan kedepannya, sehingga tidak menjadi temuan berulang sebagai upaya untuk pengendalian resiko di perusahaan.

[8]

Referensi

[1] Chanopas, A., Krairit, D. & Khang, D. B., 2006. Managing Information Technology Infrastructure:
A New Flexibility Framework. Management Research News, p. 21.
[2] Weill, Peter and Ross, Jeanne W. (2004). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. Massachusetts: Harvard Business School Press.
[3] Isa, Irwan. 2012. *Evaluasi Pengontrolan Sistem Informasi*. Yogyakarta: Graha Ilmu.
[4] *ISO Indonesia center*. Diakses pada Oktober 2020 https://isoindonesiacenter.com/iso-27001-information-security/.
[5] Rainer & Cegielski, "*Introduction to Information Systems: Enabling and Transforming Business*", 2013
[6] Alan Calder, Steve Watkins, "*IT Governance: An International Guide to Data Security and ISO27001/ISO27002*", 2012.
[7] Reza Zulfikar Ruslam, dkk 2013 "Audit Kepatuhan Keamanan Informasi Dengan Menggunakan Framework ISO27001/ISMS" Jakarta : Universitas Indonesia