Pembuatan Dokumen Sop Keamanan Aset Informasi Yang Mengacu Pada Kontrol Kerangka Kerja Iso 27002:2013 (Studi Kasus : Cv Cempaka Tulungagung)

Dheni Indra, Apol Pribadi, dan Eko Wahyu Tyas
Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS)
Jl. Raya ITS Kampus ITS Sukolilo, Surabaya 60111
e-mail: apol.pribadi@gmail.com, tyas.darmaningrat@gmail.com

***Abstrak*— Dalam mendukung proses bisnis utamanya, suatu organisasi membutuhkan adanya dukungan teknologi informasi. Penggunaan Teknologi Informasi di banyak perusahaan telah menjadi satu hal penting dalam meningkatkan efektifitas dan efisiensi operasional bisnis yang mendukung tercapainya tujuan perusahaan, termasuk juga pada CV Cempaka Tulungagung. Dalam memenuhi kebutuhan keamanan aset informasi tersebut maka diperlukan adanya sebuah tata kelola dalam bentuk dokumen SOP (Standard Operating Procedure) keamanan aset informasi untuk mengurangi adanya ancaman dan risiko serta untuk mendukung penyelarasan pencapaian tujuan organisasi dalam proses bisnisnya. Metode penelitian yang digunakan yaitu OCTAVE sebagai pengolah hasil informasi yang didapatkan dari wawancara dan FMEA digunakan untuk menghitung seberapa tinggi dampak untuk perusahaan jika risiko itu terjadi dan membuat ranking prioritas untuk masing-masing risiko. Kemudian basis yang digunakan dalam membuat prosedur kendali akses aset informasi sebagai manajemen risiko adalah kerangka kerja ISO/IEC:27002:2013. Dalam penelitian ini, hasil akhir yang didapatkan adalah sebuah dokumen SOP yang sesuai dengan kebutuhan keamanan informasi bagi perusahaan CV Cempaka berdasarkan pada kontrol kerangka kerja ISO27002:2013.**

***Kata Kunci*— Keamanan Aset, Standart Operating Procedure, Risiko, Manajemen Risiko, ISO 27002:2013.**

I. PENDAHULUAN

KEAMANAN aset informasi merupakan aspek penting dari digunakanya teknologi informasi pada sebuah organisasi, tetapi sangat disayangkan masalah keamanan ini seringkali kurang mendapat perhatian dari para pemilik dan pengelola teknologi informasi. Seringkali masalah keamanan berada di urutan kedua, atau bahkan diurutan terakhir dalam daftar hal-hal yang dianggap penting. Pada survey yang dilakukan oleh IBM melalui internet, 92 % dari bisnis yang dilakukan tidak memiliki persiapan apapun apabila terjadi bencana terkait teknologi informasi [1]

Salah satu bentuk dukungan dalam menjaga keamanan aset informasi yang dapat diimplementasikan pada perusahaan CV Cempaka adalah dengan membuat sebuah prosedur yang terdokumentasi dengan baik dalam bentuk sebuah dokumen SOP (*Standard Operational Procedure*) mengenai kemanan aset informasi agar risiko dari keamanan informasi dapat dikurangi atau dihindari. SOP dapat berguna untuk mendefinisikan seluruh konsep, teknik, dan persyaratan dalam menjalankan suatu proses yang dituliskan ke dalam suatu dokumen yang langsung dapat digunakan oleh pegawai maupun karyawan yang bersangkutan dalam melaksanakan tugas dalam proses bisnisnya [2].

Sebelumnya sudah ada penelitian serupa mengenai pembuatan Dokumen SOP yang menggunakan kerangka kerja 27002:2013. Namun berdasarkan analisis penelitian terdahulu, belum ada yang melibatkan perusahaan dibidang industri rokok seperti halnya CV Cempaka. Juga terdapat beberapa kelemahan dalam dokumentasi tindakan, instruksi kerja dan kebijakan yang masih minim. Sehingga diperlukan adanya pembuatan dokumen SOP untuk mengatur dan membuat proses TI di CV Cempaka lebih terstruktur, juga dapat meningkatkan kualitas keamanan informasi yang ada.

Pada penelitian yang dilakukan kali ini, kerangka kerja yang akan digunakan adalah standard ISO/IEC 27002:2013 yang berisi panduan penerapan keamanan informasi dengan menggunakan bentuk-bentuk kontrol tertentu agar mencapai sasaran kontrol yang ditetapkan [3]. ISO/IEC27002 tidak mengharuskan bentuk-bentuk kontrol yang tertentu tetapi menyerahkan kepada pengguna untuk memilih dan menerapkan kontrol yang tepat sesuai kebutuhannya, dengan mempertimbangkan hasil analisa risiko yang telah dilakukan.

II. DASAR TEORI

A. Kemanan Informasi

Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), meminimasi risiko bisnis (*reduce business risk*) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis [3].

B. ISO 27002 : 2013

ISO 27002 memberikan best practice bagi organisasi dalam mengembangkan dan mengelola standard keamanan dan bagi manajemen untuk meningkatkan keamanan informasi dalam organisasi [3].

ISO / IEC 27002:20013 ini dimaksudkan sebagai dasar umum dan pedoman praktis untuk mengembangkan standar keamanan organisasi dan praktek manajemen keamanan yang

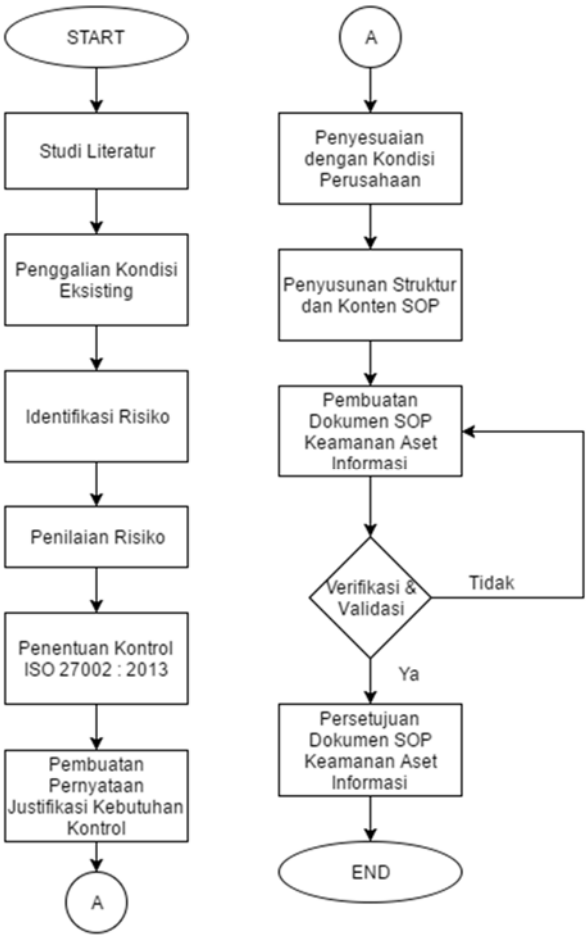
efektif, dan untuk membantu membangun kepercayaan dalam kegiatan antar-organisasi. Banyak sistem informasi belum dirancang untuk menjadi aman. Keamanan yang dapat dicapai melalui cara-cara teknis terbatas, dan harus didukung oleh manajemen yang tepat dan prosedur.

C. SOP (Standart Operasional Prosedur)

Pengertian standar operasional prosedur (SOP) menurut Istyadi Insani, dalam bukunya yang berjudul standar operasional prosedur (SOP) sebagai pedoman pelaksanaan administrasi perkantoran dalam rangka peningkatan pelayanan dan kinerja organisasi pemerintah menyatakan bahwa "SOP adalah dokumen yang berisi serangkaian instruksi tertulis yang dibakukan mengenai berbagai proses penyelenggaraan administrasi perkantoran yang berisi cara melakukan pekerjaan, waktu pelaksanaan, tempat penyelenggaraan dan aktor yang berperan dalam kegiatan." [8].

III. METODOLOGI PENELITIAN

Pada bagian ini akan membahas mengenai metodologi penelitian. Metodologi penelitian yang digunakan adalah jenis penelitian *kualitatif* dengan pendekatan *deskriptif*. Penelitian *kualitatif* adalah sebagai prosedur penelitian yang menghasilkan data *deskriptif* berupa kata-kata tertulis atau lisan dari orang-orang dan perilaku yang dapat diamati. Gambaran umum mengenai penelitian ini akan disajikan dalam bagan metodologi berikut ini :



Gambar 1. Metodologi Penelitian

IV. HASIL DAN PEMBAHASAN

Dalam uraian penelitian ini akan dijelaskan lebih detail mengenai *:*

A. Penggalian Kondisi Eksisting

Proses penggalian kondisi eksisting dilakukan dengan cara wawancara terstruktur dan tidak terstruktur, serta mempelajari prosedur, kebijakan dan laporan tahunan perusahaan yang telah dilakukan sebelumnya. Wawancara dilakukan kepada departemen perusahaan yang aset informasinya terkait dengan proses bisnis, untuk menggali data dan informasi atas penelitian yang dilaksanakan. Sedangkan proses observasi ini dilakukan mengumpulkan data melalui studi lapangan langsung untuk menganalisis risiko. hal ini dilakukan untuk membuat penelitian ini sesuai dengan kebutuhan dan kondisi perusahaan.

B. Identifikasi Risiko

Dalam Identifikasi risiko akan berdasar dengan metode pada *framework* Octave yaitu dengan mengidentifikasi terlebih dahulu aset yang dimiliki perusahaan, kebutuhan keamanan perusahaan, praktek keamanan terkini yang telah atau sedang dilakukan, aset kritis dan kelemahan infrastruktur TI yang ada saat ini. Hasil dari identifikasi risiko kemudian akan dilanjutkan pada proses identifikasi pemilik risiko. Hasil luaran dari proses mengidentifikasi risiko adalah sebuah daftar risiko. Daftar risiko tersebut selanjutnya akan menjadi masukan untuk proses analisis risiko.

C. Penilaian Risiko

Dalam penilaian risiko, metode yang digunakan dalam penelitian adalah metode FMEA. Dalam metode FMEA terdapat keiteria dalan melakukan penilaian risiko yaitu berdasarkan pada nilai dampak (*severity*), nilai kemungkinan (*occurence*) dan nilai deteksi (*detection*). Setelah mendapatkan nilai dari setiap faktor *severity, occurance* dan *detection*, kemudian nilai tersebut akan dikalikan sehinga menghasilkan sebuah nilai *Risk Priority Number* (RPN).

Berdasarkan penilaian risiko yang telah dilakukan, CV Cempaka memiliki satu risiko yang termasuk dalam level *very high* dengan total RPN 240 yaitu risiko kehilangan data yang disebabkan oleh kelalaian administrator. Kemudian terdapat beberapa risiko dengan level *high* seperti kerusakan server, kerusakan PC, kerusakan kabel LAN, manipulasi data, *sharing* password, dan risiko data tidak valid karena kesalahan input.

Risiko-risiko tersebut yang mendasari aktivitas dalam melakukan pemetaan terhadap kontrol yang mengacu pada ISO 27002:2013.

D. Penentuan Kontrol ISO 27002:2013

Dalam pemetaan kontrol dengan kerangka kerja ISO27002:2013 terdapat 11 klausul yang digunakan adalah :

1. Klausul 7.1.2. *Terms and conditions of employment* dan 7.2.2. *Information security awareness, education and training*. Kontrol tersebut digunakan untuk memitigasi risiko yang disebabkan oleh pegawai perusahaan seperti sharing password aplikasi dan salah input data.
2. Klausul 9.1.1 *Access control policy*, 9.2.3 *Management of privileged access right*, 9.3.1 *Use of secret*

authentication information, 9.4.1 *Information access restriction*, 9.4.2 *Secure log-on procedures*, dan 9.4.3 *Password management system*. Kontrol tersebut berperan sebagai acuan dalam memberikan rekomendasi mitigasi risiko terkait pengelolaan hak akses sistem atau pengaturan username dan password pegawai.

3. Klausul 11.2.3 *Cabling security* dan 11.2.4 *Equipment maintenance*. Kontrol tersebut digunakan untuk memitigasi risiko pada perusahaan yang disebabkan oleh perangkat keras maupun jaringan yang dimiliki. Seperti kerusakan server, kerusakan PC, dan juga kerusakan kabel LAN.
4. Klausul 12.3.1. *Information backup*, 12.4.1 *Event logging*, 12.4.2 *Protection of log information*, dan 12.4.3 *Administrator & Operator logs*. Kontrol tersebut membahas mengenai pentingnya memiliki record aktivitas (log) pengguna atau administrator. Yang mana informasi log tersebut harus disimpan secara berkala, dan dilindungi terhadap gangguan. Sehingga diharapkan mampu memitigasi risiko seperti data hilang ataupun data tidak valid karena kelalaian administrator.

E. Penyesuaian dengan Kondisi Perusahaan

Dalam bagian ini, merupakan proses penyesuaian kontrol yang sudah ditentukan dengan kondisi pada perusahaan yaitu menyesuaikan aktivitas-aktivitas pada suatu kontrol dengan aktivitas praktik keamanan yang telah dilakukan oleh perusahaan agar dapat diimplementasikan sepenuhnya oleh perusahaan, sehingga mendapatkan rekomendasi pengendalian risiko yang tepat.

F. Perancangan SOP

Format SOP akan dikembangkan sesuai dengan struktur standard dengan acuan dari peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia mengenai pedoman penyusunan standar operasional prosedur nomor 35 tahun 2012. Berdasarkan panduan tersebut, peneliti merancang struktur dan konten dokumen SOP yang terdiri dari 5 bab, yaitu :

1) Pendahuluan

Bab ini berisi mengenai tujuan dibuatnya dokumen SOP CV Cempaka, ruang lingkup SOP, dan juga evaluasi penilaian risiko yang dimiliki oleh CV Cempaka

2) Kebijakan

Bab ini berisi tujuan dibuatnya kebijakan, ruang lingkup kebijakan, dan penjelasan secara detail aktivitas-aktivitas yang perlu dilakukan pada kebijakan tersebut

3) Prosedur

Bab ini berisi deskripsi umum prosedur, rincian prosedur yang perlu dilakukan dan ditampilkan dalam bentuk flowchart

4) Instruksi Kerja

Bab ini berisi tentang penjelasan secara detail mengenai instruksi yang harus dijalankan oleh pelaksana. Sehingga prosedur mampu terlaksana dengan baik.

5) Formulir

Bab ini berisikan tentang formulir-formulir yang berperan sebagai tools pendukung tiap prosedur yang sedang dijalankan.

G. Hasil Perancangan SOP

Berikut menampilkan pemetaan dari perancangan SOP dengan formulir dan instruksi yang digunakan pada setiap prosedur.

Tabel 1.
Hasil perancangan dokumen SOP

Nama Dokumen SOP	No Dokumen	Dokumen Terkait
PO – 01 Prosedur pengelolaan hak akses	KB – 01	Kebijakan pengendalian hak akses
	FM – 01	Formulir pengelolaan hak akses
	FM – 02	Formulir kontrak hak akses
	FM – 03	Formulir log pengelolaan hak akses
	IN – 01	Instruksi Pembaruan Hak Akses
PO – 02 Prosedur pengelolaan password	KB – 02	Kebijakan Kemanan Informasi
	FM – 04	Formulir perbaikan sistem informasi
	FM – 05	Formulir reset password
	IN – 04	Instruksi Reset Password
PO – 03 Prosedur *backup and restore*	KB – 02	Kebijakan Kemanan Informasi
	FM – 06	Formulir klasifikasi data
	FM – 07	Formulir Log backup data
	FM – 08	Kebijakan pengelolaan hardware dan jaringan
	IN – 02	Instruksi Backup Data
	IN – 03	Instruksi Restore Data
PO – 04 Prosedur perawatan hardware	KB – 03	Kebijakan pengelolaan hardware dan jaringan
	FM – 09	Formulir pemeliharaan perangkat TI
	FM – 10	Formulir berita acara kerusakan
	FM – 11	Formulir laporan evaluasi penggunaan fasilitas TI
PO – 05 Prosedur keamanan kabel	KB – 03	Kebijakan pengelolaan hardware dan jaringan
	FM – 09	Formulir pemeliharaan perangkat TI
	FM – 10	Formulir berita acara kerusakan
PO – 06 Prosedur pengelolaan dan pengembangan SDM	KB – 04	Kebijakan human resource security
	FM – 12	Formulir data pegawai
	FM – 13	Formulir evaluasi kegiatan pengembangan kompetensi

H. Hasil Pengujian SOP

Pengujian SOP dilakukan melalui dua cara yakni verifikasi dan validasi. Verifikasi dilakukan dengan cara wawancara untuk memastikan kebenaran informasi yang terkandung dalam SOP, sedangkan validasi dilakukan dengan simulasi untuk mengetahui ketepatan SOP ketika implementasi dalam kasus nyata.

Tabel 2.
Metode Pengujian SOP

	Tujuan	Metode	Sasaran
Verifikasi	Untuk melakukan verifikasi terhadap dokumen untuk memastikan kebenaran dari informasi-informasi yang didefinisikan dan termuat di dalam dokumen SOP	Wawancara	Pihak yang memiliki kedudukan paling tinggi pada bagian Personalia dan umum yaitu Kepala bagian personalia dan umum CV Cempaka
Validasi	Untuk melakukan validasi dokumen dengan melihat apakah SOP dapat berjalan sesuai dengan kondisi yang ada dan untuk menemukan kekurangan dari SOP yang telah dibuat sehingga dapat dilakukan koreksi dan selanjutnya dapat diterapkan	Simulasi Pengujian dokumen SOP	Pelaksana SOP, yakni : Fungsional bisnis perusahaan yang terlibat

V. KESIMPULAN PENELITIAN

Kesimpulan yang dapat diambil dari pengerjaan Tugas Akhir ini yakni sebagai berikut:

1) Analisis risiko kemanan aset informasi CV Cempaka Tulungagung berdasarkan tahap penilaian risiko pada kerangka kerja ISO 27002:2013

Analisis risiko dilakukan dengan menggunakan metode FMEA dan menganalisis ancaman serta kerentanan dari aset informasi yaitu perangkat lunak (*software*), perangkat keras (*hardware*), data, jaringan dan sumber daya manusia (*people*). Berdasarkan hasil evaluasi penilaian risiko, dapat diketahui bahwa CV Cempaka memiliki 1 risiko yang bernilai sangat tinggi hingga 240 yaitu risiko kehilangan data.

2) SOP Keamanan Aset Informasi yang mengacu pada kontrol kerangka kerja ISO 27002:2013

Dokumen Standard Operasional Prosedur. Keamanan Aset Informasi CV Cempaka di Tulungagung telah berhasil dilakukan dengan menggunakan acuan kontrol kerangka kerja ISO 27002 : 2013 dengan menggunakan beberapa klausul yaitu Keamanan Sumber Daya Manusia (Klausul 7), Kontrol Akses (Klausul 9), Keamanan Fisik dan Lingkungan (Klausul 11), dan Keamanan Operasional (Klausul 12).

3) Hasil pembuatan Dokumen Standard Operating Procedure (SOP) Keamanan Aset Informasi .

Berdasarkan hasil penelitian keamanan informasi yang menyesuaikan dari hasil identifikasi dan analisa risiko pada aset informasi, maka dapat tersusun dokumen SOP keamanan aset informasi yang terdiri dari 4 Kebijakan, , 6 prosedur, 4 Instruksi Kerja dan 13 Formulir.

4) Hasil Pengujian dokumen SOP

Hasil dari pengujian tersebut menghasilkan perubahan antara lain : 1) Pemisahan kebijakan pengendalian hak akses denngan keamanan informasi 2) Penambahan kebijakan human resource security 3) Penghapusan proses pada prosedur pengelolaan hak akses 4) Perubahan pelaksana dalam prosedur pergantian password 5) Perubahan pelaksana dalam prosedur keamanan kabel.

DAFTAR PUSTAKA

[1] IBM, IBM survey of 224 Business Leaders, s.l: IBM, 2009.

[2] R. Stup, Standart Operating Procedures : Managing The Human Variables, Pennsylvania: Pennsylvania State University, 2002.

[3] ISO/IEC:27002, Information Technology - Security Techniques, Geneva, 2013.

[4] S. M. IKIT, Akutansi Penghimpun Dana Bank Syariah, Yogyakarta: CV Budi Utama, 2015.

[5] H. Siahaan, Manajemen Resiko, Jakarta: PT Elex Media Comoutindo, 2007.

[6] Hughes, "Ancaman dalam IT," 2006. [Online]. Available: http://xondis.blogspot.com/2015/03/pengukuran-resiko-teknologi-informasi.html.

[7] E. Humphreys, Implementing the ISO/IEC 27002 ISMS Standart, Norwood: Artech House, 2015.

[8] M. Budihardjo, Panduan Praktis Menyusun SOP, Yogyakarta: Gadjah Mada University Press, 2014.